BSC

Design Calculation or Analysis Cover Sheet

Complete only applicable items.

1. QA: QA
2. Page 1

3. System	4. Document Identifier
Monitored Geologic Repository	050-PSA-WH00-00200-000-00A

5. Title

Wet Handling Facility Reliability and Event Sequence Categorization Analysis

6. Group

Preclosure Safety Analyses

7. Document Status Designation

☐ Preliminary ☒ Committed ☐ Confirmed ☐ Cancelled/Superseded

8. Notes/Comments

See Page 2 for list of authors.

NOTICE OF OPEN CHANGE DOCUMENTS - THIS DOCUMENT IS IMPACTED BY THE LISTED CHANGE DOCUMENTS AND CANNOT BE USED WITHOUT THEM.

---

1) CACN-001, DATED 04/17/2008

Attachments		Total Number of Pages
Attachment A.	Event Trees	174
Attachment B.	System/Pivotal Event Analysis – Fault Trees	391
Attachment C.	Active Component Reliability Data Analysis	51
Attachment D.	Passive Equipment Failure Analysis	91
Attachment E.	Human Reliability Analysis	266
Attachment F.	Fire Analysis	140
Attachment G.	Event Sequence Quantification Summary Tables	2
Attachment H.	SAPHIRE Model and Supporting Files	2 + CD

RECORD OF REVISIONS

9. No.	10. Reason For Revision	11. Total # of Pgs.	12. Last Pg. #	13. Originator (Print/Sign/Date)	14. Checker (Print/Sign/Date)	15. EGS (Print/Sign/Date)	16. Approved/Accepted (Print/Sign/Date)
00A	Initial Issue	1,375	H-2	Howard Lambert/See Page 2	See Page 3	Michael Frank 3/12/08	Mark Wisenburg 3/12/2008

DISCLAIMER

The analysis contained in this document was developed by Bechtel SAIC Company, LLC (BSC) and is intended solely for the use of BSC in its work for the Yucca Mountain Project.

Section	Section Name	Originators	Signature/Date
1	Purpose	Guy Ragan	
2	References	Howard Lambert	
3	Assumptions	Howard Lambert	
4	Methodology	NA	
4.1	Quality Assurance	Guy Ragan	
4.2	Use Of Software	Guy Ragan	
4.3	Description Of Analysis Methods	Doug Orvis Erin Collins Pierre Macheret Dan Christman David Bradley Paul Amico Mary Presley Joe Minarick	
5	List Of Attachments	NA	
6	Body Of Calculation	NA	
6.0	Initiating Event Screening	Howard Lambert	
6.1	Event Tree Analysis	Howard Lambert	
6.2	Initiating And Pivotal Event Analysis	Howard Lambert	
6.3	Data Utilization	Erin Collins Dan Christman David Bradley Suzanne Loyd	
6.4	Human Reliability Analysis	Paul Amico Mary Presley Doug Orvis Erin Collins	
6.5	Fire Analysis	Paul Amico and Laura Plumb under supervision of Paul Amico	
6.6	(Not Used)		
6.7	Event Sequence Quantification	Suzanne Loyd	
6.8	Event Sequence Grouping And Categorization	Suzanne Loyd	
6.9	Defined ITS SSCs and Procedural Safety Controls Requirements	Suzanne Loyd	
7	Results And Conclusions	Howard Lambert	
Att A	Event Trees	Howard Lambert	
Att B	System/Pivotal Event Analysis – Fault Trees	Howard Lambert	

Section	Section Name	Originators	Signature/Date
Att C	Active Component Reliability Data Analysis	Erin Collins	3/12/08
Att D (D1, D3)	Passive Equipment Failure Analysis	Dan Christman	3/12/08
Att D (D2)	Passive Equipment Failure Analysis	David Bradley	3/12/08
Att E	Human Reliability Analysis	Paul Amico Mary Presley Doug Orvis Erin Collins	3/12/08 3/12/08 3/12/08 3/12/08
Att F	Fire Analysis	Paul Amico and Laura Plumb under supervision of Paul Amico	3/12/08 3/12/08 3/12/08
Att G	Event Sequence Quantification Summary Tables	Suzanne Loyd	3/12/08
Att H	Saphire Model and Supporting Files (CD)	Suzanne Loyd	3/12/08

Kathy Ashley coordinated the issuance of the Check Copy (00Aa) and filled out the Originator's Checklist.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Andrew Burningham **Amy Primmer**	3/12/08 3/12/08	Section 1-7 Attachments A, B, C, D, E, F, G, H	Administrative check	Perform checks on the Calculations and Analyses – Checklist (Attachment 6 to EG-PRO-3DP-G04B-00037 that are administrative in nature (e.g. format, procedural compliance, links in InfoWorks, DIRS, reference format, document numbering, confirmation of SAPHIRE validation, tracking number, etc)
Alex Deng	03/12/08	Sections 1, 3, 4, and 7	Overall approach and methodology	Check that the standard approach and methodology includes changes to the methodology resulting from input from industry reviewers.
Phuoc Le / Dan Gallagher	3/12/08 3/12/08	Section 6.0 through 7.0 and Attachments A through H	Cut set check	Cut Set Check - Section 6.0 - 6.9 and Attachments A - H
Kathy Ashley	3/12/08	Section 6.9	Specialty Check	Check the correct ESD and values for Tables 6.9-1 and 6.9-2.
Dan Christman	3/12/08	Section 6.5 and Attachment F	Specialty check: Fire Initiating Events	Fire Initiating Events - Section 6.5 and Attachment F
Doug Orvis	3/12/08	Section 6.0	Specialty check: Section 6.0	Initiating Event Screening - Section 6.0

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Laura Plumb (Working for Paul Rhico)	3/12/08	Section 6.3.3 Miscellaneous Data	Specialty check: Section 6.3.3 and Supporting reference and cross-references to other sections	Section 6.3.3 Miscellaneous Data
Ching Chan	3/12/2008	Attachment B 1 Prime Mover Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date.
Stefhan Sherman	12 March 08	Attachment B - Cask Transfer Trolley Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Mary Jane Rubano for Ekachai Danupatampa	Mary Jane Rubano 3.12.08	Attachment B 3 Loading/Unloading Room Door and slide Gate Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Chris Hicks For Freddie Guerrero JABO TANG	Chris Hicks 3/12/08	Attachment B 4 Canister Transfer Machine Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
~~**Ching Chan**~~ **For Narci Encarnacion**	John S. Tang 3/12/08	Attachment B 5- Cask Cooling System ~~Fault tree~~ Fault Tree Analysis JST 3/12/08	Design Concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Len Swanson	Leonard Swanson 3/12/08	Attachment B 6 Site Transporter Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Nasser Dehkordi **For Ajit Hiranadani**	Nasser H. Dehkordi 3/12/08	Attachment B 7 Item: Heating , Ventilations and Air Conditioning (HVAC) Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Nohemi Brewer	PARTIAL CHECK (SEE E MAIL) 3/12/08 3/12/08	Attachment B 8 AC Power System Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Stephen Skochko **for Karim Vakhshoori**	For Karim Vakhshoori 3/12/08	Attachment B 9 Horizontal Cask Tractor Trailer Fault Tree Analysis	Design concurrence	Check fault tree description. Is design accurately described and do all basic events have basis in latest issued for LA information? Are success criteria accurate? Are basic events clearly phrased? Are the references to Engineering documents correct and up to date
Dan Christman	3/12/08	Attachment C- Checked once for CRCF Reliability and Event Sequence Categorization Analysis, same checked version used in corresponding IHF analysis.	Specialty check	Check Attachment C including the MathCad file for Bayesian update of reliability values
Doug Smith **Karim Vakhshoori** **Setphen Skochko**	3-12-08 For Karim Vakhshoori 3/12/08 3/12/08	Attachment C - Inputs checked once for CRCF Reliability and Event Sequence Categorization Analysis, same checked version used in corresponding WHF analysis.	Detailed references and numerical inputs	This check traced input data back to references for Attachment C.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Dan Christman	3/12/08	Attachment D	Specialty check	Check section D 2 on PEFA for thermal challenge to shielding and associated text in ~~6.3.2.2~~ 6.3.2.3 6.3.2.4 3/12/08
David Bradley	3/12/08	Attachment D	Specialty check	Check sections D 1 and D 3 on PEFA related to loss of shielding and associated text in Section 6.3.3.3, and the structural PEFA and associated text in section 6.3.2.1
Phuoc Le	3/12/08	Attachment E - Human Reliability Analysis	Specialty check	Section 6.4 and Attachment E
Clarence Smith	3/12/08	Attachment E - Human Reliability Analysis	Design concurrence	Check that the Basic Scenarios in Attachment E are consistent with the concept of operations.
Dan Christman	3/12/08	Attachment F Fire Analysis	Specialty check	Check the fire analysis calculation
Mary Jane Rubano for Ekachai Danupatampa	Mary Jane Rubano 3.12.08	Attachment F Fire Analysis	Specialty check	Check dimensions of rooms and area computation
Chris Hicks	Chris Hicks 3/12/08	Attachment F Fire Analysis	Specialty check	Check tabulation of equipment contained in each room
Sandra Castro	Sandra Castro 3/12/08	All sections and attachments	Detailed references and numerical Inputs	Check that all references to engineering documents are current
Leo Gatchalian	L Gatchalian 3/12/08	Main Body and Attachments	Detailed references and numerical Inputs	Check that all references in the body of the analysis are references to the appropriate document
Kathryn Sheffield	Kathryn Sheffield 3/12/08	All sections of the main body and Attachments	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Dale Dexheimer	D. Dexheimer 3/12/08	Section 6.8	Specialty check	Check consistency with Preclosure Consequence Analysis

CONTENTS

Page

FIGURES

Page

TABLES

Page

TABLES (Continued)

Page

ACRONYMS AND ABBREVIATIONS

Acronyms

ASME	American Society of Mechanical Engineers
ATHEANA	a technique for human event analysis
BSC	Bechtel SAIC Company, LLC
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
CTM	canister transfer machine
CTT	cask transfer trolley
CSNF	commercial spent nuclear fuel
DHLW	defense high-level radioactive waste
DOE	U.S. Department of Energy
DPC	dual-purpose canister
DSNF	DOE spent nuclear fuel
EOC	errors of commission
EOO	errors of omission
EPRI	Electric Power Research Institute
ESD	event sequence diagram
ETF	expended toughness fraction
FEA	finite element analysis
FEM	finite element modeling
FFTF	Fast Flux Test Facility
FTA	fault tree analysis
GROA	geologic repository operations area
HAZOP	hazard and operability
HCLPF	high confidence of low mean frequency of failure
HEPA	high-efficiency particulate air filter
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HVAC	heating, ventilation, and air conditioning
IET	initiator event tree
IHF	Initial Handling Facility
ITC	important to criticality
ITS	important to safety
LLNL	Lawrence Livermore National Laboratory
LOOP	loss of offsite power

ACRONYMS AND ABBREVIATIONS (Continued)

LOS	loss of shielding
LS-DYNA	Livermore Software–Dynamic Finite Element Program
MAP	mobile access platform
MCC	motor control centers
MCO	multicanister overpack
MLD	master logic diagram
MPC	multipurpose canister
N/A	not applicable
NARA	Nuclear Action Reliability Assessment
NFPA	National Fire Protection Association
NNP	normal network protection
NRC	U.S. Nuclear Regulatory Commission
NUREG	Nuclear Regulation (U.S. Nuclear Regulatory Commission)
PCSA	Preclosure Safety Analysis
PDF	probability density function
PEFA	passive equipment failure analysis
PFD	process flow diagram
PIF	performance influencing factor
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSC	procedural safety controls
QA	quality assurance
RF	Receipt Facility
SFTM	spent fuel transfer machine
SLS	steel/lead/steel
SNF	spent nuclear fuel
SPM	site prime mover
SPMRC	site prime mover railcars
SPMTT	site prime mover truck trailers
SRET	system response event tree
SSC	structure, system, or component
SSCs	structures, systems, and components
STC	shielded transfer cask
TAD	transportation, aging, and disposal
TEV	transport and emplacement vehicle
TRIGA	Training, Research, Isotopes, General Atomics
TYP-FM	type and failure mode
WHF	Wet Handling Facility

ACRONYMS AND ABBREVIATIONS (Continued)

WPTT	waste package transfer trolley
YMP	Yucca Mountain Project

Abbreviations

AC	alternating current
B	Boron
°C	degrees Celsius
DC	direct current
ft	foot, feet
gpm	gallons per minute
hp	horsepower
hr, hrs	hour, hours
K	Kelvin
kV	kilovolt
min	minute, minutes
mph	miles per hour
ppm	parts-per-minute
V	coefficient of variation
V	volt
yr, yrs	year, years

1. PURPOSE

This document on the Wet Handling Facility (WHFF) along with its companion document entitled *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37) constitutes a portion of the preclosure safety analysis (PCSA) that is described in its entirety in the safety analysis report that is being submitted to the U.S. Nuclear Regulatory Commission (NRC) as part of the Yucca Mountain Project (YMP) license application. These documents are part of a collection of analysis reports that encompass all waste handling activities and facilities of the geologic repository operations area (GROA) from the beginning of operations to the end of the preclosure period. The *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37) describes the identification of initiating events and the development of potential event sequences that emanate from them. This analysis uses the resulting event sequences developed in this analysis to perform a quantitative analysis of the event sequences for the purpose of categorization per the definition provided by 10 CFR 63.2 (Ref. 2.3.2).

The PCSA uses probabilistic risk assessment (PRA) technology derived from both nuclear power plant and aerospace methods and applications in order to perform analyses to comply with the risk informed aspects of 10 CFR 63.111 and 63.112 and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report* (Ref. 2.2.71). The PCSA, however, limits the use of PRA technology to identification and development of event sequences that might lead to direct exposure of workers or onsite members of the public; radiological releases that may affect the workers or public (onsite and offsite), and criticality.

The radiological consequence assessment relies on bounding inputs with deterministic methods to obtain bounding dose estimates. These were developed using broad categories of scenarios that might cause a radiological release or direct exposure to workers and the public, both onsite and offsite. These broad categories of scenarios were characterized by conservative meteorology and dispersion parameters, conservative estimates of material at risk, conservative source terms, conservative leak-path factors, and filtration of releases via facility high-efficiency particulate air (HEPA) filters when applicable. After completion of the event sequence development and categorization in this analysis, each Category 1 and Category 2 event sequence was conservatively matched with one of the categories of dose estimates. The event sequence analyses also serve as input to the PCSA criticality analyses by identifying the event sequences and end states where conditions leading to criticality are in Category 1 or 2.

An event sequence is defined in 10 CFR 63.2 (Ref. 2.3.2) as:

> "A series of actions and/or occurrences within the natural and engineered components of a geologic repository operations area that could potentially lead to exposure of individuals to radiation. An event sequence includes one or more initiating events and associated combinations of repository system component failures, including those produced by the action or inaction of operating personnel. Those event sequences that are expected to occur one or more times before permanent closure of the geologic repository operations area are referred to as Category 1 event sequences. Other event sequences that have at least one

> chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences."

As an extrapolation of the definition of Category 2 event sequences, sequences that have less than one chance in 10,000 of occurring before permanent closure are identified as beyond Category 2. Consequence analyses are not required for those event sequences.

10 CFR 63.112, Paragraph (e) and Subparagraph (e)(6) (Ref. 2.3.2) require analyses to identify the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. Subparagraph (e)(6) specifically notes that the analyses include consideration of "means to prevent and control criticality." The PCSA criticality analyses employ specialized deterministic methods that are beyond the scope of the present analysis. However, the event sequence analyses serve as an input to the PCSA criticality analyses by identifying the event sequences and end states where conditions leading to criticality are in Category 1 or 2. Some event sequence end states include the phrase "important to criticality." This indicates that the event sequence has a potential for reactivity increase that is analyzed to determine if reactivity can exceed the upper subcriticality limit.

In order to determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity to variations in each of the parameters important to criticality during the preclosure period. The parameters are waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor (k_{eff}) to variations in any of these parameters as a function of the other parameters. The PCSA criticality analyses determined the parameters that this event sequence analysis includes. The presence of a moderator in association with a path to exposed fuel was required to be explicitly modeled in the event sequence analysis because such events could not be deterministically found to be incapable of exceeding the upper subcriticality limit. Other situations treated in the event sequence analysis for similar reasons are multiple U.S. Department of Energy (DOE) spent nuclear fuel (SNF) canisters in the CRCF in the same general location and presence of sufficient soluble boron in the pool in the Wet Handling Facility (WHF).

The initiating events considered in the PCSA define what could occur within the GROA and are limited to those events that constitute a hazard to a waste form while it is present in the GROA. Initiating events include internal events occurring during waste handling operations conducted within the GROA and external events (e.g., seismic, wind energy, or flood water events) that impose a potential hazard to a waste form, waste handling systems, or personnel within the GROA. Such initiating events are included when developing event sequences for the PCSA. However, initiating events that are associated with conditions introduced in structures, systems, and components (SSCs) before they reach the site are not within the scope of the PCSA. The excluded from consideration offsite conditions include drops of casks, canisters, or fuel assemblies during loading at a reactor site; improper drying, closing, or inerting at the reactor site; rail or road accidents during transport; tornado or missile strikes on a transportation cask; or nonconformances introduced during cask or canister manufacture that result in a reduction of containment strength. Such potential precursors are subject to deterministic regulations such as 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR 72 (Ref. 2.3.4) and

associated quality assurance (QA) programs. As a result of compliance to such regulations, the SSCs are deemed to pose no undue risk to health and safety. Although the analyses do not address quantitative probabilities to the aforementioned excluded precursors, it is clear that the use of conservative design criteria and the implementation of QA controls result in unlikely exposures to radiation.

Other boundary conditions used in the PCSA include:

- Plant operational state. The initial state of the facility is normal with each system operating within its vendor-prescribed operating conditions.

- No other simultaneous initiating events. It is standard practice to not consider the occurrence of other initiating events (human-induced or naturally occurring) during the time span of an event sequence because: (a) the probability of two simultaneous initiating events within the time window is small and, (b) each initiating event will cause operations in the waste handling facility to be terminated, which further reduces the conditional probability of the occurrence of a second initiating event, given that the first has occurred.

- Component failure mode. The failure mode of a structure, system, or component (SSC) corresponds to that required to make the initiating or pivotal event occur.

- Fundamental to the basis for the use of industry-wide reliability parameters within the PCSA, such as failure rates, is the use of SSCs within the GROA that conform to NRC accepted consensus codes and standards, and other regulatory guidance.

- Intentional malevolent acts, such as sabotage and other security threats, are not addressed in this analysis.

As stated, the scope of the preclosure safety analysis is limited to internal initiating events originating within the GROA boundary and external initiating events that have their origin outside the GROA boundary, but can affect buildings and/or equipment within the GROA. External event analyses are documented in *External Events Hazards Screening Analysis* (Ref. 2.2.29) and *Frequency Analysis of Aircraft Hazards for License Application* (Ref. 2.2.18). Internal event identification (using a master logic diagram (MLD) and hazard and operability (HAZOP) evaluation), event sequence development and grouping, and related facility details are provided in the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37), which also documents the methodology and process employed and initiates the analysis that is completed here.

This document uses event trees from the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37) to quantify the event sequences for each waste form. Quantification refers to the process of obtaining the mean frequency of each event sequence for the purpose of categorization. This document shows the categorization of each event sequence based on:

- Mean frequency associated with the event sequence frequency distribution

- Uncertainty associated with the event sequence frequency distribution
- Material at risk for each Category 1 and 2 event sequence for purposes of dose calculations
- Important to safety (ITS) SSCs
- Compliance with the nuclear safety design bases
- Procedural safety controls required for operations.

Other PCSA documents which are not referenced here cover the reliability and categorization of external events and summarize procedural safety controls and nuclear safety design bases. The main documents that will emanate from Volume I *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37) and the current analyses are:

- *ITS SSC/Non-ITS SSC Interactions Analysis* (Ref. 2.4.1)
- *Preclosure Nuclear Safety Design Bases* (Ref. 2.4.2)
- *Preclosure Procedural Safety Controls* (Ref. 2.4.3)
- *Seismic Event Sequence Quantification and Categorization* (Ref. 2.4.4).

2. REFERENCES

2.1 PROCEDURES/DIRECTIVES

2.1.1 EG-PRO-3DP-G04B-00037, Rev. 10. *Calculations and Analyses*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0001.

2.1.2 EG-PRO-3DP-G04B-00046, Rev. 10. *Engineering Drawings.* Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG. 20080115.0014.)

2.1.3 IT-PRO-0011, REV 7. *Software Management*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: DOC.20070905.0007.

2.1.4 LS-PRO-0201, REV 5. *Preclosure Safety Analysis Process*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0021.

2.2 DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

Design Inputs are listed in this section and the Attachment sections listed in Section 2.5.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

2.2.1 *Ahrens, M. 2000. *Fires in or at Industrial Chemical, Hazardous Chemical and Plastic Manufacturing Facilities, 1988-1997 Unallocated Annual Averages and Narratives.* Quincy, Massachusetts: National Fire Protection Association. TIC: 259997.

2.2.2 *Ahrens, M. 2007. *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction.* Quincy, Massachusetts: National Fire Protection Association. TIC: 259983.

2.2.3 *A.M. Birk Engineering 2005. *Tank-Car Thermal Protection Defect Assessment: Updated Thermal Modelling with Results of Fire-Testing: Summary Report.* TP 14367E. Ontario, Canada: Transportation Development Centre of Transport Canada. ACC: MOL.20071113.0095.

2.2.4 *ANSI/ANS-58.23-2007. 2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.

2.2.5 *Apostolakis, G. and Kaplan, S. 1981. *Pitfalls in Risk Calculations*. *Reliability Engineering, 2,* 135-145. Barking, England: Applied Science Publishers. TIC: 253648.

2.2.6 ASCE/SEI 7-05. 2006. *Minimum Design Loads for Buildings and Other Structures*. Including Supplement No. 1. Reston, Virginia: American Society of Civil Engineers. TIC: 258057. ISBN: 0-7844-0809-2.

2.2.7 ASME (American Society of Mechanical Engineers), 2002. RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.* New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.

2.2.8 ASME 2004. *2004 ASME Boiler and Pressure Vessel Code.* 2004 Edition. New York, New York: American Society of Mechanical Engineers. TIC: 256479. ISBN: 0-7918-2899-9.

2.2.9 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.

2.2.10 *Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.

2.2.11 *Benhardt, H.C.; Eide, S.A.; Held, J.E.; Olsen, L.M.; and Vail, R.E. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U).* WSRC-TR-93-581. Aiken, South Carolina: Westinghouse Savannah River Company, Savannah River Site. ACC: MOL.20061201.0160.

2.2.12 *Brereton, S.J.; Alesso, H.P.; Altenbach, T.J.; Bennett, C.T.; and Ma, C. 1998. *AVLIS Criticality Risk Assessment.* UCRL-JC-130693. Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL.20080102.0002.

2.2.13 BSC 2005. (Bechtel SAIC Company) 2005 *Thermal Performance of Spent Nuclear Fuel During Dry Air Transfer-Initial Calculations.* 000-00C-DSU0-03900-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050110.0003.

2.2.14 BSC 2007. *Basis of Design for the TAD Canister-Based Repository Design Concept.* 000-3DR-MGR0-00300-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0042.

2.2.15 *BSC 2007. *Canister Receipt and Closure Facility 1 Fire Hazard Analysis.* 060-M0A-FP00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0032.

2.2.16 BSC 2007. *CRCF-1 and IHF WP Transfer Trolley Mechanical Equipment Envelope Plan & Elevations-Sh 1 of 2.* 000-MJ0-HL00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0015.

2.2.17 BSC 2007. *Emplacement and Retrieval Transport and Emplacement Vehicle Mechanical Equipment Envelope.* 800-MJ0-HE00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070918.0041.

2.2.18 BSC 2007. *Frequency Analysis of Aircraft Hazards for License Application.* 000-00C-WHS0-00200-000-00F. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070925.0012.

2.2.19 BSC 2007. *GROA External Dose Rate Calculation.* 000-PSA-MGR0-01300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071023.0003.

2.2.20 BSC 2007. *Leak Path Factors for Radionuclide Releases from Breached Confinement Barriers and Confinement Areas.* 000-00C-MGR0-01500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0002.

2.2.21 *BSC 2007. *Liquid Low-Level Waste Collection Calculation.* 100-M0C-MWL0-00100-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050922.0008.

2.2.22 BSC 2007. *Mechanical Handling Design Report for Cask Transfer Trolley.* 000-30R-HM00-00200-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071219.0001.

2.2.23 BSC 2007. *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert.* 000-00C-DNF0-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071017.0001.

2.2.24 BSC 2007. *Receipt Facility Fire Hazard Analysis.* 200-M0A-FP00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070823.0001.

2.2.25 *BSC 2007. *Utilities Facility Deionized Water System Supply Piping & Instrument. Diagram.* 25A-M60-PSD0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071015.0010.

2.2.26 BSC 2007. *Waste Form Throughputs for Preclosure Safety Analysis.* 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.

2.2.27 BSC 2007. *Wet Handling Facility General Arrangement Ground Floor Plan.* 050-P10-WH00-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0032.

2.2.28 BSC 2007. *Wet Handling Facility and Low Level Waste Facility Worker Dose Assessment.* 050-00C-WH00-00200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071017.0002.

2.2.29 BSC 2008. *External Events Hazards Screening Analysis*. 000-00C-MGR0-00500-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080219.0001.

2.2.30 *BSC 2008. *Initial Handling Facility Fire Hazard Analysis.* 51A-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0007.

2.2.31 BSC 2008. *Nuclear Facilities Slide Gate Process and Instrumentation Diagram.* 000-M60-H000-00201-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080123.0025.

2.2.32 *BSC 2008. *Pool Water Treatment and Cooling System.* 050-M0C-PW00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0002.

2.2.33 BSC 2008. *Preclosure Consequence Analyses*. 000-00C-MGR0-00900-000-00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080129.0006.

2.2.34 BSC 2008. *Preclosure Criticality Analysis Process Report.* TDR-DS0-NU-000001 REV 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080220.001.

2.2.35 BSC 2008. *Preclosure Criticality Safety Analysis.* TDR-MGR-NU-000002 REV 01. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0007.

2.2.36 BSC 2008. *Seismic and Structural Container Analyses for the PCSA.* 000-PSA-MGR0-02100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080220.0003

2.2.37 BSC 2008. *Wet Handling Facility Event Sequence Development Analysis*. 050-PSA-WH00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080225.0010.

2.2.38 *BSC 2008. *Wet Handling Facility Fire Hazard Analysis.* 050-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: 20080213.0001.

2.2.39 *BSC 2008. *Wet Handling Facility ITS Train "A" Electrical Room Equipment Layout.* 050-E4K-EEE0-00101-000 Rev 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061114.0002.

2.2.40 Not Used.

2.2.41 *CRA (Corporate Risk Associates Limited) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique.* CRA-BEGL-POW-J032. Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.

2.2.42 *Denson, W.; Chandler, G.; Crowell, W.; Clark, A; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995*. NPRD-95. Rome, New York. Reliability Analysis Center. TIC: 259757.

2.2.43 DOE (U.S. Department of Energy) 2007. *Software Independent Verification and Validation Report, Change in Operating System Version Report for SAPHIRE v7.26.* Document ID: 10325-COER-7.26-01. Las Vegas, NV: U.S. Department of Energy, Office of Repository Development. ACC: MOL.20070607.0263.

2.2.44 DOE 2007. *Transportation, Aging and Disposal Canister System Performance Specification.* WMO-TADCS-000001, Rev. 0. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070614.0007.

2.2.45 *Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Loss of Offsite Power Events: 1986-2004.* Volume 1 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants.* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0164.

2.2.46 *Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; and Rasmuson, D.M. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.* NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.

2.2.47 *Ellingwood, B.; Galambos, T.V.; MacGregor, J.G.; and Cornell, C.A. 1980. *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures.* SP 577. Washington, D.C.: National Bureau of Standards, Department of Commerce. ACC: MOL.20061115.0081.

2.2.48 EPRI (Electric Power Research Institute) and NRC (U.S. Nuclear Regulatory Commission) 2005. *Summary & Overview.* Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0061.

2.2.49 EPRI and NRC 2005. *Detailed Methodology.* Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI TR-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0062.

2.2.50 *Fischer, L.E.; Chou, C.K.; Gerhard, M.A.; Kimura, C.Y.; Martin, R.W.; Mensing, R.W.; Mount, M.E.; and Witte, M.C. 1987. *Shipping Container Response to Severe Highway and Railway Accident Conditions.* NUREG/CR-4829. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: NNA.19900827.0230.

2.2.51 *Fleming, K.N. 1975. *A Reliability Model for Common Mode Failures in Redundant Safety Systems.* GA-A13284. San Diego, California: General Atomic Company. ACC: MOL.20071219.0221.

2.2.52 *Fragola, J.R. and McFadden, R.H. 1995. "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom." *Reliability Engineering and System Safety, 47*, 255-273. New York, New York: Elsevier. TIC: 259675.

2.2.53 *Gertman, D.I.; Gilbert, B.G.; Gilmore, W.E.; and Galyean, W.J. 1989. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations*. NUREG/CR-4639, Vol. 5, Part 4, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252112.

2.2.54 *Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM.* 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.

2.2.55 *Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

2.2.56 *Lopez Droguett, E.; Groen, F.; and Mosleh, A. 2004. "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety 83*, 311–321. New York, New York. Elsevier. TIC: 259380.

2.2.57 *Marshall, F.M.; Rasmuson, D.M.; and Mosleh, A. 1998. *Common-Cause Failure Parameter Estimations.* NUREG/CR-5497. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0105.

2.2.58 *Martz, H.F. and Waller, R.A. 1991. *Bayesian Reliability Analysis.* Malabar, Florida: Krieger Publishing Company. TIC: 252996. ISBN: 0-89464-395-9.

2.2.59 *Mosleh, A. 1993. *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis.* NUREG/CR-5801. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 245473.

2.2.60 *Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques.* Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

2.2.61 *Mosleh, A.; Rasmuson, D.M; and Marshall, F.M. 1988. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106.

2.2.62 NFPA (National Fire Protection Association) 2006. *Standard for the Installation of Sprinkler Systems.* 2007 Edition. NFPA 13-2007. Quincy, Massachusetts: National Fire Protection Association. TIC: 258713.

2.2.63 *Nowlen, S.P. 1986. *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report.* NUREG/CR-4680. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0099.

2.2.64 *Nowlen, S.P. 1987. *Quantitative Data on the Fire Behavior of Combustible Materials Found in Nuclear Power Plants: A Literature Review.* NUREG/CR-4679. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0100.

2.2.65 NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

2.2.66 *NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. Final Report. NUREG/CR-2300. Two volumes: Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

2.2.67 NRC 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.* NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

2.2.68 NRC 1997. *Standard Review Plan for Dry Cask Storage Systems.* NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.

2.2.69 NRC 2000. *Standard Review Plan for Transportation Packages for Spent Nuclear Fuel.* NUREG-1617. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249470.

2.2.70 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.

2.2.71 NRC 2003. *Yucca Mountain Review Plan, Final Report.* NUREG-1804, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards. TIC: 254568.

2.2.72 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis.* HLWRS-ISG-04. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0230.

2.2.73 NRC 2007. *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation.* HLWRS-ISG-02. Washington, DC: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.

2.2.74 *Owen, A.B. 1992. "A Central Limit Theorem for Latin Hypercube Sampling." *Journal of the Royal Statistical Society: Series B, Statistical Methodology, 54*, (2), 541-551. London, England: Royal Statistical Society. TIC: 253131.

2.2.75 Regulatory Guide 1.174, Rev. 1. 2002. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.* Washington, D.C.: U. S. Nuclear Regulatory Commission. ACC: MOL.20080215.0049.

2.2.76 *SAIC (Science Applications International Corporation) 2002. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology.* SAIC-01/2650. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20080115.0138.

2.2.77 SAPHIRE V. 7.26. 2007. VMware/WINDOWS XP. STN: 10325-7.26-01. (DIRS 183846)

2.2.78 SFPE (Society of Fire Protection Engineers) 2002. *SFPE Handbook of Fire Protection Engineering.* 3rd Edition. Quincy, Massachusetts: National Fire Protection Association. TIC: 255463. ISBN: 087765-451-4.

2.2.79 *Siu, N.O. and Kelly, D.L. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment." *Reliability Engineering and System Safety, 62*, 89-116. New York, New York: Elsevier. TIC: 258633.

2.2.80 *Smith, C. 2007. *Master Logic Diagram.* Bethesda, Maryland: Futron Corporation. ACC: MOL.20071105.0153.

2.2.81 *Snow, S.D. and Morton, D.K. 2007. *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository.* EDF-NSNF-087, Rev. 0. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0063.

2.2.82 *Snow, S.D. 2007. *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-Foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations.* EDF-NSNF-085, Rev. 0. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0062.

2.2.83 *Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; and Yoshimura, H.R. 2000. *Reexamination of Spent Fuel Shipment Risk Estimates.* NUREG/CR-6672. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20001010.0217.

2.2.84 *Swain, A.D. and Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report.* NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.

2.2.85 *Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings.* VTT Technical Research Centre of Finland. Ph.D. Dissertation. Espoo, Finland. TIC: 259928. ISBN: 951-38-6392-1.

2.2.86 Not Used.

2.2.87 Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook.* NUREG-0492. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 208328.

2.2.88 *Williams, J.C. 1986. "HEART - A Proposed Method for Assessing and Reducing Human Error." *9th Advances in Reliability Technology Symposium – 1986*. Bradford, England: University of Bradford. TIC: 259862.

2.2.89 NRC 2003. Interim Staff Guidance - 18. The Design/Qualification of Final Closure Welds on Austenitic Stainless Steel Canisters as Confinement Boundary for Spent Fuel Storage and Containment Boundary for Spent Fuel Transportation. ISG-18. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 254660.

2.2.90 BSC 2007. *Shielding Requirements and Dose Rate Calculations for WHF and LLW*. 050-00C-WH00-00300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0017.

2.2.91 NRC (U.S. Nuclear Regulatory Commission) 2000. *Standard Review Plan for Spent Fuel Dry Storage Facilities.* NUREG-1567. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 247929.

2.3 DESIGN CONSTRAINTS

2.3.1 10 CFR Part 50. 2007. Energy: Domestic Licensing of Production and Utilization Facilities.

2.3.2 10 CFR Part 63. 2007. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada.

2.3.3 10 CFR Part 71. 2007. Energy: Packaging and Transportation of Radioactive Material. ACC: MOL.20070829.0114.

2.3.4 10 CFR Part 72. 2007. Energy: Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste.

2.4 DESIGN OUTPUTS

2.4.1 BSC 2008. *ITS SSC/Non-ITS SSC Interactions Analysis*. 000-PSA-MGR0-02300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company.

2.4.2 BSC 2008. *Preclosure Nuclear Safety Design Bases*. 000-30R-MGR0-03500-000-000. Las Vegas, Nevada: Bechtel SAIC Company.

2.4.3 BSC 2008. *Preclosure Procedural Safety Controls*. 000-30R-MGR0-03600-000-000 REV 00. Las Vegas, Nevada: Bechtel SAIC Company.

2.4.4 BSC 2008. *Seismic Event Sequence Quantification and Categorization*. 000-PSA-MGR0-01100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company.

2.5 ATTACHMENT REFERENCES

2.5.1 Attachment A: Design Input references are listed in Section 2.2 of the main report.

2.5.2 Attachment B: Design Input references are listed in Sections B1.1; B2.1; B3.1; B4.1; B5.1; B6.1; B7.1; B8.1; B9.1.

2.5.3 Attachment C: Design Input references are listed in Section C1.2.

2.5.4 Attachment D: Design Input references are listed in Section D4

2.5.5 Attachment E: Design Input references are listed in Section E9.

2.5.6 Attachment F: Design Input references are listed in Section F2.

2.5.7 Attachment G: This attachment does not contain Design Input references.

2.5.8 Attachment H: This attachment does not contain Design Input references.

3. ASSUMPTIONS

3.1 ASSUMPTIONS REQUIRING VERIFICATION

There are no assumptions requiring verification.

3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION

3.2.1 General Analysis Assumptions

Assumption–Equipment and SSCs designed and purchased for the Yucca Mountain repository are of the population of equipment and SSCs represented in United States industry-wide reliability information sources. Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population.

Rationale–Although the repository features some unique pieces of equipment at the system level (such as the waste package transfer trolley (WPTT) and the cask transfer trolley (CTT)), at the component level, the repository relies on proven and established technologies. The industry-wide information sources include historical reliability information at the component level. Such experience is relevant to the repository because the repository relies on components that are similar to the ones represented in the information sources. In some cases, system-level information, such as crane load-drop rates, from industry-wide information sources are used. It is appropriate to use such information because it represents similar pieces of equipment at the system level. In addition, drawing from a wide spectrum of sources takes advantage of many observations, which yields better statistical information regarding the uncertainty associated with the resulting reliability estimates.

4. METHODOLOGY

4.1 QUALITY ASSURANCE

This analysis has been prepared in accordance with *Calculations and Analyses* (Ref. 2.1.1) and *Preclosure Safety Analysis Process* (Ref. 2.1.4). Therefore, the approved version is designated as "QA: QA."

In general, input designated "QA: QA" is used. However, some of the inputs that are cited are designated "QA: N/A." The suitability of these diagrams for the intended use is justified as follows:

Documentation of suitability for intended use of "QA: N/A" drawings: Engineering drawings are prepared using the "QA: QA" procedure *Engineering Drawings* (Ref. 2.1.2). They are checked by an independent checker and reviewed for constructability and coordination before review and approval by the engineering group supervisor and the discipline engineering manager (Ref. 2.1.2, Attachments 3 and 5). The check, review, and approval process provides assurance that these drawings accurately document the design and operational philosophy of the facility. For this reason, they are suitable for their intended use as sources of input to this analysis.

Documentation of suitability for intended use of sketches (which are "QA: N/A"): In a few instances, sketches are used as inputs to this analysis. The use of sketches is acceptable for committed analyses, such as the present analysis, provided that the results are not used for procurement, fabrication, or construction purposes. Because the present analysis is not used for procurement, fabrication, or construction purposes, the use of sketches is acceptable. Therefore, the sketches that are used as inputs are suitable for their intended uses

Documentation of suitability for intended use of "QA: N/A" engineering calculations or analyses: Engineering calculations and analyses are prepared using the "QA: QA" procedure *Calculations and Analyses* (Ref. 2.1.1). They are checked by an independent checker and reviewed for coordination before review and approval by the engineering group supervisor and the discipline engineering manager. The check, review, and approval process provides assurance that these calculations and analyses accurately document the design and operation of the facility. For this reason, they are suitable for their intended use as sources of input to this analysis.

Documentation of suitability for intended use of engineering studies (which are "QA: N/A"): In a few instances, studies are used as inputs to this analysis. The uses of inputs from studies are made clear by the context of the discussion at the point of use. The use of studies is acceptable for committed analyses, such as the present analysis, provided that the results are not used for procurement, fabrication, or construction purposes. Because the present analysis is not used for procurement, fabrication, or construction purposes, the use of studies is acceptable. Therefore, the studies that are used as inputs are suitable for their intended uses.

Documentation of suitability for intended use of BSC design guides (which are "QA: N/A"): The uses of inputs from design guides are made clear by the context of the discussion at the point of use. Design guides are used as inputs only when specific design documents, such as drawings, calculations, and design reports are not available at the present level of design

development. Therefore, the design guides that are used as inputs are suitable for their intended uses.

Documentation of suitability for intended use of BSC engineering standards (which are "QA: N/A"): Engineering standards are used in this analysis as the basis for the numbering system for basic events. The uses of inputs from BSC engineering standards are made clear by the context of the discussion at the point of use. Therefore, the design guides that are used as inputs are suitable for their intended uses.

Documentation of suitability for intended use of BSC Interoffice memorandum: Due to the early nature of the design of some systems, the only available sources for the information used are interoffice memorandum. The information used from these sources is conservative estimates and appropriate for their intended use.

Documentation of suitability for intended use of inputs from outside sources: The uses of inputs from outside sources are made clear by the context of the discussion at the point of use. These uses fall into the following categories and are justified as follows (in addition to the justifications provided at the point of use).

1. Some inputs are cited as sources of the methods used in the analysis. These inputs are suitable for their intended uses because they represent commonly accepted methods of analysis among safety analysis practitioners or, more generally, among scientific and engineering professionals.

2. Some inputs are cited as examples of applications of methods of analysis by others. These inputs are suitable for their intended uses because they illustrate applicable methods of analysis.

3. Some inputs are cited as sources of historical safety-related data. These inputs are suitable for their intended uses because they represent historical data that is commonly accepted among safety analysis practitioners.

4. Some inputs are cited as sources of accepted practices as recommended by codes, standards, or review plans. These inputs are suitable for their intended uses because they represent codes, standards, or review plans that are commonly accepted by practitioners of the affected professional disciplines.

5. Some inputs provide information specific to the Yucca Mountain repository that was produced by organizations other than BSC. These inputs are suitable for their intended uses because they provide information that was developed for the Yucca Mountain repository under procedures that apply to the organization that produced the information.

4.2 USE OF SOFTWARE

4.2.1 Level 1 Software

This section addresses software used in this analysis as Level 1 software, as defined in *Software Management* (Ref. 2.1.3, Attachment 12). SAPHIRE Version 7.26 STN 10325-7.26-01

(Ref. 2.2.77) is used in this analysis for PRA simulation and analyses. The SAPHIRE software is used on a personal computer running Windows XP inside a VMware virtual machine; it is also listed in the current *Qualified and Controlled Software Report*, and was obtained from Software Configuration Management. The SAPHIRE software is specifically designed for PRA simulation and analyses, and has been verified to show that this software produces precise solutions for encoded mathematical models within the defined limits for each parameter employed (Ref. 2.2.43). Therefore, SAPHIRE version 7.26 is suitable for use in this analysis.

The SAPHIRE project files for this analysis are listed in Attachment H. They are contained on a compact disc, which is included as part of Attachment H. SAPHIRE project files contain all of the inputs that SAPHIRE requires to produce the outputs that are documented in this analysis.

4.2.2 Level 2 Software

This section addresses software used in this analysis that are classified as Level 2 software, as defined in *Software Management* (Ref. 2.1.3, Attachment 12). The software is used on personal computers running either Windows XP Professional or Windows 2000 operating systems.

- Word 2003, a component of Microsoft Office Professional 2003, and Visio Professional 2003 are listed in the current *Level 2 Usage Controlled Software Report*. Visio 2003 and Word 2003 are used in this analysis for the generation of graphics and text. The accuracy of the resulting graphics and text is verified by visual inspection. The precise means of verification is left to the discretion of the checker in compliance with applicable procedures.

- Excel 2003, a component of Microsoft Office Professional 2003, and Mathcad versions 13.0 and 14.0 are listed in the current *Level 2 Usage Controlled Software Report*. Crystal Ball version 7.3.1 (a commercial, off-the-shelf, Excel-based risk-analysis tool) is listed on the *Controlled Software Report* and is registered for Level 2 usage. Excel 2003, Mathcad 13.0 and 14.0, and Crystal Ball 7.3.1 are used in this analysis to calculate probability distributions for selected SAPHIRE inputs and to graphically display information. Graphical representations are verified by visual inspection. The calculations are documented in sufficient detail to allow an independent replication of the computations. The user defined formulas and inputs are verified by visual inspection. The results are in some cases verified by independent replication of the computations. However, in some cases, for example, for some Excel calculations and Mathcad 13.0 and 14.0 calculations, the results are verified by visual inspection. The precise means of verification is left to the discretion of the checker in compliance with applicable procedures

- WinZip 9.0, a file compression utility for Windows, is listed in the current *Level 2 Usage Controlled Software Report*. WinZip 9.0 is used in this analysis to compress files for presentation on compact disc in Attachment H.

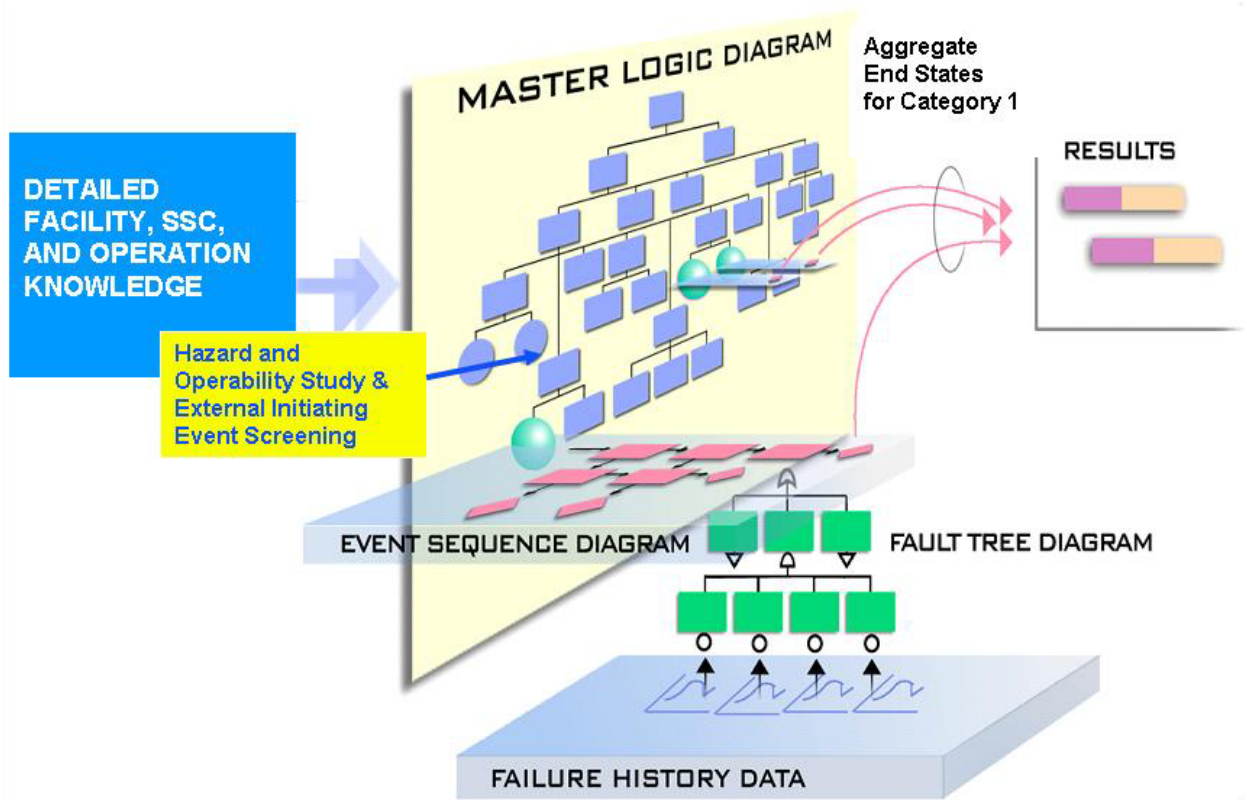
4.3 DESCRIPTION OF ANALYSIS METHODS

This section presents the PCSA approach and analysis methods in the context of overall repository operations. As such, it includes a discussion of operations that may not apply to the

WHF. Specific features of the WHF and its operations are not discussed until Section 6, where the methods described here are applied to the WHF. The PCSA uses the technology of PRA as described in references such as *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.7). The PRA answers three questions:

1. What can go wrong?
2. What are the consequences?
3. How likely is it?

PRA may be thought of as an investigation into the responses of a system to perturbations or deviations from its normal operation or environment. The PCSA is a simulation of how a system acts when something goes wrong. Relationships between the methodological components of this PCSA are depicted in Figure 4.3-1. Phrases in ***bold italics*** in this section indicate methods and ideas depicted in Figure 4.3-1. Phrases in *normal italics* indicate key concepts.



Source: Modified from *Master Logic Diagram* (Ref. 2.2.80)

Figure 4.3-1. Event Sequence Analysis Process

The PCSA starts with analysts obtaining sufficient knowledge of the design and operations of facility, equipment, and SSCs to understand how the YMP waste handling is conducted. This is largely performed and documented in the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37). An understanding of how a facility operates is a prerequisite for developing event sequences that depict how it would fail. *Success criteria* are important additional inputs to the PCSA. A success criterion states the minimum functionality that

constitutes acceptable, safe performance. For example, a success criterion for a crane is to pick-up, transport, and put-down a cask without dropping it. The complementary statement of a success criterion is a failure mode (e.g., crane drops cask).

The basis of the PCSA is the development of ***event sequences***. An event sequence may be thought of as a string of events beginning with an *initiating event* and eventually leading to potential consequences (*end states*). Between initiating events and end states within a scenario, are *pivotal events* that determine whether and how an initiating event propagates to an end state. An event sequence answers the question "What can go wrong?" and is defined by one or more initiating events, one or more pivotal events, and one end state. Initiating events are identified by MLD development, cross-checked with an evaluation based on applied HAZOP techniques. Event sequences unfold as a combination of failures and successes of pivotal events. An end state, the termination point for an event sequence, identifies the type of radiation exposure or potential criticality, if any, that results. In this analysis, eight mutually exclusive end states are of interest:

1. "OK"–Indicates the absence of radiation exposure and potential for criticality.

2. Direct Exposure, Degraded Shielding–Applies to event sequences where an SSC providing shielding is not breached, but its shielding function is jeopardized. An example is a lead-shielded transportation cask that is dropped from a height great enough for the lead to slump toward the bottom of the cask at impact, leaving a partially shielded path for radiation to stream. This end state excludes radionuclide release.

3. Direct Exposure, Loss of Shielding–Applies to event sequences where an SSC providing shielding fails, leaving a direct path for radiation to stream. For example, this end state applies to a breached transportation cask, with a canister inside maintaining its containment function. In another example, this end state applies to shield doors inadvertently opened. This end state excludes radionuclide release.

4. Radionuclide Release, Filtered–Indicates a release of radioactive material from its confinement, through a filtered path, to the environment. The release is filtered when it is confined and filtered through the successful operation of the HVAC system over its mission time. This end state excludes moderator intrusion.

5. Radionuclide Release, Unfiltered–Indicates a release of radioactive material from its confinement, through the pool of the WHF or through an unfiltered path, to the environment. This end state excludes moderator intrusion.

6. Radionuclide Release, Filtered, Also Important to Criticality–This end state refers to a situation in which a filtered radionuclide release occurs and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.

7. Radionuclide Release, Unfiltered, Also Important to Criticality–This end state refers to a situation in which an unfiltered radionuclide release occurs and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.

8. Important to Criticality–This end state refers to a situation in which there has been no radionuclide release and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.

The answer to the second question, "What are the consequences?" requires consideration of radiation exposure and the potential for criticality for Category 1 and Category 2 event sequences. Consideration of the consequences of event sequences that are Beyond Category 2 is not required by 10 CFR 63 (Ref. 2.3.2). Radiation doses to individuals from direct exposure and radionuclide release are addressed in a companion consequence analysis by modeling the effects of bounding event sequences related to the various waste forms and the facilities that handle them.

The radiological consequence analysis develops a set of bounding consequences. Each bounding consequence represents a group of like event sequences. The group (or bin) is based on such factors as characteristics of the waste form involved, availability of HEPA filtration, location of occurrence (in water or air), and characteristics of the surrounding material (such as transportation cask or waste package). Each event sequence is mapped to one of the bounding consequences, for which conservative doses have been calculated.

Criticality analyses are performed to ensure that any Category 1 and Category 2 event sequences that terminate in end states that are important to criticality would not result in a criticality. In order to determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity of variations in each of the parameters important to criticality during the preclosure period. The parameters are: waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor to variations in any of these parameters as a function of the other parameters. The deterministic sensitivity analysis covers all reasonably achievable repository configurations that are important to criticality. Refer to Section 4.3.9 for detailed discussion of the treatment of criticality in event sequences.

The third question, "How likely is it?" is answered by the estimation of event sequence frequencies. The PCSA uses ***failure history*** records (for example, *Nonelectronic Parts Reliability Data* (Ref. 2.2.42) and *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations*. NUREG/CR-4639 (Ref. 2.2.53)), structural reliability analysis, thermal stress analysis, and engineering and scientific knowledge about the design as the basis for estimation of probabilities and frequencies. These sources coupled with the techniques of probability and statistics, for example, *Handbook of Parameter Estimation for Probabilistic Risk Assessment* (Ref. 2.2.10), are used to estimate frequencies of initiating events and event sequences and the conditional probabilities of pivotal events.

The PCSA uses ***event sequence diagrams (ESDs***), event trees, and ***fault trees*** to develop and quantify event sequences. The ESDs and event trees are described and developed in the event sequence development analyses. The present analysis uses fault trees to disaggregate an SSC or item of equipment to a level of detail that is supported by available reliability information from

failure history records. Various techniques of probability and statistics are employed to estimate failure frequencies of mechanical, electrical, electro-mechanical, and electronic equipment. Such frequencies, or *active-component* unreliability's, provide inputs to the fault tree models of items of equipment. Fault trees are used in some instances to model initiating events and in other instances to model pivotal events.

Some pivotal events are related to structural failures of containment (e.g., canisters) and others are related to shielding (e.g., transportation casks). In these cases, probabilistic structural reliability analysis methods are employed to calculate the mean conditional probability of containment or shielding failure given the initiating event (e.g., a drop from a crane). Other pivotal events require knowledge of response to fires. Calculation of failure probabilities given a fire is accomplished by the appropriate analysis using applicable material properties and traditional methods of heat transfer analysis, structural analysis, and fire dynamics. The probabilities so derived are called *passive-equipment* failure probabilities.

All pivotal events in the PCSA are characterized by *conditional probabilities* because their values rely on the conditions set by previous events in an event sequence. For example, the failure of electrical or electronic equipment depends on the operating temperature. Therefore, if a previous event in a scenario is a failure of a cooling system, then the probability of the electronic equipment failure would depend on the operation (or not) of the cooling system.

The frequency of occurrence of an event sequence is the product of the frequency of its initiating event and the conditional probabilities of its pivotal events. This is true whether or not the frequency and probabilities are expressed as single points or probability distributions. To group together event sequences for the purpose of categorization, the frequencies of event sequences within the same ESD that result in the same end state, are summed. The concept of ***aggregating event sequences*** to obtain aggregated end-state results is depicted in Figure 4.3-1.

The PCSA is described above as a system simulation. This is important in that any simulation or model is an approximate representation of reality. Approximations may lead to uncertainties regarding the frequencies of event sequences. The event sequence quantification presented in this document propagates input uncertainties to the calculated frequencies of event sequences using Monte Carlo techniques. Figure 4.3-1 illustrates the ***results*** as horizontal bars to depict the uncertainties that give rise to potential ranges of results.

As required by the performance objectives for the GROA through permanent closure in 10 CFR 63.111 (Ref. 2.3.2), each aggregated event sequence is categorized based on its frequency. Therefore, the focus of the analysis in this document is to:

1. Quantify the frequency of each initiating event that is identified in *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37).

2. Quantify the conditional probability of the pivotal events in each event sequence.

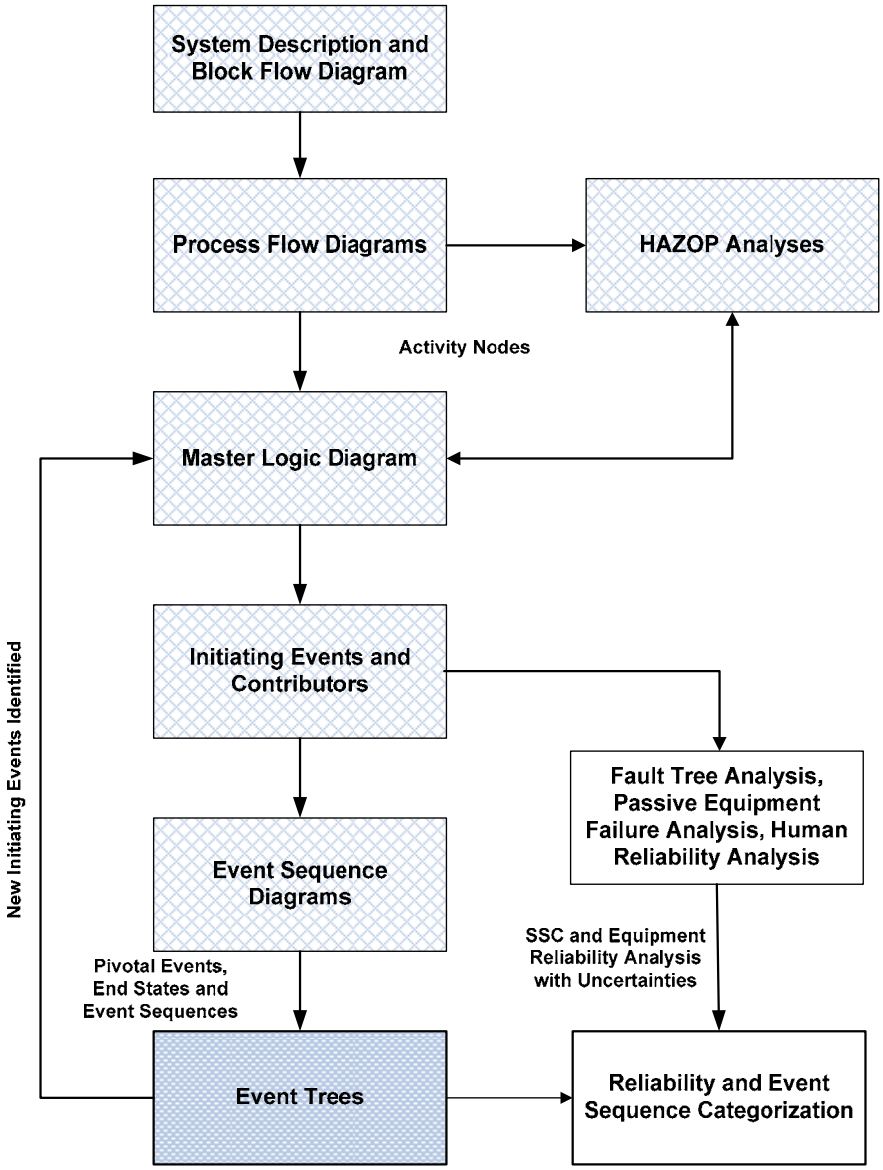
3. Calculate the frequency of each event sequence (i.e., calculate the product of the initiating event frequency and pivotal event conditional probabilities).

4. Calculate the frequencies of the aggregated event sequences.

5. Categorize the aggregated event sequences for further analysis.

The activities required to accomplish these objectives are illustrated in Figure 4.3-2 and described below.

The cross-hatched boxes in Figure 4.3-2 serve as a review of the analysis performed for the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37). The interface between the event sequence development analysis and the present categorization analysis is the set of event trees, as represented by the darkly shaded box. The event trees from the event sequence development analysis are passed as input into the present analysis. The unshaded boxes represent the analysis performed in this study, the methods of which are described later in Section 4.



NOTE: HAZOP = hazard and operability (study/analysis); SSC = structure, system, or component.

Source: Modified from Ref. 2.2,37, Figure 2.

Figure 4.3-2. Preclosure Safety Assessment Process

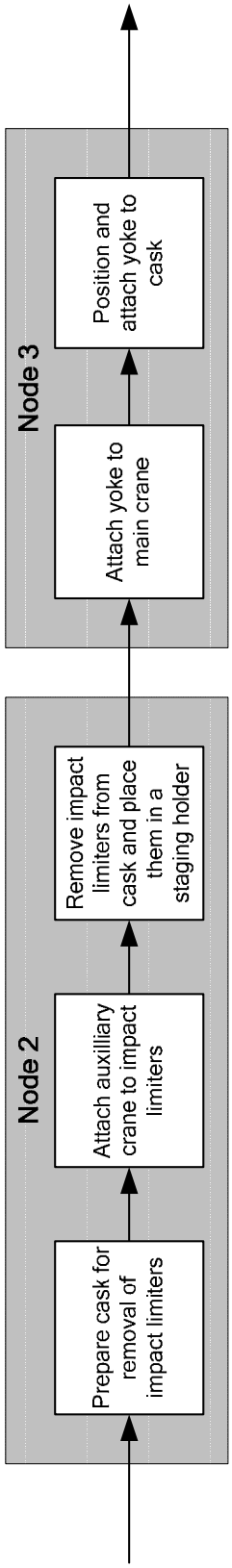
The event sequences that are categorized in the present analysis can be more fully understood by consulting the event sequence development analysis (Ref. 2.2.37). The remainder of this subsection presents a refresher of the event sequence development process

A simplified process flow diagram (PFD) is developed to clearly delineate the process and sequence of operations to be considered within the analysis of the facility. An excerpt from an example PFD is shown in Figure 4.3-3. The PFD guides development of the MLD and the conduct of the HAZOP evaluation. The PFD is broken down into nodes to identify specific processes and operations that are evaluated with both a MLD and HAZOP evaluation to identify potential initiators.

Development of the MLD is accomplished by deriving specific failures from a generalized statement of the undesired state. As a "top-down" analysis, the MLD starts with a top event, which represents a generalized undesired state. The top event includes direct exposure to radiation and exposure as result of a release of radioactive material. The basic question answered by the MLD is "How can the top event occur?" Each successively lower level in the MLD hierarchy divides the identified ways in which the top event can occur with the aim of eventually identifying specific initiating events that may cause the top event. In the MLD, the initiating events are shown at the next-to-lowest level. The lowest level provides an example of contributors to the initiating event. This process for the PCSA is detailed in *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37, Section 4.3.1.2).

The HAZOP evaluation focuses on identifying potential initiators that are depicted in the lower levels of the MLD. It is a "bottom-up" approach that supplements the "top-down" approach of the MLD. The HAZOP evaluation is also a systematic analysis of repository operations during the preclosure phase. As an early step in the performance of the HAZOP evaluation, the intended function, or intention, of each node in the PFD is defined. The intention is a statement of what the node is supposed to accomplish as part of the overall operation. The HAZOP analysts work their way through the PFD, node by node, and postulate deviations from normal operations. A "deviation" is any out-of-tolerance variation from the normal values of parameters specified for the intention. Although the repository is in some ways to be the first of its kind, the operations are based on established technologies: for example, transportation cask movement by truck and rail, crane transfers of casks and canisters, rail-based trolleys, air-based conveyances, robotic welding, and SNF pool operations. The team assembled for the HAZOP evaluation (and available on call as questions arose) had experience with such technologies and was well equipped to perform the evaluation.

The MLD and HAZOP evaluation are strongly interrelated. The MLD is cross-checked to the HAZOP evaluation. That is, the MLD is modified to include any initiators and contributors that are identified in the HAZOP evaluation but not already included in the MLD. The entire process is iterative in nature (Figure 4.3-2, iteration not shown) with insights from succeeding steps often feeding back to predecessors. The top-down MLD and the bottom-up HAZOP evaluation provide a diversity of viewpoints that adds confidence that no important initiating events have been omitted. Details on implementation of the HAZOP evaluation are presented in *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37, Section 4.3.1.3).

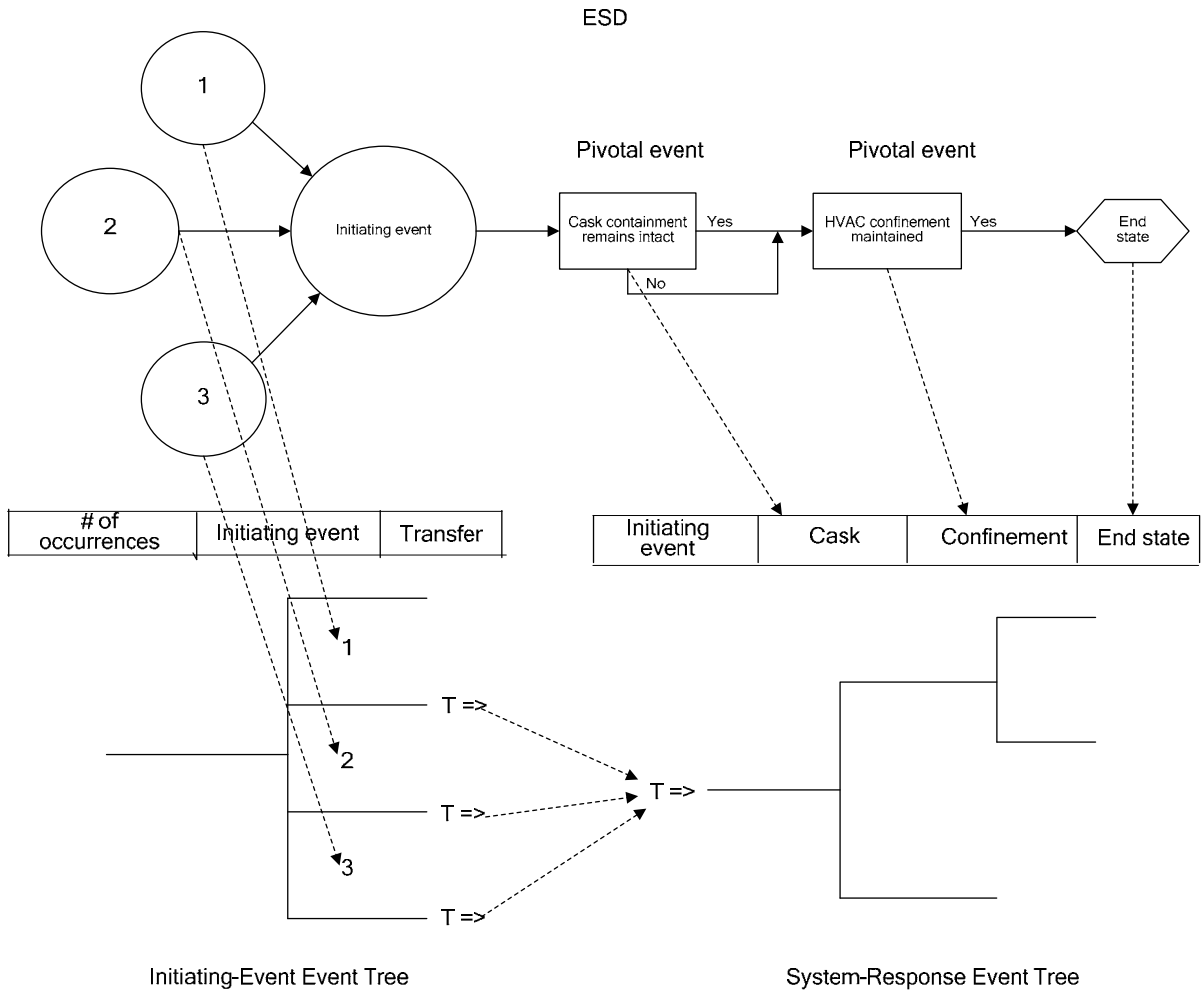


NOTE: This diagram illustrates a small portion of the overall handling operations for a typical waste handling facility.

Source: Original

Figure 4.3-3. Portion of a Simplified Process Flow Diagram for a Typical Waste-Handling Facility

An overview of the pertinent human and SSC responses to an initiating event is depicted in an ESD. As shown in Figure 4.3-4, an ESD represents event sequences in terms of initiating events, pivotal events, and end states. The boxes (pivotal events) represent events that have binary outcomes: success (yes) or failure (no). Because the future is uncertain, the analyst does not know which of the alternative scenarios might occur. The ESD depicts the alternative scenarios as paths that can be traced through the diagram. Each alternative path from an initiating event to an end state represents an event sequence. The events that may occur after the initiating event are identified by asking and answering the question "What can happen next?" Typically, questions about the integrity of radionuclide containment (e.g., cask, canister, or waste package) and confinement (e.g., HVAC) become pivotal events in the ESD.



Source: Original

Figure 4.3-4. Event Sequence Diagram–Event Tree Relationship

The initiating events that are represented in the MLD are transferred to events depicted as "little bubbles" (Figure 4.3-4; 1, 2, and 3) in the ESDs. One or more initiating events identified on the MLD may be included in a single little bubble, but all of the initiating events included in the little bubble must have the same pivotal events (i.e., human and SSC responses) and the same conditional probability for each pivotal event. Initiating events represented by little bubbles may be aggregated further into "big bubbles" as depicted in Figure 4.3-4. The big bubble represents the failures associated with a major function in a specific location depicted in the PFD and establishes the level of aggregation for the categorization of the event sequence (as Category 1, Category 2, or Beyond Category 2).

For example, all initiating events that challenge the containment function of a canister would include pivotal events that question the containment integrity of the canister and the availability of HVAC confinement. The knowledge to develop such ESDs and appropriately group the initiating events comes from a detailed knowledge of the SSCs and operations derived from developing the PFD, MLD, and HAZOP evaluation. The pivotal event conditional probabilities are the same for all initiating events in a little bubble. All initiating events represented by the big bubble have the same human and SSC responses and, therefore, may be represented by the same event sequences. However, the conditional probability for each pivotal event is not necessarily the same for each little bubble.

4.3.1 Event Tree Analysis and Categorization

Also illustrated in Figure 4.3-4, is the relationship of the YMP ESDs to their equivalent event trees. Event trees contain the same information as ESDs but in a form suitable to be used by software such as SAPHIRE (Ref. 2.2.43), which ultimately stores event trees, fault trees, and reliability data, and quantifies the event sequences. Event tree depiction of ESDs provides little new information. In an event tree, each event sequence has its separate line so that the connections between initiating events and end states is more explicit than in ESDs (Ref. 2.2.66, Section 3.4.4.2). Any path from left to right that begins with the initiating event and terminates with an end state is an event sequence. Every path must be associated with an end state. As illustrated in the event tree portion of Figure 4.3-4, each intersection of a horizontal and vertical line is referred to as a node (or branch point). Each node is associated with a conditional probability of following the vertical downward branch. By convention, the description of each branch is stated as a success, and the downward branch indicates a failure. The complement is the probability of taking the vertical upward branch, that is, the probability of success. To quantify the event sequence, the initiating event frequency (or expected number of occurrences) is multiplied by the conditional probability of each subsequent pivotal event node in the event sequence until an end state is reached.

The YMP PCSA uses the concept of linked event trees (Ref. 2.2.66). Each facility has its own set of event trees. The first event tree simply represents the little bubbles, one horizontal line per little bubble. This is called the initiator event tree (IET). The second event tree contains the pivotal events and end states. This is called the system response event tree (SRET). An event sequence would start with each of the horizontal lines as if it were the initiating event on the SRET, as indicated in Figure 4.3-4. Each set of IET and SRET is quantified for each waste container type (e.g., dual-purpose canisters (DPCs), transportation, aging, and disposal (TAD) canisters, DOE SNF that is handled in a facility. The event in the IET labeled "# of occurrences"

represents the number of handlings (i.e., demands) for that initiating event. For example, each lift of a transportation cask provides an opportunity for a drop. An event sequence quantification includes the frequency (or number of occurrences) of each end state (e.g., radionuclide release), associated with a single lift, and multiplies it by the number of lifts to obtain the expected number of drops over the preclosure period. This approach is consistent with a binomial model of reliability.

Categorization of event sequences is based on the aggregated "big bubble" initiating event. Each line on the IET coupled with the SRET is quantified separately. Using Figure 4.3-4, this would mean three quantifications, corresponding to the three initiating event frequencies and three corresponding sets of pivotal event probabilities. (By SAPHIRE convention, the top line is a dummy initiating event.) Each event sequence, therefore, would have three values. In order to obtain the total frequency of an event sequence for purposes of categorization, per 10 CFR 63.111 *Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada* (Ref. 2.3.2), the three frequencies are probabilistically summed. Doing this summation is equivalent to basing categorization on the big bubble. If an event sequence has only one little bubble, then only the SRET needs to be used with the initiating event in the place so denoted, in the second event tree. In this case, summation of event sequences is not necessary and not performed.

Because each event sequence is associated with a mean number of occurrences over the preclosure period, categorization is straightforward. Those event sequences that are expected to occur one or more times before permanent closure of the GROA are Category 1 event sequences. Other event sequences that have at least one chance in 10,000 of occurring but less than one occurrence before permanent closure are Category 2 event sequences. Sequences that have less than one chance in 10,000 of occurring before permanent closure are identified as Beyond Category 2. As described in Section 4.3.6, event sequence quantification considers uncertainties and categorization is performed on the basis of an event sequence mean value of the underlying probability distribution. The preclosure period lasts 100 years but actual emplacement operations occupy 50% of this time (Ref. 2.2.14, Section 2.2.2.7).

An initiating event for an event sequence may have the potential to affect several waste form types (for instance, a high-level radioactive waste (HLW) canister and a DOE standardized canister, or a TAD canister and a DPC). For example, the seismically-induced event sequence leading to a collapse of a surface facility could cause the breach of all the waste forms inside that facility. Similarly, a large fire affecting an entire facility also affects all the waste forms inside the facility. The number of occurrences over the preclosure period of an event sequence that affects more than one type of waste form is equal to the number of occurrences of the event sequence, evaluated for one of the waste form types, multiplied by the probability that the other waste form types are present at the time the initiating event occurs. Because a probability is less than or equal to one, the resulting product is not greater than the number of occurrences of the event sequence before multiplication by the probability. The number of occurrences of an event sequence is calculated for a given waste form type, without adjustment for the probability of presence of other waste form types. The results of the event sequence categorization (reported in Section 6.8.3) show that the event sequences that have the potential to cause personnel exposure to radiation from more than one type of waste form are either Category 2 event sequences resulting in a direct exposure, or Beyond Category 2 event sequences resulting in a radionuclide

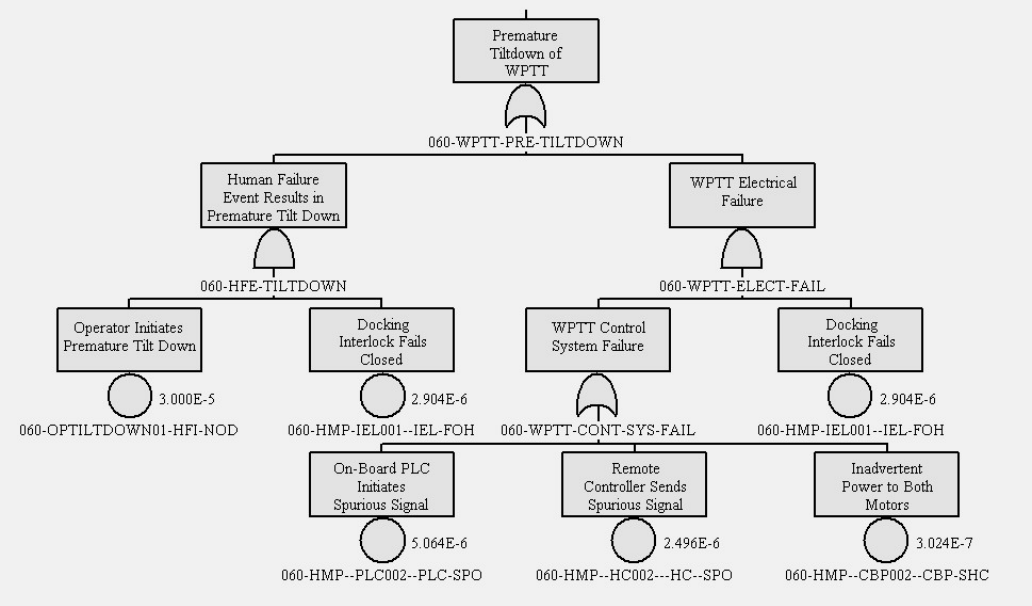
release. In the first case, doses from direct radiation after a Category 2 event sequence have no effect on the public because of the great distances from the locations of offsite receptors. In the second case, Beyond Category 2 event sequences do not require a consequence calculation. Thus, the demonstration that the performance objectives of 10 CFR 63.111 (Ref. 2.3.2) are met is not dependent on the waste form at risk in the event sequences that may involve more than one type of waste form. It is appropriate, therefore, to evaluate event sequences separately for each relevant type of waste form.

4.3.2 Initiating and Pivotal Event Analysis

The purpose of this analysis is to develop the frequency (i.e., number of occurrences over the 50-year operating lifetime of the facility) of each event sequence in order to categorize event sequences in accordance with 10 CFR 63.2 (Ref. 2.3.2). (In this document, the term frequency is used interchangeably with the expected number when discussing event sequence quantification). This involves developing the frequency of each initiating event and conditional probability of each pivotal event. Some pivotal events in this analysis are associated with structural or thermal events. In these cases, passive equipment failure analyses (PEFAs) are performed. The PEFAs include probabilistic structural or thermal analyses as summarized later in this section to develop mean conditional probabilities of failure directly associated with pivotal events. Often, however, the events depicted in ESDs or event trees cannot easily be mapped to such a calculation or to reliability data (e.g., failure history records). This is because large aggregates of components (e.g., systems or complicated pieces of equipment such as the WPTT) may be unique to the YMP facility with little or no prior operating history. The components, however, of which it is composed, have usually been used before and there is an adequate set of reliability data for these components. The PCSA used fault trees for this mapping. As a result, the PCSA disaggregates or breaks down the initiating events and pivotal events, when needed, into a collection of simpler components. All initiating events use fault trees and the pivotal event associated with confinement is analyzed via a fault tree of the HVAC system. In effect, the use of fault trees creates a mapping between ESD or event tree events and the available reliability data.

4.3.2.1 Fault Tree Analysis

Construction of a fault tree is a deductive reasoning process that answers the question “What are all combinations of events that can cause the top event to occur?” Figure 4.3-5 demonstrates this:



NOTE: This fault tree is presented for illustrative purposes only and is not intended to represent results of the present analysis.
PLC = programmable logic controller; WPTT = waste package transfer trolley.

Source: Original

Figure 4.3-5. Example Fault Tree

This top-down analytical development defines the combinations of causes for the initiating or pivotal events, into an event sequence, in a way that allows the probability of the events to be estimated.

As the name implies, fault tree events are usually failures or faults. Fault trees use logic or Boolean gates. Figure 4.3-5 shows two types of gates: the AND gate (mound shaped symbol with a flat bottom) and the OR gate (mound shaped symbol with a concave bottom). An AND gate passes an output up the tree if all events immediately attached to it occur. An OR gate passes an output up the tree if one or more events immediately attached to it take place. An AND gate often implies components or system features that back up each other, so that if one fails, the other continues to adequately perform the function. The success criterion of the SSC or equipment being analyzed is important in determining the appropriate use of gates.

The bottom level of the fault tree contains events with circles beneath them indicating a *basic event*. Basic events are associated with frequencies from industry-wide active equipment reliability information, PEFA, or human reliability analysis (HRA).

Fault trees are Boolean reduced to "minterm" form, which expresses the top event in terms of the union of minimal cut sets. Minimal cut sets, which are groups of basic events that must all occur to cause the top event in the fault tree, result from applying the Boolean Idempotency and Absorption laws. Fault tree analysis, as used in the PCSA, is well described in the *Fault Tree Handbook.* NUREG-0492 (Ref. 2.2.87). Each minimal cut set represents a single basic event or a combination of two or more basic events (e.g., a logical intersection of basic events) that could

result in the occurrence of the event sequence. Minimal cut sets are minimal in the sense that they contain no redundant basic events (i.e., if any basic event were removed from a minimal set, the remaining basic events together would not be sufficient to cause the top event). Section 4.3.6 continues the discussion about utilization of minimal cut sets in the quantification of event sequences.

As illustrated in Figure 4.3-5, the organization of the fault trees in the PCSA is developed to emphasize two primary elements, which together result in the occurrence of the top event: 1) human failure events, and 2) equipment failures. The human failure events include postulated unintended crew actions and omissions of crew actions. Identification and quantification of human failure events (HFEs) are performed in phases. Initial identification of HFEs led to design changes to either eliminate them or reduce the probability that they would cause the fault tree top event. For example, Figure 4.3-5 shows an HFE logically intersected with an electro-mechanical interlock such that both a crew error of commission and failure of the interlock must occur for premature WPTT tiltdown to occur.

Event trees and fault trees are complementary techniques. Often used together, they map the system response from initiating events through damage levels. Together, they delineate the necessary and sufficient conditions for the occurrence of each event sequence (and end state). Because of the complementary nature of using both inductive and deductive reasoning processes, combining event trees and fault trees allow more comprehensive, concise, and clearer event sequences to be developed and documented than using either one exclusively. The selection of and division of labor among each type of diagram depends on the analyst's opinion. In the PCSA, the choice was made to develop event trees along the lines of major functions such as crane lifts, waste container containment, HVAC and building confinement, and introduction of moderator. Fault trees disaggregate these functions into equipment and component failure modes for which unreliabilities or unavailabilities were obtained.

4.3.2.2 Passive Equipment Failure Analysis

Passive equipment (e.g., transportation casks, storage canisters, waste packages) may fail from manufacturing defects, material variability, defects introduced by handling, long-term effects such as corrosion, and normal and abnormal use. Industry codes, such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.6) and *2004 ASME Boiler and Pressure Vessel Code* (Ref. 2.2.8) establish design load combinations for passive structures (such as building supports) and components (such as canisters). These codes specify design basis load combinations and provide the method to establish allowable stresses. Typical load combinations for buildings involve snow load, dead (mass) load, live occupancy load, wind load, and earthquake load. Typical load combinations for canisters and casks are found in *2004 ASME Boiler and Pressure Vessel Code* (Ref. 2.2.8) and would include, for example, preloads or pre-stresses, internal pressurization and drop loads, which are specified in terms of acceleration. Design basis load combinations are purposefully specified to conservatively encompass anticipated normal operational conditions as well as uncertainties in material properties and analysis. Therefore, passive components, when designed to codes and standards and in the absence of significant aging, generally fail because of load combinations or individual loads that are much more severe than those anticipated by the codes. Fortunately, the conservative nature of establishing the design basis, coupled with the low probability of multiple design basis loads

occurring concurrently, often means a significant margin or factor of safety exists between the design point and actual failure. The approach used in the PCSA takes advantage of the design margins (or factor of safety).

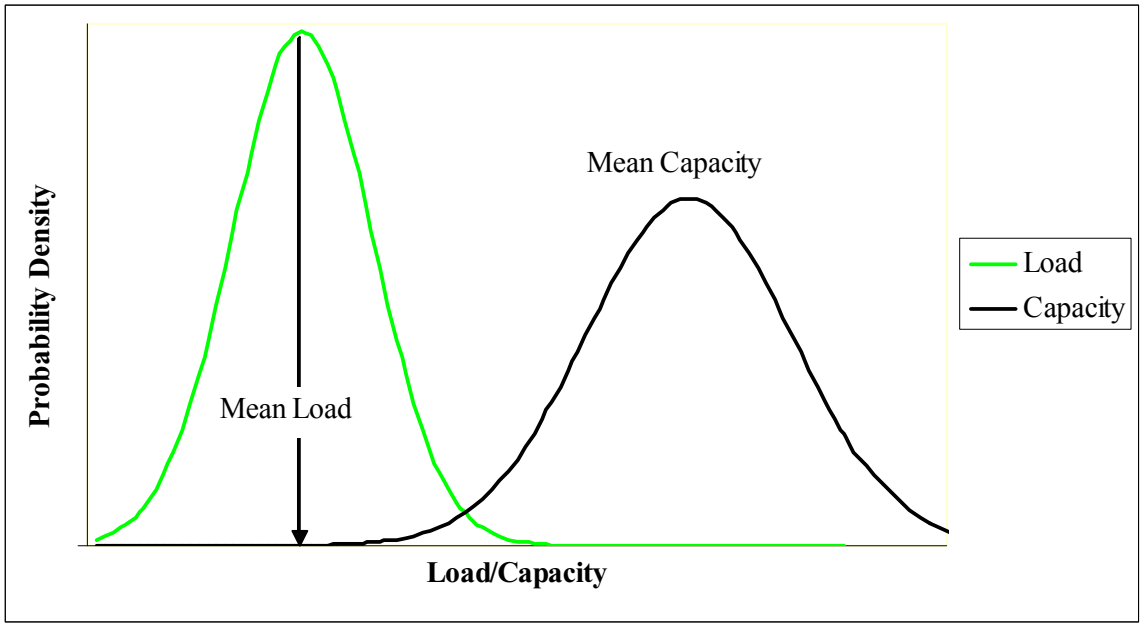
The development of code requirements for minimum design loads in buildings and other structures in the late 1970's considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures* (Ref. 2.2.47). This document refers to classic structural reliability theory. In this theory, each structure has a limit state (e.g., yield or ultimate), such that, loads and resistances are characterized by Equation 1:

$$g(x_1,x_2,....x_i,...x_n) = 0 \qquad \text{(Eq. 1)}$$

In Equation 1, g is termed the limit-state variable where failure is defined as $g < 0$ and the x_i are resistance (sometimes called capacity or fragility) variables or load (sometimes called stress or demand) variables. The probability of failure of a structure is given, in general, by Equation 2:

$$P_f \quad \int ... \int f_x(x_1, x_2, ...x_i ...x_n) dx_1 dx_2 ... dx_n \qquad \text{(Eq. 2)}$$

Where f_x is the joint probability density function of x_i and the integral is over the region in which $g < 0$. The fact that these variables are represented by probability distributions implies that absolutely precise values are not known. In other words, the variable values are uncertain. This concept is illustrated in Figure 4.3-6. Codes and standards such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.6), guide the process of designing structures such that there is a margin, often called a factor of safety, between the load and capacity. The factor of safety is established in recognition that quantities, methods used to evaluate them, and tests used to ascertain material strength give rise to uncertainty. A heuristic measure of the factor of safety is the distance between the mean values of the two curves.



Source: Original

Figure 4.3-6. Concept of Uncertainty in Load and Resistance

In the case in which Equations 1 and 2 are approximated by one variable representing capacity and the other representing load, each of which is a function of the same independent variable *y*, the more familiar load-capacity interference integral results as shown in Equation 3.

$$P_f \quad \int F(y)h(y)dy \qquad \text{(Eq. 3)}$$

P_f is the mean probability of failure and is appropriate for use when comparing to a probability criterion such as one in a million. In Equation 3, *F(y)* represents the cumulative density function (CDF) of structural capacity and *h(y)* represents the probability density function (PDF) of the load. The former is sometimes called the fragility function and the later is sometimes called the hazard function.

To analyze the probability of breach of a dropped canister, *y* is typically in units of strain, *F* is typically a fragility function, which provides the conditional probability of breach given a strain; and *h* is the probability density function of the strain that would emerge from the drop. For seismic risk analysis, *h* represents the seismic motion input, *y* is in units of peak ground acceleration, and *F* is the seismic fragility. The seismic analysis of the YMP structures is documented separately in *Seismic Event Sequence Quantification and Categorization* (Ref. 2.4.4). Degradation of shielding owing to impact loads uses a strain to failure criterion within the simplified approach of Equation 4, described below. For analysis of the conditional probability of breach owing to fires, *y* is temperature, *F* is developed from fire data for non-combustible structures, and *h* is developed using probabilistic heat transfer calculations. Analysis for heating up casks, canisters, and waste packages associated with loss of building forced convection cooling was similarly accomplished, but Equation 4 was used.

If load and capacity are known, then Equations 2 and 3 provide a single valued result, which is the mean probability of failure. Each function in Figure 4.3-6 is characterized by a mean value, $\overline{L}$ and $\overline{R}$, and a measure of the uncertainty, generally the standard deviation, usually denoted by σ_L and σ_R for L and R, respectively. The spread of the functions may be expressed, alternatively, by the corresponding coefficient of variation (V) given by the ratio of standard deviation to mean, or $V_L = \sigma_L/\overline{L}$ and $V_R = \sigma_R/\overline{R}$ for load and resistance, respectively. The coefficient of variation may be thought of as a measure of dispersion expressed in terms of the number of means.

In the PCSA, the capacity curve for developing the fragility of casks and canisters against drops was constructed by a statistical fit to tensile elongation to failure tests (Ref. 2.2.36). The load curve may be constructed by varying drop height. A cumulative distribution function may be fit to a locus of points each of which is the product of drop height frequency and strain given drop height.

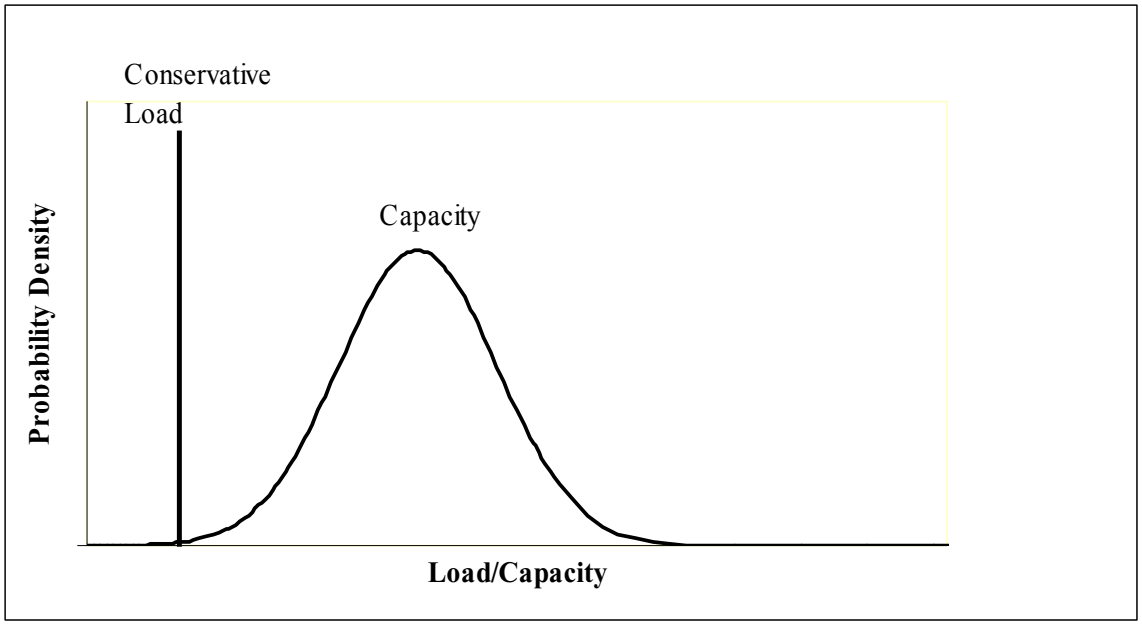
Impact Events Associated with Containment Breach

A simplification of Equation 3, consistent with *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73), and shown in Equation 4 is used in the PCSA. It is illustrated in Figure 4.3-7.

$$P_f = \int_0^h F(y)dy \qquad \text{(Eq. 4)}$$

In Equation 4, h is a single value conservative load.

The load is a single value estimated by performing a calculation for a condition more severe than the mean. For example, if the normal lift height of the bottom of a canister is 23 feet, a drop height of 32.5 feet is more severe and may be conservatively applied to all drop heights equal to or below this height. The conditional probability of breach is an increasing function of drop height. Strain resulting from drops is calculated by dynamic finite element analysis using Livermore Software–Dynamic Finite Element Program (LS-DYNA) for canisters and transportation cask drops (Ref. 2.2.36). Therefore, use of a higher than mean drop height for the load for all drop heights, results in a conservative estimate of breach probability. As an additional conservatism, a lower limit of breach probability of 1E-05 was placed on drops of casks, canisters, and waste packages. To perform the analyses, representative canisters and casks were selected from the variety of available designs in current use which were relatively thin walled on the sides and bottom. This added another conservative element.



Source: Original

Figure 4.3-7. Point Estimate Load Approximation Used in PCSA

The PCSA applies passive equipment failure analysis (PEFA) to a wide variety of event sequences including those associated with:

- Canister drops
- Canister collisions with other objects and structures
- Other objects dropped on canisters
- Transportation cask drops and subsequent slap-downs (analyzed without impact limiters)
- Conveyance derailments and collisions when carrying transportation casks and canisters (conveyances would be trucks, railcars, cask transfer trolleys (CTT), and site transporters)
- Other objects dropped on transportation casks
- Waste package drops
- Waste package collision with other waste packages
- Transport and emplacement vehicle (TEV) collisions with structures and another TEV when carrying a waste package

- Objects dropped on waste packages
- Objects dropped on TEV.

Many of these, such as collisions, derailments, and objects dropped onto casks/canisters, involve far lower energy loads than drop events. For impact loads that are far less energetic than drops, the drop probability is ratioed by impact energy to estimate the less energetic situation.

Shielding Degradation Events

Impact loads (such as drops) may not be severe enough to breach a transportation cask, but might lead to degradation of shielding such that onsite nearby personnel are exposed.

The shielding degradation analysis is based primarily on results of finite-element modeling (FEM) performed for, four generic transportation casks types for transportation accidents as reported in *Reexamination of Spent Fuel Shipment Risk Estimates.* NUREG/CR-6672 (Ref. 2.2.83). The results of the FEM analysis were used to estimate threshold drop heights and thermal conditions at which loss of shielding (LOS) may occur in repository event sequences. The four cask types include one steel monolith rail cask, one steel/depleted uranium truck cask, one steel/lead/steel (SLS) truck cask and one SLS rail cask. The study performed structural and thermal analyses for both failure of containment boundaries and loss of shielding for accident scenarios involving rail cask and truck cask impacting unyielding targets at various impact speeds from 30 mph to greater than 120 mph. Impact orientations included side, corner, and end. The study also correlated the damage to impacts on real targets, including soil and concrete.

Reexamination of Spent Fuel Shipment Risk Estimates. NUREG/CR-6672 (Ref. 2.2.83) addresses two modes of shielding degradation in accident scenarios: Deformations of lid and closure geometry that permit direct streaming of radiation; and/or reductions in cask wall thickness, or relocation of the depleted uranium or lead shielding. The shielding degradation due to lid/closure distortion can be accompanied by air-borne releases if the inner shell of the cask is also breached.

The structural analyses do not credit the energy absorption capability of impact limiters. Therefore, the results are deemed applicable to approximate the structural response of transportation and similar casks in drop scenarios for the WHF.

Principal insights reported in Ref. 2.2.83 are the following:

- Monolithic steel rail casks do not exhibit any shielding degradation, but there may be some radiation streaming through gaps in closures in any of the impact scenarios.
- Steel/depleted uranium/steel truck cask exhibited no shielding degradation, explained by modeling that included no gaps between forged depleted uranium segments so that no displacement of depleted uranium could occur.
- The SLS rail and truck casks exhibit shielding degradation due to lead slumping. Lead slump occurs mostly on end-on impact, with a lesser amount in corner orientation. For side-on orientation, there is no significant reduction in shielding.

Therefore, this analysis focuses on SLS casks to estimate the drop or collision conditions that could result in shielding degradation from lead slumping. Since it is not possible to predict at this time the fraction of casks to be delivered during the preclosure period that will be of the steel-lead-steel type, all transportation casks are analyzed as described below.

The *Shipping Container Response to Severe Highway and Railway Accident Conditions* NUREG/CR-4829 (Ref. 2.2.50) defines three levels of cask response, characterized by the maximum effective plastic strain within the inner shell of a transport cask. Of these, level S3 has strain levels between 2.0% and 30% which produces large distortions, seal leakage likely and lead slump likely. The minimum strain level associated with S3 was applied to the strain versus impact speed results from the FEM (Ref. 2.2.83) to establish a median threshold impact speed for the onset of shielding degradation. The threshold speeds are translated into equivalent drop heights, using calculated bottom corner drops for impact loads onto real concrete targets, not idealized rigid targets. Use of a conservative coefficient of variation coupled with the median, allowed a lognormal fragility curve as a function of drop height (or equivalently impact speed), to be developed. Each event sequence may be characterized by a conservative impact speed. For example, the maximum speed of onsite vehicles is 2.5 mph by design (with exception of 9 mph for the site prime mover) and a cask drop height of 15 feet is unlikely, by design, to be exceeded. Using Equation 4, the fragility curve was combined with the maximum or a conservative estimate of impact speed (or equivalent drop height).

Fire Events Associated with Possible Containment Breach

Fire initiated events are included in the PCSA, which probabilistically analyzes the full range of possible fires that can occur, as well as variations in the dynamics of the heat transfer and uncertainties in the failure temperature of the target. This analysis focuses on fires that might directly impact the integrity of cask, canister, and waste package containment. Equation 3 is used for this purpose. The fragility analysis includes the uncertainty in the temperature that containment will be breached, and the uncertainty in the thermal response of the canister to the fire. In calculating the thermal response of the canister, variations in the intensity and duration of the fire are considered along with conditions that control the rate of heat transfer to the container (e.g., convective heat transfer coefficients, view factors, emissivities, etc). In calculating the failure temperature of the canister, variations in the material properties of the canister are considered, along with, variations in the loads that lead to failure. The load or demand is associated with uncertainty in the fire severity.

Fire severity is characterized by the fire temperature and duration, since these factors control the amount of energy that the fire could transfer to a cask, canister, or waste package. (In this analysis, these are referred to as targets.) The duration of the fire is taken to be the amount of time a particular container is exposed to the fire, and not necessarily the amount of time a fire burns. Probability distributions of the fire temperature and fire duration are based on the unavailability of manual or automatic suppression, which leads to an assessment that significantly overstates the risk of fires.

4.3.2.2.1 Uncertainty in Fire Duration

An uncertainty distribution for the fire duration is developed by considering test data and analytical results reported in several different sources; some specific to the YMP facilities and some providing more generic information. In general, the fire durations are found to depend upon the amount, type, and configuration of the available combustible material.

Based on a review of the available information, it is determined that two separate uncertainty distributions would be needed: one for conditions without automatic suppression and one for conditions with automatic suppression. The derivation of these two distributions is discussed below.

Uncertainty in fire duration was developed from:

- Utilisation of Statistics to Assess Fire Risks in Buildings (Ref. 2.2.85)
- Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report. NUREG/CR-4680 (Ref. 2.2.63)
- Quantitative Data on the Fire Behavior of Combustible Material in Nuclear Power Plants: A Literature Review. NUREG/CR-4679 (Ref. 2.2.64).

The derivation of the distribution of fire duration is described in Attachment D, Sections D2.1.1.2 and D2.1.1.3.

The fire temperature used in this calculation is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. 2.2.78, p. 2-56). Fires within an YMP facility may involve both combustible solid and liquid materials. A probability distribution for the fire temperature was derived by combining fire severity information for compartment fires discussed in *SFPE Handbook of Fire Protection Engineering* (Ref. 2.2.78, Section 2, Chapter 2) with information about liquid hydrocarbon pool fires (Ref. 2.2.3 and Ref. 2.2.78, p. 2-56). The derivation of this distribution is described in Attachment D, Section D2.1.2. The fire temperature is normally distributed with a mean of 1,072°K (799°C) and a standard deviation of 172°K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C specified in 10 CFR 71.73 (Ref. 2.3.3).

Fire temperature and duration are negatively correlated. Intense fires with high fire temperatures tend to be short-lived because the high temperature results from very rapid burning of the combustible material. In determining the joint probability distribution of fire duration and temperature, a negative correlation coefficient of -0.5 was used (refer to Attachment D, Section D2.1.3).

The thermal response of the canister is calculated using simplified radiative, convective, and conductive heat transfer models, which have been calibrated to more precise models. The simplified models are found to accurately match predictions for heating of the canister in either a cask or waste package. The heat transfer models are simplified in order to allow a probabilistic analysis to be performed using Monte Carlo sampling. The models consider radiative and

convective heat transfer from the fire to the canister, cask, waste package, or shielded bell. This analysis conservatively models the fire completely engulfing the container.

When calculating the heat load on the target for a fully engulfing fire, radiation is the dominant mode of heat transfer between the fire and the target. The magnitude of the radiant heating of the container depends on the fire temperature, the emissivity of the container, the view factor between the fire and the container, also the duration of the fire.

The total radiant energy deposited in the container can be roughly estimated using Equation 5:

$$Q_{rad} \quad \varepsilon F_{cf} \sigma (T_{fire})^4 A t \qquad \text{(Eq. 5)}$$

Where:

Q_{rad} = incident radiant energy over the fire duration (J)

ε = emissivity of the container

F_{cf} = container-to-fire view factor

σ = Stefan-Boltzmann constant ($W/m^2 K^4$)

T_{fire} = equivalent blackbody fire temperature (K)

A = container surface area (m^2)

t = duration of the fire (s).

The following variables in this equation are treated as uncertain: fire temperature, view factor, and fire duration. In the case of a canister inside a waste package, cask, or shielded bell, a more complicated set of equations is used to simulate outer shell heat up and subsequent heat transfer to layers of containment or shielding and then to the canister itself. The model also includes heating of the canister by decay heat from the spent fuel or high-level radioactive waste.

To estimate the uncertainty associated with target fragility, two failure modes were considered:

1. *Creep-Induced Failure.* Creep is the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load. This mode of failure is possible for long duration fires.

2. *Limit Load Failure.* This failure mode occurs when the load exerted on a material exceeds its structural strength. As the temperature of the canister increases in temperature, its strength decreases. Failure is generally predicted at some fraction (usually around 70%) of the ultimate strength.

Failure is considered to occur when either of the failure thresholds is exceeded.

Equation 3, along with the heat transfer equations, are solved using Monte Carlo simulation (described in Section 4.3.6) with the above described fragility and target fire severity probability distributions, and distributions for the uncertain heat transfer factors. For each Monte Carlo trial, the calculated maximum canister temperature is compared to the sampled target failure temperature. If the maximum temperature of the target exceeds the sampled failure temperature, then target failure is counted. The failure probability in this method is equal to the fraction of the samples for which failure is calculated.

Uncertainty in the calculated canister failure probability is given by a calculated mean and standard deviation, where the mean is simply the number of failures divided by the total number of samples and the standard deviation is given by Equation 6 for the standard deviation of a binomial distribution:

$$\sigma \quad \sqrt{\frac{\frac{n_{fail}}{N}\left(\frac{N - n_{fail}}{N}\right)}{N}} \qquad \text{(Eq. 6)}$$

Where: n_{fail} is the number of trials in which failure occurs and N is the total number of Monte Carlo trials.

Fire Event Associated with Shielding Degradation

The thermal analyses in *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672 (Ref. 2.2.83) indicates that the probability of shielding degradation in a fire scenario should be based on the probability of having a fire that is equivalent to a 1,000°C engulfing fire that lasts for more than a half-hour. However, shielding degradation does not occur unless there is a coincident puncture or breach in the cask that allows a pathway for melted lead to flow out of its usual configuration. These threshold conditions apply to all cask types and would result in radiation streaming from the cask.

The transportation cask is present within the YMP facilities in only three areas: vestibules, preparation rooms, and unloading rooms. The fire ignition frequencies of these areas are summed up in Section 6.5 and Attachment F, Table F5.2-1. Furthermore, the method described above for obtaining the probability distribution of fire severity from input distributions of fire temperature and fire duration, resulted in an estimate of the conditional probability of the threshold fire given a fire ignition. This is a conservative calculation because it did not include the conditional probability that a puncture or failure through the wall to the lead shielding must also occur for shielding degradation.

Other Thermal Events Associated with Possible Breach

The PCSA focuses on the potential of cask, canister, and waste package breach associated with fires. As described above, the fires of most interest were those that surround the target containment. However, heatup associated with loss of building cooling was also considered.

The analysis of loss of building cooling on containment integrity takes a similar, conservative, analytical approach. A bounding set of conditions and configurations are postulated, and then

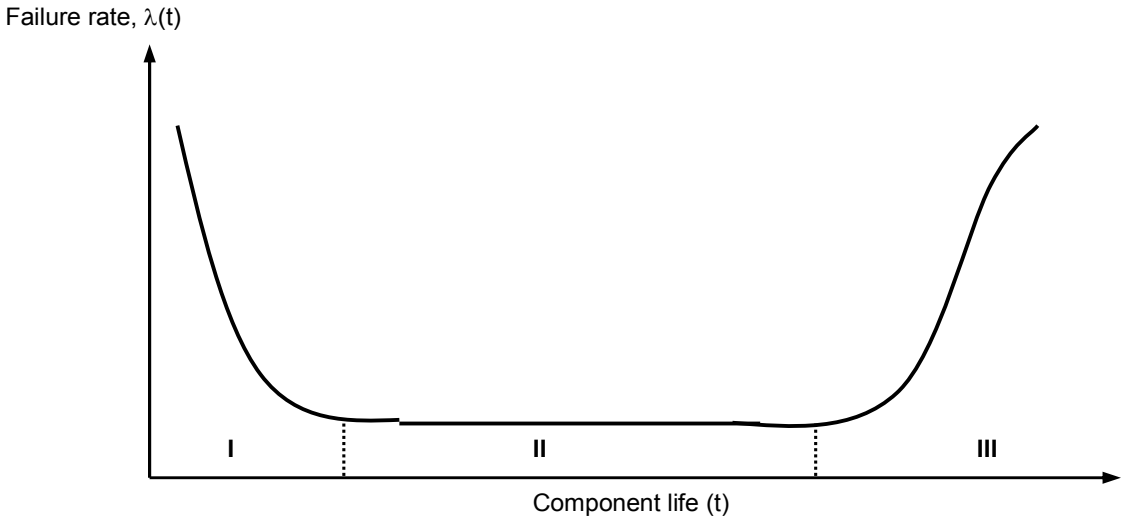
using the ANSYS code (Ref. 2.2.13), the maximum steady state temperature is compared to the temperature at which the component would be expected to fail. In no case is a containment barrier found to be near its failure threshold from loss of building cooling.

4.3.3 Utilization of Industry-Wide Reliability Data

4.3.3.1 Use of Population Variability Data

The quantification of event sequence probabilities via event tree and fault tree modeling requires information on the reliability of active equipment and components, as usually represented in fault tree basic events. The PCSA attempts to anticipate event sequences before they happen, which means that associated equipment reliabilities are uncertain.

As presented in *Fault Tree Handbook* (Ref. 2.2.87, Figure X-8, p. X-23), the typical model of failure probability for a component is depicted as a "bathtub curve" illustrated in Figure 4.3-8. The curve is divided into three distinct phases. Phase I represents the component failure probability during the "burn-in" period. Phase II corresponds to the "constant failure rate function" where the exponential distribution can be applied to calculate the probability of failure within a specified "mission time." Toward the end of the component life or the wear-out period, which is represented by Phase III of the curve; the probability of failure increases.



Source: *Fault Tree Handbook* (Ref. 2.2.87, Figure X-8, p. X-23)

Figure 4.3-8. Component Failure Rate "Bathtub Curve" Model

As is usually done in PRA, the PCSA uses Phase II because Phase I failures are identified by burn-in testing of equipment before repository operations occur and Phase III failures are eliminated by preventive maintenance which includes manufacturer recommended replacement intervals. In Phase II, the component time-to-failure probability can be represented with the exponential distribution. The probability of failure of a given component (or system) depends on the value of the constant failure rate, λ, and the mission time, t_m, as follows in Equation 7:

$$P_F(\lambda,t_m) = 1 - \exp(-\lambda t_m) \quad \text{(Eq. 7)}$$

When the product λt_m is small (<0.1), the failure probability may be calculated by the following Equation 8 approximation, which introduces less than a 10% error:

$$P_F(\lambda,t_m) \cong \lambda t_m \quad \text{(Eq. 8)}$$

The PCSA also uses the concept of unavailability to estimate basic event probabilities. This applies to standby equipment such as the emergency diesel generators and fire suppression. In accordance with reliability theory, after each test the component or system is considered "good as new" with a "resetting" of the time-to-failure "clock" for the exponential failure model. The unavailability factor is evaluated as the probability of failure during the time between tests, τ. The average unavailability factor, or failure on demand of the standby unit, q_d, is calculated as shown in Equation 9:

$$q_d(\lambda,\tau) = \tfrac{1}{2}(\lambda\tau) \quad \text{(Eq. 9)}$$

In this model, the component failure rate is constant between tests, the test does not require any time, and the test neither introduces another failure mode nor changes the failure rate of the component.

Failure on demand is also needed for equipment, such as cranes, that is challenged in discrete steps. This model is not based on time in service; it is based on the number of times the component or system is called upon to perform its safety function.

Information about hardware failure is characterized as one of the following:

1. Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (e.g., operational experience).

2. Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (e.g., test data).

3. Historical performance of successes and failures of a similar piece of equipment or similar category of equipment under conditions that may or may not be those under analysis (e.g., another program's test data or data from handbooks or compilations).

4. General engineering or scientific knowledge about the design, manufacture, and operation of the equipment or an expert's experience with the equipment.

The YMP repository has not yet operated, and test information on prospective equipment has not yet been developed. The equipment and SSCs designed and purchased for the Yucca Mountain repository will be of the population of equipment and SSCs represented in U.S. industry-wide reliability information sources (Assumption 3.2.1). Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population. Attachment C contains the list of industry-wide reliability information sources used in the PCSA.

The lack of actual operating experience, the use of industry-wide data, and the consideration of uncertainties (Ref. 2.2.73) suggested that a Bayesian approach was appropriate for the PCSA. A

Bayesian approach and the use of judgment in expressing the state-of-knowledge of basic event unreliability is a well-recognized and accepted practice (Ref. 2.2.58, Ref. 2.2.10, and Ref. 2.2.66). Furthermore, to paraphrase *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73), reliability estimates for high reliability SSC may include the use of engineering judgment, supported by sufficient technical basis; and empirical reliability analyses of a SSC, could include values based on industry experience and judgment (Ref. 2.2.73).

Let λ_j be one failure rate of a set of possible failure rates of a component and E be a new body of evidence. Knowledge of the probability of λ_j given E, is represented by $P(\lambda_j/E)$. For a failure rate, frequency, or probability of active equipment, Bayes' theorem is stated as follows in Equation 10:

$$P(\lambda_j / E) \quad \frac{P(\lambda_j)L(E / \lambda_j)}{\sum_j P(\lambda_j)P(E / \lambda_j)} \qquad \text{(Eq. 10)}$$

In summary, this states that the knowledge of the "updated" probability of λ_j, given the new information E, equals the "prior" probability of λ_j, before any new information, times the likelihood function, $L(E/\lambda_j)$. The likelihood function is a probability that the new information really could be observed, given the failure rate λ_j. The numerator in Equation 10 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of λ_j equals unity. If there is actual operational experience available, then the steps in an application of Bayes' theorem would be as follows: 1) estimate the prior probability using one or more of the four reliability data types; 2) obtain new information in the form of tests or experiments; 3) characterize the test information in the form of a likelihood function; and 4) perform the calculation in accordance with Equation 10 to infer the updated probability.

The PCSA used industry-wide reliability data to develop Bayesian prior distributions for each active equipment/component failure mode in the fault trees. Updates per Equation 10 will await actual test and operations. The following summarizes the methods used to develop the Bayesian prior distributions.

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution, g, representing the source-to-source variability, also called population variability, of the component reliability (Ref. 2.2.10, Section 8.1). In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. The population-variability distributions developed in this analysis attempt to encompass the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the PCSA. As indicated in *Bayesian Parameter Estimation in Probabilistic Risk Assessment* (Ref. 2.2.79, Section 5.1.2), this method is a pragmatic

approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

Applying the parametric empirical Bayes method requires first, to categorize the reliability data sources into two types: those that provide information on exposure data, (i.e., the number of failures that were recorded over an exposure time (in case of a failure rate)), or over a number of demands (in case of a failure probability), and those that do not provide such information. In the latter case, reliability estimates for a failure rate or failure probability are provided in the form of a mean or a median value, along with an uncertainty estimate, typically an error factor.

For each data source, the reliability information about a component's failure rate of failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. 2.2.79, Section 4.2). When no exposure data is available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution (Ref. 2.2.79, Section 4.4) and (Ref. 2.2.56, pp. 312, 314, and 315).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. 2.2.10, Section 8.2.1), which have the advantage of resulting in relatively simpler calculations. This technique, however, is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of *The Combined Use of Data and Expert Estimates in Population Variability Analysis* (Ref. 2.2.56, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the population-variability distribution in its lognormal form is noted $g(x,\nu,\tau)$, where x is the reliability parameter for the component (failure rate or failure probability), and ν and τ, the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided in the latter case that any tail truncation above $x = 1$ has a negligible effect (Ref. 2.2.79, p. 99). The validity of this can by confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1 of Attachment C, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98 percent of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

To determine v and τ, it is first necessary to express the likelihood for each data source as a function of v and τ only, (i.e., unconditionally on x). This is done by integrating, over all possible values of x, the likelihood function evaluated at x, weighted by the probability of observing x, given ν and τ. For example, if the data source i indicates that r failures of a component occurred out of n demands, the associated likelihood function $L_i(v,\tau)$, unconditional on the failure probability x, is as follows in Equation 11:

$$L_i(v,\tau) \quad \int_0^1 Binom(x,r,n) \times g(x,v,\tau) dx \qquad \text{(Eq. 11)}$$

Where: $Binom(x,r,n)$ represents the binomial distribution evaluated for r failures out of n demands, given a failure probability equal to x, and $g(x,v,\tau)$ is defined as previously indicated. This equation is similar to that shown in *Bayesian Parameter Estimation in Probabilistic Risk Assessment* (Ref. 2.2.79, Equation 37). If the component reliability is expressed in terms of a failure rate and the data source provides exposure data, the binomial distribution in Equation 11 would be replaced by a Poisson distribution. If the data source provided expert opinion only (no exposure data), the binomial distribution in Equation 11 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine ν and τ (Ref. 2.2.79, p. 101). The maximum likelihood estimators for v and τ are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each data source (Ref. 2.2.56, Equation 4). To find the maximum likelihood estimators for ν and τ, it is equivalent and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of v and τ completely determines the population-variability distribution g for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution g, which are calculated using the formulas given in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.10, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to $\exp(\nu + \tau^2/2)$ and the error factor is equal to $\exp(1.645 \times \tau)$. A discussion of the adequacy of the empirical Bayes method for the YMP analysis is found in Attachment C.

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, *External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom* (Ref. 2.2.52, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between 2×10^{-8}/hr (5th percentile) and 6×10^{-5}/hr (95th percentile). Using the definition of the error factor given in *Handbook of Parameter Estimation for Probabilistic Risk Assessment. NUREG/CR-6823* (Ref. 2.2.10, Section A.7.3), this corresponds to an error factor of $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}}$ 55. Therefore, in the PCSA, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a

value greater than 55, are too diffuse to adequately represent the population-variability distribution of a component. In such instances (i.e., the two cases in the entire PCSA database when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution, and therefore is unaffected by the value taken by the error factor. Based on *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.10, Section A.7.3), the median is calculated as $\exp(\nu)$, where ν is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the PCSA is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.10, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution, and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using the data source that yields the most diffuse likelihood using one of the two methods described in the next paragraph.

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean, and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data, i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities, the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffrey's non-informative prior distribution as indicated in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.10, Section 6.2.2.5.2). This non-informative prior conveys little prior belief or information, thus allowing the data to speak for itself.

4.3.3.2 Dependent Events

Dependent events have long been recognized as a concern for those responsible for the safe design and operation of high-consequence facilities because these events tend to increase the probability of failure of multiple systems and components. Two failure events, A and B, are dependent upon when the probability of their coincidental occurrence is higher than expected if A and B were each an independent event. Dependent events occur from four dependence mechanisms: functional, spatial, environmental, and human:

1. **Functional dependence** is present when one component or system relies on another to supply vital functions. An example of a functional dependence in this analysis is electric power supply to HVAC. Functional dependence is explicitly modeled in the event tree and fault tree logic.

2. **Environmental dependence** is in play when system functionality relies on maintaining an environment within designed or qualified limits. Here, an example is material property change as a result of temperature change. Environmental effects are modeled in the system reliability analyses as modifications (e.g., multiplying factors) to system- and component-failure probabilities and are also included in the passive equipment failure analyses. External events such as earthquakes, lightning strikes, and high winds that can degrade multiple SSCs are modeled explicitly as initiating events and are discussed in other documents (Ref. 2.2.29) and (Ref. 2.4.4).

3. **Spatial dependence** is at work when one SSC fails by virtue of close proximity to another. For example, during an earthquake one SSC may impact another because of close proximity. Another example is inadvertent fire suppression actuation which wets SSCs below it. Spatial dependences are identified by explicitly looking for them in the facility layout drawings. Inadvertent fire suppression is modeled explicitly in the event trees and fault trees.

4. **Human dependence** is present when a structure, system, component, or function fails because humans intervene inappropriately or failed to intervene. In the YMP, most human errors are associated with initiating events (inadvertent actuation) or are pre-initiator failures (failure to restore after maintenance). The PCSA includes an extensive human reliability analysis (HRA) which is described later in this section, in Section 6.4 and in Attachment E. The results of the HRA are integrated into the event tree and fault tree models for a complete characterization of event sequence frequency.

4.3.3.3 Common-Cause Failures

Common-cause failures (CCFs) can result from any of the dependence mechanisms described above. The term common-cause failure is widely employed to describe events in which the same cause degrades the function of two or more SSCs that are relied upon for redundant operations, either at the same time or within a short time relative to the overall component mission time. Because of their significance to overall SSC reliability when redundancy is employed, CCFs are a special class of dependent failures that are addressed in the PCSA.

Because CCFs are relatively uncommon, it is difficult to develop a statistically significant sample from monitoring only one system or facility, or even several systems. The development of CCF techniques and data, therefore, rely on a national data collection effort that monitors a large number of nuclear power systems. Typically, the fraction of component failures associated with common causes leading to multiple failures ranges between 1% and 10% (Ref. 2.2.51, Ref. 2.2.61, and Ref. 2.2.57). This fraction depends on the component; level of redundancy (e.g., two, three, or four); duty cycle; operating and environmental conditions; maintenance interventions; and testing protocol, among others. For example, equipment that is operated in cold standby mode (i.e., called to operate occasionally on demand) with a large amount of preventive maintenance intervention tends to have a higher fraction of CCFs than systems that continuously run.

It is not practical to explicitly identify all CCFs in a fault tree or event tree. Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: 1) the Beta Factor method (Ref. 2.2.51) the Multiple Greek Letter method (Ref. 2.2.60), which is an extension of the Beta Factor method, and 3) the Alpha Factor method (Ref. 2.2.61). These methods do not require an explicit knowledge of the dependence failure mode.

The PCSA uses the Alpha Factor method (Ref. 2.2.61) which is summarized below. After identifying potential CCF events from the fault trees, appropriate alpha factors are identified according to the procedure described in *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis,* NUREG/CR-5801 (Ref. 2.2.59). The general equations for estimating the probability of a CCF event in which k of m components fail are as follows in Equation 12, Equation 13, and Equation 14:

$$Q(k,m) \quad \frac{k}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad \text{For staggered test} \qquad \text{(Eq. 12)}$$

$$Q(k,m) \quad \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad \text{For non-staggered test} \qquad \text{(Eq. 13)}$$

where α_k denotes the alpha factor for size k, Q_t denotes the total failure probability, and:

$$\alpha_t \quad \sum_{k\ 1}^{m} k\alpha_k \qquad \text{(Eq. 14)}$$

Generic alpha factors used in the PCSA are taken from *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis.* NUREG/CR-5801 (Ref. 2.2.59). The process of applying these alpha factors is explained further in Attachment C, Section C3.

4.3.4 Human Reliability Analysis

Human interactions that are typically associated with the operation, test, calibration, or maintenance of an SSC (e.g., drops from a crane when using slings) are implicit in the empirical

data. If this is the case, empirical data may be used, provided human errors that cause the SSC failures are explicitly enumerated and determined to be applicable to YMP operations. When this was the case in the PCSA, the appropriate method of Section 4.3.3.1 was applied. Otherwise, an HRA was performed, the methodology of which is summarized in this section. The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.7) and incorporates the guidance in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. 2.2.72). It emphasizes a comprehensive qualitative analysis and uses applicable quantitative models.

The HRA task identifies, models, and quantifies HFEs postulated for YMP operations to assess the impact of human actions on event sequences modeled in the PCSA. YMP operations differ from those of traditional nuclear power plants, and the HRA reflects these differences. Appendix E.IV of Attachment E includes further discussion of these differences and how they influence the choice of methodology.

The overall steps to the PCSA HRA are identification of HFEs, preliminary analysis (screening), and detailed analysis. The HRA task ensures that the HFEs identified by the other tasks (e.g., HAZOP evaluation, MLD development): (1) are created on a basis that is consistent with the HRA techniques used, (2) are appropriately reincorporated into the PCSA (modeled HFEs derived from the previously mentioned PCSA methods), and (3) provide appropriate human error probabilities (HEPs) for all modeled HFEs. The HRA work scope largely depends on boundary conditions defined for it.

4.3.4.1.1 HRA Boundary Conditions

Unless specifically stated otherwise, the following general conditions and limitations are applied throughout the HRA task. The first two conditions always apply. The remaining conditions apply unless the HRA analyst determines that they are inappropriate. This judgment is made for each individual action considered:

1. Only HFEs made in the performance of assigned tasks are considered. Malevolent behaviors (e.g., deliberate acts of sabotage) are not considered in this task.

2. All personnel act in a manner they believe to be in the best interests of operations and safety. Any intentional deviation from standard operating procedures is made because employees believe their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.

3. Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include SNF handling at reactor sites having independent spent fuel storage and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the GROA facilities, once they are built and operating (including

crew structures, training, and interactions), are adequately represented by these currently operating facilities.

4. The YMP is initially operating under normal conditions and is designed to the highest quality human factor specifications. The level of operator stress is optimal unless the analyst determines that the human action in question cannot be accommodated in such a manner as to achieve optimal stress.

5. In performing the operations, the operator does not need to wear protective clothing unless it is an operation similar to those performed in other comparable facilities where protective clothing is required.

6. The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are to be experienced and have functioned in their present positions for a sufficient amount of time to be proficient.

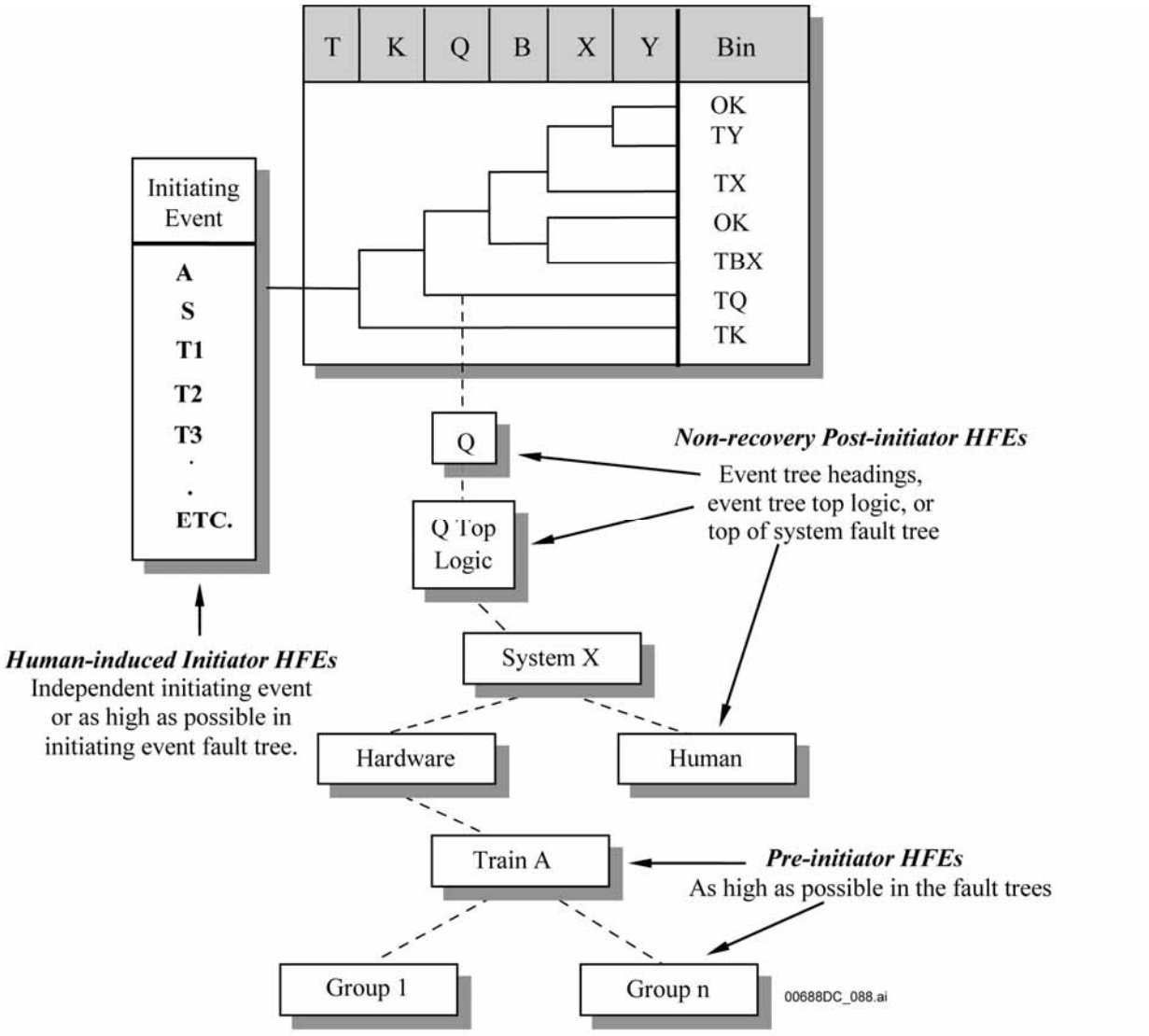
7. The environment inside each YMP facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination, and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made regarding optimal weather conditions.

8. While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill-of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

4.3.4.2 HRA Methodology

The HRA consists of several steps that follow the intent of ASME RA-S-2002, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.7) and the process guidance provided in *Technical Basis and Implementation Guidelines for Technique for Human Event Analysis (ATHEANA)* NUREG-1624 (Ref. 2.2.70). The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt material that is based on nuclear power plants to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. 2.2.70). Section 10.3 of *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. 2.2.70), provides an overview of the method for incorporating HFEs into a PRA. Figure 4.3-9 illustrates this integration method.



NOTE: HFE = human failure event.

Source: Original

Figure 4.3-9. Incorporation of Human Reliability Analysis within the PCSA

Step 1: Define the Scope of the Analysis—The objective of the YMP HRA is to provide a comprehensive qualitative assessment of the HFEs that can contribute to the facility's event sequences resulting in radiological release, criticality, or direct exposure. Any aspects of the work that provide a basis for bounding the analysis are identified in this step. In the case of the YMP, the scope is bounded by the design state of the facilities and equipment.

Step 2: Describe Base Case Scenarios—In this step, the base case scenarios are defined and characterized for the operations being evaluated. In general, there is one base case scenario for each operation included in the model. The base case scenario represents the most realistic description of expected facility, equipment, and operator behavior for the selected operation.

Step 3: Identify and Define HFEs of Concern—Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then becomes the error-forcing context (EFC) for a specific HFE. As defined by ATHEANA (Ref. 2.2.70), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses. The analyses performed in later steps (e.g., Steps 6 and 7) may identify the need to define additional HFEs or unsafe actions.

Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis—The preliminary analysis is a type of screening analysis used to identify HFEs of concern. This type of analysis is commonly performed in HRA to conserve resources for those HFEs that are involved in the important event sequences. The preliminary quantification process consists of the following subtasks:

1. Identification of the initial scenario context.
2. Identification of the key or driving factors of the scenario context.
3. Generalization of the context by matching it with generic, contextually anchored rankings or ratings.
4. Discussion and justification of the judgments made in subtask 3.
5. Refinement of HFEs, associated contexts, and assigned HEPs.
6. Determination of final preliminary HEP for HFE and associated context.

Once preliminary values have been assigned, the model is run, and HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, that sequence is Category 1 or Category 2 according to the performance objectives in 10 CFR Part 63.111 (Ref. 2.3.2)).

Step 5: Identify Potential Vulnerabilities—This information collection step defines the context for Step 6 in which scenarios that deviate from the base case are identified. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in the HFEs and/or unsafe actions identified in Step 4. The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). The HRA analysts rely on experience in other similar operations.

Step 6: Search for HFE Scenarios—In this step, the analyst must identify deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These deviations are referred to as HFE scenarios. The method for identifying HFE scenarios in the YMP HRA is stated in Step 3. This process continues throughout the event sequence development and quantification. The result is a description of HFE scenarios, including system and equipment conditions, along with any resident or triggered human factor concerns (e.g., PSFs). These combinations of conditions and human factor concerns then become the EFC for a specific HFE.

Step 7: Quantify Probabilities of HFEs—Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with 10 CFR 63.111 performance objectives (Ref. 2.3.2) after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CRF 63.111 performance objectives (Ref. 2.3.2). The activities of a detailed HRA are as follows:

- Qualitative analysis (e.g., identification of PSFs, definitions of important characteristics of the given unsafe action, assessment of dependencies)
- Selection of a quantification model
- Quantification using the selected model
- Verification that HFE probabilities are appropriately updated in the PCSA.

The four quantification approaches that are in the PCSA, either alone or in combination, follow:

1. Cognitive Reliability and Error Analysis Method (CREAM) (Ref. 2.2.54)
2. Human Error Assessment and Reduction Technique (HEART)/Nuclear Action Reliability Assessment (NARA) (Ref. 2.2.88)/(Ref. 2.2.41).
3. Technique for Human Error Rate Prediction (THERP) (with some modifications) (Ref. 2.2.84).

When an applicable failure mode cannot be reasonably found in one of the above methods, then the following HRA method is used:

4. ATHEANA expert elicitation approach (Ref. 2.2.70).

The selection of a specific quantification method for the failure probability of an unsafe action(s) is based upon the characteristics of the HFE quantified. Appendix E.IV of Attachment E provides a discussion of why these specific methods were selected for quantification, as well as a discussion of why some methods, deemed appropriate for HRA of nuclear power plants, are not suitable for application in the PCSA. It also gives some background about when a given method is applicable based on the focus and characteristics of the method.

Step 8: Incorporate HFEs into PCSA—After HFEs are identified, defined, and quantified, they must be reincorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. 2.2.70) provides an overview of the state-of-the-art method for performing this step in PRAs. The term reincorporated is used because some HFEs are identified within the fault tree and event tree analysis. All event sequences that contain multiple HFEs are examined for possible dependencies. Figure 4.3-9 shows how the different types of HFEs discussed previously are incorporated into the model based on their temporal phase, which determines where in the model each type of HFE is placed. More detailed discussion of how this is done is provided in Attachment E.

Step 9: Evaluation of HRA/PCSA Results and Iteration with Design—This last step in the HRA is performed after the entire PCSA is quantified. HFEs that ultimately prove to be important to categorization of event sequences are identified. Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is not in compliance with the performance objectives of 10 CFR 63.111 (Ref. 2.3.2) because the probability of a given HFE dominates the probability of that event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or completely eliminate the HFE. An example of such iteration includes the interlocks that ensure that cask lids are securely grappled. The interlocks might have a bypass feature when a yoke is attached to a grapple. An operator might fail to void the bypass when attempting to grapple a heavy load. The design changed such that the bypass would automatically be voided (by an electromechanical interlock) as soon as a yoke is attached to a grapple.

4.3.4.3 Classification of HFEs

HFEs are classified to support the HRA preliminary analysis, selection of HRA quantification methods, and detailed quantification. A combination of four classification schemes is used in the YMP HRA. The first three schemes are familiar standards in HRA. The fourth scheme has its basis in behavioral science and has been used in some second-generation HRA methods. The four classification schemes are as follows:

1. The three temporal phases used in PRA modeling:

    A. Pre-initiator.
    B. Human-induced initiator.
    C. Post-initiator.

2. Error modes:

    A. Errors of omission (EOOs).
    B. Errors of commission (EOCs).

3. Human failure types:

    A. Slips/lapses.
    B. Mistakes.

4. Informational processing failures:

    A. Monitoring and detection.
    B. Situation awareness.
    C. Response planning.
    D. Response implementation.

These classification schemes are used in concert with each other. They are not mutually exclusive. The first three schemes have been standard PRA practice; additional information on these three schemes can be found in Section E5.1 of Attachment E. The fourth scheme is summarized below.

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is used for the YMP HRA is based on the discussion in Chapter 4 of *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. 2.2.70) and consists of the following elements:

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.

- Situation awareness—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents the operator's understanding of the present situation and their expectations for future conditions and consequences.

- Response planning—This term is defined as the process by which operators decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.

- Response implementation—This term is defined as the activities involved with physically carrying out the actions identified in response planning.

When there are short time frames for response and the possibility of severely challenging operating conditions (e.g., environmental conditions) exists, then failures in all information processing stages must be considered. Also, slips/lapses and mistakes are considered for each information processing stage. Response implementation failures are expected to dominate the pre-initiator failures that are modeled. Post-initiator failures and failures that initiate event sequences can occur for all information processing stages, although detection failures are likely to be important only for events requiring response in very short time frames.

4.3.5 Fire Analysis

Fire event sequence analysis consists of four parts:

1. Development of fire ignition frequencies for each location in the facility or operations area. These are all called fire initiating event frequencies.

2. Development of the fire severity in terms of both temperature and durations. This was discussed in Section 4.3.2.

3. Development of the conditional probability of fire damaging a cask, canister, or waste package target. This was also discussed in Section 4.3.2.

4. Development of and quantification of fire event sequence diagrams and event trees. Development of the ESDs and event trees was discussed in *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37). Quantification of fire event trees is conducted exactly like quantification of any other event tree and is described in Sections 4.3, Section 4.3.1, and Section 4.3.7.

This section summarizes the method for the fire initiating event analysis performed as a part of the PCSA. The analysis was performed as part of an integrated analysis of internal fires in the surface and subsurface facilities. The full fire analysis and detail on the methods and data are documented in Attachment F to this volume. The fire analysis is subject to the boundary conditions described in the following section.

4.3.5.1 Boundary Conditions

The general boundary conditions used during the fire analysis are compatible with those described in Section 4.3.10. The principal boundary conditions for the fire analysis are listed below:

- Plant Operational State. Initial state of the facility is normal with each system operating within its limiting condition of operation limits.

- Number of Fire Events to Occur. The facility is analyzed to respond to one fire event at a given time. Additional fire events as a result of independent causes or of re-ignition once a fire is extinguished are bounded by the one fire event.

- Ignition Source Counting. Ignition sources are counted in accordance with applicable counting guidance contained in *Detailed Methodology*. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. 2.2.49).

- Fire Cable and Circuit Failure Analysis. Unlike nuclear power plants, which depend on the continued operation of equipment to prevent fuel damage, the YMP facilities cease operating on loss of power or control. Therefore, fire damage in rooms that do not contain waste cannot result in an increased level of radiological exposure. See Section 6.0 for a more detailed explanation involving treatment of loss of electrical power.

- HVAC Fire Analysis. HVAC is not relied upon to mitigate potential releases associated with fire event sequences in recognition that a large amount of fire generated, non-radiological particulates could render the HVAC filters ineffective.

- No Other Simultaneous Initiating Events. The facility is analyzed to respond to one initiating event at a given time. Additional initiating events as a result of independent causes are bounded by the one initiating event.

- Data Collection Scope. The fire ignition data collection and analysis are performed for locations relevant to waste handling in the facilities.

- Component Failure Modes. The failure mode of a SSC affected by a fire is the most severe with respect to consequences. For example, the failure mode for a canister could be the overpressurization of a reduced strength canister.

- Component Failure Probability. Fires large enough to fail waste containment components will be large enough to fail all active components in the same room. Active components fail in a de-energized state for such fires.

4.3.5.2 Analysis Method

Nuclear power plant fire risk assessment techniques have limited applicability to facilities such as the WHF or other facilities in the GROA. The general methodological basis of the PCSA fire analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76). Chemical agent disposal facilities are similar to those in the GROA in that these facilities are handling and disposal facilities for highly hazardous materials. This is a "data based" approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the YMP waste handling facilities. To the extent applicable to a non-reactor facility, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,* NUREG/CR-6850: Volumes 1 and 2 (Ref. 2.2.48 and Ref. 2.2.49) are also considered in the development of this analysis method. The method complies with the applicable requirements of *Fire PRA Methodology* (Ref. 2.2.4)) that are relevant to a non-reactor facility. The steps in the analysis are summarized below and described in detail in Attachment F, Section F4.

A. Identification of initiating events. Current techniques in fire risk assessment for nuclear power plants focus on fire that can damage electrical and control circuits or impact other equipment that can compromise process and safety systems. This type of approach is not generally applicable to YMP because loss of electric power is a safe state except for the need for HVAC after a release of radionuclides. In general, when systems are affected by fire, they cease to function. While at a nuclear power plant this is of concern, as described in Section 6.0 for YMP waste handling facilities, this means that fuel handling stops and initiating events capable of producing elevated levels of radioactivity are essentially unrealizable. The fire analysis, therefore, focused on the potential for a fire to directly affect the waste containers and cause a breach that would result in a release, rather than analyzing fires that would remove power from fuel handling systems. After a release of radionuclides, the HVAC

system, with its HEPA filtration, aids in the abatement radioactivity that is released from buildings. However, the occurrence of fires tends to significantly reduce the effectiveness of HEPA filtration and the fire event sequence analysis, therefore, does not rely on this system. Consideration is given both to fires that start in rooms containing waste and fires that start in other rooms and propagate to where the waste is located. The four steps of this process are as follows:

1. Identify fire-rated barriers and designate fire zones. The facility is broken into fire zones based on the location of fire-rated barriers. The rating of the barriers is not significant to the methodology, so barriers of all ratings are considered. In order for a fire zone to exist, the penetrations, doorways, and ducts must also be limited to the perimeter of the zone. Note that a floor is always considered to be a fire barrier as long as it is solid. Zones are identified by a number, determined by the analyst, and will consist of one or more rooms.

2. Identify the rooms where waste can be present. Each room where waste can be present, even if only for a brief time, is listed. The first set of fire initiating events to be considered in the PCSA is fires that affect each of these rooms, but do not affect other rooms that could contain waste.

3. Define local initiating events. Fire ignition occurrences are identified for each room within a fire zone. The total occurrences of a fire within a room containing a waste form is composed of the occurrences of ignitions in that room plus the occurrences of ignitions in surrounding rooms, within the fire zone, which propagate across room boundaries to the room containing the waste form. The locations of fire initiating events were identified in the MLD (Ref. 2.2.37).

4. Define large fire initiating events. Traditional fire risk studies for nuclear power plants have tended to ignore large fires, arguing that the fire barriers in place will prevent such occurrences. However, actual observed historical data shows that large fires in buildings occur. Large fires are defined for this study as those that spread to encompass the entire building. This is recognized in the latest fire risk guidance from the NRC and Electric Power Research Institute (EPRI) (Ref. 2.2.49, Section 11.5.4 and Ref. 2.2.48) in which potential large fire initiating events are identified. The general approach is as follows:

    a) In the YMP facilities waste containers, except during the short time they are being lifted by a canister transfer machine (CTM), are on the ground floor. Continuing with the focus on rooms that contain waste forms, large fires may be divided two ways. One is associated with fires that start on the ground floor and spread to the entire building and the other is a fire that starts anywhere else in the building.

    b) As a practical analysis technique, any fire that spreads out of a fire area is considered a large fire.

B. Quantification of fire ignition frequency. The quantification of initiating event frequency involves three steps. First, the overall frequency of fire ignition for the facility is determined, then that frequency is allocated to the individual room in the facility based on the number and types of ignition sources in the rooms. Types of ignition sources are characterized in general terms such as mechanical, electrical, combustible liquid. Finally, propagation probabilities are applied to determine the overall frequency that a fire reaches the area of the waste. Quantification uses data from the following sources for equipment ignition frequencies and conditional probabilities of propagation:

1. Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. 2.2.85).

2. *Detailed Methodology*. Volume 2 of EPRI/NRC-RES *Fire PRA Methodology for Nuclear Power Facilities*. EPRI TR-1011989 and NUREG/CR-6850 (Ref. 2.2.49).

3. *Summary & Overview.* Volume 1 of EPRI/NRC-RES *Fire PRA Methodology for Nuclear Power Facilities,* EPRI-1011989, and NUREG/CR-6850 (Ref. 2.2.48).

4. *Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Facilities:* 1988–1997. Unallocated Annual Averages and Narratives (Ref. 2.2.1).

5. *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction:* 1980 – 1998 (Ref. 2.2.2).

6. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76).

C. Determine initiating event frequency. The definition of each initiating event includes the implicit condition that the fire actually threatens a target that contains radioactive material. Therefore, for each initiating event, the initiating event frequency considers two aspects: the fraction of time there is a waste container in the room, and the probability of a fire propagates to that waste container. The probability of the presence of a target waste form is the fraction of time that the waste form(s) is in the area affected by the fire; (e.g., for a room fire, it is the fraction of time a waste form is in the room). There are two types of propagation that are considered: propagation within a room and propagation between rooms.

1. Fire propagation within rooms. The question is whether the fire, which can ignite wherever there is an ignition source in the room, reaches the area within the room in which the waste is located. Equation 15 obtains:

$$f_{ier\text{-}i} = P_{wri} [f_i (FR_a + (FR_n \times (P_{pc} + P_{rc})) + (FR_f \times P_{rc}))] \quad \text{(Eq. 15)}$$

Where:

$f_{ier\text{-}i}$ = frequency of fire affecting waste form, i-th room

P_{wri} = probability that a waste form is in the i-th room

f_i = frequency of ignition, i-th room

FR_a = fraction of ignition sources at the waste form

FR_n = fraction of ignition sources near the waste form

P_{pc} = conditional probability for fire confined to part of room of origin

FR_f = fraction of ignition sources far from the waste form

P_{rc} = conditional probability for fire confined to room of origin.

The values for P_{wri}, P_{pc}, and P_{rc} in the previous equation were developed from the analysis performed by National Fire Protection Association (NFPA) (Ref. 2.2.2). The frequency f_i is the sum of frequencies of ignition of all ignition sources in the room. The fraction of ignition sources at, near, and far from the waste form was developed from equipment layout drawings such as:

a) *Wet Handling Facility ITS Train "A" Electrical Room Equipment Layout* (Ref. 2.2.39).

b) *Wet Handling Facility General Arrangement Ground Floor Plan* (Ref. 2.2.27).

2. Fire propagation to large fire. The probability of a large fire (defined for this study as one that propagates beyond the fire area of origin) is developed from Equation 16:

$$f_{ief\text{-}fj\text{-}ri} = f_i \times P_{fc} \qquad \text{(Eq. 16)}$$

Where:

$f_{ief\text{-}fj\text{-}ri}$ = frequency of fire in zone j starting in room i

f_i = frequency of ignition, *i-th* room

P_{fc} = conditional probability for fire extending beyond the fire area of origin.

The probability of a fire extending beyond the fire area of origin is found from NFPA (Ref. 2.2.2).

The final initiating event frequency is determined by multiplying the frequency of the fire reaching the waste form (in occurrences per year) times the probability that a waste form is present (fraction of time per waste form) times 50 (years/ operating lifetime during the preclosure period). This yields the initiating event frequency for a fire of a specific severity affecting a waste form, per waste form

processed, over the preclosure period. The remainder of the event sequence quantification follows in Section 4.3.6.

4.3.6 Event Sequence Quantification

4.3.6.1 Overview of Quantification

Event sequences are represented by event trees and are quantified via the product of the initiating event frequency and the pivotal event probabilities. Event sequences that lead to a successful end state (designated as "OK") are not considered further. The result of quantification of an event sequence is expressed in terms of the number of occurrences over the preclosure period. This number is the product of the following factors:

1. The number of demands (sometimes called trials) or the time exposure interval of the operation or activity that gives rise to the event sequence. For example, this could be the total number of transfers of a cask in a facility preparation area.

2. The frequency of occurrence per demand or per time interval of the initiating event. For example, this could be the frequency of cask drop per transfer by a crane. Initiating event frequencies are developed either using fault trees or by direct application of industry-wide data, as explained in Section 4.3.2. Factors one and two are represented in the initiator event trees.

3. The conditional probability of each of the pivotal events of the event sequence, which appear in the associated system-response event tree. These probabilities are the results of a passive equipment failure analyses, fault tree analyses (e.g., HVAC), and direct probability input (e.g., moderator introduced), or judgment. For example, the conditional probability of cask failure given a drop from 12 feet or less is less than 1E-05.

SAPHIRE Version 7.26 (Section 4.2) is used as the integrating software for the Boolean reduction and quantification of event sequences. All fault trees and event trees are entered into or produced directly in SAPHIRE. All reliability information relevant to quantification is input into SAPHIRE. Following analyst input instructions or rules, SAPHIRE performs the following functions for this analysis:

- Following analyst instructions, links the initiator event tree with the appropriate system response event tree.

- Following analyst instructions, called rules, links the fault trees and direct pivotal event input probabilities that are involved in an event sequence.

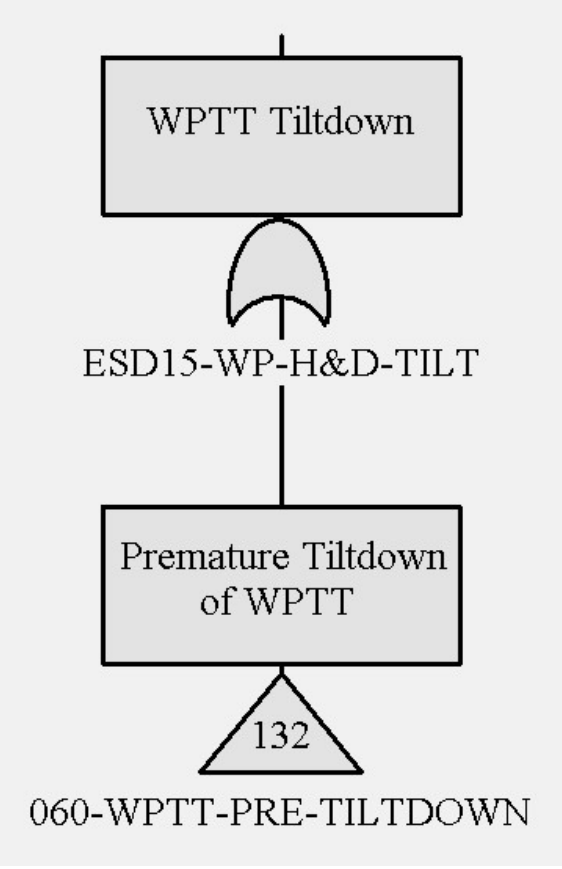
- Performs the Boolean manipulations to obtain minimal cut sets.

- Combines the minimal cut sets of each event sequence and each end state.

- Combines the minimal cut sets of each end state of all little bubbles to obtain the set of minimal cut sets of an end state for a big bubble initiating event.

- Obtains a point estimate number of occurrences of the minimal cut sets using the entered reliability information.
- Obtains the probability distributions of the minimal cut sets using the entered uncertainty information.
- Provides reports, as specified by the analyst, for each end state of each big bubble.

Development of analyst instructions, or rules, is facilitated by the following naming convention. The names identified in the initiating event fault trees are defined to be unique to the event tree. Fault trees are linked by development of a linking fault tree to transfer the appropriate fault tree to the event tree pivotal event or initiating event. . Figure 4.3-10 shows an example of this. ESD15-WP-H&D-TILT is the unique identifier that is assigned to the initiating event tree to represent the initiating event for a premature WPTT tiltdown. The benefit to using this method is that many smaller, specific fault trees can be linked together into a single initiating or pivotal event, thereby reducing the work associated with development of event sequence specific fault trees.



NOTE: WPTT = waste package transfer trolley.

Source: Original

Figure 4.3-10. Transfer from Event Tree to Fault Tree

The frequency of each minimal cut set is the product of the frequency and conditional probabilities of the events that compose it. The frequency of each event sequence is a probabilistic sum of the frequencies of each minimal cut set.

SAPHIRE, developed by Idaho National Laboratory, stands for "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations." It is 32-bit software that runs under Microsoft Windows. Features of SAPHIRE that help an analyst build and quantify a set of event trees and fault trees are as follows:

- A listing of where a basic event appears, including within cut sets. Conversely, the basic events that are *not* used are known and can be easily removed when it comes time to "clean" the database.

- Context-driven menu system that performs actions (report cut sets, view importance measures, display graphics, etc.) on objects such as fault trees, event trees, and event sequences.

Fault trees can be constructed and analyzed to obtain different measures of system unreliability. These system measures are:

- Overall initiating or pivotal event failure frequency
- Minimal cut sets size, number, and frequency
- Built in features include:
  - Generation, display, and storage of cut sets
  - Graphical editors (fault tree and event tree)
  - Database editors
  - Uncertainty analysis
  - Data input/output via ASCII text files (MAR-D)
  - Special seismic analysis capability.

SAPHIRE is equipped with two uncertainty propagation techniques: Monte Carlo and Latin Hypercube sampling. To take advantage of these sampling techniques, twelve uncertainty distributions are built such that the appropriate distribution may be selected. SAPHIRE contains a cross-referencing tool, which provides an overview of every place a basic event, gate, initiating, or pivotal event is used in the model.

4.3.6.2 Propagation of Uncertainties and Event Sequence Categorization with Uncertainties

The fundamental viewpoint of the PCSA is probabilistic in order to develop information suitable for the risk informed nature of 10 CFR Part 63 *Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada* (Ref. 2.3.2). Any particular event sequence may or may not occur during any operating time interval, and the quantities of the parameters of the models may not be precisely known. Characterizing uncertainties and propagating these uncertainties through the event tree/fault tree model is an essential element of the PCSA. The PCSA includes both aleatory and epistemic uncertainties. Aleatory uncertainty refers to the inherent variation of a physical process over many similar trials or occurrences. For

example, development of a fragility curve to obtain the probability of canister breach after a drop would involve investigating the natural variability of tensile strength of stainless steel. Epistemic uncertainty refers to our state of knowledge about an input parameter or model. Epistemic uncertainty is sometimes called reducible uncertainty because gathering more information can reduce the uncertainty. For example, the calculated uncertainty of a SSC failure rate developed from industry-wide data will be reduced when sufficient GROA specific operational information is included in a Bayesian analysis of the SSC failure rate.

Uncertainty in the value of any input parameter and the event sequence frequency is expressed by a probability distribution. Probability distribution is propagated through models using SAPHIRE. As described in Section 4.3.1, categorization is performed using the mean value of event sequences emanating from the big bubble in Figure 4.3-4. By the definition of the term, mean values are derived solely from probability distributions.

Using the screening criteria set out in 10 CFR 63.2 (Ref. 2.3.2), the categorization of an event sequence that is expected to occur m times over the preclosure period (where m is the mean or expected number of occurrences) is carried out as follows:

- A value of m greater than or equal to one places the corresponding event sequence into Category 1.

- A value of m less than one indicates that the corresponding event sequence is not expected to occur before permanent closure. To determine whether the event sequence is Category 2, its probability of occurrence over the preclosure period needs to be compared to 10^{-4}. A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to m. The probability, P, that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution, $P = 1 - \exp(-m)$, a value of P greater than or equal to 10^{-4} implies that the value of m is greater than or equal to $-\ln(1 - P) = m$, which is numerically equal to 10^{-4}. Thus, a value of m greater than or equal to 10^{-4}, but less than one, implies the corresponding event sequence is a Category 2 event sequence.

- Event sequences that have a value of m less than 10^{-4} are designated as Beyond Category 2.

Using either Monte Carlo or Latin Hypercube methods allows probability distributions to be arithmetically treated to obtain the probability distributions of minimal cut sets and the probability distributions of event sequences. The PCSA used Monte Carlo simulation with 10,000 trials and a standard seed so the results could be reproduced. The number of trials for final results was arrived at by increasing the numbers of trials until the median, mean, and 95th percentile were stable within the standard Monte Carlo error.

The adequacy of categorization of an event sequence is further investigated if its expected number of occurrences m over the preclosure period is close to a category threshold.

If m is greater than 0.2, but less than 1, the event sequence, which a priori is Category 2, is reevaluated differently to determine if it should be recategorized as Category 1. Similarly, if m is greater than 2×10^{-5}, but less than 10^{-4}, the event sequence, which a priori is Beyond Category 2, is reevaluated to determine if it should be recategorized as Category 2.

The reevaluation begins with calculating an alternative value of m, designated by m_a, based on an adjusted probability distribution for the number of occurrences of the event sequence under consideration. The possible distributions that are acceptable for such a purpose would essentially have the same central tendency, embodied in the median (i.e., the 50th percentile), but relatively more disparate tails, which are more sensitive to the shape of the individual distributions of the basic events that participate in the event sequence. Accordingly, the adjusted distribution is selected as a lognormal that has the same median M as that predicted by the Monte Carlo sampling. Also, to provide for a reasonable variability in the distribution, an error factor (EF) = 10 is used, which means that the 5th and 95th percentiles of the distribution are respectively lesser or greater than the median by a factor of 10.

If the calculated value of m_a is less than 1, the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., Category 2. Similarly, if the calculated value of m_a is less than 10^{-4}, the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., Beyond Category 2.

In contrast, if the calculated value of m_a is greater than 1, the alternative distribution indicates that the event sequence is Category 1, instead of Category 2 found in the original determination. In such a case, the conflicting indications are resolved by conservatively assigning the event sequence to Category 1.

Similarly, if the calculated value of m_a is greater than 10^{-4}, the alternative distribution indicates that the event sequence is Category 2, instead of Beyond Category 2 found in the original determination. In such a case, the conflicting indications are resolved by conservatively assigning the event sequence to Category 2.

The calculations carried out to quantify an event sequence are performed using the full precision of the individual probability estimates that are used in the event sequence. However, the categorization of the event sequence is based upon an expected number of occurrences over the preclosure period given with one significant digit.

4.3.7 Identification of ITS SSCs, Development of Nuclear Safety Design Bases, and Development of Procedural Safety Controls

4.3.7.1 Identification of ITS SSCs

ITS SSCs are subject to nuclear safety design bases that are established to ensure that safety functions and reliability factors applied in the event sequence analyses are explicitly defined in a manner that assures proper categorization of event sequences.

ITS is defined in 10 CFR 63.2 (Ref. 2.3.2) as:

> *Important to safety*, with reference to structures, systems, and components, means those engineered features of the geologic repository operations area whose function is:
>
> (1) To provide reasonable assurance that high-level radioactive waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of § 63.111(b)(1) for Category 1 event sequences; or
>
> (2) To prevent or mitigate Category 2 event sequences that could result in radiological exposures exceeding the values specified at § 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site.

Structures are defined as elements that provide support or enclosure such as buildings, free standing tanks, basins, dikes, and stacks. Systems are collections of components assembled to perform a function, such as HVAC, cranes, trolleys, and transporters. Components are items of equipment that taken in groups become systems such as pumps, valves, relays, piping, or elements of a larger array, such as digital controllers.

Implementation of the regulatory definition of ITS produces the following specific criteria in the PCSA to classify SSCs. A SSC is classified as ITS if it appears in an event sequence and at least one of the following criteria apply:

- The SSC is relied upon to reduce the frequency of an event sequence from Category 1 to Category 2.
- The SSC is relied upon to reduce the frequency of an event sequence from Category 2 to Beyond Category 2.
- The SSC is relied upon to reduce the aggregated dose of Category 1 event sequences by reducing the event sequence mean frequency.
- The SSC is relied upon to perform a dose mitigation or criticality control function.

A SSC is classified as ITS in order to assure safety function availability over the operating lifetime of the repository. The classification process involves the selection of the SSCs in the identified event sequences (including event sequences that involve nuclear criticality) that are relied upon to perform the identified safety functions such that the preclosure performance objectives of 10 CFR Part 63 (Ref. 2.3.2) are not exceeded. The ITS classification extends only to the attributes of the SSCs involved in providing the ITS function. If one or more components of a system are determined to be ITS, the system is identified as ITS, even though only a portion of the system may actually be relied upon to perform a nuclear safety function. However, the specific safety functions that cause the ITS classification are delineated.

Perturbations from normal operations, human errors in operations, human errors during maintenance (preventive or corrective), and equipment malfunctions may initiate Category 1 or Category 2 event sequences. The SSCs supporting normal operations (and not relied upon as

described previously for event sequences) are identified as non-ITS. In addition, if an SSC (such as permanent shielding) is used solely to reduce normal operating radiation exposure, it is classified as non-ITS.

4.3.7.2 Development of Nuclear Safety Design Bases

Design bases are established for the ITS SSCs as described in 10 CFR 63.2 (Ref. 2.3.2):

> Design bases means that information that identifies the specific functions to be performed by a structure, system, or component of a facility and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be constraints derived from generally accepted "state-of-the-art" practices for achieving functional goals or requirements derived from analysis (based on calculation or experiments) of the effects of a postulated event under which a structure, system, or component must meet its functional goals...

The safety functions for this analysis were developed from the applicable Category 1 and Category 2 event sequences for the SSCs that were classified as ITS. In general, the controlling parameters and values were grouped in, but were limited to, the following five categories:

1. Mean frequency of SSC failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of failure (e.g., failure to operate, failure to breach), with consideration of uncertainties, less than or equal to the stated criterion value.

2. Mean frequency of seismic event-induced failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of a seismic event-induced failure (e.g., tipover, breach) of less than 1E-04 over the preclosure period, considering the full spectrum of seismic events less severe than that associated with a frequency of 1E-07/yr.

3. High confidence of low mean frequency of failure. It shall be demonstrated by analysis that the ITS SSC will have a high confidence of low mean frequency of failure associated with seismic events of less than or equal to the criterion value. The high confidence of low mean frequency of failure value is a function of uncertainty, expressed as β_c, which is the lognormal standard deviation of the SSC seismic fragility.

4. Preventive maintenance and/or inspection interval. The ITS SSCs shall be maintained or inspected to assure availability, at intervals not to exceed the criterion value.

5. Mean unavailability over time period. It shall be demonstrated by analysis that the ITS SSCs (e.g., HVAC and emergency electrical power) will have a mean unavailability over a period of a specified number of days, with consideration of uncertainties, of less than the criterion value.

These controlling parameters and values ensure that the ITS SSCs perform their identified safety functions such that 10 CFR Part 63 (Ref. 2.3.2) performance objectives are met. The controlling parameters and values include frequencies or probabilities in order to provide a direct link from the design requirements for categorization of event sequences. The PCSA will demonstrate that these controlling parameters and values are met by design of the respective ITS SSCs.

Table 6.9-1 in Section 6.9 presents a list of ITS SSCs, the nuclear safety design bases of the ITS SSCs, the actual value of the controlling parameter developed in this analysis, and a reference to that portion of the analysis (e.g., fault tree analysis), which demonstrates that the criterion is met.

4.3.7.3 Identification of Procedural Safety Controls

10 CFR 63.112(e) (Ref. 2.3.2) requires that the PCSA include an analysis that "identifies and describes the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences" and "identifies measures taken to ensure the availability of safety systems." This section describes the approach for specifying and analyzing the subset of procedural safety controls (PSCs) that are required to support the event sequence analysis and categorization.

The occurrence of an initiating or pivotal event is usually a combination of human errors and equipment malfunctions. A human reliability analysis is performed for the human errors. Those human actions that are relied upon to reduce the frequency of or mitigate the consequence of an event sequence are subject to PSCs.

The approach for deriving PSCs from the event sequence analysis is outlined in the following:

1. Use event tree and supporting fault tree models for initiating events and pivotal events to identify HFEs.

2. Identify the types of PSCs necessary to support the HRA analysis for each of the HFEs. For example, provide clarifications about what is to be accomplished, time constraints, use of instrumentation, interlock and permissives that may back-up the human action.

3. Perform an event sequence analysis using screening HRA values. Identify the PSCs that appear to be needed to reduce the probability of or mitigate the severity of event sequences. The same criteria are used to identify ITS SSCs.

4. Work with the design and engineering organizations to add equipment features that will either eliminate the HFE or support crew and operators in the performance of the action. In effect, this entails development of design features that appear instead of a human action or under an AND gate with a human action.

5. Quantify event sequences again, identifying HFEs for which detailed HRA must be performed. The detailed HRA would lead to specific PSCs that are needed to reduce the frequency of event sequences or mitigate their consequences.

4.3.8 Event Sequence to Dose Relationship

Outputs of the event sequence analysis and categorization process include tabulations of event sequences by expected number of occurrences, end state, and waste form. The event sequences are sorted by Category 1, Category 2 and Beyond Category 2. Summaries of the results are tabulated in Section 6.8 and Attachment G with the following information:

1. Event sequence group identifier. A unique designator is provided for each event sequence to permit cross-references between event sequence categorization and consequence and criticality analysis.

2. End state. One of the following is provided for each event sequence:

   A. DE-SHIELD-DEGRADE or DE-SHIELD-LOSS (Direct Exposure). Condition leading to potential exposure due to degradation of shielding provided by the cask or the aging overpack.

   B. RR-FILTERED (Radionuclide Release, Filtered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister). However, the availability of the secondary confinement (structural and HVAC with HEPA filtration) provides mitigation of the consequences. This end state is not used for the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.

   C. RR-UNFILTERED (Radionuclide Release, Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister), and a breach in the secondary confinement boundary (e.g., no HEPA filtration to provide mitigation of the consequences or breach of the structural confinement).

   D. RR-FILTERED-ITC and RR-UNFILTERED-ITC (Radionuclide Release, Important to Criticality, Filtered or Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister) with or without HEPA filtration. In addition, the potential of exposing the unconfined waste form to moderator could result in conditions important to criticality. This characteristic of the end state is used by both the dose consequence analysts and the criticality analysts. The RR-FILTERED-ITC end state is not used for the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.

   E. ITC (Important to Criticality). This end state is not used for the IHF, RF, Intrasite and Subsurface because all potential criticality initiators are associated with a radiological release (i.e., end state RR-UNFILTERED-ITC).

3. General description of the event sequence. This is a high level description that will be explained by the other conditions described above. For example, "Filtered radionuclide release resulting from a drop from a crane that causes a breach of both sealed transportation cask and sealed TAD canister."

4. Material-at-risk. Identify and define the number of each waste form that contributes to the radioactivity or criticality hazard of the end state (e.g., number of TAD canisters, DPCs, uncanistered commercial SNF assemblies, etc., involved in the event sequence).

5. Expected number of occurrences. Provide the expected mean number of occurrences of the designated event sequences over the preclosure period and associated median and standard deviation.

6. The event sequence categorization. Provide the categorization of the designated event sequence and the basis for the categorization.

7. The bounding consequences. Provide the bounding consequence analysis cross-reference, as applicable, for each Category 1 or 2 event sequence to the bounding event number from the preclosure consequence analysis.

10 CFR 63.111 (Ref. 2.3.2) requires that the doses associated with Category 1 and Category 2 event sequences meet specific performance objectives. There are no performance objectives for Beyond Category 2 event sequences. Dose consequences associated with each Category 1 and Category 2 event sequence are evaluated in preclosure consequence analyses, by comparison, to pre-analyzed release conditions (or dose categories) that are intended to characterize or bound the actual event sequences (Ref. 2.2.33). As such, the results of the event sequence analysis and categorization serve as inputs to the consequence analysis for assignment to dose categories.

4.3.9 Event Sequence to Criticality Relationship

The requirements for compliance with preclosure safety regulations are defined in 10 CFR 63.112 (Ref. 2.3.2). Particularly germane to criticality considerations, is the requirement in 10 CFR 63.112, Paragraph (e) and Subparagraph (e)(6) (Ref. 2.3.2). Paragraph (e) requires an analysis to identify the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. This is a general requirement imposed on all event sequence analyses. Subparagraph (e)(6) specifically notes that the analyses should include consideration of "means to prevent and control criticality." The PCSA criticality analyses (Ref. 2.2.35) employ specialized methods that are beyond the scope of the present calculation. However, the event sequence development analyses inform the PCSA criticality analyses by identifying the event sequences and end states that may have a potential for criticality. As noted in Section 4.3, some event sequence end states include the phrase "important to criticality." This indicates that the end state implies the potential for criticality and that a criticality investigation is indicated

To determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity of variations in each of the parameters important to criticality during the preclosure period, that is, waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor (k_{eff}) to variations in any of these parameters as a function of the other parameters. These criticality calculations demonstrate that one of the following is true for each parameter:

- It is bounding (i.e., its analyzed value is greater than or equal to the design limit) or its effect on k_{eff} is bounded and does not need to be controlled. This is designated as a no in Table 4.3-1.

- It needs to be controlled if another parameter is not controlled (conditional control). This is designated as a Conditional in Table 4.3-1.

- It needs to be controlled because it is the primary criticality control parameter. This is designated as a yes in Table 4.3-1.

The criticality control parameters analysis, which comprises the background calculations that led to Table 4.3-1, is presented in detail in the *Preclosure Criticality Safety Analysis* (Ref. 2.2.35). Event sequences that impact the criticality control parameters that have been established as needing to be controlled are identified, developed, quantified, and categorized. These event sequences are referred to as event sequences ITC. The following matrix elements, indicating the need for control, are treated in the current event sequence analysis:

- Conditional: needs to be controlled if moderator is present
- Conditional: needs to be controlled during a boron dilution accident
- Yes: moderation is the primary criticality control
- Yes: interaction for DOE standardized SNF canisters needs to be controlled.

Table 4.3-1. Criticality Control Parameter Summary

Operation / Parameter	Commercial SNF (Dry Operations)	Commercial SNF (WHF Pool and Fill Operations)	DOE SNF	HLW
Waste Form Characteristics	No[a]	No[a]	No[b]	No[c]
Moderation	Yes[d]	N/A	Yes[d]	No
Interaction	No	Conditional[g]	Yes[e]	No
Geometry	Conditional[f]	Conditional[g]	Conditional[f]	No
Fixed Neutron Absorbers	Conditional[f]	Conditional[g]	Conditional[f]	No
Soluble Neutron Absorber	N/A	Yes[h]	N/A	N/A
Reflection	No	No	No	No

NOTE: [a] The *Preclosure Criticality Safety Analysis* (Ref. 2.2.35) considers bounding waste form characteristics. Therefore, there is no potential for a waste form misload.
[b] The *Preclosure Criticality Safety Analysis* (Ref. 2.2.35) considers nine representative DOE SNF types. Because the analysis is for representative types and loading procedures for DOE standardized SNF canisters have not been established yet, consideration of waste form misloads is not appropriate
[c] Criticality safety design control features are not necessary for HLW canisters because the concentration of fissile isotopes in an HLW canister is too low to have criticality potential.
[d] Moderation is the primary criticality control parameter.
[e] Placing more than four DOE standardized SNF canisters outside the staging racks or a codisposal waste package is controlled by design features.
[f] Needs to be controlled only if unborated water or other moderator is present within a waste container. The presence of moderator is controlled by design features of the facility and by the welded or bolted waste containers.
[g] Needs to be controlled only if the soluble boron concentration in the pool and transportation cask/DPC fill water is less than the minimum required concentration.
[h] Minimum required soluble boron concentration in the pool is 2500 mg/L boron enriched to 90 atom % ^{10}B.
DOE = U.S. Department of Energy; HLW = high-level radioactive waste; SNF = spent nuclear fuel; WHF = Wet Handling Facility.

Source: *Preclosure Criticality Safety Analysis* (Ref. 2.2.35, Table 6)

4.3.10 Boundary Conditions and Use of Engineering Judgment Within a Risk Informed Framework

4.3.10.1 Boundary Conditions

The initiating events considered in the PCSA define what could occur within the site GROA and are limited to those events that constitute a hazard to a waste form while it is present in the GROA. Initiating events include internal events occurring during waste handling operations conducted within the GROA and external events (e.g., seismic, wind energy, or flood water events) that impose a potential hazard to a waste form, waste handling systems, or personnel within the GROA. Such initiating events are included when developing event sequences for the PCSA. However, initiating events that are associated with conditions introduced in SSCs before they reach the site are not within the scope of the PCSA. The excluded from consideration offsite conditions include drops of casks, canisters, or fuel assemblies during loading at a reactor site; improper drying, closing, or inerting at the reactor site; rail or road accidents during

transport; tornado or missile strikes on a transportation cask; or nonconformances introduced during cask or canister manufacture that result in a reduction of containment strength. Such potential precursors are subject to deterministic regulations (e.g., 10 Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4)) and associated QA programs. As a result of compliance to such regulations, the SSCs are deemed to pose no undue risk to health and safety. Although the analyses do not address quantitative probabilities to the aforementioned excluded precursors, it is clear that conservative design criteria and QA controls result in unlikely exposures to radiation.

Other boundary conditions used in the PCSA include:

- Plant operational state. Initial state of the facility is normal with each system operating within its vendor prescribed operating conditions.

- No other simultaneous initiating events. It is standard practice to not consider the occurrence of other initiating events (human-induced and naturally occurring) during the time span of an event sequence because: a) the probability of two simultaneous initiating events within the time window is small and, b) each initiating event will cause operations in the waste handling facility to be terminated which further reduces the conditional probability of the occurrence of a second initiating event, given the first has occurred.

- Component failure modes. The failure mode of a SSC corresponds to that required to make the initiating or pivotal event occur.

- Fundamental to the basis for the use of industry-wide reliability parameters within the PCSA, such as failure rates, is the use of SSCs within the GROA that conform to NRC accepted consensus codes and standards, and other regulatory guidance.

4.3.10.2 Use of Engineering Judgment

10 CFR Part 63 (Ref. 2.3.2) is a risk-informed regulation rather than a risk-based regulation. The term risk-informed was defined by the NRC to recognize that a risk assessment can not always be performed using only quantitative modeling. Probabilistic analyses may be supplemented with expert judgment and opinion, based on engineering knowledge. Such practice is fundamental to the risk assessment technology used for the PCSA.

10 CFR Part 63 (Ref. 2.3.2) does not specify analytical methods for demonstrating performance, estimating the reliability of ITS SSCs (whether active or passive), or calculating uncertainty. Instead, the risk-informed and performance-based preclosure performance objectives in 10 CFR Part 63 (Ref. 2.3.2) provide the flexibility to develop a design, and demonstrate that it meets performance objectives for preclosure operations including the use of well established (discipline-specific) methodologies. As exemplified in the suite of risk-informed regulatory guides developed for 10 CFR 50 (Ref. 2.3.1) facilities (e.g., Regulatory Guide 1.174 (Ref. 2.2.75) and NUREG-0800 (Ref. 2.2.67, Section 19)), such methodologies use deterministic and probabilistic inputs and analysis insights. The range of well established techniques in the area of PRA, which is used in the PCSA, often relies on the use of engineering judgment and

expert opinion (e.g., in development of seismic fragilities, human error probabilities, and the estimation of uncertainties).

As described in Section 4.3.3, for example, active SSC reliability parameters will be developed using a Bayesian approach; and the use of judgment in expressing prior state-of-knowledge is a well-recognized and accepted practice (Ref. 2.2.58), (Ref. 2.2.5), (Ref. 2.2.10), and (Ref. 2.2.66).

The NRC issued *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73) to provide guidance for compliance to 10 CFR 63.111 and 112 (Ref. 2.3.2). This document states that "treatment of uncertainty in reliability estimates may depend on the risk-significance (or reliance) of a canister system in preventing or reducing the likelihood of event sequences." Furthermore, *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73) indicates that reliability estimates for high reliability SSCs may include the use of engineering judgment supported by sufficient technical basis; and empirical reliability analyses of a SSC could include values based on industry experience and judgment (Ref. 2.2.73).

In a risk-informed PCSA, therefore, the depth, rigor of quantitative analysis and the use of judgment depends on the risk-significance of the event sequence. As such, decisions on the level of effort applied to various parts of the PCSA are made, based on the contribution to the frequency of end states and the severity of such end states. An exhaustive analysis need not be performed to make this resource allocation. Accordingly, the PCSA analyst has flexibility in determining and estimating the reliability required for each SSC, at the system or component level, and in selecting approaches in estimating the reliability. The quantified reliability estimates used to reasonably screen out initiating events, support categorization, or screening of event sequences must be based on defensible and traceable technical analyses. The following summarizes the approaches where judgment is applied to varying degrees.

All facility safety analyses, whether or not risk-informed, take into account the physical conditions, dimensions, materials, human-machine interface, or other attributes such as operating conditions and environments to assess potential failure modes and event sequences. Such factors guide the assessment of what can happen, the likelihood, and the potential consequences. In many situations, it could be considered obvious that the probability of a particular exposure scenario is very small. In many cases, it is impractical or unnecessary to actually quantify the probability when a non-probabilistic engineering analysis provides sufficient assurance and insights that permit the event sequence to be either screened out, or demonstrated to be bounded by another event sequence. Examples of such are provided in Section 6.0.

When Empirical Information is Not Available

There is generally no or very little empirical information for the failure of passive SSCs such as transportation casks and spent fuel storage canisters. Such failures are postulated in predictive safety and risk analyses and then the SSCs are designed to withstand the postulated drops, missile impacts, seismic shaking, abnormal temperatures, pressures, and etc. While in service, few if any SSCs have been subjected to abnormal conditions that approach the postulated abnormal scenarios so there is virtually no historical data to call on.

Therefore, structural reliability analyses are used in the PCSA to develop analysis-based failure probabilities for the specific event sequences identified within the GROA. Uncertainties in the calculated stresses/strains and the capacity of the SSCs to withstand those demands include the use of judgment, based on standard nuclear industry practices for design, manufacturing, etc., under the deterministic NRC regulatory requirements of 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), or 10 CFR Part 72 (Ref. 2.3.4). It is standard practice to use the information basis associated with the consensus standard and regulatory requirement information as initial conditions of a risk-informed analysis. This approach is acceptable for the PCSA subject to the following:

1. The conditions associated with the consensus codes and standards and regulatory requirements are conservatively applicable to the GROA.

2. Equivalent QA standards are applied at the GROA.

3. Operating processes are no more severe than those licensed under the aforementioned deterministic regulations.

Use of Empirical Reliability Information

In those cases where applicable, quantitative historical component reliability information is available, the PCSA followed Section 4.3 including the application of judgment that is associated with Bayesian analysis. Similarly, as described in Sections 4.3.5, 4.3.6, and 4.3.7, historical data is applied in human reliability, fire, and flooding analyses with judgment-based adjustments as appropriate for the WHF and GROA operating conditions.

Use of Qualitative Information When Reliability Information is Not Available

In those cases where historical records of failures to support the PCSA are not available, qualitative information may be used to assign numerical failure probabilities and uncertainty. This approach is consistent with the Bayesian framework used in the PCSA, consistent with *Interim HLWRS-ISG-02* (Ref. 2.2.73), and involves the use of judgment in the estimation of reliability or failure probability values and their associated uncertainties. In these cases, the PCSA analyst may use judgment to determine probability and reliability values for components.

The following guidelines are used in the PCSA when it is necessary to use judgment to assess the probability of an event. The analyst will select a median at the point believed to be just as likely that the "true" value will lie above as below. Then, the highest probability value believed possible is conservatively assigned as a 95th percentile or error factor (i.e., the ratio of the 95th percentile to median), rather than a 99th or higher percentile, with a justification for the assignments. A lognormal distribution is used because it is appropriate for situations in which the result is a product of multiple uncertain factors or variables. This is consistent with the *A Central Limit Theorem for Latin Hypercube Sampling* (Ref. 2.2.74). The lower bound, as represented by the 5th percentile, is checked to ensure that the distribution developed using the median and 95th percentile does not cause the lower bound to generate values for the variable that are unrealistic compared to the knowledge held by the analyst.

In some cases, an upper and lower bound is defensible, but no information about a central tendency is available. A uniform distribution between the upper and lower bound is used in such cases.

Another way in which risk-informed judgment is applied to obtain an appropriate level of effort in the PCSA, involves a comparison of event sequences. For example, engineering judgment readily indicates that a 23-foot drop of a canister onto an unyielding surface would do more damage to the confinement boundary, than a collision of a canister with a wall at maximum crane speed (e.g. 40 feet per minute). A rigorous probabilistic structural analysis of the 23-foot drop is performed and these results may be conservatively applied to the relatively benign slow speed collision.

5. LIST OF ATTACHMENTS

		Number of Pages
Attachment A	Event Trees	174
Attachment B	System/Pivotal Event Analysis – Fault trees	391
Attachment C	Active Component Reliability Data Analysis	51
Attachment D	Passive Equipment Failure Analysis	91
Attachment E	Human Reliability Analysis	266
Attachment F	Fire Analysis	140
Attachment G	Event Sequence Quantification Summary Tables	2
Attachment H	SAPHIRE Model and Supporting Files	2 + CD

6. BODY OF ANALYSIS

The *Wet Handling Facility Event Sequence Development Analysis*, which describes the WHF, its equipment, and its operations (Ref. 2.2.37, Section 6.1.2, Attachment A, and Attachment B), should be consulted in conjunction with the present analysis.

6.0 INITIATING EVENT SCREENING

The NRC's interim staff guidance for its evaluation of the level of information and reliability estimation related to the Yucca Mountain repository, *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73, p. 3), states that there are multiple approaches that DOE could use to estimate the reliability of SSCs that contribute to initiating events or event sequence propagation (i.e., pivotal events), including the use of judgment. 10 CFR 63.102(f) (Ref. 2.3.2) provides that initiating events are to be considered for inclusion in the PCSA for determining event sequences only if they are reasonably based on the characteristics of the geologic setting and the human environment, and are consistent with the precedents adopted for nuclear facilities with comparable or higher risks to workers and the public.

This section provides screening arguments that eliminate extremely unlikely initiating events from further considerations. Screening of initiating events is a component of a risk-informed approach that allows attention to be concentrated on important contributors to risk. The screening process eliminates those potential initiators that are either incapable of initiating an event sequence having radiological consequences or are too improbable during the preclosure period to warrant further consideration. The screening arguments are based on either a qualitative or quantitative analysis documented under separate cover, or through engineering judgment based on considerations of site and design features documented herein.

Initiating events are screened out and are termed beyond Category 2 if they satisfy either of the following criteria:

- The initiating event has less than one chance in 10,000 of occurring during the preclosure period.
- The initiating event has less than one chance in 10,000 over the preclosure period of causing physical damage to a waste form that would result in the potential for radiation exposure or inadvertent criticality.

In some instances, initiating event screening analysis is based on engineering or expert judgment. Such judgment is based on applications of industry codes and standards, comparison to results of analyses for other similar event sequences that are included, or plausibility arguments based on the combinations of conditions that must be present to allow the initiating event to occur and the event sequence to propagate.

6.0.1 Boundary Conditions for Consideration of Initiating Events

6.0.1.1 General Statement of Boundary Conditions

Manufacturing, loading, and transportation of casks and canisters are subject to regulations other than 10 CFR Part 63 (e.g., 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4)) and associated quality assurance programs. As a result of compliance with such regulations, the affected SSCs are deemed to provide reasonable assurance that the health and safety of the public is protected. However, if a potential precursor condition could result in an airborne release that could exceed the performance objectives for Category 1 or Category 2 event sequences, or a criticality condition, then a qualitative argument that the reasonableness of boundary condition is provided. A potential initiating event that is outside of the boundary conditions but has been found to require a qualitative discussion is the failure to properly dry a SNF canister or transportation cask containing bare SNF prior to sealing it and shipping it to the repository.

6.0.1.2 Specific Discussion of Receipt of Properly Dried SNF Canisters

Under the boundary conditions stated for this analysis, canisters shipped to the repository in transportation casks are received in the intended internally dry conditions. Shipments of SNF received at the repository, whatever their origin, are required to meet the requirements of 10 CFR Part 71 (Ref. 2.3.3). NUREG-1617 (Ref. 2.2.69) provides guidance for the NRC safety reviews of packages used in the transport of spent nuclear fuel under 10 CFR Part 71 (Ref. 2.3.3). The review guidance, NUREG-1617 (Ref. 2.2.69., Section 7.5.1.2), instructs reviewers that, at a minimum, the procedures described in the safety analysis report should ensure that:

> Methods to drain and dry the cask are described, the effectiveness of the proposed methods is discussed, and vacuum drying criteria are specified.

NUREG-1536 (Ref. 2.2.68, Chapter 8, section V) refers to an acceptable process to evacuate water from SNF canisters. No more than about 0.43 gram-mole of water (about 8 grams) will be left in the canister if adequate vacuum drying is performed (Ref 2.2.68). The following example is cited as providing adequate drying (Ref. 2.2.68, Chapter 8, Section V):

> The cask should be drained of as much water as practicable and evacuated to less than or equal to 4E-4 MPa (3.0 mm Hg or 3.0 Torr). After evacuation, adequate moisture removal should be verified by maintaining a constant pressure over a period of about 30 minutes without vacuum pump operation. The cask is then backfilled with an inert gas (e.g., helium) for applicable pressure and leak testing. The cask is then re-evacuated and re-backfilled with inert gas before final closure. Care should be taken to preserve the purity of the cover gas and, after backfilling; cover gas purity should be verified by sampling.

The procedure described appears to ensure that very little water is left behind. However, the probability of undetected failure when performing the process is not addressed in the deterministic regulation (10 CFR Part 71 (Ref 2.3.3) or in NUREG-1536 (Ref 2.2.68)). Indeed, there is no after-the-fact water or error detection method in NUREG-1536 or in the regulation. Therefore, some unknown number of canisters may arrive at the GROA with more residual water

than is expected with proper drying. Because the canisters are welded and are not required to provide for sampling inside the canister, nondestructive measurement of the residual water content would be difficult. The following discussion provides reasonable assurance that no significant risks are omitted from the analysis due to adoption of the boundary condition that canisters shipped to the repository in transportation casks are received in the intended internally dry conditions.

1. The YMP will be accepting, handling, and emplacing TAD canisters in a manner consistent with the specifications laid out in the TAD canister system performance specification (Ref. 2.2.44) which prescribes the use of consensus codes and standards along with design requirement associated with GROA specific event sequences.

2. **Criticality**. There is no credible potential for criticality resulting from the failure to properly dry a SNF canister or transportation cask containing bare SNF prior to sealing it and shipping it to the repository as discussed in *Preclosure Criticality Safety Analysis* (Ref. 2.2.34, Section 2.3.12)

3. **Hydrogen explosion or deflagration**. Radiation from SNF can generate radiolytic hydrogen and oxygen gas in a SNF canister if water is inadvertently left in the canister before it is sealed. Given a processing error that leaves enough residual water, the gas concentrations could conceivably reach levels where a deflagration event could occur. However, precautions taken at the generator sites are expected to make receipt of a canister that was improperly dried unlikely. In addition, an ignition source would be required for an explosion or deflagration to occur. High electrical conductivity of the metal canister would dissipate any high voltage electrical discharge (which is unlikely in any case) and preclude arcing within the canister. Normal handling operations do not subject the canisters to energetic impacts that could cause frictional sparking inside the canister. Therefore, a further unlikely event, such as a canister drop would have to occur to ignite the gas. Considering the combination of unlikely events that must occur, event sequences involving this combination of failures are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.

4. **Overpressurization due to residual water**. Given a processing error that leaves an excessive amount of residual water, the internal pressure due to vaporization of water could conceivably breach the canister. If sufficient water were to be left in the canister, overpressurization would occur within hours of the canister being welded closed. Therefore overpressurization, would occur while the canister is still in the supplier's possession and not in the GROA. Ambient environmental conditions on the GROA are similar to those that would be encountered by the canister while it is at the supplier's site and during transportation to the GROA. If there is not enough water to cause an overpressurization before the canister reaches the GROA, then overpressurization would not occur at the GROA. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable for loaded canisters received from offsite.

6.0.2 Screening of External Initiating Events

6.0.2.1 Initial Screening of External Initiating Events

The *External Events Hazards Screening Analysis* (Ref. 2.2.29) identifies potential external initiating events at the repository for the preclosure period and screens a number of them from further evaluation based on severity or frequency considerations. The four questions that constitute the evaluation criteria for external events screening are:

1. Can the external event occur at the repository?

2. Can the external event occur at the repository with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

3. Can the external event, severe enough to affect the repository and its operation, occur at the repository with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

4. Can a release that results from the external event severe enough to affect the repository and its operations occur with a frequency greater than 10^{-6}/yr, that is, have a 1 in 10,000 chance of occurring in the 100 year preclosure period?

The screening criteria are applied for each of the external event categories listed in Table 6.0-1. Each external event category is evaluated separately with a definition and the required conditions for the external event to be present at the repository. Then the four questions are applied. Those external event categories that are not screened out are retained for further evaluation as initiating events in the event sequences for the preclosure safety analysis.

As noted in Table 6.0-1, the potential external initiating event categories that are retained for further evaluation are seismic activity and loss of power. Seismically induced event sequences are developed, categorized, and documented in a separate analysis (Ref. 2.4.4). Loss of offsite power (LOSP) is treated together with internal causes of power loss in Section 6.0.2.

Table 6.0-1. Retention Decisions from External Events Screening Analysis

External Event Category	Retention Decision. If Not Retained, Basis for Screening.
Seismic activity	YES. Retained for further analysis.
Nonseismic geologic activity	NO. Except for one of the subcategories, drift degradation, the external events in this category are not applicable to the site or do not occur at a rate that could affect the repository during the preclosure period. The chance of drift degradation severe enough to affect the repository and its operation over the preclosure period is less than 1/10,000.
Volcanic activity	NO. The chance of volcanic activity occurring at the repository over the preclosure period is less than 1/10,000.
High winds/tornadoes	NO. The chance of a high wind or tornado event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
External floods	NO. The chance of a flood event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Lightning	NO. The chance of a lightning event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Loss of power event	YES. Retained for further analysis. See Section 6.0.2.2 for a screening analysis of loss of electrical power as an initiating event.
Loss of cooling capability event	NO. The primary requirements for cooling water at the Yucca Mountain site during the preclosure period are makeup water for the WHF pool and cooling of HVAC chilled water. The chance of a loss of cooling capability occurring at the repository over the preclosure period is less than 1/10,000.
Aircraft crash	NO. The chance of an accidental aircraft crash occurring at the repository over the preclosure period is less than 1/10,000.
Nearby industrial/military facility accidents	NO. The chance of an industrial or military facility accident occurring at the repository over the preclosure period is less than 1/10,000.
Onsite hazardous materials release	NO. The chance of an accident event sequence initiated by the release of onsite hazardous materials at the repository over the preclosure period is less than 1/10,000.
External fires	NO. The chance of an external fire severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Extraterrestrial activity	NO. Extraterrestrial activity is defined as an external event involving objects outside the earth's atmosphere and enters the earth's atmosphere, survive the entry through the earth's atmosphere and strike the surface of the earth. Extraterrestrial activity include: meteorites, asteroids, comets, and satellites. The chance of an occurrence at the repository over the preclosure period is less than 1/10,000.

NOTE: The source document defines the external event categories.
HVAC = heating, ventilation, and air conditioning; WHF = wet handling facility.

Source: Adapted from *External Events Hazards Screening Analysis* (Ref. 2.2.29, Sections 6 and 7).

6.0.2.2 Screening of Loss of Electrical Power as an Initiating Event

Loss of electrical power, whether caused by onsite or offsite failures, is expected to occur during the preclosure period. Conveyances, cranes, and CTMs that rely on electric power will stop upon loss of power, but are designed to hold loads indefinitely. A set of redundant emergency diesel generators and the associated ITS electrical distribution system would start upon LOSP in order to continue operation of the ITS HVAC confinement system.

LOSP is not shown as an initiating event in the event trees because, by itself, it does not cause mechanical handling equipment to malfunction in a way that causes a drop or other mechanical impact of a waste container. Therefore, load drop and LOSP may be treated as independent events. The following calculation demonstrates that a loss of offsite power and coincident load drop is Beyond Category 2.

The LOSP frequency is estimated at 3.6E-02/yr (Ref. 2.2.45, Table 3-8), with a failure to recover power within 24 hours of 1.8E-02 (Ref. 2.2.45, Table 4-1). Thus, during 50-year portion of the preclosure period in which waste handling operations are conducted, the expected number of LOSP events is:

$$\text{LOSP \#} = 3.6\text{E-}02/\text{yr} \times 50\ \text{yr}$$
$$= 1.8;$$

The initiating frequency of a LOSP lasting more than 24 hours would be:

$$\text{LOSP-IE} = 3.6\text{E-}02/\text{yr} \times (1.8\text{E-}02) \times 50\ \text{yr}$$
$$= 3.2\text{E-}02/\ \text{preclosure period}$$

An independent load drop from a crane following a LOSP would probably be caused by crane holding and emergency brake failures or random hoist cable breaks (each CTM and crane uses multiple wire ropes) because no other movement induced failure modes have been identified. Crane brake failures are more frequent than wire rope breaks, and for this calculation, the brake failure rates are used to determine a load drop probability. Two failure modes for the brakes have been modeled: failure of the brake to set and failure of the brakes to hold for an extended period. As documented in Attachment C, Table C4-1, estimated crane brake failure rates are:

- Holding (pneumatic) brake (BRP-FOD & BRP-FOH): 5.0E-05 per demand (initial setting of the brake) and 8.4E-06 per hour (holding the load for the duration of the power loss)

- Emergency brake (BRK-FOD & BRK-FOH): 1.5E-06 per demand (initial setting of the brake) and 4.4E-06/hr (holding the load for the duration of the power loss).

The four components of LOSP and brake failures are:

1. Both the holding brake and emergency brake fail to set on a LOSP resulting in a load drop.

2. Holding brake fails to set at LOSP. Emergency brake sets at LOSP but fails to hold during an extended loss of power (720 hours) resulting in a load drop

3. Emergency brake fails to set at LOSP. Holding brake sets at LOSP but fails to hold during an extended loss of power (720 hours) resulting in a load drop

4. Both brakes set at LOSP but fail to hold during an extended loss of power (720 hours) resulting in a load drop.

The failure components described above are analogous to the failure modes of a two train system in standby where at least on train must successfully start and run for a specified mission time to prevent system failure.

The fourth component described above dominates probabilistically and its calculation is described below. The sum of the other three is more than two orders of magnitude lower.

The likelihood of an extended LOSP has been estimated by using the probability of a LOSP exceeding 24 hours, which is the longest non-recovery period identified in NUREG/CR-6890 (Ref. 2.2.45). The 720 hour period for which a brake holding failure has been modeled should provide ample time to either recover offsite power or for operators to implement an alternative means to safely lower any load. Provision for manual lowering of loads is provided in NOG-1 cranes (Ref. 2.2.9).

The probability of the fourth component described above – the combination of LOSP and load drop (brakes set but fail to hold over a 720-hr mission time) is:

LOSP-IE × Holding brake fails × Emergency brake fails =
= 3.2E-02 × (8.4E-06 × 720) × (4.4E-06 × 720)
= 6.1E-07

Thus, the LOSP load drop probability over the preclosure period is estimated to be 6E-07. This number of occurrences of the compound initiating event is much less than one chance in 10,000 (1E-4) during the preclosure period. Therefore, event sequences with LOSP and a coincident drop load as the initiating event are beyond Category 2.

The possibility of inadvertent direct exposure of workers due to a loss of electrical power is considered next. Canisters are always shielded during facility operations by a transportation cask, a canister preparation platform, concrete floors and walls, the CTM shield bell and shield skirt, the WPTT, facility shield doors, and the TEV shield compartment. Loss of electrical power to any of these simply stops operations while maintaining shielding. For example, inadvertent shield bell and shield door motion can not occur in the absence of electrical power. Therefore, direct exposure to workers owing to loss of electrical power is considered to be beyond Category 2.

It has been shown that loss of electrical power in conjunction with other failures is screened out as an initiating event. Nevertheless, this compound failure mode is included in the initiating and pivotal event fault trees as appropriate. For example, the hoist brake on the CTM requires electrical power to remain unengaged. A loss of power would cut power to the brake, leading to its automatic engagement. If the brake fails in conjunction with a loss of power in this scenario, a drop of the load could occur, initiating an event sequence. This failure scenario is included in the CTM fault tree. For the overhead cranes, the initiating event frequencies are based on industry-wide empirical data for cranes. The ITS HVAC system depends on continued electrical power and it is explicitly modeled in the fault tree for this pivotal event.

6.0.3 Screening of Internal Initiating Events

All facility safety analyses, whether risk-informed or not, takes into account the physical conditions, dimensions, materials, human-machine interface, and other attributes such as operating conditions and environments, to assess potential failure modes and event sequences. Such accounting guides the assessment of what can happen, the likelihood, and the potential consequences. In many situations, it is obvious that the probability of a particular exposure scenario is very low. In many cases, it is impractical or unnecessary to actually quantify the probability when a non-probabilistic engineering analysis provides sufficient assurance and insights that permit the scenario to be either screened out or demonstrated to be bounded by another scenario.

Potential initiating events were qualitatively identified in *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37) for quantitative treatment in the present analysis. For completeness, some events that were identified in the event sequence development analysis are extremely unlikely or physically unrealizable and can reasonably be qualitatively screened from further consideration. A qualitative screening argument for certain internal initiating events is developed in the present analysis as documented in Table 6.0-2. The first column of Table 6.0-2 indicates the branch of the initiator event tree (where applicable) that pertains to the screened initiating event. Each branch of an initiator event tree represents an initiating event or an initiating event group that includes other similar initiating events and corresponds to a little bubble on an ESD (Ref. 2.2.37, Attachments F and G). Some of the initiating events that are addressed in Table 6.0-2 were implicitly screened out in the event sequence development analysis and for that reason there is no applicable event tree. The screening argument for internal flooding is presented in Section 6.0.4. The screened initiating events are assigned frequencies of zero in the quantification of the model.

Table 6.0-2. Bases for Screening Internal Initiating Events

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
WHF-ESD01-CSNF (#2) (Figure A5-2)	Rollover of a truck trailer carrying a transportation cask in the Cask Preparation Area or Transportation Cask Vestibule	For a truck trailer to roll over, its center of mass has to move laterally beyond the wheel base of the trailer. This could occur upon traversing a significantly uneven surface, running over a very large object, or turning sharply at high speed. There are no uneven surfaces in the Cask Preparation Area or the Transportation Cask Vestibule. The area in question has a flat concrete surface. There are no objects that could be run over that could significantly shift the trailer's center of mass. Turning sharply at high speed is not possible inside the building because the rooms are is too narrow and the truck comes to a complete stop outside the closed entrance door prior to the door opening and the truck entering. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
WHF-ESD07-DPC (#4) (Figure a5-14) WHF-ESD08-CSNF (#3) (Figure a5-15) WHF-ESD09-DPC (#4) (Figure a5-16)	Operator drops cask during cask preparation activities	The 20-ton auxiliary crane, rather than the 200-ton crane, is used in the lid-removal operation. Because the cask is not intentionally lifted in this step, dropping the cask would require a series of extraordinary human failures. For DPCs, a cask drop would require a series of human failures as follows: During lid removal, the crew must fail to remove some fraction of the lid bolts, fail to properly use the check list to verify bolt removal, and use the wrong crane (the 20-ton crane would be incapable of lifting the cask). The crane operator and at least two other crewmembers will be standing on the platform in direct view of the cask during lid removal and they all would have to fail to notice that the entire cask is being lifted before the bolts break. Therefore, event sequences associated with this initiating event are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part. For casks other than DPC casks, the lid is not removed from the cask at this point. Therefore, no configuration that could result in a crane lifting the cask occurs for such casks. This initiating event, as it relates to casks other than DPC casks, is considered to be unrealizable.
WHF-ESD10-DPC (#2) (Figure a5-17) WHF-ESD14-DPC (#3) (Figure a5-24)	Structural damage to transportation cask due to impact from the crane hook or rigging while under the cask preparation platform	In this operation, the lid is unbolted and the lid lift fixture is attached. The cask is flush or recessed with respect to the cask preparation station, and therefore cannot be impacted. Therefore, event sequences associated with these initiating events are considered to be physically unrealizable.
WHF-ESD13-TAD (#8) (Figure A5-23)	Canister dropped inside shield bell	Drops within the shield bell have been subsumed within event sequences for drops from the operational lift height, and not separately addressed. This is conservative because the drop height within the shield bell is less than the operational lift height.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened out from further analysis in Section 6.0.4.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Canister dropped into the Cask Unloading Room or Loading Room with no STC or aging overpack present	Lowering a canister by the CTM through a port without a STC or aging overpack present is prevented by interlocking the port slide gate opening with a sensor that shows there is a receptacle (STC or aging overpack) located beneath. The design incorporates an interlock to prevent the opening of the port slide gate when an STC or an aging overpack is not present (Ref. 2.2.31). The combination of (a) failure to stage the receptacle, (b) failure of more than one operator to notice that it is not staged, (c) failure of the hardwired interlock, and (d) drop of the canister are required for such an initiating event to occur. Considering the combination of unlikely events that must occur to cause this initiating event, event sequences involving this combination of failures are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.
WHF-ESD10-DPC (#2) (Figure A5-17)	Tipover of CTT	The CTT is designed to prevent tipover (Ref. 2.2.22, Section 3.2). The CTT is normally set on the floor inside a preparation platform. The size, weight, low center of gravity, and low speed of the CTT ensure that no tipover can occur. As such, tipover is not physically realizable during preparation activities. During transit, the CTT glides slowly on a cushion of air, an inch or less above the floor. If air pressure is lost, air to the CTT is cut and the CTT, with its load, settles to the floor. While the CTT is in transit, or after settling to the floor, any applied force from facility operations in incapable of tipping over the CTT. Due the slow travel of the CTT, a loss of air pressure or a collision with other equipment or a facility structure will not result in tipover. Therefore, tipover of the CTT is considered physically unrealizable for internal events. CTT tipover, however, is analyzed in the Seismic Event Sequence and Categorization Analysis.
WHF-ESD23-POOL (#5) (Figure A5-38)	Improper decontamination of DPC/STC	This event is not considered an event sequence. It is considered as part of the normal or off-normal operations, and mishaps during the normal operations are evaluated elsewhere.
WHF-ESD23-POOL (#4) (Figure A5-38)	Operator exposed during pool filter change-out	This event is not considered an event sequence. It is considered as part of the normal or off-normal operations, and mishaps during the normal operations are evaluated elsewhere.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
WHF-ESD26-TAD (#2) (Figure A5-42)	Failure to fully dry TAD canisters	As described in Section 6.0.7, NUREG-1567 (Ref. 2.2.91) discusses a process to evacuate water from SNF canisters. If the process is followed, the NRC has concluded in their various safety evaluation reports that there is reasonable assurance that less than 1 gram mole of water will be left in the canister. The YMP process will conform to this process. Hence failure to fully dry TAD canisters is screened out.
WHF-ESD27-TAD (#2) (Figure A5-44)	Operator fails to detect bad weld during inspection	As discussed in Section 6.0.6, bad welds are detected during the welding and drying process. The design of the welding machine incorporates weld testing device that test the weld as it is laid. In addition, the structural integrity of the weld is also confirmed during the TAD drying and inerting–if there is a crack on weld, the inerting pressure will not hold. Additional ultrasonic testing (UT) can be performed (if needed) to confirm the weld integrity after the TAD canister drying and inerting process. Based on these steps, the chance of having a bad weld is negligible, and the associated event sequence is screened from further consideration.
WHF-ESD30-DPC (#2) (Figure A5-48)	Operator exposed during decontamination operations	This event is not considered an event sequence. It is considered as part of the normal or off-normal operations, and mishaps during the normal operations are evaluated elsewhere.
ESD12-DPC-DOOR (Figure A5-20)	Conveyance carrying a cask, STC, or aging overpack collides with a shield door, causing the door to dislodge from its supports and fall onto the waste form	The shield doors are designed to withstand collision of the conveyance into the door without dislodging from their supports such that the stress of all support mechanisms of the door stay below yield. Therefore, this initiating event is considered physically unrealizable

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event tree	Water dilution event in WHF pool results in criticality	For normal operations, it is not physically possible to dilute the boron concentration in the WHF pool sufficiently to cause criticality and hence this event is screened out by the following argument. The only water source in Room 1016 is the de-ionized water system and this system does not have enough water to dilute the boron concentration to levels to cause criticality. According to *Utilities Facility Deionized Water System Supply Piping & Instrument. Diagram* (Ref. 2.2.25), the maximum amount of water that can be drained from de-ionized water system due to a pipe rupture is 19,600 gallons. The WHF pool contains 1.4 million gallons of water. *Pool Water Treatment and Cooling System* (Ref. 2.2.32). The addition of 19,600 gallons reduces the boron concentration by 1.4%. According to *Preclosure Criticality Safety Analysis* (Ref 2.2.35) the minimum required concentration of soluble boron in the pool is 2500 mg/L of boron enriched to 90 atom % ^{10}B. For all normal WHF pool operations, subcriticality is maintained crediting no more than 15% of this minimum required soluble boron concentration. Hence, there is a factor of safety of 85%/1.4% = 60.7 and water dilution is not a credible scenario leading to criticality in the WHF pool for normal operations.
No applicable event trees	Explosion of site prime mover fuel tank	The fuel tank of the site prime mover has safety features that preclude fuel tank explosion. Therefore, this initiating event is considered physically unrealizable.
WHF-ESD13-DPC (#3) (Figure A5-22) WHF-ESD13-TAD (#3) (Figure A5-17)	Side impact from a slide gate	Slide gate impacts during CTM transfer are included in the CTM fault tree as a cause of canister drop, rather than as an independent initiating event.
WHF-ESD13-DPC (#8) (Figure A5-22) WHF-ESD13-TAD (#8) (Figure A5-17)	Canister dropped inside shield bell (with CTM slide gate closed)	Drops within the shield bell are subsumed within the initiating event for drops from the operational lift height, and are not separately addressed. This is conservative because the drop height within the shield bell is less than the operational lift height.

Table 6.0-2. Bases for Screening Internal Initiating Events (Continued)

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Moderator introduced during sampling event	During sampling of the DPC or transportation cask with uncanistered fuel assemblies, there are no credible source of water intrusion. Connections of the sampling lines are designed to prevent wrong hook ups. Thus, the associated event sequence is considered to be not realizable.

NOTE: Initiator event trees are provided in Attachment A in the figures cited. The branch numbers are shown in each figure under the column labeled "#". AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ST = site transporter; STC = shielded transfer cask; TAD = transportation, aging, and disposal canister.

Source: Original

6.0.4 Screening of Internal Flooding as an Initiating Event

By the definition of an event sequence, a flood inside a facility would be an initiating event if it led to a sequence of events that would either breach waste containers, causing a release, or caused elevated radiological exposure without a release (i.e., direct exposure of personnel). Internal floods, whether caused by random failure or earthquakes, emerge from two sources. The first is inadvertent actuation of the fire-suppression system. The second is failure of water-carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems. Drains, channels and curbs are situated to remove water from these sources. However, the following discussion does not rely on these.

Transportation casks, canisters, and waste packages are not physically susceptible to breach associated with water in the short-term. With extremely long exposure to water, corrosion may be a factor but intervention to drain water from the buildings would prevent such exposure. Short-term breaches do not occur owing to exposure to water. Canisters are surrounded by transportation casks, and waste packages. Casks are elevated as all times at least five feet above the floor by railcar or truck and canister transfer trolley. Waste packages are similarly elevated on the waste package transfer trolley. Inside the TEV, the waste package is elevated approximately one foot above the floor. A lifted canister or/and cask is higher than these minimum elevations. Therefore, water from fire suppression and other water systems is unlikely to attain a depth that would contact transportation casks, waste packages, or canisters. Of greater significance, however, is that the fuel is contained in canisters within an overpack nearly all the time and these containers do not fail from short-term exposure to flood water. In this context, short-term is a time period that is at least 30 days but less than the length of time that significant corrosion may occur.

Water impingement on electrical equipment (e.g., motor control centers, motors, and switchgear cabinets) would ordinarily trigger circuit protection features that would open the circuit and cause a loss of electrical power (which is covered in Section 6.0.2.2). If a short circuit occurred as a result of water impingement, normal circuit protection features or overheating of the wires would subsequently open the affected circuit. In an extreme situation, an electrical fire might be started. Fires from all causes are covered in Section 6.5.

The possibility of inadvertent direct exposure of workers due to internal flooding is considered next. Direct exposure to workers during a flood would occur if shielding were disabled as a result of the flooding. Canisters are always shielded during facility operations by transportation casks, canister preparation platforms, CTT, concrete floors and walls, the CTM shield bell or shield skirt, or shield doors. Loss of electrical power to any of these simply stops operation without affecting the shielding. Flooding might also cause hot shorts in control boxes. However, hardwired interlocks between the CTM slide gate, shield bell skirt, and shield doors prevent such inadvertent motion. Therefore, internal flooding cannot initiate an event sequence that causes increased levels of radiological exposure.

Moderator intrusion into canisters resulting from event sequences that might breach a waste container are treated quantitatively as described in the pivotal event descriptions of Section 6.2.

6.0.5 Screening Argument for Release Due to Rupture of Bare Fuel in Transportation Cask Exposed to Fire

If a transportation cask containing bare fuel rods is exposed to fire, the fuel rods could be heated to the point of degradation, allowing release of radionuclides within the sealed transportation cask. If in addition, the fire reaches the top of the transportation cask and causes failure of the lid seals, the radionuclides could be released to the surroundings.

An assessment of the temperature at which spent fuel rods would fail is summarized in NUREG/CR 6672 (Ref. 2.2.83, Section 7.2.5.2). A critical review of accident conditions indicates that rod rupture is expected to occur at temperatures near 725°C to 750°C. After correcting for differences in burnup and internal pressure, data in the Cask Designers Guide suggest that spent fuel rods may fail due to creep rupture at temperatures as low as 700°C or require temperatures as high as 850°C. Because the release of cesium vapors will be greater when rods fail at higher temperatures than lower temperatures, the middle of the range, about 750°C, is taken as the temperature at which rods fail by thermal rupture.

The probability of fuel rod failure at 750°C is 2.7×10^{-4} given exposure to fire (Table D2.1-11). The probability of exposure of a transportation cask containing bare fuel to fire in the WHF is 1×10^{-5} (Attachment F, Table F5.7-2). The overall probability that a transportation cask is exposed to a fire sufficient to cause rupture of the fuel rods contained within and release of radionuclides to the surroundings is 3×10^{-9} for the WHF.

The analysis includes some extreme conservatisms:

- A view factor of 1 was used for determining the probability that the fuel rods would heat up to the failure temperature given exposure of the transportation cask to fire. Not all fires to which a transportation cask is exposed would be positioned such that a complete radiation exposure would be possible.

- The lid seals are at the top of the transportation cask which is approximately 15 feet tall. Only a limited fraction of the fires to which a transportation cask would be exposed would be large enough to cause failure of the lid seals even if the lower portion of the cask got hot enough to allow rupture of the fuel rods.

Thus it is concluded that this event is beyond Category 2 and can be screened from further analysis.

6.0.6 Screening of Operator Failing to Detect Bad Welds During Inspection

TAD canister closure is the process that closes the loaded TAD canister by welding the shield plug and fully draining and drying the TAD canister interior, followed by backfilling the TAD canister with helium and fully welding the TAD canister lid around its circumference onto the body of the TAD canister.

The process control program for the closure welds produced by the TAD canister closure system is controlled as a special process by the Quality Assurance Program (DOE 2007).

TAD canister closure is done at the TAD canister closure station in the cask preparation area. The shielded transfer cask containing a loaded TAD canister is transferred from the pool to the TAD canister closure station using the cask handling crane. The shielded transfer cask lid is unbolted and then removed using the TAD canister closure jib crane. The TAD canister is then partially drained via the siphon port in order to lower the water level below the shield plug in preparation for welding. The TAD canister welding machine is positioned onto the TAD canister shield plug using the TAD canister closure jib crane, and the shield plug is welded in place. After a weld is completed, visual examination of the weld is performed in addition to the eddy current testing and ultrasonic testing that are performed by the TAD canister welding machine.

A draining, drying, and inerting system is connected to the siphon and vent ports in the shield plug and used to dry the interior of the TAD canister, followed by backfilling it with helium gas. Port covers are then placed over the siphon and vent ports and welded in place using the TAD canister welding machine. The TAD canister welding machine is removed, and the outer lid is placed onto the TAD canister using the TAD canister closure jib crane. The TAD canister welding machine is positioned onto the TAD canister outer lid, and the lid is welded in place. The TAD canister welding machine is removed, and the shielded transfer cask lid is placed onto the shielded transfer cask using the TAD canister closure jib crane and installed. Hoses are connected to the fill and drain ports on the shielded transfer cask, and the water is sampled for contamination. If the water is clean, the ports are opened to drain the annulus between the TAD canister and the shielded transfer cask. If the water is contaminated, then the annulus is flushed with treated borated water as needed. A drying system is then used to dry the annulus. The potential for contamination is kept to a minimum by the use of the inflatable seal.

The qualification of the TAD canister final closure welds is in accordance with SFPO-ISG-18 (Ref. 2.2.89). Adherence to this guidance is deemed to provide reasonable assurance that weld defects occur at a low rate.

6.0.7 Water in TAD Canister

NUREG-1567 (Ref. 2.2.91) discusses a process to evacuate water from SNF canisters. If the process is followed, the NRC has concluded in their various safety evaluation reports that there is reasonable assurance that less than 1 gram mole of water will be left in the canister. The YMP process will conform to this process.

Potential initiating events, should water be left in the canister, during the preclosure period, include saturated vapor pressurization or development of hydrogen and subsequent recombination reactions. Facility operating processes are similar to those covered by 10 CFR Part 71 and 10 CFR Part 72 (Ref. 2.3.3 and Ref. 2.3.4), (e.g., in the use of cranes) and there are no processes or conditions that would exacerbate adverse effects associated with abnormal amounts of water retention. These processes are highly reliable as indicated by no overpressure ruptures of canisters on utility sites to date.

Hydrogen generation by radiolysis is a very slow process requiring decades to generate flammable or explosive mixtures in TAD sized canisters. However, if sufficient water is left in the canister, overpressurization owing to hydrogen recombination is extremely unlikely to occur because of several reasons.

1. Hydrogen and oxygen must be well mixed for an efficient burn or explosion– because of density differences; gaseous hydrogen would tend to separate and stay separate from oxygen.

2. Detonation from a rapidly moving flammable wave front is physically unrealizable for closed containers.

3. An ignition source must be present and water vapor tends to inhibit hydrogen combustion by raising the lower flammability limit.

4. Typically, burning of hydrogen and oxygen in close proximity when not well mixed would generate heat intermittently allowing time for heat removal through the canister walls.

5. Any such burning would tend to drive apart the hydrogen and oxygen components.

It is judged that the joint probability of water remaining in the canister and the confluence of all factors that might lead to an overpressurization during the preclosure period is beyond Category 2.

Vapor pressurization would occur soon after TAD canister welding as the water vapor at saturation equilibrates with the internal canister temperature. Internal canister temperatures will normally exceed 212 F causing boiling and vaporization. If sufficient water is left, then the vapor and water would come to its saturation pressure. Saturated vapor pressures would not exceed canister internal pressure capability during normal conditions. During off-normal conditions of abnormal heat removal (e.g. loss of building air flow), saturated vapor temperatures may challenge the integrity of the canister. Overpressurization would occur within a couple of hours after the TAD canister is closed while it is still in the WHF. Rupture of the canister under these conditions are not expected to be worse than rupture as a result of a fire in which hoop stress limits are exceeded. The coincidence of release owing to water left in a canister is expected to be beyond Category 2 because of the low frequency of water left in the canister, low conditional probability of large amounts of water that would lead to saturated vapor conditions, and low frequency of loss of cooling.

6.1 EVENT TREE ANALYSIS

The event trees that are quantified in this analysis were developed from ESDs in the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37, Attachments F and G). This section describes the use of SAPHIRE (Section 4.2) to model event sequences. The event trees are discussed and presented in Attachment A.

6.1.1 Event Tree Analysis Methods

6.1.1.1 Linked Event Trees and Fault Trees

As described in Section 4, the PCSA uses linked event trees with linked fault trees to calculate the frequency of occurrence of event sequences. The SAPHIRE computer program (Section 4.2) is used for this purpose. The event tree quantification is supported by fault tree analysis (FTA) (Section 6.2 and Attachment B), PEFA (Section 6.3.2 and Attachment D), and HRA (Section 6.4 and Attachment E). The YMP preclosure handling is performed using four kinds of buildings as summarized below:

1. The Receipt Facility (RF) accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.

2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program (NNPP) for placement in waste packages destined for emplacement in the repository emplacement drifts.

3. The WHF accepts DPCs and transportation casks containing uncanistered commercial SNF and transfers the SNF to TAD canisters which are destined for the CRCF or the aging pads.

4. The Initial Handling Facility (IHF) accepts SNF canisters from the NNPP and some canisters containing high-level radioactive waste for placement in waste packages destined for emplacement in the repository emplacement drifts.

Preclosure waste handling as modeled in the PCSA also includes TEV and Subsurface Operations. The TEV accepts waste packages from the CRCF and IHF and, by means of rail, transports and deposits it into its designated location in the emplacement drifts. All other extra-building transportation, low-level waste handling, and balance of plant is called Intra-Site Operations.

Event sequences are developed for each of the four building types, TEV and Subsurface Operations, and Intra-Site Operations. Because each type of waste container in the WHF has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container. As described in the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37), event sequences are also developed separately for each major group of waste handling processes by location within the building. Therefore, event sequences also distinguish among the various steps in waste handling.

As described in Section 4.3, event sequences result in one of the following end states:

1. "OK."
2. Direct Exposure, Degraded Shielding.
3. Direct Exposure, Loss of Shielding.
4. Radionuclide Release, Filtered (HVAC).
5. Radionuclide Release, Unfiltered (HVAC system is not operating).
6. Radionuclide Release, Filtered, Also Important to Criticality.
7. Radionuclide Release, Unfiltered, Also Important to Criticality.
8. Important to Criticality.

Radionuclide release describes a condition where radioactive material has been released from the container creating a potential inhalation or ingestion hazard, accompanied by the potential for immersion in a radioactive plume and direct exposure.

The SAPHIRE computer program has advanced features that permit the analyst to control the inputs and conditions for quantifying linked event trees and fault trees. One feature is the use of "basic rules" by which the analyst tells the program how and when to link certain variations of fault trees and basic event data that describe a given initiating and pivotal event. This allows path dependent development of sequence minimal cut sets and probabilities.

The primary inputs to the program are the following:

- Event tree logic models
- Fault tree logic models for initiating and pivotal events
- Initiating event frequencies derived from waste-form throughputs and numbers of opportunities for initiating an event sequence
- Basic event data that provides failure rates for active and passive equipment and for HFEs. (The basic event data also includes a probability distribution of uncertainty associated with each basic event. The event tree and fault tree logic models are linked to the basic event library.)

Each basic event is characterized by a probability distribution. SAPHIRE's Monte Carlo sampling method is employed to propagate the uncertainties to obtain event sequence mean values and parameters of the underlying probability distribution such as variance. As described in Section 4.3.6, categorization is done on aggregated event sequences, whose resultant probability distributions are also obtained by Monte Carlo simulation. SAPHIRE accounts for the correlation between analogous basic events sharing the same reliability information, which ensures the spread of the probability distribution of the event sequences in which these basic events intervene is not underestimated.

6.1.1.2 Initiator, System-Response, and Self-Contained Event Trees

Event sequences are described and graphically depicted using one or two event trees depending on whether the ESD considered has one or more initiating events:

1. **Self-contained event trees.** Self-contained event trees are used when only one initiating event appears in the corresponding ESD (Ref. 2.2.37, Attachment F). An example is WHF-ESD12-DPC, which is shown in Figure A5-20 in Attachment A. The feed on the left side of the event tree is an event that represents the frequency of challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of transportation casks containing DPCs that are handled over the preclosure period in the WHF. The initiating event is presented next, followed by the pivotal events. By convention, the description of each branching event is stated as a success. The branching under each event heading represents success by an upward branch and failure by a downward branch. If a given pivotal event cannot occur in a given sequence due to a prior pivotal event or is irrelevant to the sequence, it does not appear in the event sequence as illustrated in the corresponding ESD and no branching occurs in the event tree. Each pathway through a self-contained event tree terminates in an end state. End states that are labeled "OK" mean that the sequence of events does not result in one of the specifically identified undesired outcomes. "OK" often means that normal operation can continue. The undesired end states represent a release of airborne radioactivity, a direct exposure to radiation, or a potential criticality condition.

2. **Separate initiator and system-response event trees**. Separate event trees for initiating events and the system response are used when more than one initiating event appears in the corresponding ESD (Ref. 2.2.37, Attachment F). The initiator event tree decomposes a group of initiating events into the specific failure events that comprise the group. For example, an initiator event tree, WHF-ESD01-CSNF, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, RESPONSE-TCASK-CSNF, is shown in Figure A5-3. The feed to the left side of the initiator event tree is an event that represents the frequency of challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of transportation casks containing uncanistered spent nuclear fuel that are received during the preclosure period. Initiator event trees do not end at end states but transfer to a system response event tree. System response event trees contain only pivotal events. The user specifies the models to be used for the initiating events associated with each initiator event tree and the pivotal events associated with the corresponding system response event tree by writing "basic rules," which are attached to the initiator event tree in SAPHIRE. In accordance with the user-specified basic rules, the SAPHIRE program links a specific fault tree model or basic event to a given initiating event or pivotal event. Because the conditional probability of each pivotal event may be specific to the initiating event for each event sequence, the same system response event tree is quantified by SAPHIRE as many times as there are initiating events in the initiator event tree.

6.1.1.3 Summary of the Major Pivotal Events

A self-contained event tree or a system response event tree may include pivotal events concerning the success or failure of the waste package, transportation cask, canister, shielding properties, HEPA filtration availability, and moderator intrusion susceptibility. The pivotal events are summarized in Attachment A, Section A3.

Each of the specific failure events included in a self-contained or system-response event tree may be linked to a basic event or to the top event of a fault tree. Two kinds of fault trees are developed and represented in Attachment B. The first type represents equipment fault trees including HFEs that contribute directly to the specific pivotal or initiating event. The second type links initiating and pivotal events to these equipment fault trees (via transfer gates) and miscellaneous events. This second type is called a linking or connector fault tree. The equipment fault tree models are, in turn, linked to basic event reliability information separately entered into SAPHIRE. Some of the pivotal events do not have associated fault trees because they are linked directly to basic events in the reliability database entered into SAPHIRE. Section 6.2 provides more information about the reliability information developed for this analysis.

6.1.2 Waste Form Throughputs

Each initiator event tree and self-contained event tree begins with the container throughputs, that is, the numbers of waste form units (such as casks, canisters, or fuel assemblies) to be handled over the life of the WHF. The throughputs are identified in Table 6.1-1 and are drawn into the descriptions of specific event trees as needed. With the number of waste form units as a multiplier in the event tree and the initiating events specified as a probability per waste form unit, the value passed to the system response is the number of occurrences of the initiating event expected over the life of the facility.

Table 6.1-1. Waste Form Throughputs for the WHF Over the Preclosure Period

Waste Form Unit	WHF Throughput Over the Preclosure Period	Comment
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	3,775	Total number of transfers
Transportation casks or horizontal shielded transfer casks containing a DPC	346	One canister per cask
Aging overpack containing a DPC	346	One canister per aging overpack
Aging overpack containing a TAD canister	1,165	One canister per aging overpack
DPCs (64 BWR or 25 PWR SNF assemblies per canister)	346	Same as number of DPC casks, Number of transfers by a CTM inside the WHF.
TAD canisters produced at the repository	1,165	Same as number of TAD canister casks (44 BWR or 21 PWR SNF assemblies per canister)
SNF assemblies transferred in the pool of the WHF (from a bare-fuel transportation cask or DPC to a staging rack, and from a staging rack to a TAD canister)	66,208	Total number of transfers

NOTE: BWR = boiling water reactor; CTM = canister transfer machine; DPC = dual-purpose canister; PWR = pressurized water reactor; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal; WHF = Wet Handling Facility.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4).

6.1.3 Guide to Event Trees

Event trees are located in Attachment A. Table 6.1-2 contains the crosswalk from the ESD (Ref. 2.2.37, Attachment F) to the initiating event tree and response tree figure location in Attachment A.

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD01	Event Sequences for Activities Associated with Receipt of Transportation Cask with Spent Nuclear Fuel in the Transportation Cask Vestibule and Movement into Cask Preparation Area	WHF-ESD01-CSNF	Figure A5-2	RESPONSE-TCASK-CSNF	Figure A5-3

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD02	Event Sequences for Activities Associated with Receipt of Transportation Cask with DPC in the Transportation Cask Vestibule and Movement into Cask Preparation Area	WHF-ESD02-DPC	Figure A5-4	RESPONSE-TCASK-DPC	Figure A5-5
WHF-ESD03	Event Sequences for Activities Associated with Receipt of Aging Overpack in the Site Transporter Vestibule	WHF-ESD03-AODPC	Figure A5-6	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD04	Event Sequences for Activities Associated with Receipt of Horizontal STC/DPC in the Transportation Cask Vestibule and Movement into the Cask Preparation Area	WHF-ESD04-DPC	Figure A5-8	RESPONSE-STC1	Figure A5-9
WHF-ESD05	Event Sequences for Activities Associated with TC/CSNF Removal of Impact Limiters, Upending, and Removal from Conveyance and Transfer to Preparation Station	WHF-ESD05-CSNF	Figure A5-10	RESPONSE-TCASK-CSNF	Figure A5-3
WHF-ESD06	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending, and Removal of Transportation Cask from Conveyance and Transfer to CTT	WHF-ESD06-VTC WHF-ESD06-TTC	Figure A5-11 Figure A5-13	RESPONSE-TCASK	Figure A5-12
WHF-ESD07	Event Sequences for Associated Cask Preparation Activities (i.e., Installation of Lid Lift Fixture on Transportation Cask/DPC)	WHF-ESD07-DPC	Figure A5-14	RESPONSE-TCASK	Figure A5-12

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD08	Event Sequences for Associated Cask Preparation Activities (i.e., Installation of Cask Lid Lift Fixture on Transportation Cask/CSNF)	WHF-ESD08-CSNF	Figure A5-15	RESPONSE-TCASK-CSNF	Figure A5-3
WHF-ESD09	Event Sequences for Associated Cask Preparation Activities (i.e., Lid Removal, or Installation of DPC Lid Lift Fixture, STC/DPC or Transportation Cask/DPC)	WHF-ESD09-DPC	Figure A5-16	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD10	Event Sequences Associated with Transfer of Cask on CTT from Preparation Area to Cask Unloading Room	WHF-ESD10-DPC	Figure A5-17	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD11	Event Sequences Associated with Transfer of an Aging Overpack/DPC or Aging Overpack/TAD on Site Transporter, through Site Transporter Vestibule, Aging Overpack Access Platform, and Loading Room (Receipt or Export)	WHF-ESD11-AODPC WHF-ESD11-AOTAD	Figure A5-18 Figure A5-19	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD12	Event Sequences Associated with Aging Overpack (DPC or TAD) on Site Transporter or STC/TAD on CTT Colliding with Cask Loading Shield Door	WHF-ESD12-DPC WHF-ESD12-TAD	Figure A5-20 Figure A5-21	N/A	N/A
WHF-ESD13	Event Sequences for Activities Associated with the Transfer of a Canister to or from an Aging Overpack, STC, or Transportation Cask with the CTM	WHF-ESD13-DPC WHF-ESD13-TAD	Figure A5-22 Figure A5-23	RESPONSE-CANISTER1	Figure A5-7

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD14	Event Sequences for Activities Associated with the Transfer of STC/DPC from the Cask Unloading Room to the Preparation Station	WHF-ESD14-DPC	Figure A5-24	RESPONSE-STC1	Figure A5-9
WHF-ESD15	Event Sequences for Activities Associated with the Transfer of STC/DPC from the Preparation Station to the DPC Cutting Station	WHF-ESD15-DPC	Figure A5-25	RESPONSE-STC1	Figure A5-9
WHF-ESD16	Event Sequences for Activities Associated with the STC/DPC Preparation at the Preparation Station	WHF-ESD16-CSNF	Figure A5-26	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD17	Event Sequences for Activities Assoicated with the STC/DPC Preparation Activities at the DPC Cutting Station	WHF-ESD17-DPC	Figure A5-28	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD18	Event Sequences for Activities Associated with the STC/DPC Preparation Activities – DPC Cutting at DPC Cutting Station	WHF-ESD18-DPC	Figure A5-29	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD19	Event Sequences Associated with Transfer of STC/DPC from DPC Cutting Station to Pool Ledge	WHF-ESD19-DPC	Figure A5-30	RESPONSE-POOLMOVE RESPONSE-STC1	Figure A5-31 Figure A5-9
WHF-ESD20	Event Sequences Associated with Transfer of Transportation Cask/CSNF from Preparation Station to Pool Ledge	WHF-ESD20-CSNF	Figure A5-32	RESPONSE-POOLMOVE RESPONSE-TCASK-CSNF	Figure A5-31 Figure A5-3
WHF-ESD21	Event Sequences for Activities Involving Lowering STC/DPC or Transportation Cask/CSNF to the Pool Floor	WHF-ESD21-CSNF WHF-ESD21-DPC WHF-ESD21-TAD	Figure A5-33 Figure A5-34 Figure A5-35	RESPONSE-POOLMOVE	Figure A5-31

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD22	Event Sequences for Pool Activities Involving Transfer of Fuel Assembly to TAD Canister or Fuel Staging Rack	WHF-ESD22-FUEL	Figure A5-36	RESPONSE-POOLCONFINE	Figure A5-37
WHF-ESD23	Event Sequences for Activities Associated with Handling of Low Level Liquid Waste	WHF-ESD23-POOL	Figure A5-38	N/A	N/A
WHF-ESD24	Event Sequences for Activities Associated with the Transfer of STC/TAD from the Pool Ledge to the TAD Canister Closure Station	WHF-ESD24-TAD	Figure A5-39	RESPONSE-POOLMOVE RESPONSE-STC1	Figure A5-31 Figure A5-9
WHF-ESD25	Event Sequences for Activities Associated with Preparation of STC/TAD and Closure of TAD Canister	WHF-ESD25-TAD	Figure A5-40	RESPONSE-TAD	Figure A5-41
WHF-ESD26	Event Sequences for Activities Associated with Closure of TAD Canister – TAD Drying and Inerting Process	WHF-ESD26-TAD	Figure A5-42	N/A	N/A
WHF-ESD27	Event Sequences for Activities Associated with TAD Closure – Welding, Drying, and Inerting Process	WHF-ESD27-TAD	Figure A5-43	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD28	Event Sequences for Activities Associated with Transfer of STC/TAD from TAD Closure Station to CTT in the Preparation Station	WHF-ESD28-TAD	Figure A5-44	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD29	Direct Expsoure Event Sequences for Activities Associated with Cask Preparation or CTM Movement	WHF-ESD29-DPC WHF-ESD29-TAD	Figure A5-45 Figure A5-46	N/A	N/A
WHF-ESD30	Direct Exposure Event Sequences for Activities Associated with Pool Operations	WHF-ESD30-DPC WHF-ESD30-FUEL	Figure A5-47 Figure A5-48	N/A	N/A

Table 6.1-2. Figure Locations for Initiating Event Trees and Response Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD31	Event Sequences for Activities Associated with Fires Occurring in the WHF	WHF-ESD31-CSNF WHF-ESD31-DPC WHF-ESD31-TAD	Figure A5-49 Figure A5-51 Figure A5-52	RESPONSE-FIRE	Figure A5-50

NOTE: CSNF = commercial spent nuclear fuel; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; IE = initiating event; STC = shielded transportation cask; TAD = Transportation, aging, and disposal canister; TC = transportation cask; VTC = a transportation cask that is upended on a railcar.

Source: Attachment A, Table A5-1

6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS

6.2.1 Approach to Analysis of Initiating and Pivotal Events for Linking to Event Sequence Quantification

Section 4.3.2 provides a brief introduction to the application of FTA for initiating and pivotal events, including an example fault tree. Many of the initiating events involve faults in complex machinery for which no historical data exists at the system level, an exception being, historical data on load drops from cranes. Therefore, FTA is employed to map elements of equipment design and operational features to various failure modes of components down to a level of assembly, termed "basic events" for which historical data is available. Attachment B presents the fault tree logic and stand-alone quantifications.

Much of the equipment used in the WHF is also used in other surface facilities and the Intra-Site operations. Furthermore, a given system, such as the site transporter, may affect the event sequences for several operational nodes of the same facility or several kinds of waste forms, as it does for the WHF. Therefore, the logic of the fault trees described in this section and Attachment B are linked to event trees where appropriate, via an intermediate top event name that is unique to the event sequence per the waste form involved and operational node. In this way, the logic structure of the system fault tree may be used over and over but, by virtue of the rules feature of SAPHIRE, the inputs to each fault tree can be tailored to fit the event sequence.

The fault trees are linked to the event trees via the initiating event tree rules file and the application of linking fault trees. The rules file specifies the names of the linking fault trees for initiating event and pivotal event fault trees to be substituted into the event tree top events during quantification. The rules files also specify the use of particular values for basic events and other probabilistic factors that affect the event sequence quantification. The linking fault trees have unique names for the facility and the operational nodes for each event tree. The linking fault trees are very simple, usually having a single top event that is an OR gate that connects to one of the system fault trees. This allows for application of unique top event probabilities to the different initiating events modeled in the initiating event tree.

Attachment B, Sections B1 through B9 presents all of the system fault trees. This section describes the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B10 presents the linking fault trees used in the WHF analysis. The linking fault trees are self explanatory. No quantification is performed for the linking trees alone.

A top event occurs when one of the success critera for a given SSC fails to be achieved. At least one success criteria is defined for each system. Multiple success criteria are defined for systems that perform multiple safety functions in the WHF.

Each of the top events for the initiating event fault trees represent the conditional probability that the top event will occur when the system is put into service. That is, the results of the FTA answer a question such as "what is the probability given each canister lift that the CTM drops the canister, given a lift?" The expected number of canister drop initiating events during the preclosure period is the product of the number of times a canister is lifted during the preclosure operations and the conditional probability of the top event. Such values for the expected number of canister drops are not developed directly, however. Instead, the initiating event tree in SAPHIRE links the various fault tree logic models to the canister, or other waste form, and the throughput values to generate the initial portions of event sequence cut sets that are subsequently processed as part of the solution of the complete event sequence that includes pivotal events.

By contrast, the top event for the confinement function of the HVAC represents the conditional probability that the confinement feature is not achieved for the required duration following an airborne release of radioactive material inside the WHF. The quantification of the top event, as summarized in Section 6.2.2.7 and detailed in Attachment B, Section B7, is expressed as unavailability. The results provide insight into the reliability of the HVAC and its contribution to event sequence quantification. Again, the quantified top event is not used directly in the event sequence quantification. Instead, the fault tree logic for the HVAC is linked to event sequence analysis via SAPHIRE.

In general, each of the FTAs in Attachment B is developed to include both 1) HFEs, and 2) mechanical failures that result in the occurrence of the top event. The HFEs include postulated unintended operator actions that could potentially occur during the facility activity and, as applicable, hardware failures for those SSCs whose function are to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (electrical, mechanical, etc.) and failures from the loss of a supporting system (e.g., loss of power).

For quantification of the probability of the top event, failure probabilities are developed for each basic event (hardware or HFE) and are used to compute the probability of each cut set. For component failure data that is expressed as "failures per hour," a "mission time" must be defined. In many instances in the FTA quantification, a mission time of one hour is used if this value is conservative. Where mission time is critical, appropriate times are justified and incorporated into the event sequence quantification. Hardware failure probabilities are taken from the reliability analysis data discussed in Sections 6.3. HFE probabilities are taken from the HFE analysis discussed in Section 6.4.

Uncertainties in the probabilities of basic events are included in the inputs to the SAPHIRE analysis. The uncertainties are propagated through the FTA to yield the uncertainty distribution of the top event.

Issues that are addressed in the fault trees, in addition to the mapping of the descriptions of the physical system into a fault tree logic diagram based on explicit effects of mechanical and hardware failures, include the following:

- Basic event data
- Common-cause and common mode failures such as failures induced by common training, maintenance practices, fabrication, common electrical supplies, etc.
- Support systems and subsystems such as filtering (HVAC, HEPA filters), electrical, etc.
- System interactions
- HFEs
- Control logic malfunctions.

The following subsections provide summaries of the analyses detailed in Attachment B. For each fault tree, the following information is provided:

- Physical description
- Operation
- Control system
- System/pivotal event success criteria
- Mission time
- Fault tree results.

6.2.2 Summary of Fault Tree Analysis

6.2.2.1 Site Prime Mover Fault Tree Analysis

The FTA is detailed in Attachment B, Section B1. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B1 for sources of information on the physical and operational characteristics of the SPM.

6.2.2.1.1 Physical Description

The site prime mover (SPM) is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs for both the Intra-Site operations and within the WHF. Movement of the SPM with railcars (termed SPMRC) or SPM with truck trailers (termed SPMTT) within the WHF is limited to the entry vestibule and the Cask Preparation Room.

Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations. The driving and braking power comes directly from the road tires, as they are in contact with the rails. A diesel engine provides the energy to operate the SPM outside the facilities. Inside the WHF, the SPM is electrically driven via an umbilical cord (or remote control) from electrical power obtained from the WHF main electrical supply.

6.2.2.1.2 Operations

In-facility SPM operations begin after the SPM has positioned the railcar or truck trailer outside the WHF. The site prime mover diesel engine is shut down and the outer is opened. Facility power is connected to the SPM for all operations inside the facility. The operator connects the pendant controller or uses a remote (wireless) controller to move the SPM to push the railcar or truck trailer into the vestibule.

In the event of loss of power, the SPM is designed to stop, retain control of the railcar or truck trailer, and enter a locked mode where it remains until operator action is taken, to return to normal operations.

6.2.2.1.3 Control System

A simplified schematic of the functional components on the SPMRC/truck trailer is shown in Attachment B1, Figure B1.2-1.

The control system provides features for preventing initiating events:

- The SPM is designed to stop whenever: 1) commanded to stop, or 2) when there is a loss of power.
- The operator can stop the SPM by either commanding a stop from the start/stop button or by releasing the palm switch which initiates an emergency stop.
- At anytime there is a loss of power detected, the SPM will immediately stop all movement and enter into “lock mode” safe state. The SPM will remain in this locked mode until power is returned and the operator restarts the SPM.

6.2.2.1.4 System/Pivotal Event Success Criteria

Success criteria for the SPM are the following:

- Prevent SPMRC AND SPMTT collisions
- Prevent SPMRC derailment
- Prevent SPMTT rollover.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event of a fault tree for the SPM.

6.2.2.1.5 Mission Time

A nominal one-hour mission time is used to calculate the failure probability for components having a time-based failure rate. One hour is conservative because it does not require more than one hour to disconnect the SPM from the railcar and remove it from the facility. Otherwise, failure-on-demand probabilities are used.

For railcar derailment, the probability is based on the distance traveled inside the WHF (0.04 miles) and industry data derailment rate of 1.18E-5 per hour traveled (Attachment C, Table C4-1, DER-FOM).

6.2.2.1.6 Fault Tree Results

The detailed description in Attachment B, Section B1 documents the application of basic event data, CCFs, and HRA.

The SPMRC or SPMTT has three credible failure scenarios:

1. SPMRC collides with WHF structures.
2. SPMTT collides with WHF structures.
3. SPMRC Derailment.
4. SPMTT Rollover.

Each failure mode may occur with various waste forms that are received in the transportation casks.

Results of the analysis are summarized in Table 6.2.-1.

Table 6.2-1. Summary of Top Event Quantification for the SPM

Top Event	Mean Probability	Standard Deviation
SPMRC collides with WHF structures	4.3E-03	1.1E-02
SPMTT collides with WHF structures	4.3E-03	1.0E-02
SPMRC derailment	4.7E-07	7.4E-09
SPMTT rollover (operator error)	0.0E+00	0.0E+00

NOTE: RC = railcar; SPM = Site Prime Mover; TT = truck trailer; WHF = Wet Handling Facility;

Source: Attachment B, Section B1, Figures B1.4-1, B1.4-6, B1.4-11 and Section B1.4.4.5

6.2.2.2 Cask Transfer Trolley Fault Tree Analysis

The FTA for the CTT is detailed in Attachment B, Section B2. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B2 for sources of information on the physical and operational characteristics of the CTT.

6.2.2.2.1 Physical Description

The CTT is an air powered machine that is used to transport various vertically oriented transportation casks from the Cask Preparation Area to the Cask Unloading Room. The trolley consists of a platform, a cask support assembly, a pedestal assembly, a seismic restraint system, and an air system.

The CTT will handle a number of different casks so several different pedestals are used to properly position the cask height. Each pedestal sub-component is designed for its respective cask to sit down in a "cavity." In addition, the cask is restrained in the longitudinal and transverse directions by the cavity walls and restrained in the vertical down direction by the pedestal itself. This design also ensures the cask is positioned correctly. The trolley is positioned within a set tolerance under the cask port in the Canister Transfer Room using bumpers and stops that are bolted to the floor of the Cask Unloading Room and which are designed with bolts that would break to allow the CTT to slide during a seismic event.

In addition, the cask is restrained by two electric powered linkage systems that prevent side motions during a seismic event. Different cask diameters are handled by bolting unique interface clamps on the seismic restraints. When the restraint system is properly positioned next to the cask, two locking pins are pneumatically actuated to secure the position of the system. If the locking pins are not secured, the CTT will not be able to power up and move/levitate.

The facility compressed air supply inflates air casters beneath the trolley platform, which allow the CTT to rise above the steel floor. The platform mounted hose reel has an air-powered return, a ball valve shut-off, quick disconnect fittings, and a safety air fuse. A main "off/on" control valve and separate flow control/monitoring valves for each air bearing allow adjustment and verification of pressure/flow for each individual bearing. Interlocks for the air are provided to verify the main incoming pressure is not too high, and to verify that all bearings have sufficient air pressure.

End mounted turtle style drive units that are 360-degrees steerable, are used to steer the CTT. Traction is produced by down-pressure on the wheels provided by a small air bag on each drive unit.

The CTT is evaluated for a collision with another object while carrying the cask. The speed of the drives, 10 feet per minute (fpm), has been set so that the forces the cask experiences during a seismic event would envelope a collision. The speed is controlled in two ways. First, the electrical control system is designed to only give a proportional signal to the air valve that produces a speed of 0 to 10 fpm. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, allows a maximum amount of air through at any time to prevent a "run-away" condition.

6.2.2.2.2 Operation

Initially, the CTT is located in the Cask Preparation Area with the battery fully charged, the seismic restraints retracted, and with no air or electrical power connected. Based on the next planned cask to be loaded onto the trolley, the corresponding pedestal components are installed

into the base, and bumpers are bolted onto the seismic restraints and supports. The air hose is then connected to the CTT.

The overhead crane moves a cask onto the pedestal. With the cask still attached to the crane, the operator remotely operates the seismic restraints and secures the cask to the CTT. When the restraints are in place, the locking pins are pneumatically inserted remotely. With the cask secured to the CTT, the overhead crane is disengaged from the cask.

When the locking pins are inserted properly, an interlock allows the air bearings and drive motors to be operated. Once all preparations of the cask are complete, the CTT can be raised and moved to the Canister Transfer Room. Guides bolted to the floor insure that the CTT can only move forward and back, and will position the CTT so that the cask is directly below the transfer port. Once in position, the air pressure to the bearings is stopped and the CTT rests in position. The shield doors that separate the Cask Preparation Area from the Canister Transfer Room are then closed.

6.2.2.2.3 Control System

The control system is relay based and includes a pendant station as its operator interface.

No programmable logic controller (PLC) is used–all interlocks are hard wired. The pendant is a standard crane pendant that has all of the controls for the unit including:

- Deadman handle – operator must depress both handles to allow air to flow to the system so the CTT can levitate or move horizontally.
- E-stop (emergency stop) button on the pendant control and on the CTT.
- Clockwise/counterclockwise momentary switch to turn the drive units for horizontal movement. This rotational characteristic is used to move the CTT to storage or maintenance location after it leaves the Cask Preparation Area.
- Forward/reverse switch to determine direction of the drive units.
- Drive speed – variable speed control switch.
- Cask restraint – selector switch that actuates the motor to close the restraints and automatically engage the locking pin.

During normal operations, the controls operate off a battery system contained on the CTT. Only one operator is needed to drive the CTT since it only travels in one direction when it is carrying a cask.

The main air supply valve is a pilot operated solenoid valve that is fail safe (i.e., it is a spring valve that closes upon loss of electrical power or loss of air pressure). The air supply valve opens when the locking pins actuate the limit switches and the pendant deadman switches are actuated.

6.2.2.2.4 System/Pivotal Event Success Criteria

Success criteria for the CTT are the following:

- Ensure the CTT remains stationary with no spurious movement during transportation cask placement onto the CTT, transportation cask preparation, or during unloading.
- Prevent collisions while moving the CTT with cask from the Cask Preparation Area to the Cask Unloading Room.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event of a fault tree for the CTT.

6.2.2.2.5 Mission time

In all cases a conservative mission time of one hour per cask transfer is used for each fault tree.

6.2.2.2.6 Fault Tree Results

The detailed analysis is presented in Attachment B, Section B2.

There are four fault trees associated with the CTT:

1. Spurious movement in the Cask Preparation Room while loading a cask onto the CTT.
2. Spurious movement in the Cask Preparation Room during unbolting and lid adapter installation.
3. Spurious movement at the Cask Unloading Room while unloading canisters from the CTT.
4. Collision with an object or structure while moving a cask from the Cask Preparation Area to the Canister Transfer Room.

The results of the analysis are summarized in Table 6.2-2. Four fault trees were developed where the top events correspond to one of the scenarios listed above.

Table 6.2-2 Summary of Top Event Quantification for the CTT

Top Event	Mean Probability	Standard Deviation
Spurious movement of the CTT during cask loading	1.8E-9	5.7E-9
Spurious movement of the CTT during cask preparation	1.2E-4	2.0E-4
CTT collision into structure	9.8E-4	1.2E-3
Spurious movement during canister transfer	2.8E-14	1.3E-13

NOTE: CTT = cask transfer trolley.

Source: Attachment B, Section B2, Figures B2.4-1, B2.4-5, B2.4-8 and B2.4-12.

6.2.2.3 Shield Door and Slide Gate Fault Tree Analysis

The WHF Cask Unloading Room and Loading Rooms have a slide gate providing access to the Canister Transfer Room and a shield door providing access to either the Cask Preparation Area or the Site Transport Vestibule. The shield doors and slide gates provide shielding during cask unloading and loading.

The FTA is detailed in Attachment B, Section B3. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B3 for sources of information on the physical and operational characteristics of the shield doors and slide gates.

6.2.2.3.1 Physical Description

The Cask Unloading Room's shield doors are opened to allow cask-carrying equipment, such as the site transporter, to enter the room. Once equipment is positioned properly in a Cask Unloading Room, shield doors may be shut in preparation for removing canisters from the cask. Once the shield doors are shut, the slide gate may be opened, to allow the CTM to perform cask unloading operations. Aging overpack loading operations in the Loading Room are analogous to cask unloading operations.

The shield doors consist of a pair of large heavy doors that close together. The doors are operated by individual motors that have over-torque sensors to prevent crushing of an object. Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand lever that must be enabled by an enable/disable switch. An emergency-open switch exists enabling the doors to be opened in case of an emergency situation.

Similar to the shield doors, the slide gate consists of two gates that close together between the Loading/Unloading Rooms and the Canister Transfer Room. The gates are operated by individual motors that also have over-torque sensors. Each gate has limit switches to indicate open or closed gates. A CTM skirt-in-place switch is interlocked to the slide gate to prevent the gates from opening without the CTM in place and a CTM in-place bypass hand switch exists for maintenance activities. Slide gate operation is controlled by a hand switch coupled with an enable/disable switch and shield door interlocks prevent the slide gate from opening when the shield door is open. Open/closed and CTM in-place indicators exist to assist operators in their activities.

6.2.2.3.2 Operation

The Cask Unloading Room shield doors are opened to allow cask-carrying equipment, such as the SPM, to enter the room. Once equipment is positioned properly in an Unloading Room, shield doors are shut in preparation for removing canisters from the cask. Once the shield doors are shut, the slide gate may be opened to allow the CTM to perform cask unloading operations.

6.2.2.3.3 Control System

The control systems have hard-wired interlocks for the following functions:

- Redundant hardwire interlocks prevent the shield door from opening while the slide gate is open.
- The shield door system will not have any test, maintenance or other modes/settings that will allow bypass of interlocks.
- A single interlock prevents the slide gate from opening when the CTM skirt is not in place.
- An obstruction sensor is provided to detect objects between the shield doors and prevent door closure initiation.
- Motor over-torque sensors are provided to prevent shield doors from causing damage to casks or waste packages in the event of closure on a conveyance.
- Shield doors and slide gates are equipped with redundant hardwire interlocks to prevent one another from opening when the other is open.

6.2.2.3.4 System/Pivotal Event Success Criteria

Success criteria for the shield door and slide gate are the following:

- Prevent inadvertent opening of shield door
- Prevent inadvertent opening of the slide gate
- Prevent concurrent opening of the shield door and slide gate when waste is present
- Prevent shield door closing on CTT carrying a transportation cask or site transporter carrying an aging overpack.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event for a fault tree for the CTT.

6.2.2.3.5 Mission Time

Most of the basic events in the fault tree models are “failure on demand” for equipment failures and “failure per operation” for HFEs. A mission time of one hour is used to calculate the probability of a spurious signal being sent due to PLC failure.

6.2.2.3.6 Fault Tree Results

The detailed analysis is presented in Attachment B, Section B3.

The slide gate and shield door system has three credible failure scenarios:

1. Inadvertent opening of the shield door.
2. Inadvertent opening of the slide gate.
3. Shield door closes on conveyance.

The results of the analysis are summarized in Table 6.2-3. Three fault trees were developed where the top events correspond to one of the scenarios listed above.

Table 6.2-3. Summary of Top Event Quantification for the Shield Doors and Slide Gate

Top Event	Mean Probability	Standard Deviation
Inadvertent Opening of the Shield Door	1.3E-07	2.0E-07
Inadvertent Opening of the Slide Gate	3.5E-09	1.2E-08
Shield Door Closes on Conveyance	1.9E-06	2.8E-06

Source: Attachment B, Section B3, Figures B3.4-1, B3.4-4 and B3.4-7

6.2.2.4 Canister Transfer Machine Fault Tree Analysis

The FTA is detailed in Attachment B, Section B4. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B4 for sources of information on the physical and operational characteristics of the CTM.

6.2.2.4.1 Physical Description and Functions

The two types of canisters moved in the CTM for WHF operations are TAD canisters and DPCs.

Specifically the following three CTM operations apply to the WHF:

1. Transfer a DPC from a transportation cask to a shielded transfer cask (STC) (occurs solely in Cask Unloading Room).

2. Transfer a TAD canister from a STC to an aging overpack (TAD canister is unloaded in the Cask Unloading Room and moved in the Transfer Room to the Cask Loading Room to be placed in an aging overpack).

3. Transfer a DPC in an aging overpack to a STC (DPC is unloaded in Cask Loading Room and moved in the Canister Transfer Room to the Cask Unloading Room and placed into an STC).

The ports in the floor of the Canister Transfer Room provide access to the Cask Unloading Room and Loading Room.

The CTM is an over head crane bridge with two trolleys. The first is a canister hoist trolley with a grapple attachment and hoisting capacity of 70 tons. The second is a shield bell trolley that supports the shield bell. The bottom end of the shield bell is attached to a larger chamber to accommodate cask lids. The CTM bottom plate assembly supports a thick motorized slide gate.

The slide gate, when closed, provides bottom shielding of the canister once the canister is inside the shield bell. Around the perimeter of the bottom plate, a thick shield skirt is provided which can be raised and lowered to prevent lateral radiation shine during a canister transfer operation.

6.2.2.4.2 Operations

Typical operation for the WHF CTM includes the transfer of a TAD canister from a STC to an aging overpack.

The CTM is moved to a position over the center of the port above the loaded STC in the unloading room. The shield skirt is lowered to rest on the floor, and the port slide gate is opened. The CTM slide gate is opened and the canister grapple is lowered through the shield bell to engage and lift the cask lid. The port slide gate is closed and the shield skirt is raised so the CTM can be moved to a cask lid staging area to set down the lid.

The CTM is moved back over the port above the loaded cask to align the canister grapple. The shield skirt is lowered, the port slide gate is opened, and the grapple is lowered to engage the TAD canister lifting feature. The TAD canister is raised into the shield bell. The CTM slide gate and the port slide gate are closed and the shield skirt is raised so the CTM can be moved to the port above the empty aging overpack in the Cask Loading Room. Operation 1, transfer a DPC from a transportation cask to an STC, occurs solely in the Unloading Room. Operation 1 of the CTM is somewhat similar to operation 2 except the CTM holds the DPC in the bell in the Canister Transfer Room above the port gate until the empty STC is moved in the unloading room. Operation 3, transfer of a DPC in an aging overpack to a STC, is essentially the reverse of that described for operation 2. .

The CTM canister grapple is used for handling large diameter canisters such as TAD canisters and DPCs. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Room floor and lowering the CTM hoist until the CTM grapple is accessible in the room below.

The CTM is normally controlled from the facility Operations Room, but a local control station is also provided.

Generally, under off normal conditions the CTM is not in operation. Following a loss of alternating current (offsite power), all power to the CTM motors (e.g., hoist, bridge, trolley, and bell trolley) is lost. If a transfer is underway when power is lost, all of the CTM motors would stop and the hoist holding brake engages. Operations would be suspended until power is restored and the load can be safely moved. Under other off-normal conditions, transfer operations would be suspended and the CTM would remain idle.

6.2.2.4.3 Control System

Hard-wired interlocks are provided to:

- Prevent bridge and trolley movement when the shield bell skirt is lowered
- Prevent raising the shield bell skirt when the slide gate is open

- Prevent hoist movement unless the grapple is fully engaged or disengage
- Stop the hoist and erase the lift command when a canister clears the shield bell slide gate
- Stop a lift before upper lift heights are reached (two interlocks are provided for this function)
- Prevent opening of the port gate unless the shield bell skirt is lowered and in position
- Prevent hoist movement unless the shield bell skirt is lowered
- Prevent lifting of a load beyond the operational limit of the CTM (load cells).

Some of these interlocks can be bypassed during maintenance. The most significant of these interlocks that can be bypassed is the interlock between the shield skirt position and the position of the slide gate (the shield skirt cannot be raised unless the slide gate is closed or the maintenance bypass is engaged.) The design of the grapple interlock ensures that the bypass is voided when a canister is grappled.

Much of the operational controls are provided by non-ITS PLCs. Spurious or failed operation of the PLCs is in the FTA when such operation may contribute to a drop or collision event.

6.2.2.4.4 System/Pivotal Event Success Criteria

Success criteria for the CTM are the following:

- Prevent a canister drop from a height below the design basis height for canister damage from any cause during the lifting, lateral movement, and lowering portions of the canister transfer
- Prevent a canister drop from above the canister design limit drop height from any cause during the lifting, lateral movement, and lowering portions of the canister transfer
- Prevent a drop of any object onto the canister from any cause during the lift, lateral movement, and lowering portions of the canister transfer
- Prevent CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the WHF.

The failure to achieve each success criterion defines the top event for a fault tree for the CTM.

6.2.2.4.5 Mission Time

The mission time for the ITS CTM is set to one (1) hour.

6.2.2.4.6 Fault Tree Results

The analysis is detailed in Attachment B, Section B4.

There are five scenarios associated with the CTM that represent potential initiating events:

1. The CTM drops a canister from a height below the design basis height for canister damage (this includes canister drops within the shield bell once the bell slide gate has been closed and drops through the Canister Transfer Room ports to the loading/unloading areas that can occur before the bell slide gate is closed).

2. The CTM drops a canister from a height above the design basis height for canister damage.

3. The CTM drops an object onto a canister.

4. The CTM, while carrying a canister, moves in such a manner (spurious movements, exceeding bridge or trolley end of travel limits) as to cause an impact of the canister with the shield bell.

5. The CTM moves when the canister being transferred is being lifted and is between the WHF floors resulting in shear forces being applied to the canister.

The results of the analysis are summarized in Table 6.2-4. Five fault trees were developed. The top events correspond to the four potential initiating events defined above.

Table 6.2-4 Summary of Top Event Quantification for the CTM

Top Event	Mean Probability	Standard Deviation
CTM drop all heights	1.4E-5	1.0E-5
CTM high drops from two blocking events	2.2E-8	6.3E-8
Drop of object onto canister	1.4E-5	1.0E-5
CTM collision	3.9E-6	2.7E-7
Spurious movement of bridge/trolley breaches canister (shear)	6.7E-9	1.4E-8

NOTE: CTM = canister transfer machine.

Source: Attachment B, Section B4, Figures B4.4-1, B4.4-17, B4.4-22, B4.4-39, and B4.4-49.

6.2.2.5 Cask Cooling Fault Tree Analysis

The FTA is detailed in Attachment B, Section B5. The FTA considered two kinds of leaks or ruptures in the cask cooling system leading to a radiological release:

1. Non-pressurized leaks or ruptures.
2. Pressurized leaks or ruptures.

The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B5 for sources of information on the physical and operational characteristics of the cask cooling system.

6.2.2.5.1 Physical Description

The cask cooling system is a pump driven system that will be used to cool casks by introducing borated water into the cask. The system consists of two motor-driven pumps, a pressure relief valve, two non-hardwired interlocks, water piping, four quick disconnects, two sections of flexible tubing, and a separator vessel.

The pumps serve to direct water from the pool, into the cask, and back to the pool. The positive displacement pump drives water out of the pool and into the cask, while the centrifugal pump directs water out of the cask and back into the pool for reuse. Borated water is injected via the drain pipe which is below the bottom of the spent fuel assemblies. Steam leaves the cask through the vent piping.

The water delivery and removal systems consist of a series of pipes, tubing, and quick disconnects. The flexible tubing connects the supply and return piping to the cask, with connections provided by quick disconnects. System piping runs from the pool to the flexible tubing which supplies the cask, and from the cask return to the separator vessel.

Two lines of piping follow out of the separator vessel: one providing water for treatment, the other routing air to off-gas treatment. The separator vessel serves the purpose of separating air and water delivered from the cask.

6.2.2.5.2 Operations

The cask handling crane places the cask into the preparation station. At the preparation station, the gas sampling port is opened and the drain valve and drain port cover plates are removed. The borated water line is connected to the drain port, and the vent line is connected to the gas sampling port. Borated water is then introduced into the cask as the steam is vented. Once the cask is satisfactorily cooled, the lines are disconnected, and the cover plates are reinstalled.

6.2.2.5.3 Control System

The pump failures and blockages which can cause cask over pressurization may be controlled by two features which would negate the over pressurization. The first of these features are interlocks (not hardwired) which are designed to detect excess pressure/water at the filling and venting ends of the cooling system. Should an interlock detect such a scenario, the positive displacement pump is shut down. If this shut down does not occur, or the interlock does not detect the condition, a pressure relief valve is in place to be physically affected by the over-pressurization to open and relieve the pressure. Should both of these features fail, an over-pressurization of the cask will result in the release of contaminated steam or water. However, these interlocks depend upon PLCs and are not credited in the fault tree analysis. The pressure relief valve is the only credited safety feature.

6.2.2.5.4 System/Pivotal Event Success Criteria

A pressure relief valve shall remedy a cask overfilling or over-pressurization failure. This valve is physically activated by the presence of an exceeding pressure, causing the valve to open and relieve the excess pressure.

6.2.2.5.5 Mission Time

A nominal eight-hour mission time is used to calculate the failure probability for components having a time-based failure rate. Otherwise, failure-on-demand probabilities are used.

6.2.2.5.6 Fault Tree Results

The detailed description in Attachment B, Section B5 documents the application of basic event data, CCFs, and HRA.

There are two fault trees associated with the cask cooling system:

1. Break of non-pressurized sample line.
2. Cask over-pressurization.

Results of the quantitative fault tree analysis are summarized in Table 6.2-5.

Table 6.2-5. Summary of Top Event Quantification for Cask Cooling

Top Event	Mean Probability (per cask)	Standard Deviation
Sample line break non-pressurized	2.0E-05	6.1E-5
Cask/sample line overpressurized	7.8E-06	5.1E-5

Source: Attachment B, Section B5, Figures B5.4-1 and B5.4-6.

6.2.2.6 Site Transporter Fault Tree Analysis

The FTA for the site transporter is detailed in Attachment B, Section B6. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B6 for sources of information on the physical and operational characteristics of the site transporter.

6.2.2.6.1 Physical Description

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a concrete and steel ventilated aging overpack. The transport occurs both within the Intra-site and within the WHF. The analysis described herein is limited to movement of the site transporter within the WHF: the entry vestibule, the Cask Preparation Area, and the Cask Unloading Room.

The site transporter is a track driven vehicle with four synchronized tracks (two on each side). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not ITS. An integrated diesel powered electric generator provides the energy to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

A rear fork assembly and a pair of support arms are used to lift and lower the cask. The rear forks are inserted in two rectangular slots near the base of the aging overpack. Casks are carried in a vertical orientation with the lid at the top. Access to the top of the casks is unobstructed.

A passive restraint system provides stabilization during cask movement. These restraints are brought into contact with the cask after it has been raised to the desire height. A pin is inserted into each of the three restraint arms to keep the restraint in place should there be a failure of the electromechanical assembly. The pins also serve as an interlock that prevents movement of a loaded site transporter without the restraints being properly installed.

6.2.2.6.2 Control System

There are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter. All safety interlocks and controls of the site transporter are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No PLC or computer is used to control the machine.

6.2.2.6.3 Normal Operations

The site transporter operator lines up the front opening of the site transporter to envelop the aging overpack and positions the rear fork down and in-line with the rectangular lifting slots near the bottom of the aging overpack and moves the site transporter forward until the aging overpack is centered in the interior of the site transporter.

The rear forks are raised to contact the bottom of the lift slots but no attempt to lift the cask is made at this time. The operator and interlocks (torque and/or position) are incorporated to prevent lifting with the rear forks only.

The operator initiates the lift support arm's interface sequence with the rear forks and cask to prepare for lifting. After the operator and machine's switches have confirmed that the rear forks and lift support are properly aligned with one another, the lift sequence is initiated. The control system will sequence the lift motors so all screws operate together.

When the lift is completed, the operator performs the final positioning of the upper restraint arms and inserts a pin in each arm. When the pins are properly installed, the site transporter can move.

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. At the facility, the operator stops the site transporter outside the entrance vestibule and turns off the diesel generator and then an electric power cable is attached.

Once driven inside the building, the operator positions the site transporter in either the Cask Preparation Area or in the Cask Unloading Room. During the various movements inside the WHF, the operator disengages the restraint arms for lower and lift operations at the various stations. Each time, the operator removes or replaces the pins from the restraint arms, as appropriate. The movement interlock is engaged when the pins are removed.

6.2.2.6.4 System/Pivotal Event Success Criteria

Success criteria for the site transporter are the following:

- Prevent a collision of the site transporter with objects, structures, or shield doors
- Prevent runaway situations
- Prevent site transporter movements in the wrong direction
- Preventing a rollover of the site transporter
- Prevent spurious site transporter movements
- Prevent a load drop during lift/lower or transport operations.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event for a fault tree for the site transporter.

6.2.2.6.5 Mission Time

For quantification of the site transporter fault trees in Attachment B, Section B6, a mission time of one hour per cask transfer is used.

6.2.2.6.6 Fault Tree Results

There are seven basic site transporter fault trees developed for the WHF. The scenarios represented and the variations by these fault trees are the following:

1. Site transporter collides with WHF structures:

   A. Importing aging overpack to Cask Preparation Room.
   B. Transfer from Cask Preparation Room to Cask Unloading Room.
   C. Transfer from Cask Unloading Room to Cask Preparation Room.

2. Collision of site transporter with Cask Unloading Room shield door.

3. Site transporter load drop during lift/lower.

4. Site transporter tip over.

5. Site transporter impact.

6. Site transporter rigging.

7. Site transporter spurious movement.

The results of the analysis are summarized in Table 6.2-6 for the seven fault trees.

Table 6.2-6. Summary of Top Event Quantification for the Site Transporter

Top Event	Mean Probability	Standard Deviation
Collides with WHF structures	4.6E-3	1.6E-2
ST rollover	2.3E-6	1.9E-6
ST spurious movement	2.0E-13	6.1E-13

NOTE: WHF = Wet Handling Facility; ST = site transporter.

Source: Attachment B, Section B6, Figure B6.4-1, B6.4-6, B6.4-9.

6.2.2.7 HVAC FAULT TREE ANALYSIS

The FTA is detailed in Attachment B, Section B7. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B7 for sources of information on the physical and operational characteristics of the HVAC system.

6.2.2.7.1 HVAC Description and Function

The ITS HVAC is a two (2) train system of identical components. One train is always operational and one train is in standby mode. This system is not configured to run both trains at the same time without bypassing control circuitry. This off-normal situation is not addressed in this analysis.

In the WHF, the train A HVAC equipment is located on the opposite end of the building from train B HVAC equipment. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. Although these trains are interconnected through interior duct work, the trains are independent. A back-draft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

This HVAC system is composed of four subsystems:

- A series of dampers are used to control pressure, flow, as well as flow direction in this system.
- Three HEPA filters, each consisting of one medium efficiency roughing filter (60 to 90% efficiency), two high efficiency filters for particulate removal in air (99.97% efficiency), and a mister/demister for maintaining proper humidity levels.
- One exhaust fan with a rated capacity of 40,500 cubic feet per minute (cfm) and an exhaust fan motor rated at 200 horsepower (hp).
- Control circuitry with logic contained in an erasable programmable read-only memory located in the adjustable speed drive controller used for controlling the speed of the operating fan and on fault detection, and for off-nominal conditions, shutting down the operating train and transmitting signals to the standby system to start.

6.2.2.7.2 Success Criteria

One success criterion is defined for the each of independent trains, A and B, for providing the HVAC confinement function–maintain negative differential pressure in the WHF for the specified mission time.

The respective trains of the ITS portions of the HVAC are identical. Various design features are provided to achieve each of the success criteria for the respective trains and for the combined system.

The HVAC FTA for the HVAC includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the HVAC.

6.2.2.7.3 Mission Time

The mission time for the HVAC system is 720 hours for a canister breach event and radionuclide release. (Attachment B, Section B7.4.1.4). However, the mission time for the backup system has been taken as, half of the active system, (i.e., 360 hours). This is to account for the difference in failure rates between active and passive systems.

The SAPHIRE model was re-run, changing only the mission time. For a sample line break during cask cooling, a mission of time for the HVAC system is 24 hours. 24 hours corresponds to the time required to rectify the situation and seal the leak.

6.2.2.7.4 Fault Tree Results

The top event in this fault tree is "Delta pressure not maintained in WHF facility." This is defined as the inability of the ITS HVAC system to maintain proper delta pressure within the facility. The system failure probability and standard deviation, including failure of electrical power, are as follows:

For a 720 hour mission time:

- The mean HVAC system probability of failure, including loss of electrical power is 2.5E-2
- The standard deviation is 6.5E-2 (Reference Attachment B, Figure B7.4-1).

For a 24 hour mission time:

- The mean HVAC system probability of failure, including loss of electrical power is 1.1E-3
- The standard deviation is 6.4E-3 (Reference Attachment H).

The above values are for the HVAC system coupled with a loss of electrical power, which is described in the next section. The values for the failure of the HVAC system alone, decoupled from the electrical power fault trees, are as follows:

For a mission time of 720 hours:

- The mean probability of failure for the HVAC system alone is 2.7E-2
- The standard deviation for the HVAC system alone is 6.9E-2.

For a mission time of 24 hours:

- The mean probability of failure for the HVAC system alone is 7.7E-4
- The standard deviation for the HVAC system alone is 4.9E-3 (Reference Attachment H).

6.2.2.8 ITS AC Power Fault Tree Analysis

The FTA is detailed in Attachment B, Section B8. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B8, for sources of information on the physical and operational characteristics of the ITS AC power system.

6.2.2.8.1 System Description

The ITS AC power system supplies power to the ITS systems (the HVAC Systems). The ITS power system consists of two elements; those used during normal operations and those used during off-normal conditions. During normal operations, AC power is supplied from one of two offsite 138kV offsite power lines through the 138kV to 13.8kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site. Off-normal conditions for the distribution of AC power occur during a loss of offsite power (LOSP).

A LOSP may be the result of problems on the power grid, or may be the result of failures within the plant AC power systems. Under these conditions, the AC power source for the WHF ITS equipment is two onsite ITS diesel generators. Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each ITS diesel generator supplies power to one division (A or B) of ITS systems. Each ITS diesel generator, its associate support systems, and the power distribution system are independent and electrically isolated from the other ITS diesel generator, its support systems and power distribution system.

The ITS loads within the WHF are powered via two ITS 480V load centers and two ITS motor control centers (MCC) located within separate areas in the WHF. Each division of the AC power supply from the 13.8kV ITS switchgears to the WHF passes through a 13.8kV to a 480 V transformer.

The ITS on site power portion of the ITS power supply system is intended to provide back-up power to selected buildings and operations in the event of a main transmission loss of power (LOSP). The primary components in each division include: a diesel generator, support systems for the diesel generator, and a load sequencer. Both ITS diesel generators are located in the Emergency Diesel Generator Building (EDGB). Each is sized to provide sufficient 13.8 kV

power to support all ITS loads in one division in six facilities (i.e., three CRCFs, the WHF, the RF, and the EDGB).

The ITS diesel generator starts upon detection of an undervoltage condition via an undervoltage relay of the diesel generator switchgear. Each ITS diesel generator is equipped with a complete independent set of support systems including HVAC systems, uninterruptible and DC power systems, a fuel oil system, diesel generator start subsystem, diesel generator cooling subsystem and lube oil subsystem.

The load sequencer controls sequence of events that occur after a LOSP and the ITS diesel generator starts. Upon a LOSP, the load sequencer opens the WHF ITS load center feed breaker. After the ITS diesel generator starts and reaches rated capacity, the load sequence connects the ITS diesel generator to the 13.8 kV ITS switchgear and then reconnects the WHF loads.

6.2.2.8.2 Operations

Under normal operating conditions, AC power is supplied from two 138kV offsite power lines. Power is passed through the 138kV to 13.8kV switchyard to the two independent 13.8kV ITS switchgear. From here, power is transmitted via separate lines to a 13.8kV to 480V transformers supporting divisions A and B of the WHF. Power to individual ITS components within each facility is provided via two ITS 480V load centers and two ITS 480V MCCs (one of each for division A and one of each for division B in each facility) powered through these transformers.

During a LOSP, both ITS diesel generators are required to start and accept loads in a timely manner. Upon a LOSP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8kV ITS switchgear and the switchyard 13.8kV switchgear in each division automatically opens. Both diesel generators start automatically and are connected to the 13.8kV ITS switchgear when the connecting breaker is closed by the load sequencer. The load sequencer then reconnects the WHF loads to the 13.8kV ITS switchgear. Both ITS diesel generators continue to supply AC power until normal power is restored.

Environmental systems are provided to maintain the temperature in the various EDGB rooms and WHF ITS electrical rooms within acceptable levels.

6.2.2.8.3 Control System

The ITS diesel generator starts upon detection of an undervoltage condition via an undervoltage relay of the 13.8kV ITS switchgear. The 13.8kV ITS switchgears are isolated from the main switchyard upon a loss of power in the switchyard. The loads in the WHF are shed upon a loss of power indication.

A load sequencer controls the loading of the ITS diesel generator onto the 13.8kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the WHF loads onto the AC power system.

6.2.2.8.4 System/Pivotal Event Success Criteria

Success criterion for the AC power system is defined in terms of its support function for the ITS HVAC confinement function. The AC power system must operate in support of the HVAC system for as long as necessary to successfully provide confinement after the potential release of radioactive material inside the WHF. There are two independent trains of HVAC and each of these must be supported by an independent AC power system. Therefore, the following success criteria apply to the respective AC power supply trains:

- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG A) to the HVAC division powered through WHF ITS Load Center A and ITS MCC A1 for the mission time of 720 hours.

- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG B) to the HVAC division powered through WHF ITS Load Center A and ITS MCC B1 for the mission time of 720 hours.

The respective trains of the ITS portions of the AC power system are essentially identical. Various design features are provided to achieve each of the success criteria for the respective trains.

The FTA for the AC power system includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the AC power system.

6.2.2.8.5 Mission Time

The mission time for the ITS AC power system is the same as for the HVAC system, 720 hours for a canister breach event and radionuclide release (Attachment B, Section B8.2.5.1.1). For a sample line break during cask cooling, a mission of time for the ITS power system is the same as the HVAC system which is 24 hours.

6.2.2.8.6 Fault Tree Results

Two fault trees are developed for the AC power system, one for train A and one for train B. The respective top events are:

- "Loss of AC power at ITS Load Center A for the WHF," defined as a failure of the normal and ITS onsite power supplies to provide power to ITS Load Center A.

- "Loss of AC power at ITS Load Center B for the WHF," defined as a failure of the normal and ITS onsite power supplies to provide power to ITS Load Center B.

The results are the same (see Attachment B, Figures B8.4-1 and B8.4-3) for the trains:

For a mission time of 720 hours:

- The mean probability of failure is 3.2E-2
- The standard deviation is 7.8E-02.

For a mission time of 24 hours:

- The mean failure probability of failure is 1.3E-3
- The standard deviation is 6.3E-3 (Reference Attachment H).

6.2.2.9 Horizontal Cask Tractor and Trailer Fault Tree Analysis

The FTA for the horizontal cask tractor and trailer (HCTT) is detailed in Attachment B, Section B9. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B9 for sources of information on the physical and operational characteristics of the HCTT.

The tractor is a large, four-wheel drive, diesel tractor designed specifically for pulling the transfer trailer. The tractor has redundant brakes in addition to having a fail-safe emergency brake. The tractor has independently mounted non-driven hydraulic pendular axles with a minimum of four tires per axles that will ensure the cask remains level during transportation across uneven terrain. In addition to the pendular axles, the trailer has three other hydraulic systems: (1) stabilizing jacks, (2) cask support skid and positioning system, and (3) hydraulic ram.

6.2.2.9.1 Operation

After receipt in the Transportation Cask Vestibule, the entrance door from the Transportation Cask Vestibule to the Cask Preparation Area is opened to allow the HCTT to move to the receipt area within the Cask Preparation Area. There, the HCTT carrying the cask/waste form is moved into a position where the cask can be removed. The HCTT is then secured in place as required by procedures. The HCTT tractor is detached from the HCTT trailer and moved out of the Cask Preparation Area. The entrance door is closed and the vestibule door is opened to allow departure of the HCTT tractor.

Only activities associated with the HCTT while in the WHF are addressed in this document.

6.2.2.9.2 Control System

Once the HCTT is properly positioned in the WHF, the brakes on both the tractor and trailer are engaged. The brakes are spring applied with hydraulic release calipers. There is a backup system on the tractor consisting of a split master cylinder.

Stabilizing jacks provide vertical support during the loading and unloading of the cask on the HCTT.

6.2.2.9.3 System/Pivotal Event Success Criteria

The success criterion for the HCTT is the prevention of a collision with other vehicles, facility structures, or equipment.

Various design features are provided to achieve each of the success criteria. These include redundant braking systems in the tractor and parking brakes that fail safe. The failure to achieve each success criterion defines the top event for a fault tree for the HCTT.

6.2.2.9.4 Mission Times

A conservative mission time of one hour is used to account for the time it takes the HCTT loaded with a transportation cask to move through the Transportation Cask Vestibule doors to the Cask Preparation Area inside the WHF.

6.2.2.9.5 Fault Tree Results

The HCTT fault tree analysis is detailed in Attachment B, Section B9.

There is one fault tree associated with the HCTT that represent a potential initiating event:

> HCTT collision with other vehicles, WHF facility structures or equipment when loaded with a transportation cask.

The results of the analysis are summarized in Table 6.2-7.

Table 6.2-7. Summary of Top Event Quantification for the HCTT

Top Event	Mean Probability	Standard Deviation
HCTT Collision	5.0E-2	3.0E-2

NOTE: HCTT = horizontal cask tractor and trailer.

Source: Attachment B, Section B9, Figure B9.4-1

6.2.2.10 Potential Moderator Sources

6.2.2.10.1 Internal Floods

Internal floods are potential sources of moderator addition into a canister associated with pivotal events in the event sequences included in Section 6.1. Moderator addition into a canister can occur following a breach of the canister and a subsequent internal flood. The internal flooding analysis considers all waste handling facilities.

During most of its handling at the repository, a canister is surrounded by at least one other barrier to water intrusion: a transportation cask, a transportation cask within a CTT, an aging overpack, a waste package, a waste package within a WPTT, or a waste package within a TEV.

Each facility is equipped with a normally dry, double-preaction sprinkler system in areas where waste forms are handled (Ref. 2.2.15, Ref. 2.2.30, Ref. 2.2.24, and Ref. 2.2.38). Such systems,

which require both actuation of smoke and flame detectors to allow the preaction valve to open and heat actuation of a fusible link sprinkler head to initiate suppression, have a very low frequency of spurious operation. A 30-day period from the occurrence of the canister breach to the time definitive action can be taken to prevent introduction of water into the canister is reasonable and is the same as the period used to assess dose for a radiological release. The spurious actuation frequency over a 30 day mission time after a breach is calculated below.

An estimate of the probability of spurious actuation was developed using a simplified screening model that addressed the following cut sets that result in actuation:

- Spurious preaction valve opens before canister breach × failure of a sprinkler head during post-breach mission time (30 days)
- Failure of a sprinkler head during building evacuation × water left in dry piping after last test (first quarter following annual test).

The frequency of sprinkler failure is estimated using an individual sprinkler head failure frequency of 1.6E-6/yr (Ref. 2.2.12, Table 1), the estimated number of sprinklers (1 per 130 ft^2 based on NFPA 13 (Ref. 2.2.62, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2.21 Table 10). At 130 ft^2 per sprinkler, 58 sprinklers are estimated. The failure of any sprinkler in the room is then estimated to be 58 × 1.6E-6/yr × 1/8760 hrs/yr, or 1.1E-8/hr.

The frequency of preaction valve spurious open is estimated using the solenoid valve spurious open data in Section 6.3 of 8.1E-07/hr. This is reasonable because a solenoid valve must open to relieve the air pressure from the diaphragm which keeps the valve closed.

The value of the first cut set is (1.6E-6/yr × 1/8760 hrs/yr × 720 hrs) × (8.1E-7/hr × 720 hrs) = 8E-11/sprinkler head. The second cut set is more significant: 0.025 (human error screening value) × (1.6E-6/yr × 1/8760 hrs/yr × 720 hrs) = 3E-9/sprinkler head.

Applying the sum of these values, 3E-9 per sprinkler head, to the number of sprinklers calculated for the waste handling areas of the four facilities results in the following estimates of the probability of spurious sprinkler actuation found in Table 6.2-8.

Table 6.2-8. Probability of Spurious Sprinkler Actuation

Facility	Waste Handling Area (ft^2) [a]	Number of Sprinkler Heads	Probability of Spurious Actuation in 30 day Period in Waste Handling Areas
CRCF(ea)	42,000	330	1E-6
IHF	30,000	240	9E-7
RF	19,000	150	5E-7
WHF	28,000	215	6E-7

NOTE: [a]CRCF area based on room numbers 1005E, 1016-1026, 2004,2007, 2007A, and 2007B;
IHF area based on room numbers 1001-1003, 1006-1008, 1011,1012, 1026, and 2004;
RF area based on room numbers 1013, 1015, 1016, 1017, 1017A, and 2007;
WHF area based on room numbers 1007-1010, 1016, 2004, 2006, and 2008.
CRCF = Canister Receipt and Closure Facility, IHF = Initial Handling Facility, RF = Receipt Facility, WHF = Wet Handling Facility.

Source: Original

Piping carrying water is present in the waste form handling areas of the CRCF, IHF and WHF. Piping lengths in these areas of the CRCF and WHF are below 100 feet per facility. The probability of a pipe crack in a 30 day period is estimated using the pipe leak data from *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*, *NUREG/CR-6928* (Ref. 2.2.46, Table 5-1). Piping leaks and large break rates applicable to non-service water applications are used in the analysis. These values are considered appropriate for repository systems because the conditioning applied to the fluids in the systems is typical of commercial NPPs:

$$\text{External leak small (1 to 50 gpm): leak rate} = 2.5\text{E-}10\ hr^{-1}ft^{-1}$$

$$\text{External leak large (> 50 gpm): leak rate} = 2.5\text{E-}11\ hr^{-1}ft^{-1}$$

Multiplying the sum of the small and large leak frequencies ($2.8\text{E-}10\ hr^{-1}ft^{-1}$) by the length of piping in the waste handling areas of each facility, and the number of hours in a 30 day period (720 hr), a conditional probability of water leakage in all waste handling areas given a breach is approximated as follows:

$$\text{CRCF} = 2.8\text{E-}10\ hr^{-1}ft^{-1} \times 100\ ft \times 720\ hrs = 2.0\text{E-}05$$

$$\text{IHF} = < 2.8\text{E-}10\ hr^{-1}ft^{-1} \times 6800\ ft \times 720\ hrs = 1.4\text{E-}03$$

$$\text{RF} = 2.8\text{E-}10\ hr^{-1}ft^{-1} \times 0\ ft \times 720\ h = 0$$

$$\text{WHF} = 2.8\text{E-}10\ hr^{-1}ft^{-1} \times 75\ ft \times 720\ hrs = 1.5\text{E-}05.$$

It is appropriate to use the waste handling area piping lengths because they are separated by concrete walls from the non-waste handling areas of buildings.

The above applies to event sequences that do not involve fires as an initiating event. During fire initiating event sequences, fire suppression would actuate in the locations sufficiently heated by

the fire. The fire initiating event analysis is described in Section 6.5, and the conditional probability of canister failure owing to fires is described in Section 6.3. The analysis is performed without the salutary effects of fire suppression in order to demonstrate large margins of safety during fire event sequences. Furthermore, the location of each fire is analyzed as around the outer shell of the overpack that surrounds the canister. The frequency of containment breach due to fire is significantly overestimated because of this conservative approach.

For fires that occur in locations that contain canisters sealed within bolted transportation casks, the fire location is floor level and the transportation casks rise as much as 20 feet above the floor. Casks are relatively thick walled compared to canisters and sustain a relatively small internal pressurization when compared to canisters. Therefore, if a fire is large enough, it will fail the internal canister first, as indicated in Attachment D. This will cause the bolted and sealed cask to bear the overpressure that is inside the canister. The cask bolts might act as elastic springs allowing the top to break the seal and relieve the internal pressure. This would be a mechanism that prevents cask breach. However, a hot fire may result in sufficient loss of strength of the bottom portion of the stainless steel cask such that it breaches. If failure occurs because of bolt stretching the cask lid remains on top of the cask preventing fire suppression water from entering. Commercial DPCs and TAD canisters will require at least 100 liters of water to enter the canister if optimally distributed among the fuel rods (Ref. 2.2.35, Section 2.3.10.1). Casks are raised above the floor. They lay on top of railcars, are lifted from there by cranes, sit inside a CTT, or lay sideways on a pallet. They are at least five feet from the floor. If the bottom portion of the canister breaches, there is no physical mechanism for this much water to enter the cask and then the canister, remain as water (not boil off), and optimally mix with the fuel rods.

This latter situation also applies to canisters sealed within a welded waste package. The waste package sits inside a WPTT or is inside a TEV. In the former case it is more than three feet from the floor (Ref. 2.2.16) and in the latter case, about one foot from the floor (Ref. 2.2.17). In the latter case, however, the TEV offers an additional layer of protection against fires. In addition, it is physically unrealistic for a sufficient amount of available fire suppression water to cause 100 liters to leak into a breached canister, but not extinguish the fire or at least reduce the severity of the fire such that a breach would not occur.

For a canister inside of an open transportation cask or waste package, the orientation of these is always vertical, and the cask and waste package are always elevated above the floor where the fire occurs. The occurrence of a fire of sufficient severity will fail the canister first as described above. An open transportation cask or waste package might allow fire suppression water to spray in from the top. The building configuration, however, precludes this occurrence. The cask lids are removed while in the upload cell below the CTM. The cask and waste package ports are above the casks and waste package. There is no fire suppression piping spanning the ports because the ports must be kept clear in order to perform lift and load operations. In the Cask Preparation Area and welding area, the lid is on the waste package and fire suppression piping can not be above an open waste package because of the welding machine. In the DPC cutting cell in which a cask is open (WHF only), there can be no fire suppression piping above an open cask because of the cutting equipment.

Upon failure of the canister inside the cask, the cask will not be susceptible to pressurization failures as above. Instead, water can only enter a cask (or waste package) if the cask body melts

through. Fires capable of melting stainless steel or Alloy 22, however, have an occurrence frequency within the waste handling facilities of less than 1E-05 over the preclosure period (Attachment D). Thus, breach of the cask or waste package in a manner that would allow water to enter the canister is essentially not physically realizable.

When a canister is being lifted, transferred inside the shield bell, and lowered. It is not inside an outer cask. However, fires can not be severe enough to breach a canister while being moved, as described in more detail in Attachment D. Water intrusion, therefore, is not physically realizable for this situation.

It is concluded that moderator entry into breached canisters during fire event sequences is not physically realizable because of a combination of physical mechanisms, building and equipment configuration, and overpack material properties. Furthermore, the existence of water from fire suppression is inconsistent with the fire analyses performed to obtain the probability of containment failure owing to fire. If fire suppression were indeed available, the probabilities of canister breach would be far lower. However, in order to complete an event sequence quantification, the conditional probability of moderator entry into a canister after canister breach during a fire initiating event sequence is assessed as *extremely unlikely* and assigned a lognormal distribution with a median of 0.001 and an error factor of 10. This yields a mean value of 3E-03. The large error factor is assigned because of the potential of human error to defeat some of the reasons that water will not enter the cask or waste package (e.g., neglecting to place a lid on the waste package just before a severe fire). These assignments are consistent with the methodology on the use of judgment provided in Section 4.3.10.

For fires that occur in locations that contain uncanistered spent nuclear fuel sealed within bolted transportation casks, the fire location is floor level and the transportation casks rise as much as 20 feet above the floor. Again, the analysis is performed without the salutary effects of fire suppression in order to demonstrate large margins of safety during fire event sequences. Should fire suppression be available, then cask failure would not occur (i.e., it would be orders of magnitude lower in probability). Therefore, if fire suppression water or a flood has occurred before or during the fire, there would be no breach of containment for entry into the cask. (Note that cask seal failure takes approximately one hour during a severe fire to occur. Therefore, the breach analysis that ignores fire suppression is quite conservative.) The cask failure mode is from over-pressurization and degradation of the seals between the lid and the shell, therefore, the area of the seal provides a small target for fire suppression entry. If fire suppression actuates, the fire brigade arrives, or other unborated water becomes available after the cask has failed, then as long the cask is internally pressurized, water can not enter. Because of the heat source provided by the SNF (in addition to heat generated by the fire), there will always be a higher pressure on the inside of the cask than the atmosphere on the outside of the cask. As noted above, casks are raised above the floor and water sources other than fire suppression are incapable of reaching the elevation for entry into the cask.

6.2.2.10.2 Lubricating Fluid

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a welded gear box with a leak pan below it capable of capturing the entire gearbox fluid inventory. The facility operating life of the surface facilities is 50 years. An estimate of the leakage rate through the gear box and drip pan during the 50 year period is found by multiplying the gearcase motor failure frequency (all modes) of 0.88E-06 per hour (Ref. 2.2.42, Page 2-104 and Section 6.3) by 50 years times the conditional probability of oil pan failure. A loss of lubrication would fail the crane operation and also be detected by oil pressure indicators. The conditional probability of oil pan failure may be estimated by an analogy to receiver tank leakage during the interval between gearbox failure and detection. The interval is conservatively estimated to be 30 days. The all modes failure rate of a receiver tank is 0.34 E-06 per hour (Ref. 2.2.42, Page 2-213). Using an exposure interval of 50 years, the conditional probability of lubricating fluid entering a breached canister would be less than:

$$0.88\text{E-}06/\text{hr} \times 50\ \text{yrs} \times 8760\ \text{hrs/yr} \times 0.34\text{E-}06/\text{hr} \times 720\ \text{hrs}/30\text{days} = 9.4\text{E-}05 \text{ over the preclosure period.}$$

This probability is overstated because: a) it does not account for inspections during the operating period of the facility, and b) it does not account for the conditional probability that lubricating fluid can find its way into a breached canister. Therefore, lubricating fluid is eliminated as a potential moderator.

6.3 DATA UTILIZATION

6.3.1 Active Component Reliability Data

The fault tree models described in Section 6.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. The active component reliability estimates are developed by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represented the range of the industry-wide information.

6.3.1.1 Industry-wide Reliability Data for Active Components

While data from the facility being studied are the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP is a one-of-a-kind facility and has no operating history, it is necessary to develop the required data from experience of other nuclear and non-nuclear equipment operations. Industry-wide data sources are documents containing industrial or military experience on component performance. These sources are from previous safety/risk analyses and reliability studies performed nationally or internationally, and also standards or published handbooks. For the YMP PCSA, a database is constructed using a library of industry-wide data sources of reliability data from nuclear power plants, equipment used by the military, chemical processing plants and other facilities. The sources used are listed in Attachment C, Section C1.2.

The data source scope has to be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might be used for electronics data versus mechanical data, so long as the detail and the applicability of the information provided justify its use. Lastly, the quality of the data source is considered to be a measure of the source's credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort is made in this analysis to use the highest quality data source available for each active component type and failure mode.

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, is to evaluate the similarity between the YMP operating environment and that represented in each industry-wide data source to ensure data appropriateness. The evaluation process is described in Section C1.2.

Given the fact that the YMP is a relatively unique facility (although portions are similar to the spent fuel handling and storage areas of commercial nuclear plants), the data development perspective is to collect as much relevant failure estimate information as possible to cover the spectrum of equipment operational experience. It is reasonable to expect that the YMP equipment would fall within this spectrum (Section 3.2.1). The scope of the sources selected for this data set is therefore deliberately broad to take advantage of the combined experience of many facilities, not a single plant. It is then intended to provide a combined estimate that reflects as best as possible the uncertainty ranges of the individual estimates. This ensures that the data are not skewed towards the possibly atypical behavior of one particular plant, industry or operating environment. The combinatorial process, utilizing Bayes' Theorem, is discussed in the following subsection.

Among the active components whose reliability is quantified with industry-wide data are the 200-ton cranes, jib cranes, canister maneuvering cranes, and the spent fuel transfer machine (SFTM). The rationale for using such data for these estimates is that a significant amount of crane experience exists within the commercial nuclear power industry and other applications and that this experience can be used to bound the anticipated crane performance at YMP. Furthermore, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants. Crane and SFTM handling incidents that result in a drop are included in the drop probability regardless of cause; they may be caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

Every attempt was made to find more than one data source for each TYP-FM, multiple sources are not always available for a specific piece of equipment. When data was extracted from several sources it was combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the type and failure

mode (TYP-FM). Ultimately, 53% of the TYP-FMs were quantified with one data source, 8% with two data sources, 8% with three data sources and 31% with four or more data sources.

6.3.1.2 Application of Bayes' Theorem to PCSA Database

The application of industry-wide data sources introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes' theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, NUREG/CR-6823 (Ref. 2.2.10). For the PCSA, the method known as "parametric empirical Bayes" is primarily used. This permits a variety of different sources to be statistically combined and compared, whether the inputs are expressed as the number of failures and exposure time or demands, or as means and lognormal error factors.

A typical application of Bayes' theorem is illustrated as follows. A failure rate for a given component is needed for a fault tree (e.g., a fan motor in the HVAC system). There is no absolute value for the failure rate, but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data to the YMP introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying available data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.

2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trials if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur over a certain exposure, operational, or test duration.

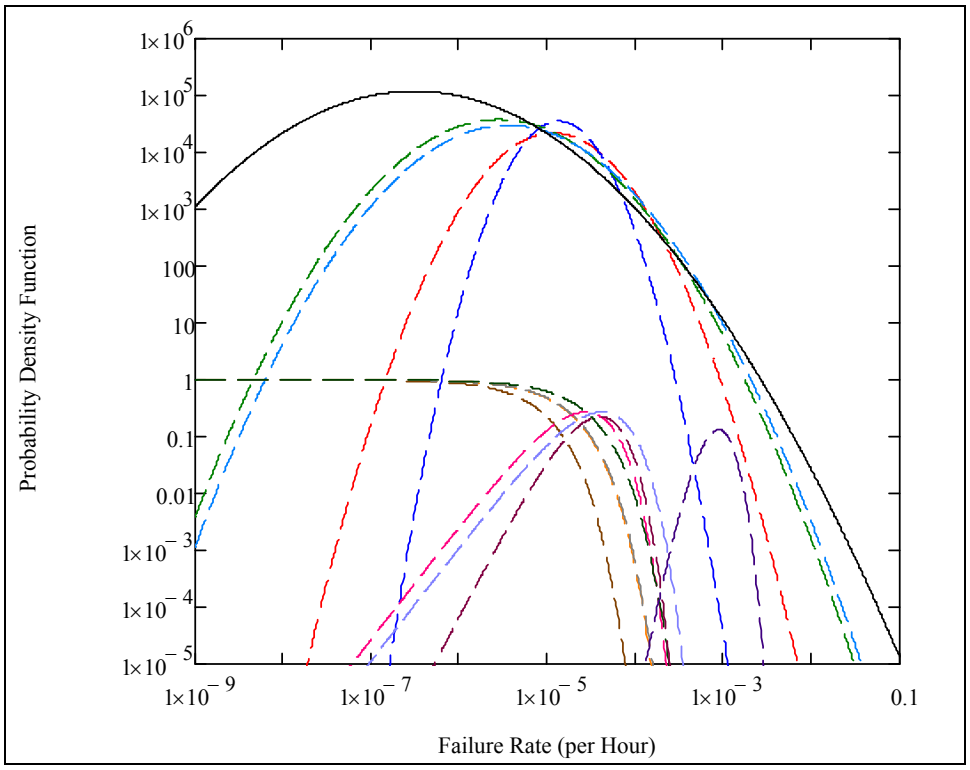
3. Update the probability distribution for the failure rate based on the new body of evidence.

The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The mathematical expression for applying Bayes' theorem to data analysis is described in Attachment C, Section C2, Equation C1.

For the analysis presented herein, MathCAD is used to calculate the population-variability (prior) distributions of active components. As described in Attachment C, Section C2.1, the

method of "The Combined Use of Data and Expert Estimates in Population Variability Analysis" (Ref. 2.2.56, pp. 311–321)) is used as the basis example for the combinations performed. In this method, the population-variability distribution of the failure rate is approximated by a lognormal distribution whose unknown parameters, v and τ, respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating v and τ involves calculating the likelihood function associated with the reliability information in each data source. For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate x, and characterized by its median value and associated error factor. For a data source providing exposure data (given in the form of a number n of recorded failures over an exposure time t), the likelihood function is a Poisson distribution, expressing the probability that n failures are observed when the expected number of failures is x times t.

The maximum likelihood method is used to calculate v and τ. This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source because the data sources are independent from each other. It is equivalent and computationally convenient to find the maximum likelihood estimators for v and τ by using the sum of the log-likelihood (logarithm of the likelihood) of each data source. As a result, the likelihood functions from the individual data sources and a population-variability probability density function for the combination are produced and plotted for comparison, as in the example shown as Figure 6.3-1.



Source: Attachment C, Figure C2.1-1

Figure 6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

If only a single data source is considered applicable to a given TYP-FM combination and if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. However, if the data source does not readily provide a probability distribution, but instead exposure data, (i.e., a number of recorded failures over an exposure time for failure rates or over a number of demands for failure probabilities), the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffrey's non-informative prior distribution (i.e., gamma for time-related failure modes and beta for demand based failure modes).

Example implementations of the methods used for these cases are provided in Attachment C Section C2.2.

6.3.1.3 Common-Cause Failure Data

Dependent failures are modeled in event tree and fault tree logic models. When possible, potential dependent failures are modeled explicitly via the logic models. For example, failure of the HVAC system is explicitly dependent upon failure in the electrical supply system that is modeled in the fault trees. Similarly, the effects of erroneous calibration or other human failure events can be explicitly included in the system fault tree models and the basic event probabilities considered during the HRA. Otherwise, potential dependencies known as CCFs are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate common-cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method, the Multiple Greek Letter (MGL) method, and the Alpha Factor Method (Ref. 2.2.61). In a parametric model, the probability of two or more components failing by a CCF is estimated by use of the equations provided in Section 4.3.3.3.

For the PCSA, common-cause failure rates or probabilities are estimated using the Alpha Factor method *NUREG/CR-5485* (Ref. 2.2.61) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in the Alpha Factor method (Ref. 2.2.61) consisted of:

1. Identifying the number of redundant components in each subsystem being reported, (e.g., two, three, or four (termed the CCF group size)).

2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, (i.e., one component at a time, two components at a time, and so on up to failure of all components in a given CCF group).

3. Calculating the alpha factor for a given component type to provide a basis for estimating the probability of CCFs involving two, three, etc., or all components. (See equation in Attachment C, Section C3).

4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produces prior distributions for the alpha factors. The results are the mean, alpha factors, and uncertainty bounds, reported in *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment* (Ref. 2.2.61, Table 5-11) and reproduced in Attachment C, Table C3-1.

These alpha-factors values are used for failure-on-demand events (e.g., pump failure to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run). For example, for a 2-out-of-2 failure on demand event, the mean alpha factor of 0.047 (shown in the far right column of Table C3-1 associated with α_2) was multiplied by the mean failure probability for the appropriate component type and failure mode (from Table C4-1) to yield the common-cause failure probability.

6.3.1.4 Input to SAPHIRE Models

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data has to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

1. BEA – attributes to assign information to the proper SAPHIRE fields.
2. BED – descriptions of the component type name and failure mode.
3. BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement such that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the PCSA case, was the TYP-FM coding). Examples of descriptions used for the PCSA template data were, clutch failed to operate, relay spurious operation, position sensor fails on demand, and wire rope breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the lognormal error factor, or the shape parameter of the Beta or Gamma distributions.

Geometric means of the input parameters from the data sources are initially used as screening values for each TYP-FM and are entered into the .BEI file, along with a default Error Factor of 10. Once the Bayesian combination process is completed for all of the TYP-FM combinations, mean and uncertainty parameter information are entered into the .BEI files, and tested in SAPHIRE before being distributed to the systems analysts.

The template data is utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the SAPHIRE code, then by using the modify event feature to link the template data to each basic event in the fault tree. This permits each active component of the same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the data investigation and Bayesian combination process.

Attachment C, Section C4, presents a more thorough discussion of the active component reliability data development process, as well as a table of the template data that is imported into SAPHIRE.

6.3.1.5 Summary of Active Component Reliability Data in WHF Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the WHF models. Development of this table is discussed in detail in Attachment C, Section C4. Mission times are discussed in Section 6.2.

Table 6.3-1. Active Component Reliability Data Summary

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-#EEE-CRCF1-B-XMR-FOH	WHF ITS Transformer Train B Failure	2.10E-04	2.91E-07	7.20E+02
050-#EEE-LDCNTRA-BUA-FOH	WHF Load Center A Fails	4.39E-04	6.10E-07	7.20E+02
050-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	1.03E-04	6.10E-07	1.68E+02
050-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A Post Maintenance	1.03E-05	0.00E+00	0.00E+00
050-#EEE-LDCNTRA-C52-FOD	Load Center A Feed Breaker Fails to Reclose	2.24E-03	0.00E+00	0.00E+00
050-#EEE-LDCNTRA-C52-SPO	Load Center A Feed Circuit Breaker Spurious Operation	3.82E-03	5.31E-06	7.20E+02
050-#EEE-LDCNTRB-BUA-FOH	WHF ITS Load Center B Fails	4.39E-04	6.10E-07	7.20E+02
050-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	1.03E-04	6.10E-07	1.68E+02
050-#EEE-LDCNTRB-BUA-ROE	Failure to Restore ITS Load Center Train B Post Maintenance	1.03E-05	0.00E+00	0.00E+00
050-#EEE-LDCNTRB-C52-FOD	13.8 ITS SWGR to WHF ITS LC B Circuit Breaker Fails on Demand	2.24E-03	0.00E+00	0.00E+00
050-#EEE-LDCNTRB-C52-SPO	WHF ITS Load Center Circuit Breaker (AC) Spur Op	3.82E-03	5.31E-06	7.20E+02
050-#EEE-LDCNTRS-C52-CCF	Common Cause Failure of the ITS Load Center Feed Breakers to Reclose	1.05E-04	0.00E+00	0.00E+00
050-#EEE-MCC0001-C52-SPO	WHF ITS MCC 0001 Feed Breaker Spurious Operation	3.82E-03	5.31E-06	7.20E+02
050-#EEE-MCC0001-MCC-FOH	WHF ITS MCC 00001 Fails	5.38E-03	7.49E-06	7.20E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-#EEE-MCC0002-C52-SPO	WHF MCC-00002 Feed Breaker Spurious Operation	3.82E-03	5.31E-06	7.20E+02
050-#EEE-MCC0002-MCC-FOH	WHF ITS MCC00002 Failure	5.38E-03	7.49E-06	7.20E+02
050-#EEE-WHFITSA-XMR-CCF	WHF ITS Transformers CCF	4.45E-06	2.91E-07	3.40E+01
050-#EEE-WHFITSA-XMR-FOH	WHF ITS Transformer Train B Failure	2.10E-04	2.91E-07	7.20E+02
050--CTT--SV401--SV--FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.87E-05	4.87E-05	0.00E+00
050-CCS-CQD1--QDV-FOH	Quick Disconnect CQD1 Fails	4.26E-06	4.26E-06	0.00E+00
050-CCS-CSKVLV1-CKV-FOD	Cask Check Valve 1 Fails to Check	6.62E-04	0.00E+00	0.00E+00
050-CCS-DRNHOSE-HOS-LEK	Cask Cooling Drain Hose Leaks	1.48E-05	1.48E-05	1.00E+00
050-CCS-DRNHOSE-HOS-RUP	Cask Cooling Drain Hose Ruptures	1.48E-06	1.48E-06	1.00E+00
050-CCS-DRNQD01-QDV-FOH	Cask Cooling QD Valve Fails	4.26E-06	4.26E-06	0.00E+00
050-CCS-DRNQD02-QDV-FOH	Cask Cooling QD 02 Valve Fails	4.26E-06	4.26E-06	0.00E+00
050-CCS-PIPBW03-PPL-RUP	Drain Piping Catastrophic - Line BW-0003	3.54E-06	4.42E-07	8.00E+00
050-CCS-PIPBW04-PPL-RUP	Drain Piping Catastrophic - Line BW-0004	3.54E-06	4.42E-07	8.00E+00
050-CCS-PIPBW05-PPL-RUP	Drain Piping Catastrophic - Line BW-0005	3.54E-06	4.42E-07	8.00E+00
050-CCS-PLCSPUR-PLC-SPO	PLC Spurious Operation Causes Pump Motor to Run Too Fast	2.92E-06	3.65E-07	8.00E+00
050-CCS-PMTRFST-MSC-FOH	Pump Motor Runs Too Fast	1.02E-03	1.28E-04	8.00E+00
050-CCS-PUMPINT-IEL-FOD	Positive Displace Pump Interlock Fails	2.75E-05	0.00E+00	0.00E+00
050-CCS-PUMPSTP-PMD-FTR	Pump P-00002 Fails to Run	2.76E-04	3.45E-05	8.00E+00
050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.54E-03	0.00E+00	0.00E+00
050-CCS-THVLVFL-NZL-FOH	Throttle Valve to Pump Fails Open	2.28E-05	2.85E-06	8.00E+00
050-CCS-VNTPIPE-PPM-PLG	Pipe BW-0003 plugs	5.81E-06	7.26E-07	8.00E+00
050-CHC-CSKDROP-CRN-DRP	Cask Handling Crane Drop	3.21E-05	0.00E+00	1.00E+00
050-CHC-SLNGDRP-CRS-DRP	Cask handling Crane Sling Drop	1.21E-04	0.00E+00	1.00E+00
050-CHC-TWOBLCK-CRN-TBK	Cask Handling Crane Two Block Drop	4.41E-07	0.00E+00	1.00E+00
050-CR---IEL001--IEL-FOD	Interlock A From Slide Gate Fails	2.75E-05	0.00E+00	0.00E+00
050-CR---IEL002--IEL-FOD	Interlock B From Slide Gate Fails	2.75E-05	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-CR---IELCCF--IEL-FOH	Common Cause Failure of Interlocks From Slide Gate	1.29E-06	0.00E+00	0.00E+00
050-CR---PLC001--PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3.65E-07	3.65E-07	0.00E+00
050-CRN-BRIDGMTR-MOE-FSO	CTM Bridge Motor (Electric) Fails to Shut Off	1.08E-07	1.35E-08	8.00E+00
050-CRN-HSTTRLMO-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1.00E+00
050-CRN-PLC0101--PLC-SPO	Crane bridge motor PLC spurious operation	3.65E-07	3.65E-07	0.00E+00
050-CRWT-BRK001--BRK-FOD	Tractor Brake A Fails	1.46E-06	0.00E+00	0.00E+00
050-CRWT-BRK002--BRK-FOD	Tractor Brake B Fails	1.46E-06	0.00E+00	0.00E+00
050-CRWT-BRK003--BRK-FOD	Trailer Brakes Fail	1.46E-06	0.00E+00	1.00E+00
050-CRWT-BRKCCF--BRK-FOD	CCF of Both Tractor Brakes	6.86E-08	6.86E-08	1.00E+00
050-CRWT-LPATH--ATH--CCF	CCF of Pendular Axle Hydraulics During Load/Unload	9.80E-06	9.80E-06	0.00E+00
050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LSJATH--ATH-CCF	CCF of Stabilizing Jacks	4.58E-06	0.00E+00	0.00E+00
050-CRWT-LSJATH1-ATH-FOH	Stabilizing Jack 1 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LSJATH2-ATH-FOH	Stabilizing Jack 2 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LSJATH3-ATH-FOH	Stabilizing Jack 3 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-LSJATH4-ATH-FOH	Stabilizing Jack 4 Failure	1.78E-03	8.91E-04	2.00E+00
050-CRWT-TRCT-STEER-FAIL	Tractor Steering System Failure	1.84E-05	0.00E+00	0.00E+00
050-CRWT-TRD0001-TRD-FOH	Front Portside Track Failure	5.89E-07	5.89E-07	0.00E+00
050-CRWT-TRD0002-TRD-FOH	Rear Portside Track Failure	5.89E-07	5.89E-07	0.00E+00
050-CRWT-TRD0003-TRD-FOH	Front Starboard Track Failure	5.89E-07	5.89E-07	0.00E+00
050-CRWT-TRD0004-TRD-FOH	Rear Starboard Track Failure	5.89E-07	5.89E-07	0.00E+00
050-CRWT-TRLR-STEER-FAIL	Trailer Steering System Failure	1.84E-05	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-CTM-##ZE0133-ECP-FOH	Bell/Grapple/Canister Alignment Position Encoder Fails	1.43E-05	1.79E-06	8.00E+00
050-CTM-##ZI0133-ALM-SPO	Bell/Grapple/Canister Alignment Position Ind Alarm Fails	4.74E-07	4.74E-07	1.00E+00
050-CTM-##ZS0133-#ZS-FOD	Bell/Grapple/Canister Alignment Limit Switch Fails	2.93E-04	0.00E+00	0.00E+00
050-CTM-#ZSH0112-1ZS-FOD	CTM Shield skirt position switch 0112 fails	2.93E-04	0.00E+00	0.00E+00
050-CTM--121122-ZS--CCF	CCF CTM Upper Limit Position Switches	1.36E-05	0.00E+00	0.00E+00
050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.93E-04	0.00E+00	1.00E+00
050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	2.93E-04	0.00E+00	1.00E+00
050-CTM--CBL0001-WNE-BRK	CTM Hoist Wire Rope Breaks	2.00E-06	0.00E+00	1.00E+00
050-CTM--CBL0002-WNE-BRK	CTM Hoist Wire Rope Breaks	2.00E-06	0.00E+00	1.00E+00
050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.40E-08	0.00E+00	0.00E+00
050-CTM--DRTRN-CT--FOD	Controller Failure	4.00E-06	0.00E+00	0.00E+00
050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	4.00E-08	0.00E+00	1.00E+00
050-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	5.02E-05	0.00E+00	1.00E+00
050-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure	2.01E-04	8.38E-06	2.40E+01
050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1.15E-06	0.00E+00	1.00E+00
050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1.15E-06	0.00E+00	1.00E+00
050-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	6.50E-06	6.50E-06	1.00E+00
050-CTM--HOLDBRK-BRK-FOD	CTM Holding Brake Failure on Demand	1.46E-06	0.00E+00	1.00E+00
050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3.52E-05	4.40E-06	8.00E+00
050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	2.75E-05	0.00E+00	1.00E+00
050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1.15E-06	0.00E+00	1.00E+00
050-CTM--OVERSP--ZS--FOD	CTM Hoist Motor Speed Limit Switch Failure on Demand	2.93E-04	0.00E+00	1.00E+00
050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	6.74E-07	6.74E-07	1.00E+00
050-CTM--PORTGT1-PLC-SPO	Port Gage 1 PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	6.74E-07	6.74E-07	1.00E+00
050-CTM--PORTGT2-PLC-SPO	Port Gage 2 PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	6.74E-07	6.74E-07	1.00E+00
050-CTM--SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM--SLIDGT2-IEL-FOD	CTM Slide Gate Interlock Failure	2.75E-05	0.00E+00	0.00E+00
050-CTM--TROLLY-MOE-SPO	Motor (Electric) Spurious Operation	6.74E-07	6.74E-07	1.00E+00
050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1.15E-06	0.00E+00	1.00E+00
050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.99E-03	0.00E+00	1.00E+00
050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	2.93E-04	0.00E+00	1.00E+00
050-CTM--YS01129-ZS--FOD	CTM Drum Brake Control Circuit Switch Fail	2.93E-04	0.00E+00	1.00E+00
050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.28E-06	1.28E-06	1.00E+00
050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller Fails	2.03E-03	0.00E+00	1.00E+00
050-CTM-BIDGMTR-#TL-FOH	CTM Bridge Motor Torque Limiter Failure	2.86E-02	8.05E-05	3.60E+02
050-CTM-BRDGPSTN-PLC-SPO	CTM Canister Alignment PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM-BRIDGETR-#PR-FOH	Passive Restraint (Bumper) Failure	1.95E-06	4.45E-10	4.38E+03
050-CTM-BRIDGETR-MOE-FSO	CTM Shield Skirt-Bridge motor Interlock Failure	1.35E-08	1.35E-08	1.00E+00
050-CTM-BRIDGMTR-#CT-FOD	CTM bridge motor controller fails	4.00E-06	0.00E+00	0.00E+00
050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	2.75E-05	0.00E+00	0.00E+00
050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	6.74E-07	6.74E-07	0.00E+00
050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	6.74E-08	6.74E-07	1.00E-01
050-CTM-HC0104##-#HC-FOD	CTM hand held radio remote controller fails	1.74E-03	0.00E+00	0.00E+00
050-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.08E-07	1.35E-08	8.00E+00
050-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation M- Shear	6.74E-08	6.74E-07	1.00E-01

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist Motor Torque limiter Failure	2.86E-02	8.05E-05	3.60E+02
050-CTM-HSTTRLLY-IEL-FOD	CTM Shield Skirt Hoist Trolley Motor Interlock Failure	2.75E-05	0.00E+00	0.00E+00
050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	6.74E-07	6.74E-07	0.00E+00
050-CTM-LM001-ZS-SPO-CCF	CCF CTM Grapple Engaged/Disengaged Position Switches	6.00E-08	6.00E-08	0.00E+00
050-CTM-MISSPOOL--DM-MSP	CTM Mis-spool Event	6.86E-07	6.86E-07	0.00E+00
050-CTM-MISSPOOL-LRG-FOH	Lifting Rig Or Hook All Modes	7.45E-07	7.45E-07	1.00E+00
050-CTM-OPSENSOR-SRX-FOH	Canister Above CTM Slide Gate Optical Sensor Fails	4.70E-06	4.70E-06	0.00E+00
050-CTM-PLC0101#-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM-PLC0101--PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3.65E-08	3.65E-07	1.00E-01
050-CTM-PLC0102--PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -Shear	3.65E-08	3.65E-07	1.00E-01
050-CTM-PLC0103--PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3.65E-07	3.65E-07	1.00E+00
050-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -Shear	3.65E-08	3.65E-07	1.00E-01
050-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) Spurious Operation-Shear	6.74E-08	6.74E-07	1.00E-01
050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.86E-02	8.05E-05	3.60E+02
050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.75E-05	0.00E+00	0.00E+00
050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	6.74E-07	6.74E-07	0.00E+00
050-CTM-SKRTCTCT-SRP-FOD	CTM Skirt Floor Contact Sensors Fail	3.99E-03	0.00E+00	0.00E+00
050-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1.10E-03	0.00E+00	1.00E+00
050-CTM-TROLLEYT-MOE-FSO	Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1.00E+00
050-CTM-TROLLYTR--PR-FOH	Passive Restraint (Bumper) Failure	1.95E-06	4.45E-10	4.38E+03
050-CTM-TROLYCNT-#HC-FOD	Hand Held Controller Failure to Stop (on Demand)	1.74E-03	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.28E-06	1.28E-06	1.00E+00
050-CTT--CT001---CT--SPO	Onboard Controller Spurious Operation	2.27E-05	2.27E-05	1.00E+00
050-CTT--DSW000--ESC-CCF	Common Cause Failure of Deadman Switches	1.18E-05	1.18E-05	1.00E+00
050-CTT--DSW001--ESC-FOD	Deadman Switch 1 Fails Closed	2.50E-04	0.00E+00	0.00E+00
050-CTT--DSW002--ESC-FOD	Deadman Switch 2 Fails Closed	2.50E-04	0.00E+00	1.00E+00
050-CTT--HC001---HC--SPO	Hand Held Radio Remote Controller Spurious Operation	5.23E-07	5.23E-07	1.00E+00
050-CTT--HC021---HC--FOD	Remote Stop Control Transmits Wrong Instruction	1.74E-03	0.00E+00	0.00E+00
050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.09E-07	4.09E-07	1.00E+00
050-CTT--SV601---SV--FOD	Main Air Supply Valve on CTT Fails to Close	6.28E-04	0.00E+00	1.00E+00
050-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	6.28E-04	0.00E+00	0.00E+00
050-CTT--ZS301---ZS--FOD	Pin Limit Switch #1 Fails	2.93E-04	0.00E+00	0.00E+00
050-CTT--ZS302---ZS--FOD	Pin Limit Switch #2 Fails	2.93E-04	0.00E+00	0.00E+00
050-CTT-FWDREVM1-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.87E-05	4.87E-05	0.00E+00
050-CTT-FWDREVM2-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.87E-05	4.87E-05	0.00E+00
050-CTT-PINLIMIT-ZS-CCF	Common Cause Failure of Limit Switches	1.38E-05	0.00E+00	0.00E+00
050-CTT-SVROTM1--SV--FOH	Failure of SV Providing Rotation to Motor 1	4.87E-05	4.87E-05	0.00E+00
050-CTT-SVROTM2--SV--FOH	Failure of SV Providing Rotation to Motor 2	4.87E-05	4.87E-05	0.00E+00
050-EXCESSIVE-WIND-SPEED	Sustained Wind Exceeds 40 MPH and Gust to 90 MPH	4.70E-03	0.00E+00	0.00E+00
050-FIRE-CSNF-PREP	Prep Area Fire Affects CSNF	5.40E-06	0.00E+00	0.00E+00
050-FIRE-CSNF-VEST	Fire Threatens CSNF in Entrance Vestibule	3.00E-06	0.00E+00	0.00E+00
050-FIRE-DPC-CTM	Fire Affects DPC in the CTM	8.30E-08	0.00E+00	0.00E+00
050-FIRE-DPC-DPCCUT	Fire Affects DPC at DPC Cutting	1.70E-05	0.00E+00	0.00E+00
050-FIRE-DPC-LARGE	Large fire affects DPC in facility	1.00E-04	0.00E+00	0.00E+00
050-FIRE-DPC-PREP	Fire affects DPC in Prep Area	8.90E-06	0.00E+00	0.00E+00
050-FIRE-DPC-UNLOAD	Fire affects DPC in Unload Room	4.90E-07	0.00E+00	0.00E+00
050-FIRE-DPC-VEST	Fire Affects DPC in Entrance Vestibule	1.20E-05	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-FIRE-LARGE-CSNF	Large Fire Affects CSNF	1.10E-05	0.00E+00	0.00E+00
050-FIRE-TAD-CLOSE	Fire Affects TAD in Closure Area	2.30E-05	0.00E+00	0.00E+00
050-FIRE-TAD-CTM	Fire Affect TAD in CTM	6.90E-08	0.00E+00	0.00E+00
050-FIRE-TAD-LARGE	Large Fire Affects TAD in WHF	6.70E-05	0.00E+00	0.00E+00
050-FIRE-TAD-LOAD	Fire Affects TAD in Loading Room	2.90E-07	0.00E+00	0.00E+00
050-FIRE-TAD-UNLOAD	Fire Affects TAD in Unload Room	3.30E-07	0.00E+00	0.00E+00
050-FIRE-TAD-VEST	Fire affects TAD in Entrance Vestibule (Bolting)	3.50E-07	0.00E+00	0.00E+00
050-FL---SC001---SC--FOH	Speed Control Failure	1.28E-04	1.28E-04	1.00E+00
050-HTTCOLLIDE---G65-FOH	Speed Limiter Fails	1.16E-05	1.16E-05	0.00E+00
050-JIBCRANE-CRJ-DRP	Jib Crane Drop	2.60E-05	0.00E+00	0.00E+00
050-LLW-RECIRC-PPM-RUP	LLW Recirculation Piping Ruptures	7.67E-06	8.75E-10	8.76E+03
050-OIL-MODERATOR	Oil Moderator Sources in WHF (Gear Boxes)	9.00E-05	0.00E+00	0.00E+00
050-OPEXPOSESAMP-HOS-RUP	Hose Ruptures During Sampling	1.48E-06	1.48E-06	1.00E+00
050-OTHER-WATER	Water Moderator From Other Sources	1.50E-05	0.00E+00	0.00E+00
050-PHC-OBJDROP-CRN-DRP	Pool Handling Crane Drop	3.21E-05	0.00E+00	0.00E+00
050-PHC-TWOBLCK-CRN-TBK	Pool Handling Crane Two Block Drop	4.41E-07	0.00E+00	1.00E+00
050-PMTT-BRK000--BRH-FOD	Hydraulic Brakes on PMTT Fail on Demand	1.46E-06	0.00E+00	0.00E+00
050-PMTT-CBP002-CBP--OPC	PMTT Power Cable - Open Circuit	9.13E-08	9.13E-08	0.00E+00
050-PMTT-CBP003--CBP-SHC	PMTT Power Cable - Short Circuit	1.88E-08	1.88E-08	0.00E+00
050-PMTT-CT000---CT--FOD	PMTT Primary Stop Switch Fails	4.00E-06	0.00E+00	0.00E+00
050-PMTT-HC001--HC--FOD	Remote Control Transmits Wrong Signal	1.74E-03	0.00E+00	0.00E+00
050-PMTT-MOE000--MOE-FSO	PMTT Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	0.00E+00
050-PMTT-PLC001--PLC-FOD	On-Board Controller Fails to Respond	3.69E-04	0.00E+00	0.00E+00
050-PMTT-SC001---SC--SPO	On-Board Controller Initiates Spurious Signal	3.65E-07	3.65E-07	0.00E+00
050-PMTT-SC021---SC--FOH	Speed Controller on PMTT Pendant Fails	1.28E-04	1.28E-04	0.00E+00
050-PMTT-SEL021--SEL-FOH	Speed Selector on PMTT Pendant Fails	2.84E-06	2.84E-06	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-PORTSLIDEGTE-IEL-FOD	Port Slide gate interlock Fails	2.75E-05	0.00E+00	0.00E+00
050-PWR-LOSS	Loss of Site Power	4.10E-06	0.00E+00	0.00E+00
050-PWR-LOSS-2	Loss of Power	5.70E-06	0.00E+00	0.00E+00
050-SD---PLC001--PLC-SPO	Spurious Signal From PLC Closes Door	3.65E-07	3.65E-07	1.00E+00
050-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.16E-03	9.62E-05	0.00E+00
050-SD---TL000---TL--CCF	Common Cause Failure of Over Torque Sensors	6.80E-04	3.78E-06	0.00E+00
050-SD---TL001---TL--FOH	Motor #1 over Torque Sensor Fails	1.44E-02	8.05E-05	0.00E+00
050-SD---TL002---TL--FOH	Motor #2 over Torque Sensor Fails	1.44E-02	8.05E-05	0.00E+00
050-SFTM-FUELDRP-SFT-DRP	Spent Fuel Transfer Machine (SFTM) Drop	5.15E-06	0.00E+00	1.00E+00
050-SFTM-TOOHIGH-SFT-RTH	Spent Fuel Transfer Machine Fuel Raised Too High	7.36E-07	0.00E+00	0.00E+00
050-SLDGATE-IEL-FOD	Slide gate interlock fails	2.75E-05	0.00E+00	0.00E+00
050-SPMRC--CT001--CT-FOD	On-Board Controller Fails to Respond	4.00E-06	0.00E+00	0.00E+00
050-SPMRC-BRK001-BRP-FOD	SPMRC Brake Failure on Demand	5.02E-05	0.00E+00	0.00E+00
050-SPMRC-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.02E-05	0.00E+00	0.00E+00
050-SPMRC-BRP000-BRP-FOH	PMRC Fails to Stop on Loss of Power	8.38E-06	8.38E-06	0.00E+00
050-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	9.13E-08	9.13E-08	0.00E+00
050-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable - Short Circuit	1.88E-08	1.88E-08	0.00E+00
050-SPMRC-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	1.91E-06	1.91E-06	0.00E+00
050-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.00E-06	0.00E+00	0.00E+00
050-SPMRC-CT002--CT--FOH	Pendant Direction Controller Fails	6.88E-05	6.88E-05	0.00E+00
050-SPMRC-CT003-CT-SPO	On-Board Controller Initiates Spurious Signal	2.27E-05	2.27E-05	0.00E+00
050-SPMRC-DERAIL-PERMILE	Derailment Failure per Mile	1.18E-05	1.18E-05	0.00E+00
050-SPMRC-G65000-G65-FOH	PMRC Speed Control (Governor) Fails	1.16E-05	1.16E-05	0.00E+00
050-SPMRC-HC001--HC--FOD	Pendant Control Transmits Wrong Signal	1.74E-03	0.00E+00	0.00E+00
050-SPMRC-HC001--HC--SPO	Spurious Command from Pendant Controller	5.23E-07	5.23E-07	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.75E-05	0.00E+00	0.00E+00
050-SPMRC-MOE000-MOE-FSO	SPMRC Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	0.00E+00
050-SPMRC-SC021--SC--FOH	Speed Controller on SPMRC Pendant Fails	1.28E-04	1.28E-04	0.00E+00
050-SPMRC-SEL021-SEL-FOH	Speed Selector on SPMRC Pendant Fails	4.16E-06	4.16E-06	0.00E+00
050-SPMRC-STU001-STU-FOH	RC End Stops Fail	2.11E-04	4.81E-08	4.38E+03
050-SPMTT--CT001--CT-FOD	On-board Controller Fails to Respond	4.00E-06	0.00E+00	0.00E+00
050-SPMTT--CT001-CT--SPO	On-Board Controller Spurious Operation	2.27E-05	2.27E-05	0.00E+00
050-SPMTT-BRK001-BRP-FOD	SPMTT Pneumatic Brakes Fail	5.02E-05	0.00E+00	0.00E+00
050-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.02E-05	0.00E+00	0.00E+00
050-SPMTT-CBP001-CBP-OPC	Power cable to SPMTT - Open Circuit	9.13E-08	9.13E-08	0.00E+00
050-SPMTT-CBP001-CBP-SHC	SPMTT Power Cable - Short Circuit	1.88E-08	1.88E-08	0.00E+00
050-SPMTT-CPL000-CPL-FOH	Truck Trailer Automatic Coupler System Fails	1.91E-06	1.91E-06	0.00E+00
050-SPMTT-CT001--CT-FOD	On-Board Controller Fails to Respond	4.00E-06	0.00E+00	0.00E+00
050-SPMTT-CT002--CT--FOH	Controller Failure	6.88E-05	6.88E-05	1.00E+00
050-SPMTT-G65000-G65-FOH	PMTT Speed Control (Governor) Fails	1.16E-05	1.16E-05	0.00E+00
050-SPMTT-HC002--HC--SPO	Spurious Signal from Pendant Controller	5.23E-07	5.23E-07	0.00E+00
050-SPMTT-IEL102-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.75E-05	0.00E+00	0.00E+00
050-SPMTT-MOE000-MOE-FSO	SPMTT Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	0.00E+00
050-SPMTT-SC021--SC--FOH	Speed Controller on SPMTT Pendant Fails	1.28E-04	1.28E-04	0.00E+00
050-SPMTT-SEL021-SEL-FOH	Speed Selector on SPMTT Pendant Fails	4.16E-06	4.16E-06	0.00E+00
050-SPMTT-STU001-STU-FOH	SPMTT End Stops Fail	2.11E-04	4.81E-08	4.38E+03
050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.46E-06	0.00E+00	0.00E+00
050-ST---CBP004-CBP--OPC	ST Power Cable - Open Circuit	9.13E-08	9.13E-08	1.00E+00
050-ST---CBP004-CBP--SHC	ST Power Cable Short Circuit	1.88E-08	1.88E-08	0.00E+00
050-ST---CT000---CT--FOD	ST Primary Stop Switch Fails	4.00E-06	0.00E+00	0.00E+00
050-ST---CT002---CT--FOH	Direction Controller Fails	6.88E-05	6.88E-05	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-ST---HC000--HC--SPO	Spurious Commands from Remote Control	5.23E-07	5.23E-07	0.00E+00
050-ST---HC001--HC--FOD	Remote Control Transmits Wrong Signal	1.74E-03	0.00E+00	0.00E+00
050-ST---HC002---HC--SPO	Spurious Command to Lift/Lower AO or STC	5.23E-07	5.23E-07	0.00E+00
050-ST---MOE000--MOE-FSO	ST Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	1.00E+00
050-ST---MOE021--MOE-FSO	Drive System on Primary Propulsion Fails	1.35E-08	1.35E-08	0.00E+00
050-ST---SC002--SC--FOH	Speed Control on ST Pendant Control Fails	1.28E-04	1.28E-04	0.00E+00
050-ST---SC021---SC--FOH	Speed Controller on ST Pendant Fails	1.28E-04	1.28E-04	0.00E+00
050-ST---SC021---SC--SPO	On-Board Controller Initiates Spurious Signal	3.20E-05	3.20E-05	0.00E+00
050-ST---SEL021--SEL-FOH	Speed Selector on ST Pendant Fails	4.16E-06	4.16E-06	0.00E+00
050-TADDRY-HOS-RUP	Hose Ruptures	1.48E-06	1.48E-06	0.00E+00
050-VCOO-NITS-PWR-FAILS	Non-ITS Power Failure to RF Supply Fan	3.54E-02	5.00E-05	7.20E+02
050-VCOO-SFAN001-FAN-FTR	Supply Fan #01 for WHF Fails	5.06E-02	7.21E-05	7.20E+02
050-VCOO-SFAN002-FAN-FTR	Supply Fan #2 for WHF Fails	5.06E-02	7.21E-05	7.20E+02
050-VCOO-SFAN003-FAN-FTR	Supply Fan #3 In Standby for WHF Fails	2.56E-02	7.21E-05	3.60E+02
050-VCSO-B000000-FAN-FTS	Train B Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCSO-DMP000A-DMP-FRO	Manual Damper for Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP000B-DMP-FRO	Manual Damper for Train B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP001A-DMP-FOH	Manual damper Input to Exhaust Fan A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP001A-DMP-FRO	Manual damper Input to Exhaust Fan A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP001B-DMP-FRO	Manual damper Input to Exhaust Fan B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP001I-DMP-FRO	Manual Damper #01 input Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP001O-DMP-FRO	Manual Damper #01 Output Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP002I-DMP-FRO	Manual Damper #02 Input Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP002O-DMP-FRO	Manual Damper #2 Output Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP003I-DMP-FRO	Manual Damper #03 in Train A Fails	6.03E-05	8.38E-08	7.20E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-VCSO-DMP003O-DMP-FRO	Manual Damper #3 Output Train A Fails	6.03E-05	8.38E-08	7.20E+02
050-VCSO-DMP005I-DMP-FRO	Manual Damper #05 input Train B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP005O-DMP-FRO	Manual Damper #05 Output Train A Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP006I-DMP-FRO	Manual Damper #06 Input Train B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP006O-DMP-FRO	Manual Damper #06 Output Train A Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP007I-DMP-FRO	Manual Damper #07 Input Train B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP007O-DMP-FRO	Manual Damper #07 Output Train A Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DMP05I-DMP-FR0	Manual Damper #5 Input Train B Fails	3.02E-05	8.38E-08	3.60E+02
050-VCSO-DRS0000-DRS-OPN	Vestibule Door Open during Receipt/Export	1.60E-04	0.00E+00	0.00E+00
050-VCSO-DTC0A-DTC-RUP	Duct Fails Between HEPA and Exhaust Fan (10 feet)	2.68E-03	3.72E-06	7.20E+02
050-VCSO-DTC0B-DTC-RUP	Duct Fails Between HEPA and Exhaust Fan (10 feet)	1.34E-03	3.72E-06	3.60E+02
050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.06E-02	7.21E-05	7.20E+02
050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.56E-02	7.21E-05	3.60E+02
050-VCSO-FAN00B-FAN-FTS	Exhaust Fan in Train B Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCSO-FANA-PRM-FOH	Speed Control Exhaust Fan Train A Fails to maintain Delta P	3.87E-04	5.38E-07	7.20E+02
050-VCSO-FANB-PRM-FOH	Speed Control Exhaust Fan Train A Fails to Start B	3.87E-04	5.38E-07	7.20E+02
050-VCSO-FSLAB0-SRF-FOH	Low Flow Train A Switch Failure	7.70E-04	1.07E-06	7.20E+02
050-VCSO-HEPA-CCF	Common Cause Failure of HEPA Filters	3.85E-05	1.07E-07	3.60E+02
050-VCSO-HEPA01-DMS-FOH	Moisture Separator/Demister HEPA 01 Fails	6.55E-03	9.12E-06	7.20E+02
050-VCSO-HEPA02-DMS-FOH	Moisture Separator/Demister HEPA 02 Fails	6.55E-03	9.12E-06	7.20E+02
050-VCSO-HEPA03-DMS-FOH	Moisture Separator/Demister HEPA 03 Fails	6.55E-03	9.12E-06	7.20E+02
050-VCSO-HEPA05-DMS-FOH	Moisture Separator/Demister HEPA 05 Fails	3.28E-03	9.12E-06	3.60E+02
050-VCSO-HEPA06-DMS-FOH	Moisture Separator/Demister HEPA 06 Fails	3.28E-03	9.12E-06	3.60E+02
050-VCSO-HEPA07-DMS-FOH	Moisture Separator/Demister HEPA 07 Fails	3.28E-03	9.12E-06	3.60E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-VCSO-HEPA0A1-HEP-LEK	HEPA #01 Train A Leaks	2.16E-03	3.00E-06	7.20E+02
050-VCSO-HEPAA01-HEP-PLG	HEPA #A01 Train A Plugged	3.07E-03	4.27E-06	7.20E+02
050-VCSO-HEPAA02-HEP-LEK	HEPA #02 Train A Leaks	2.16E-03	3.00E-06	7.20E+02
050-VCSO-HEPAA02-HEP-PLG	HEPA #A02 Train A Plugged	3.07E-03	4.27E-06	7.20E+02
050-VCSO-HEPAA03-HEP-LEK	HEPA #03 Train A Leaks	2.16E-03	3.00E-06	7.20E+02
050-VCSO-HEPAA03-HEP-PLG	HEPA #A03 Train A Plugged	3.07E-03	4.27E-06	7.20E+02
050-VCSO-HEPAA10-HEP-PLG	HEPA #A10 Train A Plugged	3.07E-03	4.27E-06	7.20E+02
050-VCSO-HEPAB05-HEP-LEK	HEPA #B05 Train B Leaks	1.08E-03	3.00E-06	3.60E+02
050-VCSO-HEPAB05-HEP-PLG	HEPA #B05 Train B Plugged	1.54E-03	4.27E-06	3.60E+02
050-VCSO-HEPAB06-HEP-LEK	HEPA #B06 Train B Leaks	1.08E-03	3.00E-06	3.60E+02
050-VCSO-HEPAB06-HEP-PLG	HEPA #B06 Train B Plugged	1.54E-03	4.27E-06	3.60E+02
050-VCSO-HEPAB07-HEP-LEK	HEPA #B07 Train B Leaks	1.08E-03	3.00E-06	3.60E+02
050-VCSO-HEPAB07-HEP-PLG	HEPA #B07 Train B Plugged	1.54E-03	4.27E-06	3.60E+02
050-VCSO-IEL0001-IEL-FOD	WHF Door Interlock Failure	2.75E-05	0.00E+00	0.00E+00
050-VCSO-PDSLA0B-SRP-FOD	Pressure Differential Train A Switch Fails	3.99E-03	0.00E+00	0.00E+00
050-VCSO-SUPFAN-CCF	Common Cause Failure of WHF Supply Fans (3 of 3)	1.35E-03	1.87E-06	7.20E+02
050-VCSO-TDMP00A-DTM-FOD	Tornado Damper Train A Fails	8.71E-04	0.00E+00	0.00E+00
050-VCSO-TDMP00A-DTM-FOH	Tornado Damper Train A Fails	1.61E-02	2.26E-05	7.20E+02
050-VCSO-TDMP00B-DTM-FOD	Tornado damper Train B Fails on Demand	8.71E-04	0.00E+00	0.00E+00
050-VCSO-TDMP00B-DTM-FOH	Tornado damper Train B Fails	8.10E-03	2.26E-05	3.60E+02
050-VCSO-TRAINB-MAINT	Train B HVAC is Off-Line for Maintenance	4.57E-03	0.00E+00	0.00E+00
050-VCSO-UDMP000-UDM-FOH	Backdraft Damper for Train B exhaust Fails	8.10E-03	2.26E-05	3.60E+02
050-VCT0-AHU0001-AHU-FTR	WHF ITS Elec AHU 00001 Fails to run	2.65E-03	3.68E-06	7.20E+02
050-VCT0-AHU0001-CTL-FOD	WHF ITS Elec AHU 00001 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-AHU0002-AHU-FTR	WHF ITS Elec AHU 00002 Fails to Run	2.65E-03	3.68E-06	7.20E+02
050-VCT0-AHU0002-CTL-FOD	WHF ITS Elec AHU 00002 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-AHU0002-FAN-FTS	WHF ITS Elec AHU 00002 Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCT0-AHU0003-AHU-FTR	WHF ITS Elec AHU 00003 Fails to Run	2.65E-03	3.68E-06	7.20E+02
050-VCT0-AHU0003-CTL-FOD	WHF ITS Elec AHU 00003 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-AHU0004-AHU-FTR	WHF ITS Elec AHU 00004 Fails to Run	2.65E-03	3.68E-06	7.20E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
050-VCT0-AHU0004-CTL-FOD	WHF ITS Elec AHU 00004 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-AHU0004-FAN-FTS	WHF ITS Elec AHU 00004 Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCT0-AHU0103-AHU-CCR	CCF of the running WHF ITS Elec AHUs to Continue to Run	6.20E-05	0.00E+00	0.00E+00
050-VCT0-AHU0202-AHU-CCR	CCF of Standby WHF ITS Elec AHUs to Start/Run	1.60E-04	0.00E+00	0.00E+00
050-VCT0-EXH-004-CTL-FOD	WHF ITS Elec Exh Fan 00004 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-EXH-004-FAN-FTR	WHF ITS Elec Exhaust Fan 00004 Fails to Run	5.06E-02	7.21E-05	7.20E+02
050-VCT0-EXH-005-CTL-FOD	WHF ITS Elec Exh Fan 00005 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-EXH-005-FAN-FTR	WHF ITS Elec Exhaust Fan 00005 Fails to Run	5.06E-02	7.21E-05	7.20E+02
050-VCT0-EXH-005-FAN-FTS	WHF ITS Elec Exh Fan 00005 Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCT0-EXH-006-CTL-FOD	WHF ITS Elec Exh Fan 0006 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-EXH-006-FAN-FTR	WHF ITS Elec Exh. Fan Fails to Run	5.06E-02	7.21E-05	7.20E+02
050-VCT0-EXH-007-CTL-FOD	WHF ITS Elec Exh fan 00007 Controller Fails	2.03E-03	0.00E+00	0.00E+00
050-VCT0-EXH-007-FAN-FTR	WHF ITS Elec Exhaust Fan 00007 Fails to Run	5.06E-02	7.21E-05	7.20E+02
050-VCT0-EXH-007-FAN-FTS	WHF ITS Elec Exh Fan 00007 Fails to Start	2.02E-03	0.00E+00	0.00E+00
050-VCT0-EXH0406-FAN-CCR	CCF of running Exh Fans for WHF ITS Elec.	1.20E-03	0.00E+00	0.00E+00
050-VCT0-EXH0507-FAN-CCF	CCF to Start/Run: Standby Exh fans for the WHF ITS Elec	1.30E-03	0.00E+00	0.00E+00
050-VSCO-HEPA-CCF	Common Cause Failure of HEPA Filters (2 of 3)	7.70E-05	1.07E-07	7.20E+02
050-WATER-FIRE-SUPPRESS	Water Moderator From Fire Suppression Failure	6.00E-07	0.00E+00	0.00E+00
26D-##EG-DAYTNKA-TKF-FOH	ITS DG A Day Tank (00002A) Fails	1.58E-04	4.40E-07	3.60E+02
26D-##EG-DAYTNKB-TKF-FOH	ITS DG B Day Fuel Tank Fails	1.58E-04	4.40E-07	3.60E+02
26D-##EG-FLITLKA-IEL-FOD	ITS DG A Fuel Transfer Pumps Interlock Failure	2.75E-05	0.00E+00	0.00E+00
26D-##EG-FLITLKB-IEL-FOD	ITS DG B Fuel Transfer Pumps Interlock Failure	2.75E-05	0.00E+00	0.00E+00
26D-##EG-FTP1DGA-PMD-FTR	ITS DG A Fuel Transfer Pump Fails to Run	1.23E-02	3.45E-05	3.60E+02
26D-##EG-FTP1DGA-PMD-FTS	ITS DG A Fuel Pump 1A Fails to Start	2.50E-03	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
26D-##EG-FTP1DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Run	1.23E-02	3.45E-05	3.60E+02
26D-##EG-FTP1DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Start	2.50E-03	0.00E+00	0.00E+00
26D-##EG-FTP2DGA-PMD-FTR	ITS DG A Fuel Transfer Pump 2A Fails to Run	1.23E-02	3.45E-05	3.60E+02
26D-##EG-FTP2DGA-PMD-FTS	ITS DG A Fuel Transfer pump 2A Fails to Start	2.50E-03	0.00E+00	0.00E+00
26D-##EG-FTP2DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Run	1.23E-02	3.45E-05	3.60E+02
26D-##EG-FTP2DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Start on Demand	2.50E-03	0.00E+00	0.00E+00
26D-##EG-FULPMPA-PMD-CCR	Common Cause Failure of ITS DG A Fuel Pumps To Run	2.90E-04	0.00E+00	0.00E+00
26D-##EG-FULPMPA-PMD-CCS	Common Cause Failure of ITS DG A Fuel Pumps to Start	1.20E-04	0.00E+00	0.00E+00
26D-##EG-FULPMPB-PMD-CCR	Common Cause Failure of ITS DG B fuel Pumps to Run	2.90E-04	0.00E+00	0.00E+00
26D-##EG-FULPMPB-PMD-CCS	Common Cause Failure of ITS DG B Fuel Pumps to Start	1.20E-04	0.00E+00	0.00E+00
26D-##EG-HVACFN1-FAN-FTR	ITS DG B room Fan 1 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-##EG-HVACFN1-FAN-FTS	ITS DG B room Fan (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-##EG-HVACFN2-FAN-FTS	ITS DG B Room Fan (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-##EG-HVACFN3-FAN-FTR	ITS DG B room Fan 3 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-##EG-HVACFN3-FAN-FTS	ITS DG B Room Fan 3 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-##EG-HVACFN4-FAN-FTS	ITS DG B Room Fan 4 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-##EG-STRTDGA-C72-SPO	ITS Switchgear A Battery Circuit Breaker (DC) Spur Op	3.85E-04	1.07E-06	3.60E+02
26D-##EG-STRTDGB-C72-SPO	13.8kV ITS SWGR Battery B Circuit Breaker (DC) Spur Op	3.85E-04	1.07E-06	3.60E+02
26D-##EG-WKTNK_A-TKF-FOH	ITS DG A Bulk Fuel Tank (00001A) Fails	1.58E-04	4.40E-07	3.60E+02
26D-##EG-WKTNK_B-TKF-FOH	ITS DG B Bulk Fuel Tank Fails	1.58E-04	4.40E-07	3.60E+02
26D-##EGBATCHRGA-BYC-FOH	ITS Switchgear A Battery: Battery Charger Failure	1.28E-03	7.60E-06	1.68E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
26D-##EGBATCHRGB-BYC-FOH	ITS DG B Battery Charger Failure	1.28E-03	7.60E-06	1.68E+02
26D-#EEE-SWGRDGA-BUA-FOH	13.8kV ITS Switchgear A Failure	4.39E-04	6.10E-07	7.20E+02
26D-#EEE-SWGRDGB-AHU-FTR	EDGB Switchgear Room Air Handling Unit Failure to Run	2.65E-03	3.68E-06	7.20E+02
26D-#EEE-SWGRDGB-BUA-FOH	13.8kV ITS Switchgear B Bus Failure	4.39E-04	6.10E-07	7.20E+02
26D-#EEESWGRDGA-AHU-FTR	13.8kV ITS Switchgear room Air Handling Unit Fails	2.65E-03	3.68E-06	7.20E+02
26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-#EEG-HVACFA1-FAN-FTS	ITS DG A room Fan 1 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room Fan 2 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-#EEG-HVACFA2-FAN-FTS	ITS DG A room Fan 2 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room Fan 3 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-#EEG-HVACFA3-FAN-FTS	ITS DG A room Fan 3 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room Fan 4 (Motor-Driven) Fails to Run	2.56E-02	7.21E-05	3.60E+02
26D-#EEG-HVACFA4-FAN-FTS	ITS DG A room Fan 4 (Motor-Driven) Fails to Start	2.02E-03	0.00E+00	0.00E+00
26D-#EEU-208_DGA-BUD-FOH	ITS DC Panel A DC Bus Failure	8.64E-05	2.40E-07	3.60E+02
26D-#EEU-208_DGB-BUD-FOH	ITS DG B DC Panel Failure	8.64E-05	2.40E-07	3.60E+02
26D-#EEY-DGALOAD-C52-FOD	DG A Load Breaker (AC) Fails to Close	2.24E-03	0.00E+00	0.00E+00
26D-#EEY-DGBLOAD-C52-FOD	ITS DG B Load Breaker (AC) Fails to Close	2.24E-03	0.00E+00	0.00E+00
26D-#EEY-DGLOADS-C52-CCF	Common Cause Failure of ITS DG Load Breakers to Close	1.05E-04	0.00E+00	0.00E+00
26D-#EEY-ITS-DGB-#DG-FTS	Diesel Generator Fails to Start	8.38E-03	0.00E+00	0.00E+00
26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.70E-01	4.08E-03	3.60E+02
26D-#EEY-ITSDG-A-#DG-FTS	Diesel Generator Fails to Start	8.38E-03	0.00E+00	0.00E+00
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS Maintenance	1.95E-03	0.00E+00	0.00E+00
26D-#EEY-ITSDG-A-#DG-RSS	Failure to Properly Return ITS DG A to Service	1.95E-04	0.00E+00	0.00E+00
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS Maintenance	1.95E-03	0.00E+00	0.00E+00
26D-#EEY-ITSDG-B-#DG-RSS	Failure to Properly Restore ITS DG-B to Service	1.95E-04	0.00E+00	0.00E+00
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B Fail to Run	1.80E-02	0.00E+00	0.00E+00

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to Start	3.90E-04	0.00E+00	0.00E+00
26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.70E-01	4.08E-03	3.60E+02
26D-#EEY-OB-SWGA-C52-FOD	13.8kV ITS SWGR Feed Breaker (AC) Fails to Open	2.24E-03	0.00E+00	0.00E+00
26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS SWGR A Feed Breaker Spurious Operation	3.82E-03	5.31E-06	7.20E+02
26D-#EEY-OB-SWGB-C52-FOD	Circuit Breaker (AC) Fails on Demand	2.24E-03	0.00E+00	0.00E+00
26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.82E-03	5.31E-06	7.20E+02
26D-#EEY-OB-SWGS-C52-CCF	Common Cause Failure of 13.8kV ITS SWGR Feed Breakers to Open	1.04E-04	0.00E+00	0.00E+00
26D-#EG-BATTERYB-BTR-FOD	ITS SWGR Control Battery B No Output	8.20E-03	0.00E+00	0.00E+00
26D-#EG-LCKOUTRL-RLY-FTP	13.8kV ITS Switchgear Feed Breaker Lockout Relay Fails to Open CB	3.15E-03	8.77E-06	3.60E+02
26D-#EG-LDSQNCRB-SEQ-FOD	ITS DG B Load Sequencer Fails	2.67E-03	0.00E+00	0.00E+00
26D-#EG-LOCKOUTB-RLY-FTP	13.8 ITS SWGR Lockout Relay (Power) Fails to Open CB	3.15E-03	8.77E-06	3.60E+02
26D-#EGLDSQNCRA-SEQ-FOD	DG A Load Sequencer Fails	2.67E-03	0.00E+00	0.00E+00
26D-EG-BATTERYA-BTR-FOD	ITS Switchgear A Battery No Output Given Challenge	8.20E-03	0.00E+00	0.00E+00
27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.82E-03	5.31E-06	7.20E+02
27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.82E-03	5.31E-06	7.20E+02
27A-#EEN-OPENBS2-BUA-FOH	13.8kV Open Bus 2 Bus Failure	4.39E-04	6.10E-07	7.20E+02
27A-#EEN-OPENBS4-BUA-FOH	13.8kV Open Bus 4 Bus Failure	4.39E-04	6.10E-07	7.20E+02
27A-#EEN-OPNBS1A-SWP-SPO	13.8kV Open Bus 2 to ITS Div A Electric Power Switch Spur. Transfer	1.12E-04	1.55E-07	7.20E+02

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability[a]	Mean Failure Rate	Mission Time (Hours)
27A-#EEN-OPNBS3B-SWP-SPO	13.8kV Open Bus 4 to ITS B Electric Power Switch Spur Transfer	1.12E-04	1.55E-07	7.20E+02

NOTE: CCF = common-cause failure; CTM = canister transfer machine; CTT = cask transfer trolley; PLC = programmable logic controller; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.
[a] Although the values in this table are shown to a precision of three significant figures, the values are not known to that level of precision. The values in Attachment C may show fewer significant figures. Such differences are not meaningful in the context of this analysis because the corresponding uncertainties (which are accounted for in the analysis) are much greater than differences due to rounding.

Source: Attachment C, Section C4.

6.3.2 Passive Equipment Failure Analysis

Many event sequences described in Section 6.1 include pivotal events that arise from loss of integrity of a passive component, namely one of the aging overpacks, casks or canisters that contain a radioactive waste form. Such pivotal events involve 1) loss of containment of radioactive material that prevents airborne releases, or 2) LOS effectiveness. Both types of pivotal events may be caused by failure modes caused by either physical impact to the container or by thermal energy transferred to the container. This section summarizes the results of the passive failure analyses detailed in Attachment D that yield the conditional probability of loss of shielding or LOS.

6.3.2.1 Probability of Loss of Containment

An overview of the methodology for calculating the probability of failure of passive equipment from drops and impact loads is presented in Section 4.3.2.2. Consistent with HLWRS-ISG-02 (Ref. 2.2.73), the methodology essentially consists of comparing the demand upon the equipment to a capacity curve. The probability of failure is the value of the cumulative distribution function for the capacity curve, evaluated at the demand upon the container. More detailed discussion is presented in Attachment D, Section D1. The methodology is applicable to all of the waste containers that are processed in the WHF, including transportation casks, aging overpacks, canisters, and waste packages. As described in Section 4.3.2.2, the condition at which a passive component is said to fail depends on the success criteria defined for the component in the WHF operation. Passive components are designed and manufactured to ensure that the success criteria are met in normal operating conditions and with margin, to ensure that the success criteria are also met when subjected to abnormal loads, including those expected during event sequences. The design margins, and in some cases materials, may be dictated by the code and standards applied to a given type of container as characterized by tensile elongation data for impact loads and by strength at temperature data for thermal loads.

As described in Section 4.3.2.2, the probability of a passive failure is often based on consideration of variability (uncertainty) in the applied load, and the variability in the strength (resistance) of the component. The variability in the physical and thermal loading are derived

from the systems analysis that defines the probabilities of physical or thermal loads of a given magnitude in a given event sequence. Such conditions arise from the event sequence analysis described in Section 6.1. For the analysis of the effects of fires on waste containers, probability distributions were developed for both the load and the response. For drops and impacts, however, an event sequence analysis is used to define conservative conditions for the load rather than deal with possible ranges of this parameter. Therefore, the calculation of the probability of passive failures is based on the response or resistance characteristics of the container, given the conservative point value for the drop or impact load defined for a given event sequence.

6.3.2.2 Probability of Loss of Containment for Drops and Impacts

Calculation of the probability of failure of the various containers is based on the variability in the strength (resistance) of the container as derived from tests and structural analysis, including Finite Element Analysis (FEA), detailed in Attachment D, Section D1. Loss of containment probability analysis has been evaluated for various containers by three different studies:

1. Seismic and Structural Container Analysis for the PCSA (Ref. 2.2.36)

2. Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations (Ref. 2.2.82) and Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository (Ref. 2.2.81)

3. Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert (Ref.2.2.23)

All analyses have applied essentially the same methods that include FEA to determine the structural response of the various canisters and cask to drop and impact loads, developing a fragility function for the material used in the respective container, and using the calculated responses (strains) with the fragility function to derive the probability of container breach

Failure probabilities for drops are summarized in Table 6.3-2. Conservative representations of drop height are defined for operations with each type of container. Sometimes more than one conservative drop height is specified, for example, for normal height crane lifts and two-block height crane lifts. Lawrence Livermore National Laboratory (LLNL) predicts failure probabilities of $<1.0 \times 10^{-8}$ for most of the events (Ref. 2.2.36). If a probability for the event sequence is less than of 1.0×10^{-8}, additional conservatism is incorporated in the PCSA by using a failure probability of 1.0×10^{-5}, which is termed "LLNL adjusted." This additional conservatism is added to account for a) future evolutions of cask and canister designs, and b) uncertainties, such as undetected material defects, undetected manufacturing deviations, and undetected damage associated with handling before the container reaches the repository, which is not included in the tensile elongation data.

LLNL calculates strains by modeling representative casks, aging overpacks, and canisters that encompass TAD canisters, naval SNF canisters, and a variety of DPCs with the dynamic finite element code, LSDyna (Ref. 2.2.36). For these canisters, only flat-bottom drops are considered to model transfers by a CTM. This is justified because these canisters fit sufficiently tightly

within the CTM and potential dropped canisters are guided by the canister guide sleeve of the CTM to remain in a vertical position.

Probability of failure is conservatively calculated by comparing the peak strain to the cumulative distribution function derived from tensile strain to failure test data. BSC FEA analysis used LSDyna to model waste packages. Alloy 22 is not stainless steel but a nickel-based alloy, and the most appropriate metric for probability of failure is a cumulative distribution function over extended toughness fraction (see Attachment D, Section D1.4). The probability of failure is calculated using the peak toughness index over the waste package, which is a measure of the alloy's energy absorbing capability.

Table 6.3-2. Failure Probabilities Due to Drops and Other Impacts

Package	Drop Height (ft)	Failure Probability	Note
Representative Transportation Cask[a]	13.1	1.0×10^{-5}	4 degrees from vertical, LLNL, adjusted, no impact limiters
	6	1.0×10^{-5}	3 degrees from horizontal, LLNL, adjusted, no impact limiters
	Slapdown after 13.1 foot drop	1.0×10^{-5}	LLNL, adjusted, no impact limiters
Representative Canister	32.5[b]	1.0×10^{-5}	Flat bottomed, LLNL, adjusted
Aging overpack	3	1.0×10^{-5}	LLNL, adjusted

NOTE: [a] Also applies to shielded transfer casks used on-site and horizontal transfer casks.
[b] For transfers by the CTM, this drop height is greater than the maximum drop height (except for CTM transfers in the IHF)
LLNL = Lawrence Livermore National Laboratory.

Source: Attachment D.

Containment failure probabilities due to other physical impact conditions, equivalent to drops, are listed in Table 6.3-3. These probabilities were modeled by LLNL using FEA, resulting in prediction of failure probabilities of $<1.0 \times 10^{-8}$. Again, additional conservatism was incorporated by using a failure probability of 1.0×10^{-5} for most of these events. The side impact event was not adjusted from the LLNL result of $< 1.0 \times 10^{-8}$ because of the very low velocities involved. A comparison of the strains induced by drops and slow speed, side impacts indicates significantly lower strains for the low velocity impacts.

Table 6.3-3. Failure Probabilities Due to Miscellaneous Events

Event	Failure Probability	Note
Derail	1.0×10^{-5}	LLNL, adjusted, analogous to 6', 3° from horizontal
Rollover	1.0×10^{-5}	LLNL, adjusted, analogous to 6', 3° from horizontal
Drop on	1.0×10^{-5}	LLNL, adjusted 10-ton load onto container
Tip over	1.0×10^{-5}	LLNL, adjusted, analogous to 13.1-foot drop plus slap-down
Side Impact from collision with rigid surface	1.0×10^{-8}	Or value for low speed collision, whichever is greater (Table 6.3-4) Crane moving 20 ft/min
Tilt down/Up	1.0×10^{-5}	LLNL, adjusted; Bounded by slap-down

NOTE: LLNL = Lawrence Livermore National Laboratory.

Source: Attachment D.

Table 6.3-4 shows failure probabilities for various collision events for various containers as a function of impact speed. For each of the events, the collision speed, whether in mph or fpm is converted to feet per second (fps), then to an equivalent drop height in feet. The drop heights are very small compared with the drop heights for the modeled situations summarized in Table 6.3-2. The damage to a container, expressed in terms of strain, is roughly proportional to the impact energy, which is proportional to the drop height, as is readily seen from the following:

> Energy from drop = $mgh \propto Fs$ and $F \propto mg$, therefore, $s \propto h$, where s = strain, F = local force on container from drop, m = mass of container, h = drop height, and g = acceleration of gravity.

For drop heights other than those for the modeled situations presented in Table 6.3-2, failure probabilities can be estimated by shifting capacity curve to match the conservative failure probabilities listed in Table 6.3-2. The mean failure drop height, H_m, is found so that the probability of failure, P, is the value listed in Table 6.3-2 for the drop height, H_d, listed in Table 6.3-2.

$$P \quad \int_{-\infty}^{x} N(t)\,dt \quad and \quad x \quad \frac{H_d / H_m - 1}{COV} \qquad \text{(Eq. 17)}$$

where

P = probability of failure for container dropped from height H_d

$N(t)$ = standard normal distribution with mean of zero and standard deviation of one

t = variable of integration

H_d = modeled drop height for which the failure probability has been determined

H_m = median failure drop height of the failure drop height distribution such that the failure probability at the modeled drop height, H_d, is P

COV = coefficient of variation = ratio of standard deviation to mean for strain capacity distribution, applied here to stress capacity or true tensile strength

The probabilities of failure for the collision cases listed in Table 6.3-4 are then determined using the above formula with H_m determined above and with H_d being the drop height corresponding to the collision speed as listed in Table 6.3-4.

Two-blocking events are also included in Table 6.3-4. The failure probabilities of these events are shown in *PEFA Chart.xls* included in Attachment H. The CTM, which lifts canisters, is designed such that drops from the height associated with two-blocking is very low probability and no higher than drops from normal operation. The design features that ensure this are: slide gate closure and two levels of shut-off switches as the normal lift height is exceeded, and a tension relief device that prevents over tensioning of hoist cables if the two-block height is reached. Transportation cask handling cranes are also equipped with the shut-off switches and the tension relief device.

During transfers by a CTM, a shear-type structural challenge was identified as a potential initiating event. This challenge is caused, for example, by the spurious movement of the CTT from which the canister is extracted, before the canister is fully lifted inside the CTM shield bell. A bounding value of one is selected for the probability of failure of the transferred canister. This conservative estimate is used because the structural response of a canister to a shear-type structural challenge was not evaluated and it probability cannot be inferred from comparison with other structural challenges to the canister.

Table 6.3-4. Failure Probabilities for Collision Events and Two-Blocking

Collision Scenario	Speed	Velocity (ft/sec)	Equivalent Drop Height (ft)[a]	Failure Probabilities for Various Container Types	
				Transportation Cask	Canister
Railcar	2.5 (mph)	3.67	0.21	1.00E-08	
Truck Trailer	2.5 (mph)	3.67	0.21	1.00E-08	
Crane	20 (fpm)	0.33	0.00	1.00E-08	
CTT	10 (fpm)	0.17	0.00	1.00E-08	1.00E-08
ST	2.5 (mph)	3.67	0.21		1.00E-08
CTM	20 (fpm)	0.33	0.00		1.00E-08
CTM	40 (fpm)	0.67	0.01		1.00E-08
Two blocking				1.00E-05	1.00E-05

NOTE: [a]Values that are less than 0.005 are reported as 0.00.
CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; fpm = feet per minute; mph = miles per hour; sec = seconds; ST = site transporter; TAD = transportation, aging, and disposal.

Source: Attachment D

6.3.2.3 Probability of Canister Failure in a Fire

In addition to passive equipment failures as a result of structural loads, passive failures can also occur as a result of thermal loads such as exposure to fires or abnormal environmental conditions, for example, loss of HVAC cooling. The PCSA evaluates the probability of loss of containment (breach) due to a fire for several types of waste form containers, including: transportation casks containing uncanistered SNF assemblies, and canisters representative of TAD canisters, DPCs, DOE standardized canisters, HLW canisters, and naval SNF canisters.

The methods for analyzing thermally-induced passive failures are discussed in Section 4.3.2.2, and detailed in Attachment D. In summary, the probability of failure of a waste form container as a result of a fire is evaluated by comparing the demand upon a container (which represents the thermal challenges of the fire vis-à-vis the container), with the capacity of the container (which represents the variability in the temperature at which failure would occur). The demand upon the container is controlled by the fire duration and temperature, because these factors control the amount of energy that the fire could transfer to the container.

In response to a fire, the temperature of the waste form container under consideration increases as a function of the fire duration. The maximum temperature is calculated using a heat transfer model that is simplified to allow a probabilistic analysis to be performed that accounts for the variability of key parameters. The model accounts for radiative and convective heat transfers from the fire, and also for the decay heat from the waste form inside a container. The

temperature evolution of waste form containers is analyzed based on a simplified geometry with a wall thickness that, for the range of waste form containers of interest in the PCSA, is representative or conservatively small. Specifically, two characteristic canister wall thicknesses are modeled: 0.5 inches and 1.0 inches, characteristic of a range of DPCs. The wall thickness of a container is an important parameter that governs both container heating and failure. Other conservative and realistic modeling approaches are introduced in the heat transfer model, as appropriate. For example, fires are conservatively considered to engulf a container, regardless of the fact that a fire at the GROA may simply be in the same room as a container. When handled, TAD canisters, DPCs, DOE standardized canisters, HLW canisters and naval SNF canisters are enclosed within another SSC, for example a transportation cask, the shielded bell of a canister transfer machine, or a waste package. Therefore, a fire does not directly impinge on such canisters. In contrast, the external surface of a transportation cask containing uncanistered SNF may be impinged upon directly by the flames of the fire.

Accounting for the uncertainty of the key parameters of the fires and the heat transfer model, the maximum temperature reached by a waste form container, which represents the demand upon the container due to a fire, is characterized with a probability distribution. The distribution is obtained through Monte Carlo simulations.

To determine whether the temperature reached by a waste form container is sufficient to cause the container to fail, the fire fragility distribution curve for the container is evaluated. In the PCSA, this curve is expressed as the probability of breach of the container as a function of its temperature. Two failure modes are considered for a container that is subjected to a thermal challenge: creep-induced failure and limit load failure. Creep, the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load, is possible for long duration fires. Limit load failure corresponds to situations where the load exerted on a material exceeds its structural strength. This failure mode is considered because the strength of a container decreases as its temperature increases. The variability of the key parameters that can lead to a creep-induced failure or limit load failure is modeled with probability distributions. Monte Carlo simulations are then carried out to produce the fire fragility distribution curve for a container.

The probability of a waste form container losing its containment function as a result of a fire is calculated by running numerous Monte Carlo simulations in which the temperature reached by the container, sampled from the probability distribution representing the demand on the container, is compared to the sampled failure temperature from the fragility curve. The model counts the simulation result as a failure if the container temperature exceeds the failure temperature. Statistics based upon the number of recorded failures in the total number of simulations are used to estimate the mean of the canister failure probability.

Table 6.3-5 shows the calculated mean and standard deviation for the failure probability of a canister in the following configurations: a canister in a transportation cask, a canister in a waste package, and a canister in a shielded bell.

Table 6.3-5. Summary of Canister Failure Probabilities in Fire

Configuration[a]	Failure Probability	
	Mean	Standard Deviation
Thin-Walled Canister in a Transport Cask	2.0×10^{-6}	1.4×10^{-6}
Thick-Walled Canister in a Transport Cask	1.0×10^{-6}	1.0×10^{-6}
Thin-Walled Canister in a Shielded Bell	1.4×10^{-4}	2.6×10^{-5}
Thick-Walled Canister in a Shielded Bell	9.0×10^{-5}	1.7×10^{-5}

NOTE: [a] Configurations not addressed in this table include any canister in an aging overpack. In this configuration, the canister is protected from the fire by the massive concrete overpack. Calculations have shown that the temperatures experienced by the canister in this configuration are well below the canister failure temperature, so that failures for these configurations can be screened. For conservatism, a screening conditional probability of 1×10^{-6} could be used.

Source: Attachment D, Table D2.1-9.

Note that no failure probability is provided for a bare canister configuration. The reason for this is that the canister is outside of a cask for only a short time. During that time, the canister is usually inside the shielded bell of the CTM. The preceding analysis addressed a fire outside the shielded bell. When in that configuration, the canister is shielded from the direct effects of the fire. A fire inside the shielded bell, which could directly heat the canister, is not considered to be credible for two reasons. First, the hydraulic fluid used in the CTM equipment is non-flammable and no other combustible material could be present inside the bell to cause a fire. Second, the annular gap between the canister and the bell is only three inches wide, but is approximately 27 feet long. Given this configuration, it is unlikely that there is sufficient inflow of air to sustain a large fire that could heat a significant portion of the canister wall. There may be sufficient inflow to sustain a localized fire, but such a fire would not be adequate to heat the canister to failure.

The canister is also outside of a cask, or shielded bell as it is being moved from a cask into the shielded bell or from the shielded bell into a waste package. The time during which the canister is in this configuration is extremely short, a matter of minutes, so a fire that occurs during this time is extremely unlikely. In addition, because the gap between the top of the cask and ceiling of the transfer cell is generally much shorter than the height of the canister, only a small portion of the canister surface is exposed to the fire. Furthermore, this exposure would only be for the short time that the canister was in motion.

For these reasons, failure of a bare canister was not considered credible and is not explicitly modeled in the PCSA.

6.3.2.4 Probability of Loss of Containment from Heatup

In addition to fire-related passive failures, the PCSA considered other passive equipment failures due to abnormal thermal conditions. The thermal event of greatest concern for the surface facilities is loss of HVAC cooling. If HVAC cooling is lost, the ambient temperature in the facility will increase. This increase is particularly significant for relatively small enclosures such as the transfer cells.

A series of bounding calculations was performed to determine the maximum temperature that could be reached by a canister following loss of HVAC cooling (Ref. 2.2.13). These calculations consider a range of decay heat levels and a loss of cooling for 30 days. These analyses indicate that the canister temperature would remain well below 500°C (773°K) (Ref. 2.2.13. This temperature is hundreds of degrees below the temperature at which the canister would fail (see Figure D2.1-4 Attachment D). For that reason, canister failure due to a loss of HVAC is physically unrealizable and considered beyond Category 2.

6.3.2.5 Probability of Loss/Degradation of Shielding

Loss or degradation of shielding probabilities is summarized in Table 6.3-6.

Shielding of a waste form that is being transported inside the GROA is accomplished by several types of shielded containers, including: transportation casks, shielded transfer casks, aging overpacks, shielded components of a WPTT, and shielded components of a TEV. In addition to a shielding function, sealed transportation casks and shielded transfer casks exert a containment function. Only those items used in the WHF are discussed further.

A structural challenge may cause shielding degradation or shielding loss. Loss of shielding occurs when an SSC fails in a manner that leaves a direct path for radiation to stream, for example as a result of a breach. Degradation of shielding occurs when a shielding SSC is not breached but its shielding function is degraded. In the PCSA, a shielding degradation probability after a structural challenge is derived for those transportation casks that employ lead for shielding. Finite-element analyses on the behavior of transportation casks subjected to impacts associated with various collision speeds, reported in *Reexamination of Spent Fuel Shipment Risk Estimates,* NUREG/CR-6672 (Ref. 2.2.83), indicate that lead slumping after an end impact could result in a reduction of shielding; transportation casks without lead are not susceptible to such shielding degradation. This information is used in Attachment D to derive the shielding degradation probability of a transportation cask at drop heights characteristic of crane operations. The distribution is developed for impacts on surfaces made of concrete, which compare to the surfaces onto which drops could occur at the GROA. No impact limiter is relied upon to limit the severity of the impact. Conservatively, the distribution is applied to transportation casks and also shielded transfer casks, regardless of whether or not they use lead for shielding. Thus, for containers that have both a containment and shielding function, the PCSA considers a probability of containment failure (which is considered to result in a concurrent loss of shielding), and also a probability of shielding degradation (which is associated with those structural challenges that are not sufficiently severe to cause loss of containment). Table 6.3-6 displays the resulting shielding degradation probabilities for transportation casks and shielded transfer casks after a structural challenge. Given that there is significant conservatism in the calculation of strain and the uncertainty associated with the fragility (strength), the resulting estimates include uncertainties and are considered conservative

Shielding loss is also considered to potentially affect an aging overpack subjected to a structural challenge, if the waste form container inside does not breach. Given the robustness of aging overpacks, a shielding loss after a 3-ft drop height is calculated to have a probability of 5×10^{-6} per aging overpack impact, based upon the judgment that this probability may be conservatively related to but lower than the probability of breach of an unprotected waste form container inside

the aging overpack (Attachment D). If the structural challenge is sufficiently severe to cause the loss of containment (breach) of the waste form container inside the aging overpack, the loss of the aging overpack shielding function is considered guaranteed to occur.

A CTM provides shielding with the shield bell, shield skirt, and associated slide gates. Also, the CTM is surrounded by shield walls and doors, which are unaffected by structural challenges resulting from internal random initiating events. Therefore, such challenges leave the shielding function intact.

The PCSA treats the degradation or loss of shielding of an SSC due to a thermal challenge as described in the following paragraphs:

If the thermal challenge causes the loss of containment (breach) of a canister, the SSC that provides shielding and in which the canister is enclosed is considered to have lost its shielding capability. A transportation cask containing uncanistered SNF is also considered to have lost its shielding if it has lost its containment function.

The shielding structure provided by the CTM is not subjected to drops. Such shields may be subjected to collisions or dropped heavy objects. The analysis detailed in Attachment D indicates there is no challenge to the shielding from these events. Therefore, these components are assigned zero probability in Table 6.3-6.

If the thermal challenge is not sufficiently severe to cause a loss of containment function, it is nevertheless postulated that it will cause shielding loss of the transportation cask, shielded transfer cask, canister transfer machine, or cask transfer trolley affected by the thermal challenge and in which the waste form container is enclosed. This is because the neutron shield on these SSCs is made of a polymer which is not anticipated to withstand a fire without failing. Note, however, that the degradation of gamma shielding of these SSCs is unlikely to be affected by a credible fire. Although credible fires could result in the lead melting in a lead-sandwich transportation cask, there is no way to displace the lead, unless the fire is accompanied by a puncture or rupture of the outer steel wall of the cask. Preliminary calculations were unable to disprove the possibility of hydraulic failure of the steel encasing due to the thermal expansion of molten lead, so loss of gamma shielding for steel-lead-steel transportation casks engulfed in fire is postulated. Conservatively, in the PCSA, transportation casks and shielded transfer casks are postulated to lose their shielding function with a probability of one, regardless of whether or not they use lead for shielding.

Aging overpacks made of concrete are not anticipated to lose their shielding function as a consequence of a fire because the type of concrete used for aging overpacks is not sensitive to spallation. In addition, it is likely that the aging overpacks will have an outer steel liner. For these reasons, a loss of aging overpack shielding in a fire has been screened from consideration in the PCSA.

Table 6.3-6. Probabilities of Degradation or Loss of Shielding

	Probability	Note
Sealed Transportation cask and shielded transfer casks shielding degradation after structural challenge	1×10^{-5}	Attachment D, Section D3.4.
Aging overpack shielding loss after structural challenge	5×10^{-6}	Attachment D, Section D3.4
CTM shielding loss after structural challenge	0	Structural challenges sufficiently mild to leave the shielding function intact
Shielding loss by fire for waste forms in transportation casks or shielded transfer casks	1	Lead shielding could potential expand and degrade. This probability is conservatively applied to transportation casks and STCs that do not use lead for shielding.
Shielded loss by fire for aging overpacks and CTM shield bell	0	Type of concrete used for aging overpacks is not sensitive to spallation; Uranium used in CTM shield bell shielding does not lose its shielding function as a result of a fire.

NOTE: CTM = canister transfer machine.

Source: Attachment D, Table D3.4-1.

6.3.2.6 Probability of Other Fire-Related Passive Failures

In addition to the canisters, other passive equipment could fail as a result of a fire. For the PCSA, only failures that would result in a radionuclide release or radiation exposure are considered. .

6.3.2.7 Application to Event Sequence Models

Table 6.3-7 summarizes passive failure events needed for the event sequence modeling. The values are either specifically developed in Attachment D, or are values from bounding events. Probabilities for some other events were obtained by extrapolation from developed probabilities as described in this section or in Attachment D. The derivation of all passive failure probabilities is described in Attachment D and shown in *PEFA Chart.xls* included in Attachment H.

It is noted that Table 6.3-7 address all passive event failures for the various waste form configurations. Table 6.3-8 identifies the specific passive failure basic events used in event sequence modeling and quantification for the WHF. The probability of each basic event is based on one of the values presented in Tables 6.3-2 through 6.3-7.

Table 6.3-7. Summary of Passive Event Failure Probabilities

	10 T dropped on container	Container vertical drop from normal operating height	Container 30-foot vertical drop	Container 45-foot vertical drop	6-foot Horizontal Drop, Rollover	2.5 mph Flat side impact/ collision	2.5 mph Localized side impact/ collision	9 mph Flat side impact/ collision	2.5 mph end-to-end Collision	9 mph end-to-end Collision	Slapdown (bounds tip over)	Thin-Walled Canister Fire	Thick-Walled Canister Fire
Loss of Containment													
Canister in Transport Cask	1.E-05	1.E-05	1.E-05	N/A	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	1.E-05	2.E-06	1.E-06
Transport Cask with Bare Fuel	1.E-05	1.E-05	1.E-05	N/A	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	1.E-05	5.E-02 [1]	6.E-03 [2]
Canister	1.E-05	1.E-05	1.E-05	1.E-05	N/A	N/A	N/A	N/A	N/A	N/A	1.E-05	N/A	N/A
Canister in Shield Bell	N/A	1.E-05	N/A	N/A	N/A	1.E-08	N/A	N/A	N/A	N/A	N/A	1.E-04	9.E-05
Canister in AO	1.E-05	1.E-05	N/A	N/A	N/A	1.E-08	1.E-08	1.E-08	N/A	N/A	1.E-05	1.E-06	1.E-06
Loss of Shielding													
Transport Cask	1.E-05	1.E-05	1.E-05	N/A	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	1.E-05	~ 1	~ 1
Aging Overpack	1.E-05	5.E-06	N/A	N/A	N/A	1.E-05	1.E-05	1.E-05	1.E-05	1.E-05	1.E-05	~ 0	~ 0
CTM	No challenge	No challenge	N/A	N/A	No challenge	No challenge	N/A	No challenge	No challenge	No challenge	No challenge	~ 0	~ 0

NOTE: 1 Truck cask
2 Rail cask
3Represents passive event failure probabilities for a drop of a HLW canister onto another HLW canister.
N/A = not applicable, no scenarios identified.

Source: Attachment D

Table 6.3-8. Passive Failure Basic Events used in WHF Event Sequence Analysis

Basic Event ID	Basic Event Description	Basic Event Value
AO-SHIELD-FAIL-DROP	Failure of AO shield due to drop	5.00E-06
AO-SHIELD-FAIL-DROPON	Failure of AO shield due to drop on	1.00E-05
AO-SHIELD-FAIL-IMPACT	AO shield fails due to impact	1.00E-05
BARE-FUEL-FAIL-FIRE	Bare fuel in cask fails due to fire	5.00E-02
CANISTER-AO-DROP-FAIL	Canister in AO fails due to drop	1.00E-05
CANISTER-AO-IMPACT-FAIL	Failure of canister in AO due to impact	1.00E-08
CANISTER-FAIL-FIRE-AO	Canister in AO fails due to fire	1.00E-06
CANISTER-FAIL-IMPACT	Canister fails due to impact	1.00E-08
CANISTER-FAIL-TWOBLOCK	Canister fails due to two blocking	1.00E-05
CANISTER-FAILS-DROP	Canister fails due to drop	1.00E-05
CANISTER-FIRE-FAIL-CTM	Canister in CTM fails in fire	1.40E-04
CANISTER-IN-AO-IMPACT	Canister in AO fails	1.00E-05
CANISTER-IN-CASK-FAIL	Canister inside cask fails	1.00E+00
CANISTER-IN-CASK-FIRE	Canister in a cask fails in fire	2.00E-06
CANISTER-SHEAR-CTM	Canister shear in CTM	1.00E+00
CASK-DROP-OPERATIONAL	Failure of cask due to drop from operational height	1.00E-05
CASK-DROP-TWOBLOCK	Cask failure due to two block event	1.00E-05
CASK-FAIL-IMPACT	Cask failure due to impact	1.00E-08
CASK-FAILS	Cask fails on impact or drop	1.00E+00
CASK-SHIELDING-DROP	Shielding failure due to drop	1.00E-05
CASK-SHIELDING-IMPACT	Cask shielding fails due to impact	1.00E-08

NOTE: Refer to Attachment D for discussion.
AO = aging overpack; CTM = canister transfer machine; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; TAD = transportation, aging, and disposal canister; TC = transfer cask.

Source: Original

6.3.3 Miscellaneous Data

Data that is not defined as Active Component Reliability Data (Section 6.3.1) or Passive Equipment Failure Data (Section 6.3.2), but are used in the reliability analysis for this facility are listed in the Table 6.3-9.

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
050-CRWT-TRCT-STEER-FAIL	Tractor Steering System Failure	1.84E-05	Probability of failure used for horizontal cask transfer trolley	Attachment B, Table B9.4-1
050-CRWT-TRLR-STEER-FAIL	Trailer Steering System Failure	1.84E-05	Probability of failure used for horizontal cask transfer trolley	Attachment B, Table B9.4-1
050-CTMOBJLIFTNUMBERD	Number of Objects dropped on canister	1.00E+00	During canister transfer from a DPC or TAD, the CTM lifts a lid over the TC. Therefore a value of 1 is assigned to this basic event.	N/A
050-DPCPREPLIFTNUMBER	Number of Object Lifts for DPC Prep	3.00E+00	There are three crane lifts associated with the preparation of the DPC in the Cask Preparation Area. Therefore, a value of 3 is assigned to this basic event.	N/A
050-DPCPREP-OBJ-MOVE	Number of object moves during DPC prep	2.00E+00	There are two crane lifts associated with the preparation of the DPC in the Cask Preparation Area. Therefore, a value of 2 is assigned to this basic event.	N/A
050-FIRE-CSNF-PREP	Prep area fire affects CSNF	5.40E-06	Frequency of a localized fire involving uncanistered SNF in transportation casks in the preparation area.	Table 6.5-4
050-FIRE-CSNF-VEST	Fire threatens CSNF in entrance vestibule	3.00E-06	Frequency of a localized fire involving uncanistered SNF in transportation casks in the entrance vestibule.	Table 6.5-4
050-FIRE-DPC-CTM	Fire affects DPC in the CTM	8.30E-08	Frequency of a localized fire involving a DPC in the CTM.	Table 6.5-4
050-FIRE-DPC-DPCCUT	Fire affects DPC at DPC cutting	1.70E-05	Frequency of a localized fire involving a DPC at the DPC cutting station.	Table 6.5-4
050-FIRE-DPC-LARGE	Large fire affects DPC in facility	1.00E-04	Frequency of a large fire involving a DPC at the DPC cutting station.	Table 6.5-4
050-FIRE-DPC-PREP	Fire affects DPC in prep area	8.90E-06	Frequency of a localized fire involving a DPC in the preparation area.	Table 6.5-4
050-FIRE-DPC-UNLOAD	Fire affects DPC in unload room	4.90E-07	Frequency of a localized fire involving a DPC in the unloading room.	Table 6.5-4
050-FIRE-DPC-VEST	Fire affects DPC in entrance vest	1.20E-05	Frequency of a localized fire involving DPCs in the entrance vestibule.	Table 6.5-4

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
050-FIRE-LARGE-CSNF	Large fire affects CSNF	1.10E-05	Frequency of a large fire involving uncanistered SNF in the facility.	Table 6.5-4
050-FIRE-TAD-CLOSE	Fire affects TAD in closure area	2.30E-05	Frequency of a localized fire involving a TAD at the TAD closure station.	Table 6.5-4
050-FIRE-TAD-CTM	Fire affect TAD in CTM	6.90E-08	Frequency of a localized fire involving a TAD in the CTM.	Table 6.5-4
050-FIRE-TAD-LARGE	Large fire affects TAD in WHF	6.70E-05	Frequency of a large fire involving a TAD in the facility.	Table 6.5-4
050-FIRE-TAD-LOAD	Fire affects TAD in loading room	2.90E-07	Frequency of a localized fire involving a TAD in the loading room.	Table 6.5-4
050-FIRE-TAD-UNLOAD	Fire affects TAD in unload room	3.30E-07	Frequency of a localized fire involving a TAD in the unloading room.	Table 6.5-4
050-FIRE-TAD-VEST	Fire affects TAD in entrance vestibule (bolting)	3.50E-07	Frequency of a localized fire involving a TAD in the entrance vestibule.	Table 6.5-4
050-LIFTS-PER-DPC-CAN	Number of lifts per DPC canister	1.00E+00	There is one CTM lift associated with the transfer of the DPC. Therefore, a value of 1 is assigned to this basic event.	N/A
050-LIFTS-PER-TAD-CAN	Number lifts of TAD canister	1.00E+00	There is one CTM lift associated with the transfer of the TAD. Therefore, a value of 1 is assigned to this basic event.	N/A
050-OBJLIFT-DPC-CUT-TRAN	Number of object lifts during DPC cutting station transfer	1.00E+00	There is one object lift associated with DPC cutting. Therefore, a value of 1 is assigned to this basic event.	N/A
050-OBJLIFT-POOL-FLOOR	Number of object moves during pool floor transfer	1.00E+00	There is one object lift associated with the movement of a DPC to the pool floor. Therefore, a value of 1 is assigned to this basic event.	N/A
050-OBJLIFT-POOL-TRANS	Number of object lifts during transfer to pool	1.00E+00	There is one object lift associated with the movement of a DPC or TAD to or from the pool ledge. Therefore, a value of 1 is assigned to this basic event.	N/A
050-OBJLIFT-TAD-CLOSE	Number of object moves during TAD closure	2.00E+00	There are three crane lifts associated with the closure of the TAD canister at the TAD canister closure station. Therefore, a value of 2 is assigned to this basic event.	N/A

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
050-OBJLIFT-TAD-EXPORT	Number of object moves during TAD export	2.00E+00	There are two crane lifts associated with the export of the TAD canister from TAD canister closure station to CTT. Therefore, a value of 2 is assigned to this basic event.	N/A
050-OIL-MODERATOR	Oil Moderator Sources in WHF (Gear Boxes)	9.00E-05	Section 6.0	Section 6.2.10.2
050-OTHER-WATER	Water moderator from other sources	1.50E-05	The WHF pool contains 1.4 million gallons of water with the minimum required concentration of soluble boron in the pool is 2500 mg/L of boron enriched to 90 atom % ^{10}B. For all normal WHF pool operations, subcriticality is maintained crediting no more than 15% of this minimum required soluble boron concentration. Boron concentration is sampled regularly and ^{10}B is added as required. For boron concentration to reach the critical 15% level would require multiple human error events in failing to sample the boron concentration when required. In addition, 0.85 x 1.4 million = 1.2 million gallons of water would have to added to dilute the ^{10}B concentration to 15%. The first human error of failing to sample is based upon a human performance limiting value of 1.0×10^{-5}/d from NARA (attachment E) for a single team. In addition, it is physically impossible to displace and add 1.2 million gallon of water. Hence a probability estimate of 1.0×10^{-6} for failure to maintain boron concentration is conservative.	Attachment E
050-SPMRC-MILES-IN-WHF	Miles Traveled in WHF	4.00E-02	(Site) prime mover travel distance on rails inside the WHF.	Section 6.2.2.1 and Ref. 2.2.27
050-PWR-LOSS	Loss of Site Power	5.70E-06	Commercial power reliability requirement	N/A
050-PWR-LOSS-2	Loss of Site Power	5.70E-06	Commercial power reliability requirement	N/A

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
050-ST-#-OF-SHIELD-DOORS	Number of Shield Doors the ST Passes Through	2.00E+00	ST goes through rooms 1023 (ST Vestibule) and 1007 (Loading Room). In this movement, it passes through two doors: an overhead door and a shield door.	Section 6.2.2.6.4 and Ref. 2.2.27
050-TRANSCTTLIFTNUMBER	Number of Crane Lifts	3.00E+00	Total number of crane lifts	
050-TRANSSTANDLIFTNUMBER	Crane Lifts with sling lift	2.00E+00	Number of lifts performed by sling lift	Section 6.4
050-UPENDOBJLIFTNUMBER	Number of object lifts	3.00E+00	Number of crane lifts performed during upending TC in Cask Preparation Area	Section 6.4
050-WATER-MODERATOR	Water Moderator Sources in WHF	5.00E-07	Section 6.2.2.10	Table 6.2-7
AO-DPC-NUMB	Number of AO/ DPC processed over the WHF life	3.46E+02	Throughput analysis	Ref. 2.2.26

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
BORON-SYSTEM-FAILS	Boron system fails	1.00E-06	The WHF pool contains 1.4 million gallons of water with the minimum required concentration of soluble boron in the pool is 2500 mg/L of boron enriched to 90 atom % ^{10}B. For all normal WHF pool operations, subcriticality is maintained crediting no more than 15% of this minimum required soluble boron concentration. Boron concentration is sampled regularly and ^{10}B is added as required. For boron concentration to reach the critical 15% level would require multiple human error events in failing to sample the boron concentration when required. In addition, 0.85 x 1.4 million = 1.2 million gallons of water would have to added to dilute the ^{10}B concentration to 15%. The first human error of failing to sample is based upon a human performance limiting value of 1.0×10^{-5}/d from (Ref. 2.2.41) or a single team. In addition, it is physically impossible to displace and add 1.2 million gallon of water. Hence a probability estimate of 1.0×10^{-6} for failure to maintain boron concentration is conservative.	Attachment E
CSNF-NUMB	Number of TCs containing CSNF processed over the WHF life	3.78E+03	Throughput analysis	Ref. 2.2.26
DPC-NUMB	Number of DPCs processed through the WHF during preclosure period	3.46E+02	Total number of DPCs received at WHF over preclosure period.	Ref. 2.2.26
FILTER-NUMBER	Number of LLW pool filters processed	1.80E+03	Total number of filters changed out during WHF facility life.	Ref. 2.2.28
FUEL-NUMB	Number of fuel assemblies processed over facility life	6.62E+04	Throughput analysis	Ref. 2.2.26

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
HVAC	HVAC failure probability	3.50E-02	Quantified mean failure probability of HVAC fault tree for handling activities other than cask cooling	Attachment B.
HVAC-FAILS-DURING-PREP	HVAC fails during cask cooling or drying	1.10E-03	Quantified mean failure probability of HVAC fault tree for cask cooling activities	Attachment B.
LOSP	Loss of offsite power	2.99E-03	Commercial power reliability requirement	N/A
LOSP-4	Failure of Off Site Power	4.10E-06	Commercial power reliability requirement	N/A
RC-DPC-NUMB	Number of rail casks containing DPC processed over the WHF life	3.46E+02	Throughput analysis; number of DPCs arriving by rail car	Ref. 2.2.26
TAD-NUMB	Number of TADs processed through the WHF during preclosure period	1.17E+03	Total number of TAD canisters received at WHF over preclosure period	Ref. 2.2.26
TIME-OVER-FLOOR-TO-CLOSE	Fraction of time over floor for movement to closure	2.00E-01	Time and motion study	Attachment F, Ref. F2.6
TIME-OVER-FLOOR-TO-POOL	Fraction of time over floor for movement into pool	6.00E-01	Time and motion study	Attachment F, Ref. F2.6
TIME-OVER-POOL-TO-CLOSE	Fraction of time over pool for movement to closure	8.00E-01	Time and motion study	Attachment F, Ref. F2.6
TIME-OVER-POOL-TO-POOL	Fraction of time over pool for movement into pool	4.00E-01	Time and motion study	Attachment F, Ref. F2.6

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; CRCF = Container Receipt and Closure Facility; CSNF = Commercial Spent Nuclear Fuel; DPC = dual-purpose canister; HVAC = Heating, Ventilation and Air Conditioning, LLW = Low Level Waste; MPH = miles per hour; PMRC = prime mover/rail car; SD = shield doors; ST = site transporter; TAD = transportation, aging, and disposal canister; TC = transportation cask; WHF = wet handling facility.

Source: Original

6.4 HUMAN RELIABILITY ANALYSIS

The PCSA has emphasized human reliability analysis because the waste handling processes include substantial interactions between equipment and operating personnel. If there are human interactions that are typically associated with the operation, test, calibration, or maintenance of a certain type of SSC (e.g., drops from a crane when using slings) and this SSC has been treated using industry-wide data per Attachment C, then human failure events may be implicit in the reliability data. The analyst is tasked with determining whether that is the case. Otherwise, the analyst includes explicit identification, qualitative modeling, and quantification of HFEs, as described in this section. The methodology applied is provided in Section 4.3.4, and the detailed description of the HRA is presented in Attachment E.

6.4.1 HRA Scope

The scope of the HRA is established in order to focus the analysis on the issues pertinent to the goals of the overall PCSA. Thus, the scope is as follows:

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers. Such scenarios may include the need for mitigation of radionuclides, for example, provided by the confinement HVAC system.

2. Pursuant to the above, the following types of HFEs are excluded:

   A. HFEs resulting in standard industrial injuries (e.g., falls).

   B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount.

   C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.

3. The identification of HFEs is restricted to those areas of the facility that handle waste forms and only during the times that waste forms are being handled (e.g., HFEs are not identified for the Cask Preparation Room during the export of empty transportation casks).

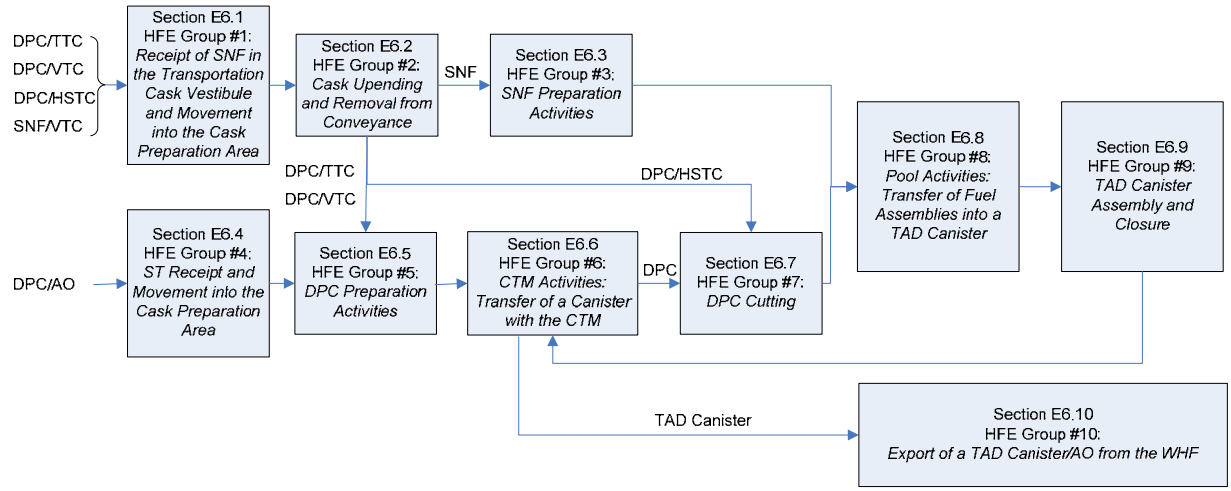
4. The exception to #3 is that system-level HFEs are considered for support systems (e.g., electrical power for confinement HVAC) when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.

5. Post-initiator recovery actions (as defined in Attachment E, Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.

6. In accordance with Section 4.3.10.1 (on boundary conditions of the PCSA), initiating events associated with conditions introduced in SSCs before they reach the site are not, by definition of 10 CFR 63.2 (Ref. 2.3.2), within the scope of the PCSA nor, by extension, within the scope of the HRA.

6.4.2 Base Case Scenarios

The first step in this analysis is to describe the WHF operations in sufficient detail such that the human reliability analysts can identify specific deviations that would lead to a radiation release, a direct exposure, or a criticality event. To do this, the WHF operations were broken into ten separate operational steps, as depicted in Figure 6.4-1.



NOTE: AO = aging overpack; CTM = canister transfer machine; DPC = dual-purpose canister; HFE = human failure event; HSTC = cask tractor and cask transfer trailer; SNF = spent nuclear fuel; ST = site transporter; TAD canister = transportation, aging, and disposal canister; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar; WHF = Wet Handling Facility.

Source: Original

Figure 6.4-1. WHF Operations

The base case scenario for each HFE group represents a realistic description of expected facility, equipment, and operator behavior for the selected operation. These scenarios are created from discussions between the human reliability analysts, other PCSA analysts, and personnel from engineering and operations. In addition to a detailed description of the operation itself, these base case scenarios include a brief description of the initial conditions and relevant equipment features (e.g., interlocks). The relationship between these HFE groups and the corresponding PFD nodes and ESDs are mapped in Attachment E, Table E6.0-1.

6.4.3 Identification of Human Failure Events

There are many possible human errors that could occur at YMP the effects of which might be significant to safety. Human errors, based upon the three temporal phases used in PRA modeling, are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs
- Post-initiator HFEs[1]:
  - Non-recovery
  - Recovery.

Each of these types of HFEs is defined in Attachment E, Section E5.1.1.1. The PCSA model was developed and quantified with pre-initiator and human-induced initiator HFEs included in the model. The safety philosophy of waste handling operations is that an operator need not take any action after an initiating event and there are no actions identified that could exacerbate the consequences of an initiating event. This stems from the definitions and modeling of initiating events and subsequent pivotal events as described in Section 6.1 and Attachment A. All initiating events are proximal causes of either radionuclide release or direct exposure to personnel. With respect to the latter, personnel evacuation was not considered in reducing the frequency of direct exposure but personnel action could cause an initiating event. With respect to the former, pivotal events address containment integrity, confinement availability, shielding integrity, and moderator availability that have no post-initiator human interactions. Containment and shielding integrity are associated only with the physical robustness of the waste containers. Confinement availability is associated with a continuously operating HVAC and the status of equipment confinement doors. Human interactions for HVAC are pre-initiator. Human actions for shielding are associated the initiator phase. Moreover, recovery post-initiator HFEs were not identified and not relied upon to reduce event sequence frequency. Thus, the focus of the HRA task is to support the other PCSA tasks to identify these two HFE phrases.

Pre-Initiator HFEs

Pre-initiators are identified by the system analysts when modeling fault trees during the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human CCF.

Human-Induced Initiator HFEs

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the facility and the SSCs in order to appropriately model the human interface. This iterative process began with the HAZOP evaluation, the MLD and event sequence development, and the event tree and fault tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the

[1] Terminology common to NPPs refer to post-initiator non-recovery events as Type C events and recovery events as Type CR events.

model. Included in this process is an extensive information collection process where industry data for potential vulnerabilities and HFE scenarios are reviewed. The following sources were examined:

- *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 – 2002*, NUREG-1774 (Ref. 2.2.55)

- *Control of Heavy Loads at Nuclear Power Plants*, NUREG-0612 (Ref. 2.2.65)

- Naval Facilities Engineering Command Internet Web Site, Navy Crane Center ("DOE Occurrence Reporting and Processing System (ORPS) Website and Naval Facilities Engineering Command (NAVFAC) Navy Crane Center Website." The database includes the following information:

  – NCC Quarterly Reports ("Crane Corner") 2001 through 2007
  – NCC Fiscal Year 2006 Crane Safety Reports (covers fiscal year 2001 through 2006)
  – NCC Fiscal Year 2006 Audit Report

- DOE Occurrence Reporting and Processing System (ORPS) Internet Web Site, Operational Experience Summaries (2002 through 2007) (http://www.hss.energy.gov/CSA/analysis/orps/orps.html)

- Institute of Nuclear Power Operations (INPO) database (https://www.inpo.org). The INPO database contains the following information:

  – Licensee event reports
  – Equipment Performance and Information Exchange System
  – Nuclear Plant Reliability Data System.

- *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)* (Ref. 2.2.11)

- All SCIENTECH/Licensing Information Service (LIS) data on ISFSI events (1994 through 2007) SCIENTECH and Dry Storage Information Forum (New Orleans, LA, May 2-3, 2001): This database includes the following information:

  – Inspection reports
  – Trip reports
  – Letters, etc.

HFEs identified include both EOOs and EOCs.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., PSFs). This combination of conditions and human factors concerns then becomes the EFC for a specific HFE. Additions and refinements to these initial EFCs are made during the preliminary and detailed analyses.

6.4.4 Preliminary Analysis

A preliminary analysis is performed to allow HRA resources for the detailed analyses to be focused on only the most risk-significant HFEs. The preliminary analysis includes verification of the validity of HFEs included in the initial PCSA model, assignment of conservative HEPs to all HFEs and verification of those probabilities. The actual quantification of preliminary values is a six-step process that is described in detail in Appendix E.III of Attachment E. Once the preliminary probabilities are assigned, the PCSA model is quantified (initial quantification) to determine which HFEs require a detailed quantification. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, that sequence is above Category 1 or Category 2 according to 10 CFR 63.111 (Ref. 2.3.2) performance objectives.

In cases where HFEs are completely mitigated by hardware (i.e., interlocks), the HFE is generally assigned a value of 1.0 unless otherwise noted, and the hardware is modeled explicitly in the fault tree.

6.4.5 Detailed Analysis

Once preliminary values have been assigned, the model is run, and HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, that sequence is Category 1 or Category 2. A dominant sequence is one that does not meet the performance objectives according to the performance objectives in 10 CFR Part 63.111 (Ref. 2.3.2). The objective of a detailed analysis is to develop a more realistic HRA and identify design features to be added that will provide compliance with the aforementioned regulation. Many of the ITS features of Section 6.9 were identified during the HRA. The remaining HFEs retain their assigned preliminary values. For the preliminary analysis, many of the HFEs are modeled in a simplified form in the event trees and fault trees; although, for the preliminary analysis, each action is separated as much as possible for the detailed analysis. This separation is done to ensure that the detailed analysis is thorough and that the relationship between the system functionality and operations crew is transparent. First an HFE is broken down into the various scenarios that lead to the failure. Then, each scenario is further broken down into specific required actions and their applicable procedures, along with the systems and components that must be operated during performance of each action. Each action in each scenario has its own unique context, dependencies, and set of PSFs, and each is quantified independently. The failure probabilities for these unsafe actions are quantified by the HRA method appropriate to the HFE, its classification (e.g., EOC, EOO, observation error, execution error), and the context. For this analysis, several HRA methods were considered, and the following four methods were selected (Appendix E.IV of Attachment E provides a discussion of the selection process):

- CREAM (*Cognitive Reliability and Error Analysis Method, CREAM* (Ref. 2.2.54))
- HEART/NARA ("HEART - A Proposed Method for Assessing and Reducing Human Error" (Ref. 2.2.88)/, and *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. 2.2.41))

- THERP with some modifications (*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report* (Ref. 2.2.84))

- ATHEANA's expert elicitation approach (*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)* (Ref. 2.2.70)).

For the preliminary analysis, HFEs are modeled at a high level where several subtasks are combined into a single task so that explicit consideration of dependencies between subtasks is eliminated. For a detailed assessment, where the various actions that constitute an HFE are explicitly quantified, dependencies are also explicitly addressed using the basic formulae in Table 6.4-1 from the THERP method (Ref. 2.2.84), where N is the independently derived HEP.

Table 6.4-1. Formulae for Addressing HFE Dependencies

Level of Dependence	Zero	Low	Medium	High	Complete
Conditional Probability	N	$\frac{1 + 19N}{20}$	$\frac{1 + 6N}{7}$	$\frac{1 + N}{2}$	1.0

Source: Modified from *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Ref. 2.2.84), Table 20-17, p. 20–33.

After estimates for HFE probabilities are generated, these results are reviewed by the HRA team and, in some cases, by knowledgeable operations personnel, as a "sanity check." Principally, such checks are used, for example, to compare the probabilities of different HFEs and determine whether or not these probabilities are consistent with the judgment of experts regarding the associated operator actions. A review of this type is particularly important for HFE probabilities that are generated using data from the THERP method (Ref. 2.2.84) since it is difficult to identify all important PSFs that are appropriate for repository operations. In addition, the HFE probability estimates are reviewed to ensure that they do not exceed the lower limit of credible human performance as defined by NARA (Ref. E2.2.41). HFE probabilities produced in this HRA are mean values; uncertainties are accounted for by applying an error factor to the mean value of the overall HFE according to the guidelines presented in Section E3.4 of Attachment E.

6.4.6 Human Failure Event Probabilities used in WHF Event Sequences Analysis

The results of the HRA are the HFE probabilities used in the event tree and fault tree quantification process, which are listed in Table 6.4-2.

Table 6.4-2. Human Failure Event Probability Summary

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-#EEE-LDCNTRA-BUA-ROE	Operator Fails to Restore Load Center (Train A) Post Maintenance	Electrical	OA (Pre-Initiator)	1.03E−05	10	Preliminary
050-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore Load Center (Train B) Post Maintenance	Electrical	OA (Pre-Initiator)	1.03E−05	10	Preliminary

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-Liddisplace1-HFI-NOD	Operator Inadvertently Displaces Lid	29	3, 5, 7, 10	N/A[b]	N/A	Omitted from Analysis
050-LLW-Cleanup	Operator Exposed during LLW cleanup	23	OA	N/A[b]	N/A	Omitted from Analysis
050-LLW-Collision	Operator Causes Collision with LLW Container	23	OA	N/A[b]	N/A	Omitted from Analysis
050-LLW-Decon-Fail	Operator Improperly Performs Decontamination Procedures	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpCaskDrop01-HFI-NOD	Operator Drops Cask during Preparation Activities	7, 8, 9	3, 5	N/A[b]	N/A	Omitted from Analysis
050-OpClCTMGate1-HFI-NOD	Operator Inappropriately Closes Slide or Port Gate during Vertical Canister Movement and Continues Lifting	13	6	1.00E−03	5	Preliminary
050-OpCollide001-HFI-NOD	Operator Causes Low-speed Collision with RC, TT, HCTT, CTT or TTC	5, 6	2	3.00E−03	5	Preliminary
050-OpCTCollide1-HFI-NOD	Operator Causes Low-speed Collision of Auxiliary Vehicle with Cask, CTT or ST	7, 8, 9, 11, 25	3, 5, 9, 10	3.00E−03	5	Preliminary
050-OpCTCollide2-HFI-NOD	Operator Causes Low-speed Collision of the CTT during Transfer between the Preparation Station to the Cask Unloading Room	10, 14	5, 7, 9	1.00E−03	5	Preliminary
050-OpCTMDirExp1-HFI-NOD	Operator Causes Direct Exposure during CTM Activities (Second Floor, All CTM Movements)	29	6	8.00E−06	10	Detailed
050-OpCTMDrInt01-HFI-COD	Operator Lifts Canister too High with CTM	13	6	1.0	N/A	Preliminary
050-OpCTMdrop001-HFI-COD	Operator Drops Object onto Canister during CTM Operations	13	6	4.00E−07	10	Detailed
050-OpCTMdrop002-HFI-COD	Operator Causes Drop of Canister during CTM Operations	13	6	5.00E−07	10	Detailed
050-OpCTMImpact1-HFI-COD	Operator Moves the CTM while Canister or Object is below or between Levels	13	6	4.00E−08	10	Detailed

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpCTMImpact2-HFI-COD	Operator Causes Canister Impact with Lid during CTM Operations [AO, STC]	13	6	N/A[b]	N/A	Omitted from Analysis
050-OpCTMImpact5-HFI-COD	Operator Causes Canister Impact with SSC during CTM Operations (All)	13	6	1.0	N/A	Preliminary
050-OpCTTImpact1-HFI-NOD	Operator Causes an Impact between an SSC and a Loaded CTT/ST due to Crane Operations	7, 9	5	3.00E−03	5	Preliminary
050-OpDirExpose1-HFI-NOD	Operator Causes Direct Exposure during CTM Activities (First Floor, All CTM Movements)	29	6	1.00E−01	3	Preliminary
050-OpDirExpose2-HFI-NOD	Operator Causes Direct Exposure During CTM Activities	29	6	1.00E−04	10	Preliminary
050-OpDPC-OVP01-HFI-NOW	Operator Causes DPC Overpressurization	17	7	7.00E−08	10	Detailed
050-OpDPCShield1-HFI-NOW	Operator Fails to Properly Shield DPC while Installing Canister Lift Fixture, Leading to Direct Exposure (TC/DPC only)	29	5	4.00E−04	10	Detailed
050-OpDPCShield2-HFI-NOW	Operator Causes Loss of Shielding During DPC Cutting	29	7	2.00E−04	10	Detailed
050-OpDPCShield3-HFI-NOW	Operator Causes Loss of Shielding While Removing DPC Lift Fixture (TC/DPC only)	29	7	4.00E−04	10	Detailed
050-OpExpose-Decon	Operator Exposed During Decontamination	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpExpose-Splash	Operator Exposed Due to Pool Splash	30	7	1.0	N/A	Preliminary
050-OpFailRstInt-HFI-NOM	Operator Fails to Restore Interlock after Maintenance	29	6	1.00E−02	3	Preliminary
050-OpFailSG-HFI-NOD	Operator Fails to Close the CTM Slide Gate before Moving the CTM with the Canister inside the Bell	29	6	1.00E−03	5	Preliminary
050-OpFailStop-HFI-NOD	Operator Fails to Stop the ST if the Tread Fails	3, 11	4, 5, 10	1.0	N/A	Preliminary

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-Op-Filter-Expose	Operator Exposed During Filter Change out	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpFLCollide1-HFI-NOD	Operator Causes High-speed Collision of Loaded Conveyance or Cask with Auxiliary Vehicle	5, 6, 7, 8, 9, 11, 25	2, 3, 5, 9, 10	1.0	N/A	Preliminary
050-OpFLCollide2-HFI-NOD	Operator Causes Collision of Auxiliary Vehicle with Cask at DPC Cutting Station	15	7	N/A[b]	N/A	Omitted from Analysis
050-OpFuelImpact-HFI-NOD	Operator Impacts Fuel Assembly During Transfer	22	8	N/A[b]	N/A	Omitted from Analysis
050-OpHTCollide1-HFI-NOD	Operator Causes Low-speed Collision between HCTT and facility SSC	4	1	3.00E−03	5	Preliminary
050-OpHTIntCol01-HFI-NOD	Operator Causes High-speed Collision between HCTT and facility SSC	4	1	1.0	N/A	Preliminary
050-OpImpact0000-HFI-NOD	Operator Causes Impact of Cask during Transfer from the Platform to Loading/Unloading Room	10, 11, 14	5, 7, 10	N/A[b]	N/A	Omitted from Analysis
050-OpLoadDrop-HFI-NOD	Operator Causes ST to Drop the AO	3, 11	4, 10	N/A[b]	N/A	Omitted from Analysis
050-OpNoDiscoAir-HFI-NOD	Operator Causes Spurious Movement of CTT while Canister is Being Loaded	13	6	1.00E−03	5	Preliminary
050-OpNoUnBolt00-HFI-NOD	Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tipover (AO or STC)	13	6	1.00E−03	5	Preliminary
050-OpNoUnBoltDP-HFI-NOD	Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tipover (TC/DPC)	13	6	N/A[b]	N/A	Omitted from Analysis
050-OpNoUnplugST-HFI-NOD	Operator Causes Spurious Movement of the ST while Canister is Being Loaded	13	6	1.00E−03	5	Preliminary
050-OpRCCollide1-HFI-NOD	Operator Causes Low-speed Collision between RC and facility SSC	2	1	3.00E−03	5	Preliminary

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpRCIntCol01-HFI-NOD	Operator Causes High-speed Collision between RC and facility SSC	2	1	1.0	N/A	Preliminary
050-OpRCIntCol02-HFI-NOD	Operator Causes the Mobile Access Platform to Collide into a RC	2	1	1.0	N/A	Preliminary
050-OpSampleRel2-HFI-NOD	Operator Improperly Performs Gas Sampling of Canister or Cask with Bare SNF	16, 17	3, 7	5.00E−03	5	Preliminary
050-OpSDClose001-HFI-NOD	Operator Closes Shield Door on Conveyance	12	OA (5, 7, 9, 10)	1.0	N/A	Preliminary
050-OpSpurMove01-HFI-NOD	Operator Causes Spurious Movement of the CTT in the Preparation Area or ST in the ST Vestibule	6, 7, 9, 11	2, 5, 10	1.00E−04	10	Preliminary
050-OpSTCollide3-HFI-NOD	Operator Causes Low-speed Collision of ST with an SSC while Moving to the ST Vestibule or Loading Room	3, 11	4, 5, 10	3.00E−03	5	Preliminary
050-OpSTCollide4-HFI-NOD	Operator Causes Low-Speed Collision of ST with SSC while Exporting the ST	11	10	3.00E−03	5	Preliminary
050-OpSTCShield1-HFI-COD	Operator Causes a Direct Exposure Due to Failure to Properly Install the STC Shield Ring	29	9	6.00E−05	10	Detailed
050-OpTCImpact01-HFI-NOD	Operator Causes an Impact Between Cask and SSC (Preparation Area)	5, 6, 8, 11, 15, 28	2, 3, 7, 9, 10	3.00E−03	5	Preliminary
050-OpTCImpact06-HFI-NOD	Operator Causes an Impact between the Cask and an SSC during Movement between the Pool Ledge and the Outside of the Pool	19, 20, 24	8	3.00E−03	5	Preliminary
050-OpTCImpact07-HFI-COD	Operator Causes an Impact Between Cask and SSC during Cask Movement between Pool Shelf and Pool Bottom	21	8	6.00E−03	5	Preliminary

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpTCImpact10-HFI-NOD	Operator Causes an Impact between a Cask and an SSC during TAD Canister Closure	25	9	6.00E−03	5	Preliminary
050-OpTipover001-HFI-NOD	Operator Causes Cask to Tip Over (Preparation Area)	5, 6, 7, 8, 15, 28	2, 3, 5, 7, 9	1.00E−04	10	Preliminary
050-OpTipOver002-HFI-NOD	Operator Causes Cask to Tip Over during Movement between Pool Ledge and Outside the Pool	19, 20, 24	8	3.00E−03	5	Preliminary
050-OpTipOver004-HFI-COD	Operator Causes Cask to Tip Over during Cask Movement between Pool Shelf and Pool Bottom	21	8	6.00E−03	5	Preliminary
050-OpTipOver3-HFI-NOD	Operator Causes a Tipover of CTT during Movement to the Cask Unloading Room or Tipover of ST with Jib Crane	10, 11	5, 10	N/A[b]	N/A	Omitted from Analysis
050-OpTTCollide1-HFI-NOD	Operator Causes Low-speed Collision between TT and facility SSC	1	1	3.00E−03	5	Preliminary
050-OpTTIntCol01-HFI-NOD	Operator Causes High-speed Collision between TT and facility SSC	1	1	1.0	N/A	Preliminary
050-OpTTIntCol02-HFI-NOD	Operator Causes the Mobile Access Platform to Collide into a TT	1	1	1.0	N/A	Preliminary
050-OpTTRollover-HFI-NOD	Operator Causes a TT or HCTT to Rollover as the Conveyance Moves into the Cask Preparation Area	1, 4	1	N/A[b]	N/A	Omitted from Analysis
050-TadDry-Fail	Operator Leaves Water in the TAD Canister	26	9	N/A[b]	N/A	Omitted from Analysis
050-VCSO-DR00001-HFI-NOD	Operators Open 2 or More Vestibule Doors in WHF	HVAC	OA (Pre-initiator)	1.00E−02	3	Preliminary
050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	HVAC	OA (Pre-initiator)	1.0	N/A	Preliminary
050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	HVAC	OA (Pre-initiator)	1.00E−01	3	Preliminary
050-WeldDetect-Fail	Operator Causes Defective Weld or Fails to Detect a Bad Weld	27	9	N/A[b]	N/A	Omitted from Analysis

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
26D-#EEY-ITSDG-A-#DG-RSS	Operator Fails to Restore Diesel Generator to Service (Train A)	Electrical	OA (Pre-initiator)	1.95E−04	10	Preliminary
26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator to Service (Train B)	Electrical	OA (Pre-initiator)	1.95-04	10	Preliminary
Crane Drops	Operator Causes Drop of Cask or Drop of Object onto Cask	OA (5-9, 15, 17-24, 30)	OA (2, 3, 5, 7, 8)	N/A [a]	N/A	Historical Data
Drop from SNF Transfer Machine	Operator Causes Drop of Fuel Assembly	22	8	N/A [a]	N/A	Historical Data
Fuel Transpose	Operator Misloads TAD Canister	N/A	8	N/A[b]	N/A	Omitted from Analysis
Gas Sampling	Operator Improperly Performs Gas Sampling of Cask with Canister	29	5	N/A[b]	N/A	Omitted from Analysis
Improper Boration	Operator Fails to Maintain Proper Boron Concentration	N/A	8	N/A[b]	N/A	Omitted from Analysis
Load too Heavy	Operator attempts to lift load which is greater than crane rating	OA	OA	N/A[b]	N/A	Omitted from Analysis
Moderator	Operator Introduces Moderator Source in to Moderator-Controlled Areas of the WHF	OA	OA	N/A[b]	N/A	Omitted from Analysis
RC Derailment	Operator Causes RC to Derail as the RC travels into the Cask Preparation Area	1	1	N/A [a]	N/A	Historical Data
Spurious Movement of CTT or ST during CTM Activities	Operator Causes Spurious Movement of CTT or ST while Canister is Being Loaded	13	6	N/A[b]	N/A	Omitted from Analysis

Table 6.4-2. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
ST Rollover	Operator Causes the ST to Rollover in the ST Vestibule	3, 11	4, 10	N/A[b]	N/A	Omitted from Analysis

NOTE: [a] Historical data was used to produce a probability for this HFE; this is not covered as part of the HRA, but rather addressed in Attachment C.
[b] These HFEs were initially identified, but omitted from analysis for various reasons, including a design change precluding the human failure, or the failure would require a series of unsafe actions in combination with mechanical failures, such that the event is no longer credible. See the appropriate HFE group in Attachment E for a case-by-case justification for these omissions.
AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HCTT = cask tractor and cask transfer trailer; HFE = human failure event; HSTC = horizontal shielded transfer cask; LLW = low-level radioactive waste; N/A = not applicable; OA = over arching (applies to multiple HFE groups, Section E6.0.2); RC = railcar; SNF = spent nuclear fuel; ST = site transporter; SSC = structure, system, or component; SSCs = structures, systems, and components; STC = shielded transfer cask; TAD = transportation, aging, and disposal; TC = transportation cask; TT = truck trailer; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar; WHF = Wet Handling Facility.

Source: Original (Attachment E, Table E7-1).

6.5 FIRE INITIATING EVENTS

Attachment F of this document describes the work scope, methodology, and results for the fire analysis performed as a part of the PCSA. The internal events of the PCSA model are evaluated with respect to fire initiating events and modified as necessary to address fire-induced failures that lead to exposures. The list of fire-induced failures included in the model, are evaluated as to fire vulnerability, and fragility analyses are conducted as needed (Section 6.3.2 and Attachment D, Section D2.1.5).

Fire initiating event frequencies have been calculated for each initiating event identified for the WHF. Section F5 of Attachment F details the analysis performed to determine these frequencies, using the methodology described in Section F4 of Attachment F.

6.5.1 Input to Initiating Events

Room and building areas; ignition frequencies; ignition source distributions; propagation probabilities; and residence fractions are the set of calculated values which contribute to calculating initiating event frequencies.

Room dimensions (Section F5.2.1 of Attachment F) are utilized to determine individual room areas, and the total building area. The area of the WHF is utilized to evaluate the building ignition frequency. From methodology and equations presented in Section F4.3.1 of Attachment F, the building ignition frequency over the 50 year facility operation period of 2.96, is obtained for the WHF. The results of this portion of the analysis are summarized in Table 6.5-1.

As discussed in Section F4.3.2.1 and Appendix F.II of Attachment F, an industrial building fire can begin as the result of numerous types of ignition sources, which are grouped into nine categories:

1. Electrical equipment.
2. HVAC equipment.
3. Mechanical process equipment.
4. Heat-generating process equipment.
5. Torches, welders, and burners.
6. Internal combustion engines.
7. Office and kitchen equipment.
8. Portable and special equipment.
9. No equipment involved.

Table 6.5-1. Room Areas and Total Ignition Frequency

Room	Area(sq-m)	Room	Area(sq-m)	Room	Area(sq-m)	Room	Area(sq-m)
B001	69	1018B	14	1044B	25	2002	216
B002	65	1019	186	1044C	25	2003	134
B003	38	1020	30	1045A	33	2004	1017
B004	68	1021	216	1045B	33	2005A	142
B005	35	1022	6	1045C	100	2005B	90
B006	3	1023	434	1045D	99	2006	136
B007	7	1024	20	1046	158	2007A	52
B008	62	1025	29	1201	8	2007B	197
B009	65	1026	31	1202	21	2008	522
1001	1630	1027	31	1203	34	2010	216
1002	186	1028	56	1204	40	2011A	95
1003	30	1029	28	1205	44	2011B	120
1004	216	1030	17	1206	12	2012	241
1005	9	1031	31	1207	51	2013	14
1006	160	1032	27	1208	9	2024	18
1007	182	1032A	22	1209	39	2025	45
1008	133	1033	32	1210	22	2026	31
1009	228	1034	29	1211	12	2027	31
1010	38	1035	17	1212	21	2029	17
1011A	51	1036	17	1213	15	2030	14
1011B	137	1037	7	1214	15	2032	9
1012A	49	1038	7	1215	70	2033	12
1012B	100	1039	7	1216	25	2034	29
1013	315	1042A	19	1217	25	2201	19
1014	18	1042B	19	1218A	60	2202	30
1015	6	1042C	19	1218B	30	2203	52
1016	4097	1043A	30	1218C	58	2204	12
1017	269	1043B	30	M001	474	2205	13
1018	21	1043C	30	2001	140	2206	8
1018A	14	1044A	25	2001A	46		
Total Area (sq-m)				15046			
Ignition Frequency (per sq-m/yr)				3.94E-06			
Ignition Frequency (per yr)				5.93E-02			

NOTE: sq-m = square meter; yr = year.

Source: Table F5.2-1 of Attachment F.

Each category has a fraction representing the probability that, given an ignition, that category is the source of the ignition. These fractions are combined with the number of units in each category to determine the ignition frequency per ignition source. Uncertainty distributions have been applied to the ignition frequencies, and contribute to the resulting distribution for fire initiating event frequencies. The number of ignition sources in each category is further divided by location into specific rooms. Each piece of equipment in a category is defined as one ignition source, with some exceptions:

- Motor control centers, load centers, and equipment racks contribute an ignition source for each active vertical cabinet

- An ignition source is counted for each motor over 5 hp for all equipment with motors
- A welding ignition source is counted for each hour of operation expected per year
- The ignition sources for mobile equipment are split between the rooms the equipment occupies in proportion to the amount of time the equipment will spend in each room
- An ignition source is counted for every square meter in the room for the no equipment involved category.

The distribution and determination of ignition sources is further discussed in Section F5.4 of Attachment F, and summarized in Table 6.5-2. Because the "no equipment involved" category ignition sources are equal to the square meters values (available in Table 6.5-1), and because there is no equipment for any of the facilities that falls under the heat-generating process equipment category (F5.4.4), those categories are not presented in the summary Table 6.5-2.

Table 6.5-2. Ignition Source Category and Room-by-Room Population

Room	Electrical	HVAC	Mechanical Equipment	Torches, welders, burners	Internal combustion engines	Office/ kitchen equipment	Portable Equipment
B002			2				
P001							
1001		4	3	10	22		
1002	22	2		5			4
1003	1	4					
1004		4		5			4
1006		6					4
1007					61		
1008			0.03				2
1009				5			
1013			1	5			
1016			32.97	365	78		8
1017	5		4				
1018		2		400			
1019	23	2		5			4
1020	1	4					
1021		4					4
1023		3	4		39		
1028			1				
1036			1				
1042A			1				
1042B			1				
1042C			1				
1045C			1				
1046	92						

Table 6.5-2. Ignition Source Category and Room-by-Room Population (Continued)

Room	Electrical	HVAC	Mechanical Equipment	Torches, welders, burners	Internal combustion engines	Office/ kitchen equipment	Portable Equipment
1202						1	
1205						1	
1209						1	
1210						1	
1211						1	
1212						1	
1215						1	
1216						1	
1217						1	
M001		3					4
2001	66						4
2001A	2	4					
2002		2					4
2003		1					4
2004			7	5			2
2008				5			
2010		4					4
2011A						2	
2011B						2	
2012	6					2	
2201						1	
2202						1	
2203						3	
TOTAL	**217**	**49**	**64**	**810**	**200**	**20**	**52**

NOTE: HVAC = heating, ventilation, and air conditioning.

Source: Table F5.5-1 of Attachment F.

Propagation probabilities (Section F5.6, Attachment F) are utilized in the analysis to define the probability of a fire spreading to various points specifically identified as areas in which a waste form may be vulnerable. Uncertainty distributions have been applied to the propagation probabilities, and contribute to the resulting distribution for fire initiating even frequencies.

Residence fractions (Section F5.7.1, Attachment F) developed from process throughputs define the length of time (in minutes), a waste form will be vulnerable in a particular area of the building and in a particular configuration. The minutes are converted to the fraction of time the vulnerability is present over the 50 year pre-closure surface operation period, and are summarized in Table 6.5-3.

Table 6.5-3. Residence Fractions

Initiating Event	Residence Fraction
TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	
TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel)	1.7E-06
Waste Form on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)	
TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel)	1.0E-05
TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel)	3.1E-05
TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel)	1.6E-05
TC/SNF in the Preparation Area	
TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area	3.9E-06
TC/SNF (Wet Cavity) in the Preparation Station in the Preparation Area	7.7E-06
TC/DPC or STC/DPC on CTT in the Preparation Station	
TC/DPC (all) on CTT in the Preparation Station in the Preparation Area	2.4E-05
STC/DPC (all) on CTT in the Preparation Station in the Preparation Area	3.1E-05
Waste Form on CTT in the Unloading Room	
TC/DPC (all) on CTT in the Unloading Room	2.0E-06
STC/DPC (all) on CTT in the Unloading Room	5.0E-06
STC/TAD on CTT in the Unloading Room	4.3E-06
DPC or TAD in the Transfer Room	
DPC (all) in the Transfer Room	1.1E-06
TAD in the Transfer Room	9.1E-07
STC/DPC in DPC Cutting Station in the Preparation Area	
STC/DPC in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area	6.1E-06
STC/DPC in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area	4.2E-05
STC/DPC in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area	3.4E-05
STC/TAD in TAD Closure Station in the Preparation Area	
STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area	1.6E-05
STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area	7.0E-05
STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area	4.1E-05
TAD in AO in Loading Room	
TAD in AO in Loading Room	3.7E-06
TAD in AO in Bolting Room	
TAD in AO in Bolting Room	9.7E-06
TC/SNF or TC/DPC (all) (Diesel Present)	1.7E-06
TC/SNF (No Diesel)	1.4E-05
TC/DPC (TTC) (No Diesel)	5.6E-05
TC/DPC (No Diesel)	3.9E-05
DPC (all) in CTM	1.1E-06
STC/DPC (all)	4.1E-05
STC/DPC (all) (Dry Cavity, Wet Annulus)	4.2E-05
STC/DPC (all) (Wet Cavity, Wet Annulus)	3.4E-05
TC/SNF (Wet Cavity)	7.7E-06

Table 6.5-3. Residence Fractions (Continued)

Initiating Event	Residence Fraction
STC/TAD (Wet Cavity, Wet Annulus)	4.1E-05
STC/TAD (Dry Cavity, Wet Annulus)	7.0E-05
STC/TAD (Dry Cavity, Dry Annulus)	1.9E-05
TAD in CTM	9.1E-07
TAD in AO	1.3E-05

NOTE: AO = aging overpack; CTM = canister transfer machine; DPC = dual-purpose canister; TAD = transportation, aging, and disposal; TC = transportation cask; TTC= transportation cask in the tilted position.

Source: Attachment F, Table F5.7-1.

6.5.2 Initiating Event Frequencies

The results of the fire initiating event analysis are the fire initiating event frequencies and their associated distributions, as presented in Table 6.5-4. The frequencies represent the probability, over the length of the pre-closure surface operation period, that a fire will threaten the stated waste container in the stated location. Initiating event frequencies are divided into two types of calculations, localized fires and large fires, and are calculated for all locations associated with waste handling operations and locations from which a fire can spread to a waste handling operational location. (In Attachment F, these locations are sometimes called vulnerabilities). Calculations performed to obtain the initiating event are detailed in Section F5.7 of Attachment F.

Uncertainty distributions are utilized in the contribution to initiating event frequency calculations to account for statistical uncertainty in the data. Uncertainty distributions utilized for this analysis are lognormal distribution, and normal distribution. The normal distribution can be accurately represented by a mean and 97.5% value, the lognormal distribution is represented by a median (50%) and 97.5% value. The mean and median can be inputs to calculate the error factor (EF). The 97.5 percent value is a figure that represents a point at which only 2.5 percent of all possible outcomes will vary from the mean more significantly. Three uncertainty distributions were developed for this analysis, details for which are in Appendices F.II and F.III of Attachment F.

Monte Carlo simulations are performed to determine the mean, median, standard deviation, variance, minimum, and maximum values of each of the initiating event frequencies based on the variance of the contributing data. To accomplish this, the Microsoft Excel add-on package Crystal Ball is used (Attachment F, Section F5.6 and F5.8). This software requires input of two parameters (e.g., in the lognormal case, 50 percent and 97.5 percent values. Crystal Ball software allows probability distributions to be combined per formulas or equations representing initiating event frequency inputs entered into EXCEL. The software randomly selects a value from the possibilities defined by the distribution. Ten thousand Monte Carlo trials are performed.

Crystal Ball is run for all of the initiating events, the complete output of which is available in Appendix F.VI of Attachment F. In addition to showing the initiating event frequency

distribution, the full output also shows the input distribution for the parameters that are varied, which match the distributions developed and documented in Appendices F.II and F.III of Attachment F.

Table 6.5-4. Results from Monte Carlo Simulation of Initiating Event Frequency Distributions

Initiating Event	Equipment	Mean	Median	97.5% Value	Error Factor	Type
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	Railcar/Truck					
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)		4.7E-07	4.2E-07	1.1E-06	2.2E+00	Lognormal
Localized Fire Threatens Waste Form on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)	Railcar/Truck					
Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)		2.5E-06	2.3E-06	5.7E-06	2.2E+00	Lognormal
Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)		7.6E-06	6.8E-06	1.7E-05	2.2E+00	Lognormal
Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)		4.0E-06	3.6E-06	9.0E-06	2.2E+00	Lognormal
Localized Fire Threatens TC/SNF in the Preparation Area	Preparation Station					
Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area		1.9E-06	1.7E-06	4.2E-06	2.1E+00	Lognormal
Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station in the Preparation Area		3.6E-06	3.3E-06	8.2E-06	2.1E+00	Lognormal
Localized Fire Threatens TC/DPC or STC/DPC on CTT in the Preparation Station	Cask Transfer Trolley					
Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station in the Preparation Area		4.2E-06	3.8E-06	9.8E-06	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area		5.4E-06	4.8E-06	1.3E-05	2.2E+00	Lognormal
Localized Fire Threatens Waste Form on CTT in the Unloading Room	Cask Transfer Trolley					
Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room		1.5E-07	1.4E-07	3.5E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room		3.9E-07	3.5E-07	8.9E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD on CTT in the Unloading Room		3.3E-07	3.0E-07	7.6E-07	2.2E+00	Lognormal

Table 6.5-4. Results from Monte Carlo Simulation of Initiating Event Frequency Distributions (Continued)

Initiating Event	Equipment	Mean	Median	97.5% Value	Error Factor	Type
Localized Fire Threatens DPC or TAD in the Transfer Room	Canister Transfer Machine					
Localized Fire Threatens DPC (all) in the Transfer Room		8.3E-08	7.4E-08	1.9E-07	2.2E+00	Lognormal
Localized Fire Threatens TAD in the Transfer Room		6.9E-08	6.2E-08	1.6E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC in DPC Cutting Station in the Preparation Area	DPC Cutting Station					
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area		1.2E-06	1.1E-06	2.8E-06	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area		8.3E-06	7.4E-06	1.9E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area		6.8E-06	6.0E-06	1.5E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station in the Preparation Area	TAD Closure Station					
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area		7.5E-06	6.8E-06	1.7E-05	2.1E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area		8.6E-06	7.6E-06	2.0E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area		6.8E-06	6.1E-06	1.6E-05	2.2E+00	Lognormal
Localized Fire Threatens TAD in AO in Loading Room	Site Transporter					
Localized Fire Threatens TAD in AO in Loading Room		2.9E-07	2.6E-07	6.8E-07	2.2E+00	Lognormal
Localized Fire Threatens TAD in AO in Bolting Room	Site Transporter					
Localized Fire Threatens TAD in AO in Bolting Room		3.5E-07	3.1E-07	8.3E-07	2.2E+00	Lognormal
Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present)		7.9E-07	7.0E-07	1.8E-06	2.2E+00	Lognormal
Large Fire Threatens TC/SNF (No Diesel)		6.7E-06	5.9E-06	1.6E-05	2.2E+00	Lognormal
Large Fire Threatens TC/DPC (TTC) (No Diesel)		2.6E-05	2.3E-05	6.1E-05	2.2E+00	Lognormal
Large Fire Threatens TC/DPC (No Diesel)		1.8E-05	1.6E-05	4.3E-05	2.2E+00	Lognormal
Large Fire Threatens DPC (all) in CTM		5.2E-07	4.6E-07	1.2E-06	2.3E+00	Lognormal
Large Fire Threatens STC/DPC (all)		1.9E-05	1.7E-05	4.5E-05	2.1E+00	Lognormal
Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus)		2.0E-05	1.7E-05	4.6E-05	2.4E+00	Lognormal
Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus)		1.6E-05	1.4E-05	3.7E-05	2.3E+00	Lognormal

Table 6.5-4. Results from Monte Carlo Simulation of Initiating Event Frequency Distributions (Continued)

Initiating Event	Equipment	Mean	Median	97.5% Value	Error Factor	Type
Large Fire Threatens TC/SNF (Wet Cavity)		3.6E-06	3.2E-06	8.4E-06	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Wet Cavity, Wet Annulus)		1.9E-05	1.7E-05	4.4E-05	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus)		3.3E-05	2.9E-05	7.7E-05	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus)		8.8E-06	7.8E-06	2.1E-05	2.2E+00	Lognormal
Large Fire Threatens TAD in CTM		4.3E-07	3.8E-07	1.0E-06	2.2E+00	Lognormal
Large Fire Threatens TAD in AO		5.9E-06	5.3E-06	1.4E-05	2.2E+00	Lognormal

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; TAD = transportation, aging, and disposal; TC = transportation cask; TTC=transportation cask in tilting position.

Source: Table F5.7-5 of Attachment F.

For use in the model, some fire initiating event results were summed, and are illustrated in Table 6.5-5. These are sums of distributions, and were therefore performed using Crystal Ball. Table 6.5-6 provides the fire analysis data for the basic events in this model.

Table 6.5-5 Basic Events Data Associated with Fire Analysis

Fire Initiating Events	Mean
Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)	7.6E-06
Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)	4.0E-06
Localized Fire Threatens TC/SNF or TC/DPC (including TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	4.7E-07
Total	**1.2E-05**
Localized Fire Threatens TC/SNF or TC/DPC (including TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	4.7E-07
Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)	2.5E-06
Total	**3.0E-06**
Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Cask Preparation Area	1.9E-06
Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station in the Cask Preparation Area	3.6E-06
Total	**5.4E-06**
Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station in the Cask Preparation Area	4.2E-06
Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Cask Preparation Area	5.4E-06
Total	**8.9E-06**
Localized Fire Threatens TC/DPC (all) on CTT in the Cask Unloading Room	1.5E-07
Localized Fire Threatens STC/DPC (all) on CTT in the Cask Unloading Room	3.9E-07
Total	**4.9E-07**

Table 6.5-5 Basic Events Data Associated with Fire Analysis (Continued)

Fire Initiating Events	Mean
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Cask Preparation Area	1.2E-06
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Cask Preparation Area	8.3E-06
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Cask Preparation Area	6.8E-06
Total	**1.7E-05**
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Cask Preparation Area	7.5E-06
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Cask Preparation Area	8.6E-06
Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Cask Preparation Area	6.8E-06
Total	**2.3E-05**
Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present)	7.9E-07
Large Fire Threatens TC/SNF (No Diesel)	6.7E-06
Large Fire Threatens TC/SNF (Wet Cavity)	3.6E-06
Total	**1.1E-05**
Fire Initiating Events	**Mean**
Large Fire Threatens TC/DPC (TTC) (No Diesel)	2.6E-05
Large Fire Threatens TC/DPC (No Diesel)	1.8E-05
Large Fire Threatens DPC (all) in CTM	5.2E-07
Large Fire Threatens STC/DPC (all)	1.9E-05
Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus)	2.0E-05
Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus)	1.6E-05
Total	**1.0E-04**
Large Fire Threatens STC/TAD (Wet Cavity, Wet Annulus)	1.9E-05
Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus)	3.3E-05
Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus)	8.8E-06
Large Fire Threatens TAD in CTM	4.3E-07
Large Fire Threatens TAD in AO	5.9E-06
Total	**6.7E-05**

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; SNF = spent nuclear fuel; SPM = site prime mover; STC = shielded transportation cask; TAD = transportation, aging, and disposal canister; TC= transportation cask; TTC = a transportation cask that is upended using a tilt frame; w/o = without.

Source: Original

Table 6.5-6. Basic Events Data Associated with Fire Analysis

Basic Event Name	Basic Event Description	BE Value	Bases	References
050-FIRE-CSNF-PREP	Cask Preparation Area fire affects CSNF	5.4E-06	Localized fire threatens a TC containing CSNF (dry or wet cavity) at the preparation station in the Cask Preparation Area (no diesel).	Table 6.5-5
050-FIRE-CSNF-VEST	Fire threatens CSNF in Transportation Cask Vestibule	3.0E-06	Localized fire threatens a TC containing CSNF on the railcar/trailer in the receipt area/ Transportation Cask Vestibule.	Table 6.5-5
050-FIRE-DPC-CTM	Fire affects DPC in the CTM	8.3E-08	Localized fire threatens DPC in the Canister Transfer Room.	Table 6.5-4
050-FIRE-DPC-DPCCUT	Fire affects DPC at DPC cutting station	1.7E-05	Localized fire threatens a DPC (dry or wet cavity/annulus) at the DPC cutting station in the Cask Preparation Area.	Table 6.5-5
050-FIRE-DPC-LARGE	Large fire affects DPC	1.0E-04	Large fire threatens DPC anywhere in the WHF.	Table 6.5-5
050-FIRE-DPC-PREP	Fire affects DPC in Cask Preparation Area	8.9E-06	Localized fire threatens a TC or STC containing a DPC on the CTT at the preparation station in the Cask Preparation Area.	Table 6.5-5
050-FIRE-DPC-UNLOAD	Fire affects DPC in Cask Unloading Room	4.9E-07	Localized fire threatens a TC or STC containing a DPC on the CTT in the Cask Unloading Room.	Table 6.5-5
050-FIRE-DPC-VEST	Fire affects DPC in Transportation Cask Vestibule	1.2E-05	Localized fire threatens a TC containing a DPC on a railcar/trailer in the receipt area/ Transportation Cask Vestibule.	Table 6.5-5
050-FIRE-LARGE-CSNF	Large fire affects CSNF	1.1E-05	Large fire threatens CSNF anywhere in the WHF.	Table 6.5-5
050-FIRE-TAD-CLOSE	Fire affects TAD canister in closure area	2.3E-05	Localized fire threatens an STC containing a TAD canister (dry or wet cavity/annulus) at the closure station in the Cask Preparation Area.	Table 6.5-5
050-FIRE-TAD-CTM	Fire affects TAD canister in CTM	6.9E-08	Localized fire threatens TAD canister on the CTM in the Canister Transfer Room.	Table 6.5-4
050-FIRE-TAD-LARGE	Large fire affects TAD canister	6.7E-06	Large fire threatens a TAD canister anywhere in the WHF.	Table 6.5-5

Table 6.5-6. Basic Events Data Associated with Fire Analysis (Continued)

Basic Event Name	Basic Event Description	BE Value	Bases	References
050-FIRE-TAD-LOAD	Fire affects TAD canister in Loading Room	2.9E-07	Localized fire threatens TAD canister in AO in the Loading Room.	Table 6.5-4
050-FIRE-TAD-UNLOAD	Fire affects TAD in Cask Unloading Room	3.3E-07	Localized fire threatens STC containing TAD canister on the CTT in the Cask Unloading Room.	Table 6.5-4
050-FIRE-TAD-VEST	Fire affects TAD in Transportation Cask Vestibule (bolting room)	3.5E-07	Localized fire threatens TAD canister in AO in the bolting room.	Table 6.5-4

NOTE: AO = aging overpack; CSNF = commercial spent nuclear fuel; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; STC = shielded transportation cask; TAD = transportation, aging, and disposal canister; TC= transportation cask.

Source: Original

6.6 NOT USED

6.7 EVENT SEQUENCE FREQUENCY RESULTS

This section provides the results of the event sequence quantification as produced from the SAPHIRE (Ref. 2.2.77) analyses. Quantification of an event sequence consists of calculating its number of occurrences over the preclosure period by combining the frequency of a single initiating event with the conditional probabilities of pivotal events that comprise the sequence. The quantification results are presented as an expression of the mean and median number of occurrences of each event sequence over the preclosure period, and the standard deviation as a measure of uncertainty. Section 6.8 describes the process for aggregation of similar event sequences to permit categorization as Category 1, Category 2, or beyond Category 2 event sequences.

The section presents a summary of how the quantification is performed by linking of event trees, fault trees, and basic event input parameters. The discussion includes the rationale for truncating low values and the analysis of uncertainties.

The results include a summary of all event sequences that are quantified and a table summarizing the results of the final quantification (Attachment G).

6.7.1 Process for Event Sequence Quantification

Internal event sequences that are based on the event trees presented in Section 6.1 and fault trees presented in Section 6.2 are quantified using SAPHIRE (Section 4.2). In SAPHIRE, the quantification of an event sequence is always labeled as a "frequency" in the output formats.

The event sequence quantification methodology is presented in Section 4.3.6. An event sequence frequency is the product of several factors, as follows (with examples):

- The number of times the operation or activity that gives rise to the event sequence is performed over the preclosure period, for example, the total number of transfers of a TAD canister by a CTM in the WHF over the preclosure period. In SAPHIRE, this number is entered in the first event of the initiator event tree from which the event sequence arises or in the first event of the system-response event tree if no initiator event tree exists.

- The probability of occurrence of the initiating event for the event sequence considered. Continuing with the previous example, this could be the probability of dropping a TAD canister during its transfer by the CTM in the WHF, or the probability of occurrence of a fire that could affect the TAD canister during its transfer by the CTM. The initiating event probability is modeled in SAPHIRE with a fault tree or with a basic event. In an initiator event tree, this probability is assigned on the branch associated with that initiating event , through the use of SAPHIRE rules (i.e., textual logic instructions that determine which fault tree or basic event is to be used). If no initiator event tree exists, this probability is entered in the second event of the system-response event tree.

- The conditional probability of each of the pivotal events of the event sequence, which appear in the system-response event tree. The pivotal event may represent a passive failure such as the breach of the containment boundary of the TAD canister or an active system failure such as the unavailability of the HVAC system. The conditional event probabilities of pivotal events are linked to the event sequence in SAPHIRE through the linkage to basic events in a fault tree that represents the pivotal event. The selection of pivotal event models and the associated basic event values may be determined by SAPHIRE rules.

Uncertainties in input parameters such as throughput rates, equipment failure rates, passive failure probabilities, and HFEs used to calculate basic event probabilities are propagated through the fault tree and event sequence logic to quantify the uncertainty in the event sequence quantification.

To quantify an event sequence, SAPHIRE (Section 4.2) first establishes the logic of the event sequence (i.e., the combination of individual successes and failures of pivotal events after the initiating event). SAPHIRE then links together the fault trees that support the initiating event and the pivotal events and uses Boolean logic to identify dependencies between the initiating event and the pivotal events and between pivotal events. SAPHIRE finally develops minimal cut sets for the event sequence considered. A minimal cut set for an event sequence is a Boolean reduced combination of a set of basic events that, if they occur, will cause the event sequence to occur. The event sequence frequency is calculated as the sum of frequencies of the cut sets. No cutoff probability was used to ensure that event sequences are grouped properly.

As an illustration of the above process, the quantification of the event sequence initiated by a drop of a TAD canister during a transfer in the WHF, followed by the breach of the canister, the subsequent failure of the HVAC confinement to perform its confinement and filtering function over its mission time, but no moderator entry into the canister, is outlined in the following paragraphs.

As noted, uncertainties in input parameters are propagated through the fault tree and event sequence logic to quantify the uncertainty in the event sequence quantification. The uncertainty analysis uses the Monte Carlo method that is built into SAPHIRE. Each event sequence was analyzed using 10,000 trials. The number of trials is considered sufficient to ensure accurate results for the distribution parameters.

6.7.2 Event Sequence Quantification Summary

Table G-1 of Attachment G presents the result of the event sequence quantification. Table G-1 summarizes the results of the final quantification and lists the following elements: (1) event tree from which the sequence is generated, (2) SAPHIRE event sequence designator (ID), (3) initiating event description, (4) event sequence logic, (5) event sequence end state, (6) event sequence mean value, (7) event sequence median value, and (8) event sequence variance.

6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION

An aggregation grouping process is applied prior to a categorization of event sequences as was described in Section 4.3.1.. It is appropriate for purposes of categorization, to add the frequencies of event sequences that are derived from the same ESD, that elicits the same combination of failure and success of pivotal events, and have the same end state. This is termed final event sequence quantification, discussed in Section 6.8.1, and the results give the final frequency of occurrence. Using the final frequency of occurrence, the event sequences are categorized according to the definition of Category 1 and Category 2 event sequences given in 10 CFR 63.2 (Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (Ref. 2.3.2)). Dose consequences for Category 1 and Category 2 event sequences are subject to the performance objectives of 10 CFR 63.111 (Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (Ref. 2.3.2)), which is performed in Preclosure Consequence Analyses (Ref. 2.2.33). Event sequences with a frequency of occurrence less than one chance in 10,000 of occurring before permanent closure of the repository are designated as beyond Category 2 event sequences and are not analyzed for dose consequences.

Rather than calculate dose consequences for each Category 2 event sequence identified in the categorization process, dose consequences are performed for a set of bounding events that encompass the end states and material at risk for event sequences. Therefore, dose consequences are determined for a representative set of postulated Category 2 event sequences, identified in Table 6.8-1 (Ref. 2.2.33, Table 2 and Section 7). Once event sequence categorization is complete, Category 2 event sequences are cross referenced with the bounding event number given in Table 6.8-1, thus assuring that Category 2 event sequences have been evaluated for dose consequences and compared to the 10 CFR 63.111 (Ref. 2.3.2) performance objectives.

Table 6.8-1. Bounding Category 2 Event Sequences

Bounding Event Number	Affected Waste Form	Description of End State	Material At Risk
2-01	LLWF inventory and HEPA filters	Seismic event resulting in LLWF collapse and failure of HEPA filters and ductwork in other facilities.	HEPA filters LLWF inventory
2-02*	HLW canister in transportation cask	Breach of sealed HLW canisters in a sealed transportation cask	5 HLW canisters
2-03*	HLW canister	Breach of sealed HLW canisters in an unsealed waste package	5 HLW canisters
2-04*	HLW canister	Breach of sealed HLW canister during transfer (one drops onto another)	2 HLW canisters
2-05	Uncanistered commercial SNF in transportation cask	Breach of uncanistered commercial SNF in a sealed truck transportation cask in air	4 PWR or 9 BWR commercial SNF
2-06	Uncanistered commercial SNF in pool	Breach of uncanistered commercial SNF in an unsealed truck transportation cask in pool	4 PWR or 9 BWR commercial SNF
2-07	DPC in air	Breach of a sealed DPC in air	36 PWR or 74 BWR commercial SNF
2-08	DPC in pool	Breach of commercial SNF in unsealed DPC in pool	36 PWR or 74 BWR commercial SNF
2-09	TAD canister in air	Breach of a sealed TAD canister in air within facility	21 PWR or 44 BWR commercial SNF
2-10	TAD canister in pool	Breach of commercial SNF in unsealed TAD canister in pool	21 PWR or 44 BWR commercial SNF
2-11	Uncanistered commercial SNF in pool	Breach of uncanistered commercial SNF assembly in pool (one drops onto another)	2 PWR or 2 BWR commercial SNF
2-12	Uncanistered commercial SNF in pool	Breach of uncanistered commercial SNF in pool	1 PWR or 1 BWR commercial SNF
2-13*	Combustible and noncombustible LLW	Fire involving LLWF inventory	Combustible inventory
2-14	Uncanistered commercial SNF in truck transportation cask	Breach of a sealed truck transportation cask due to a fire	4 PWR or 9 BWR commercial SNF

NOTE: Items marked with an asterisk (*) are not applicable to the WHF.
BWR = boiling water reactor; DAW = dry active waste; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; HLW = high-level radioactive waste; LLWF = Low-Level Waste Facility; PWR = pressurized water reactor; SNF = spent nuclear fuel; LLW = low-level waste; TAD = transportation, aging and disposal canister.

Source: Preclosure Consequence Analyses (Ref. 2.2.33, Table 2)

6.8.1 Event Sequence Grouping and Final Quantification

Event sequences are modeled to represent the GROA operations and SSCs. Accordingly, an event sequence is unique to a given operational activity in a given operational area, which is depicted in an ESD. When more than one initiating event (for example, the drop, collision, or

other structural challenges that could affect the canister) share the same ESD (and therefore elicit the same pivotal events and the same end states), it may be necessary to quantify the event sequence for each initiating event individually because the conditional probabilities of the pivotal events depend on the specific initiating event. In such cases, the frequencies of event sequences that are represented in the same ESD, having the same path through the event tree, and have the same end state are added together, thus comprising an event sequence grouping.

For example, an ESD may show event sequences that could occur during the transfer of a canister from one container to another by the CTM in the WHF. More than one initiating event (for example, the drop, collision, or other structural challenges that could affect the canister) may share the same ESD (and therefore elicit the same pivotal events and the same end states), but give rise to event sequences that are quantified for each initiating event because the conditional probabilities of their pivotal events depend on the specific initiating event.

By contrast, some ESDs indicate a single initiating event. Such initiating events may be composites of several individual initiating events, but because the conditional probabilities of pivotal events and the end states are the same for each of the constituents, the initiators are grouped before the event sequence quantification.

In the PCSA, event sequence grouping is performed for a given waste form configuration at the ESD level. The waste container configurations considered are as follows.

- TAD canister, by itself, in a transportation cask, or in an aging overpack
- DPC, by itself, in a transportation cask, or an aging overpack
- Transportation cask containing bare SNF assemblies
- SNF assembly (handled in the pool of the WHF)
- Low-level waste.

In SAPHIRE (Section 4.2), the grouping of event sequences is carried out using textual instructions, designated as partitioning rules. Partitioning rules gather into a single end state the minimal cut sets from the relevant individual event sequences that need to be grouped together, and further apply a Boolean reduction to ensure that nonminimal cut sets are removed. The event sequence frequencies from this step comprise the final event sequence quantification.

An illustration of the grouping of event sequences is described in the following. The potential structural challenges to a given canister during its transfer by the CTM into the WHF are partitioned among seven different initiating events such as canister drop, collision, drop of a heavy load on the canister, etc. Refer to the IETs in figures A5-22 and A5-23 and the SRET in figure A5-7. The event sequences involving the canister are quantified separately seven times, once for each initiating event. After an initiating event, the event sequences that elicit the same system response and lead to the same end state (i.e., those event sequences that follow the same path on the system-response event tree) are grouped together for purposes of categorization. Thus, the seven individual event sequences initiated by a TAD canister drop, collision, etc, that eventually result in a specific end state, for example a filtered (i.e., mitigated) radionuclide release, are grouped together for the purposes of categorization as a single aggregated event sequence with a unique name termed the “event sequence group ID”. Since there are five different end states that can lead to exposure of personnel to radiation (i.e., result in an end state

other than "OK"), there are five aggregated event sequences involving the TAD canister, each having a unique name. The frequency of each of the five aggregated event sequences represents the sum of frequencies of the seven individual event sequences.

The uncertainties in the grouped event sequences are generated by SAPHIRE as described in Section 6.7. The logic of the grouped event sequences is applied to re-calculate the output probability distribution from the input parameters such as throughput rates, equipment failure rates, passive failure probabilities, and HFEs used to calculate basic event probabilities. These probability distributions are propagated through the fault tree and event sequence logic to quantify the uncertainty in the event sequence quantification.

6.8.2 Event Sequence Categorization

Based on the resultant frequency of occurrence, the event sequences are categorized as Category 1 or Category 2, per the definitions in 10 CFR 63.2 (Ref. 2.3.2) or beyond Category 2. The categorization is done on the basis of the expected number of occurrences of each event sequence during the preclosure period. For purposes of this discussion, the expected number of occurrences of a given event sequence over the preclosure period is represented by the quantity m.

Some event sequences are not directly dependent on the duration of the preclosure period. For example, the expected number of occurrences of TAD canister drops in the WHF over the preclosure period is essentially controlled, among other things, by the number of TAD canisters and the number of lifts of these canisters. The duration of the preclosure period is not directly relevant for this event sequence, but is implicitly built into the operations. In contrast, for other event sequences, time is a direct input. For example, seismically induced event sequences are evaluated over a period of time. In such cases, event sequences are evaluated and categorized for the time during which they are relevant.

Using the parameter m for a given event sequence, categorization is performed using the screening criteria set out in 10 CFR 63.2 (Ref. 2.3.2), as follows:

- Those event sequences that are expected to occur one or more times before permanent closure of the GROA are referred to as Category 1 event sequences (10 CFR 63.2 Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (Ref. 2.3.2)). Thus, a value of m greater than or equal to one means the event sequence is a Category 1 event sequence.

- Other event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences (10 CFR 63.2 (Ref. 2.3.2)). Thus, a value of m less than one but greater than or equal to 10^{-4}, means the event sequence is a Category 2 event sequence.

- A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to m. The probability, P, that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution, $P = 1 - \exp(-m)$ (*Handbook of Parameter Estimation for Probabilistic Risk Assessment*, NUREG/CR-6823 (Ref. 2.2.10, p. A-3)). A value of P greater than or equal to 10^{-4} implies the value of m is greater than or equal to $-\ln(1 - P) = -\ln(1 - 10^{-4})$, which is approximately equal to 10^{-4}. Thus, a value of m greater than or equal to 10^{-4}, but less than one, implies the corresponding event sequence is a Category 2 event sequence.

- Event sequences that have a value of *m* less than 10^{-4} are designated as beyond Category 2.

An uncertainty analysis is performed on *m* to determine the main characteristics of its associated probability distribution, specifically the mean, 50th percentile (i.e., the median), and the standard deviation. The uncertainty analysis is performed in SAPHIRE, using Monte Carlo with 10,000 samples as described in Section 4.3.6.2.

The calculations carried out to quantify an event sequence are performed using the full precision of the individual probability estimates that are used in the event sequence. However, the categorization of event sequences is based upon the expected number of occurrences over the preclosure period with one significant digit.

6.8.3 Final Event Sequence Quantification Summary

Initially, the results of the SAPHIRE event sequence gathering and quantification process are reported in a single table of all event sequences for the WHF (Attachment G, Table G-2). Following the final categorization, the event sequences for the respective Category 2 (see Table 6.8-3) and beyond Category 2 (Attachment G, Table G-3) are tabulated separately. There are no Category 1 (Table 6.8-2) events for the WHF. As desired, other sorting may be performed. For example, event sequences that have end states important to criticality are tabulated separately (Attachment G, Table G-4).The format of the table headings and content are the same for each table as follows:

1. Event sequence group ID –assigned during the grouping process in SAPHIRE.

2. End state – taken from the event tree.

3. Event sequence description – narrative to describe the initiating event(s) and pivotal events that are involved.

4. Material at risk – describes the quantity and type of waste form involved.

5. Mean event sequence frequency (number of occurrences over the preclosure period).

6. Median event sequence frequency (number of occurrences over the preclosure period).

7. Standard deviation of the event sequence frequency (number of occurrences over the preclosure period).

8. Event sequence category – declaration of Category 1, Category 2, or Beyond Category 2.

9. Basis for categorization (e.g., categorization by mean frequency, or from sensitivity study for mean frequencies near a threshold as described in Section 4.3.6.2).

10. Consequence analysis – cross-reference to the bounding event number in the dose consequence analysis (Table 6.8-1) (Ref. 2.2.33, Table 2 and Section 7).

Table 6.8-2. Category 1 Final Event Sequences Summary

Event Sequence Group ID	End State	Description	Material-At-Risk	Mean	Median	Std Dev	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis
None									

Source: Original

Table 6.8-3. Category 2 Final Event Sequences Summary

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD29-DPC-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during operations involving a DPC (transportation cask preparation, transfer by CTM, DPC cutting). In this sequence there are no pivotal events.	1 DPC	3.E-01	3.E-01	2.E-01	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A[2]
ESD22-FUEL-SEQP-GRRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to SNF assemblies, during fuel transfer activities, resulting in an unfiltered radionuclide release in the pool. In this sequence an adequate boron concentration is maintained. This sequence occurs inside the pool.	2 SNF assemblies	3.E-01	3.E-01	2.E-01	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	2-11
ESD31-TAD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a TAD canister inside an STC, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence the canister remains intact, and the shielding fails.	1 TAD canister	1.E-01	1.E-01	4.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD16-CSNF-SEQ1-RRF	Filtered radionuclide release	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during preparation activities (sampling, gas cooling, water filling), resulting in a filtered radionuclide release. In this sequence the confinement boundary remains intact, and no condition important to criticality occurs.	1 transportation cask with uncanistered SNF assemblies	1.E-01	5.E-02	2.E-01	Category 2	Mean of distribution for number of occurrences of event sequence	2-05
ESD29-TAD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during operations involving a TAD canister (assembly and closure, transfer by CTM). In this sequence there are no pivotal events.	1 TAD canister	9.E-02	5.E-02	2.E-01	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]
ESD31-CSNF-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a transportation cask with uncanistered SNF assemblies, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence the transportation cask containment function remains intact, and the shielding fails.	1 transportation cask with uncanistered SNF assemblies	7.E-02	7.E-02	2.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD30-FUEL-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during pool operations (fuel assembly lifted too high). In this sequence there are no pivotal events.	1 SNF assembly	5.E-02	4.E-02	3.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]
ESD31-DPC-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a DPC inside a transportation cask or an STC, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence the canister remains intact, and the shielding fails.	1 DPC	5.E-02	4.E-02	2.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]
ESD30-DPC-SEQ2-DEL	Direct exposure	This event sequence represents a direct exposure during pool operations (splash of pool water). In this sequence there are no pivotal events.	liquid LLW	2.E-02	2.E-03	1.E-01	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]
ESD17-DPC-SEQ1-RRF	Filtered radionuclide release	This event sequence represents a structural challenge to a DPC, during preparation activities (sampling, gas cooling, water filling), resulting in a filtered radionuclide release. In this sequence the confinement boundary remains intact, and no condition important to criticality occurs.	1 DPC	9.E-03	5.E-03	2.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	2-07

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD18-DPC-SEQ1-RRF	Filtered radionuclide release	This event sequence represents a structural challenge to a DPC, during DPC cutting activities, resulting in a filtered radionuclide release. In this sequence the confinement boundary remains intact, and a moderator is excluded from entering the canister.	1 DPC	9.E-03	8.E-03	6.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-07
ESD31-CSNF-SEQ5-RRU	Unfiltered radionuclide release	This event sequence represents a thermal challenge to a transportation cask with uncanistered SNF assemblies, due to a fire, resulting in an unfiltered radionuclide release. In this sequence the transportation cask fails, the confinement boundary fails, and a moderator is excluded from entering the cask.	1 transportation cask with uncanistered SNF assemblies	3.E-03	3.E-03	1.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-14
ESD27-TAD-SEQ1-RRF	Filtered radionuclide release	This event sequence represents a structural challenge to a TAD canister, during TAD canister drying and inerting activities, resulting in a filtered radionuclide release. In this sequence the confinement boundary remains intact, and a moderator is excluded from entering the canister.	1 TAD canister	2.E-03	3.E-04	6.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-09

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD20-CSNF-SEQ5P-GRRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during transfer to pool, resulting in an unfiltered radionuclide release. In this sequence the transportation cask fails, and an adequate boron concentration is maintained. This sequence occurs inside the pool.	1 transportation cask with uncanistered SNF assemblies	7.E-04	3.E-04	2.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-06
ESD31-CSNF-SEQ3-RRF	Filtered radionuclide release	This event sequence represents a thermal challenge to a transportation cask with uncanistered SNF assemblies, due to a localized fire, resulting in a filtered radionuclide release. In this sequence the transportation cask fails, the confinement boundary remains intact, and a moderator is excluded from entering the cask.	1 transportation cask with uncanistered SNF assemblies	6.E-04	5.E-04	3.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	2-14

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD24-TAD-SEQ6P-GRRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a TAD canister inside an STC, during transfer from pool to closure station, resulting in an unfiltered radionuclide release. In this sequence the STC fails, and an adequate boron concentration is maintained. This sequence occurs inside the pool.	1 TAD canister	5.E-04	2.E-04	1.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-10
ESD21-CSNF-SEQ2P-GRRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during transfer to pool floor, resulting in an unfiltered radionuclide release. In this sequence the transportation cask fails, and an adequate boron concentration is maintained. This sequence occurs inside the pool.	1 transportation cask with uncanistered SNF assemblies	2.E-04	1.E-04	3.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	2-06

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD11-TAD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a structural challenge to a TAD canister inside an aging overpack, during export activities, resulting in a direct exposure from loss of shielding. In this sequence the canister remains intact, and the shielding fails.	1 TAD canister	1.E-04	9.E-05	2.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	N/A[2]
ESD16-CSNF-SEQ3-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during preparation activities (sampling, gas cooling, water filling), resulting in an unfiltered radionuclide release. In this sequence the confinement boundary fails, and no condition important to criticality occurs.	1 transportation cask with uncanistered SNF assemblies	1.E-04	4.E-05	3.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	2-14
ESD21-TAD-SEQ2P-GRRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a TAD canister inside an STC, during transfer from pool floor, resulting in an unfiltered radionuclide release. In this sequence the STC fails, and an adequate boron concentration is maintained. This sequence occurs inside the pool.	1 TAD canister	7.E-05	4.E-05	8.E-05	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Recategorization to higher category by alternative distribution	2-10

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD20-CSNF-SEQ2-DED	Direct exposure, degradation of shielding	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during transfer to pool, resulting in a direct exposure from degradation of shielding. In this sequence the transportation cask containment function remains intact, and the shielding fails. This sequence occurs outside the pool.	1 transportation cask with uncanistered SNF assemblies	7.E-05	4.E-05	8.E-05	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Recategorization to higher category by alternative distribution	N/A[2]

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID	End State	Description	Material-At-Risk[3]	Mean[4]	Median[4]	Std Dev[4]	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis[1]
ESD20-CSNF-SEQ3-RRF	Filtered radionuclide release	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during transfer to pool, resulting in a filtered radionuclide release. In this sequence the transportation cask fails, the confinement boundary remains intact, and a moderator is excluded from entering the cask. This sequence occurs outside the pool.	1 transportation cask with uncanistered SNF assemblies	7.E-05	4.E-05	8.E-05	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Recategorization to higher category by alternative distribution	2-05

NOTES: [1] The bounding event number provided in this column identifies the bounding Category 2 event sequence identified in Table 6.8-1 from Preclosure Consequence Analyses (Ref. 2.2.33, Table 2) that results in dose consequences that bound the event sequence under consideration.
[2] Because of the great distances to the locations of the offsite receptors, doses to members of the public from direct radiation after a Category 2 event sequence are reduced by more than 13 orders of magnitude to insignificant levels (GROA External Dose Rate Calculation (Ref. 2.2.19).
[3] The material at risk is, as relevant, based upon the nominal capacity of the waste form container involved in the event sequence under consideration, or accounts for the specific operation covered by the event sequence.
[4] The mean, median, and standard deviation displayed are for the number of occurrences, over the preclosure period, of the event sequence under consideration.
CTM = canister transfer machine; CTT = cask transfer trolley; DOE = U.S. Department of Energy; DPC = dual-purpose canister; WPTT = waste package transport trolley.

Source: Original

6.9 IMPORTANTTO SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS AND PROCEDURAL SAFETY CONTROL REQUIREMENTS

The results of the PCSA are used to define design bases for repository SSCs to prevent or mitigate event sequences that could lead to the release of radioactive material and/or result in radiological exposure of workers or the public. Potential releases of radioactive material are minimized to ensure resulting worker and public exposures to radiation are below the limits established by 10 CFR 63.111 (Ref. 2.3.2). This strategy requires using prevention features in the repository design wherever reasonable. This strategy is implemented by performing the PCSA as an integral part of the design process in a manner consistent with a performance-based, risk-informed philosophy. This integral design approach ensures the ITS design features and operational controls are selected in a manner that ensures safety while minimizing design and operational complexity through the use of proven technology. Using this strategy, design rules are developed to provide guidance on the safety classification of SSCs. The following information is developed in order to implement this strategy:

- Essential safety functions needed to ensure worker and public safety
- SSCs relied upon to ensure essential safety functions
- Design criteria that will ensure that the essential safety functions will be performed with a high degree of reliability and margin of safety
- Administrative and procedural safety controls that, in conjunction with the repository design ensure operations are conducted within the limits of the PCSAs.

Section 6.9.1 identifies ITS SSCs and Section 6.9.2 identifies the procedural safety controls.

6.9.1 Important to Safety Structures, Systems, and Components

Table 6.9-1 contains the nuclear safety design bases for the WHF ITS SSCs. The first three columns identify the ITS system or facility, subsystem and component. The fourth column identifies the safety function relied upon in the event sequence analysis. The fifth column provides the characteristics of the safety function (i.e. controlling parameter or value) that is demonstrated to occur or exist in the design. The sixth column provides an event sequence in which the safety function and the characteristic is relied upon. The seventh column provides the source, usually a fault tree, for the controlling parameter or value.

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Aging	Aging Handling/ Cask Transfer	Site Transporter (170-HAT0-MEQ-00001)	Protect against[c] spurious movement	1. The mean probability of spurious movement of the site transporter while the canister is being lifted or lowered shall be less than 1×10^{-9} per transfer.[e]	WHF-ESD13-TAD (Seq. 6-3)	050-9-ST-SPURMOVE
			Limit Speed	2. The speed of the site transporter shall be limited to 2.5 mi/hr.	WHF-ESD03-AODPC (Seq. 3-5)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7.
			Preclude a cask breach due to explosion	3. The site transporter fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis	See Table 6.0-2
			Reduce severity of a drop	4. The site transporter shall preclude a vertical dropping of an aging overpack from a height greater than 3 ft measured from the equipment base.	WHF-ESD03-AODPC (Seq. 2-3)	This parameter limits the conditional probability of an aging overpack breach given a drop to the appropriate value from Table 6.3-7.
		Cask Tractor (for use with the Cask Transfer Trailer) (170-HAT0-HEQ-00001)	Limit Speed	5. The speed of the cask tractor shall be limited to 2.5 mi/hr.	WHF-ESD04-DPC (Seq. 3-4)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7.

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Preclude a cask breach due to explosion	6. The cask tractor fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis	See Table 6.0-2
		Cask Transfer Trailer (for use with Transportation Casks and Horizontal Shielded Transfer Casks (HSTCs) (PWR DPC: [170-HAT0-TRLY-00001]) (BWR DPC: [170-HAT0-TRLY-00002])	Preclude a cask breach due to explosion	7. The cask transfer trailer fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis	See Table 6.0-2
			Reduce severity of a drop	8. The cask transfer trailer shall preclude dropping a cask from a height greater than 6 feet measured from the equipment base.	WHF-ESD04-DPC (Seq. 2-4)	See Table 6.0-2
			Preclude puncture of a cask	9. The cask transfer trailer shall preclude puncture of a cask due to collision.	Initiating event does not require further analysis	See Table 6.0-2
	Aging Handling/ Aging Overpack	Aging Overpack (TAD: [170-HAC0-ENCL-00003]) (Vertical DPC: [170-HAC0-ENCL-00002])	Protect against[c] direct exposure to personnel	10. The mean conditional probability of loss of shielding of the aging overpack resulting from an impact or collision shall be less than or equal to 1×10^{-5} per impact.	WHF-ESD03-AODPC (Seq. 3-2)	AO-SHIELD-IMPACT

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				11. The mean conditional probability of loss of shielding of the aging overpack resulting from a drop shall be less than or equal to 5×10^{-6} per drop.	WHF-ESD03-TAD (Seq. 2-2)	AO-SHIELD-DROP
Cask/Canister Process System	Cask Cooling	Cask/DPC Overpressure Protection Features	Protect against[c] cask failure due to overpressure	12. The mean probability of an overpressure of a cask or cooling system line during the cask cooling operation shall be less than or equal to 8×10^{-6} per cask.	WHF-ESD16-CSNF (Seq. 4-1)	OVERPRESSURIZATION
DOE and Commercial Waste Package System)	Canistered Spent Nuclear Fuel	Dual-Purpose Canister (DPC) (Analyzed as a Representative Canister)	Provide containment	13. The mean conditional probability of breach of a canister resulting from a drop of the canister shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD13-DPC (Seq. 2-3)	CANISTER-DROP
				14. The mean conditional probability of breach of a canister resulting from a drop of a load onto the canister shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD13-DPC (Seq. 5-3)	CANISTER-DROP
				15. The mean conditional probability of breach of a canister resulting from a side impact or collision shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD13-DPC (Seq. 4-3)	CANISTER-IMPACT

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
DOE and Commercial Waste Package System (continued)	Canistered Spent Nuclear Fuel (continued)	Dual-Purpose Canister (Analyzed as a Representative Canister) (continued)	Provide containment (continued)	16. The mean conditional probability of breach of a canister contained within a cask resulting from the spectrum of fires shall be less than or equal to 2×10^{-6} per fire event.	WHF-ESD31-DPC (Seq. 7-3)	CANISTER-FIRE
				17. The mean conditional probability of breach of a canister contained within an aging overpack resulting from the spectrum of fires shall be less than or equal to 1×10^{-6} per fire event.	WHF-ESD31-TAD (Seq. 4-3)	
				18. The mean conditional probability of breach of a canister located within the CTM shield bell resulting from the spectrum of fires shall be less than or equal to 1×10^{-4} per fire event.	WHF-ESD31-DPC (Seq. 5-3)	CANISTER-FIRE-CTM
		Transportation, Aging, and Disposal (TAD) Canister (Analyzed as a Representative Canister)	Provide containment	19. The mean conditional probability of breach of a canister resulting from a drop of the canister shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD13-TAD (Seq. 2-3)	CANISTER-DROP
				20. The mean conditional probability of breach of a canister resulting from a drop of a load onto the canister shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD13-TAD (Seq. 5-3)	CANISTER-DROP
				21. The mean conditional probability of breach of a canister resulting from a side impact or collision shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD13-TAD (Seq. 4-3)	CANISTER-IMPACT

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
DOE and Commercial Waste Package System (continued)	Canistered Spent Nuclear Fuel (continued)	TAD Canister (Analyzed as a Representative Canister) (continued)	Provide containment (continued)	22. The mean conditional probability of breach of a canister contained within a cask resulting from the spectrum of fires shall be less than or equal to 2×10^{-6} per fire event.	WHF-ESD31-TAD (Seq. 6-3)	CANISTER-FIRE
				23. The mean conditional probability of breach of a canister located within the aging overpack resulting from the spectrum of fires shall be less than or equal to 1×10^{-6} per fire event.	WHF-ESD31-TAD (Seq. 4-3)	CANISTER-FIRE-AO
				24. The mean conditional probability of breach of a canister located within the CTM shield bell resulting from the spectrum of fires shall be less than or equal to 1×10^{-4} per fire event.	WHF-ESD31-TAD (Seq. 5-3)	CANISTER-FIRE-CTM
Electrical Power System	ITS Power	ITS Distribution (Feeders Up to and including ITS Loads, ITS Uninterruptible Power Supply Power)	Provide electrical power to ITS Surface Nuclear Confinement HVAC Systems	25. The mean conditional probability for ITS electrical power distribution failure shall be less than or equal to 8×10^{-3} over a period of 720 hours following the breach of a cask-canister system.	WHF-ESD13-TAD (Seq. 2-5)	NSDB-ITS-DISTRIBUTION

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				26. The mean conditional probability for ITS electrical power distribution failure shall be less than or equal to 5×10^{-4} over a period of 24 hours following a cask overpressure or a cooling system line break.	WHF-ESD16-CSNF (Seq. 4-3)	NSDB-ITS-DISTRIBUTION-24
		ITS diesel generators (including ITS diesel generator fuel oil system, ITS diesel generator air start system, ITS diesel generator jacket water cooling system, ITS diesel generator lubricating oil system, ITS diesel generator air intake and exhaust system.)	Provide electrical power to ITS Surface Nuclear Confinement HVAC Systems	27. The mean conditional probability for ITS electrical power failure, given the loss of offsite power, shall be less than or equal to 3×10^{-1} over a period of 720 hours following a radionuclide release.	WHF-ESD13-TAD (Seq. 2-5)	ITS-EP-FAILURE

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Provide electrical power to ITS Surface Nuclear Confinement HVAC Systems	28. The mean conditional probability for ITS electrical power failure, given the loss of offsite power, shall be less than or equal to 5×10^{-2} over a period of 24 hours following a cask overpressure or a cooling system line break.	WHF-ESD16-CSNF (Seq. 4-3)	ITS-EP-FAILURE-24HR
Fire Protection System	Fire Suppression	Preaction valves, sprinkler heads, and system actuation panels associated with double-interlock preaction suppression systems that protect areas where there is a potential for canister breach	Maintain moderator control	29. The mean probability of inadvertent introduction of fire suppression water into a canister shall be less than or equal to 6×10^{-7} over a 720-hour period following a radionuclide release.	WHF-ESD02-DPC (Seq. 3-5)	050-WATER-FIRE-SUPPRESS
Fire Protection System) (continued)	Fire Detection	Fire Detection System for the ITS preaction valves with associated detectors and control box	Maintain moderator control	30. The mean probability of inadvertent introduction of fire suppression water into a canister shall be less than or equal to 6×10^{-7} over a 720-hour period following a radionuclide release.	WHF-ESD02-DPC (Seq. 3-5)	050-WATER-FIRE-SUPPRESS

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System	Cask Handling	Transportation Cask (Analyzed as a Representative Cask) Shielded Transfer Cask (STC) (Analyzed as a Representative Cask) (TAD: 050-HT00-HEQ-00001) (DPC: [050-HT00-HEQ-00002)	Provide containment	31. The mean conditional probability of breach of a canister in a sealed cask resulting from a drop shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD07-DPC (Seq. 5-4)	CASK-DROP
				32. The mean conditional probability of breach of a sealed cask containing uncanistered SNF resulting from a drop shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD05-CSNF (Seq. 5-3)	CASK-DROP
				33. The mean conditional probability of breach of a canister in a sealed cask resulting from a drop of a load onto the cask shall be less than or equal to 1×10^{-5} per drop	WHF-ESD07-DPC (Seq. 4-4)	CASK-DROP
				34. The mean conditional probability of breach of a sealed cask containing uncanistered SNF resulting from a drop of a load onto the cask shall be less than or equal to 1×10^{-5} per drop	WHF-ESD05-CSNF (Seq. 4-3)	CASK-DROP

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				35. The mean conditional probability of breach of a canister in a sealed cask resulting from a side impact or collision shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD07-DPC (Seq. 3-4)	CASK-IMPACT
				36. The mean conditional probability of breach of a sealed cask containing uncanistered SNF resulting from a side impact or collision shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD05-CSNF (Seq. 3-3)	CASK-IMPACT
				37. The mean conditional probability of breach of a sealed cask containing uncanistered SNF resulting from the spectrum of fires shall be less than or equal to 5×10^{-2} per fire event.	WHF-ESD31-CSNF (Seq. 4-5)	BARE-FUEL-FIRE
			Protect against[c] direct exposure to personnel	38. The mean conditional probability of loss of cask gamma shielding resulting from a drop of a cask shall be less than or equal to 1×10^{-5} per drop.	WHF-ESD05-CSNF (Seq. 5-2)	SHIELD-CASK-DROP
				39. The mean conditional probability of loss of cask gamma shielding resulting from a collision or side impact to a cask shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD05-CSNF (Seq. 3-2)	SHIELD-CASK-IMPACT
				40. The mean conditional probability of loss of cask gamma shielding resulting from a drop of a load onto the cask shall be less than or equal to 1×10^{-8} per impact.	WHF-ESD05-CSNF (Seq. 4-2)	SHIELD-CASK-DROP

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
		Site Prime Mover	Limit Speed	41. The speed of the site prime mover shall be limited to 9 mi/hr.	WHF-ESD01-CSNF (Seq. 3-3)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7.
			Preclude fuel tank explosion	42. The fuel tank of a site prime mover shall preclude fuel tank explosions.	Initiating event does not require further analysis	See Table 6.0-2
Mechanical Handling System (continued)	Cask Handling (continued)	Cask Handling Yoke (050-HM00-BEAM-00001)	Protect against[c] drop	43. The cask handling yoke is an integral part of the load-bearing path. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements
		Pool Cask Handling Yoke (050-HM00-BEAM-00002)	Protect against[c] drop	44. The pool cask handling yoke is an integral part of the load-bearing path. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements
		Cask Handling Crane; 200-ton (050-HM00-CRN-00001)	Protect against[c] drop	45. The mean probability of dropping a loaded cask from a less than the two-block height resulting from the failure of a piece of equipment within the load path supporting the cask shall be less than or equal to 3×10^{-5} per transfer with the cask yoke or 1×10^{-4} per transfer with a sling.	WHF-ESD20-CSNF (Seq. 08-3) WHF-ESD06-TTC (Seq. 2-4)	050-CHC-CSKDROP-CRN-DRP 050-CHC-SLNGDRP-CRS-DRP
			Protect against[c] drop	46. The mean probability of dropping a loaded cask from a two-block height resulting from the failure of a piece of equipment within the load-bearing path shall be less than or equal to 4×10^{-7} per transfer.	WHF-ESD20-CSNF (Seq. 09-3)	050-CHC-TWOBLCK-CRN-TBK

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Limit drop height	47. The two-block drop height shall not exceed 30 feet from the bottom of the shortest cask to the floor.	WHF-ESD20-CSNF (Seq. 09-3)	This parameter limits the conditional probability of cask breach given a two-block drop to the appropriate value from Table 6.3-7.
			Protect against[c] drop of a load onto a cask	48. The mean probability of dropping a load onto a loaded cask or its contents shall be less than or equal to 3×10^{-5} per cask handled.	WHF-ESD05-CSNF (Seq. 4-3)	050-5-200T-CRANE-DROPON
			Maintain moderator control	49. The mean probability of inadvertent introduction of an oil moderator into a canister shall be less than or equal to 9×10^{-5} over a 720-hour period following a radionuclide release.	WHF-ESD05-CSNF (Seq. 4-4)	050-OIL-MODERATOR
			Limit Speed	50. The speed limit of the trolley and bridge shall be limited to 20 ft/min.	WHF-ESD05-CSNF (Seq. 3-3)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7. (2.5 mi/hr, from Table 6.3-7, equals 220 ft/min, which bounds 20 ft/min.)
Mechanical Handling System) (continued)	Cask Handling (continued)	Pool Yoke Lift Adapter (050-HM00-TOOL-00002)	Protect against[c] drop of a cask	51. The pool yoke lift adapter is an integral part of the load-bearing path. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
		Cask Transfer Trolley (CTT) and Pedestals (Trolley: 050-HM00-TRLY-00001) (Pedestals: 050-HM00-PED-00001-5)	Limit Speed	52. The speed of the CTT shall be limited to 2.5 mi/hr.	WHF-ESD12-DPC (Seq. 10)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7.
			Protect against[c] spurious movement	53. The mean probability of spurious movement of the CTT while a canister is being lifted by the CTM shall be less than or equal to 1×10^{-9} per transfer.[e]	WHF-ESD13-TAD (Seq. 6-3)	050-9-CTT-SPUR-MOVE
		Horizontal Lifting Beam (200-HMC0-BEAM-00001) (shared with RF)	Protect against[c] drop	54. The horizontal lifting beam is an integral part of the load-bearing path. See Cask Handling Crane requirements	See Cask Handling Crane requirements	
	Cask Handling/Cask Preparation	Truck Cask Lid Adapters (050-HMH0-HEQ-00010-11) Rail Cask Lid Adapters (050-HMH0-HEQ-00012-13)	Protect against[c] drop	55. The truck and rail cask lid adapters are an integral part of the load-bearing path. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements
	Cask Handling/Cask Preparation	Auxiliary Pool Crane; 10 ton (050-HMH0-CRN-00001)	Protect against[c] a drop of a load onto canister	56. The mean probability of drop of a load onto a canister shall be less than or equal to 3×10^{-5} per lift.	WHF-ESD21-CSNF (Seq. 5-2)	050-PHC-OBJDROP-CRN-DRP

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
		Preparation Station Jib Cranes (1 and 2) (050-HMH0-CRN-00002, 3)	Protect against[c] a drop of a load onto canister	57. The mean probability of drop of a load onto a canister shall be less than or equal to 3×10^{-5} per lift.	WHF-ESD08-CSNF (Seq. 3-3)	050-JIBCRANE-JIB-DRP
		Lid Lifting Grapples (050-HMH0-HEQ-00001-4, 6) Truck Cask Lid Lifting Grapples (050-HMH0-HEQ-00007-9)	Protect against[c] drop of a load onto a canister	58. The lid lift grapple is an integral part of the load-bearing path. See Preparation Station Jib Crane requirements.	See Preparation Station Jib Cranes requirements	See Preparation Station Jib Cranes requirements
		DPC Lid Adapter (050-HMH0-HEQ-00014)	Protect against[c] drop of a DPC	59. The DPC lid adapter is an integral part of the load-bearing path. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements	See Canister Transfer Machine requirements
		Long Reach Grapple Adapter (050-HMH0-TOOL-00001-2)	Protect against[c] drop of a load	60. The long reach grapple adapter is an integral part of the load-bearing path. See Auxiliary Pool Crane requirements.	See Auxiliary Pool Crane requirements	See Auxiliary Pool Crane requirements
	Waste Transfer/Fuel Assembly Transfer	Spent Fuel Transfer Machine (SFTM) (050-HTF0-FHM-00001)	Protect against[c] drop of an SNF assembly	61. The mean probability of dropping an SNF assembly due to a failure of a piece of equipment within the load path shall be less than or equal to 5×10^{-6} per assembly transfer.	WHF-ESD22-FUEL (Seq. 3-1)	050-SFTM-FUELDRP-SFT-DRP
			Protect against[c] lifting an SNF assembly above the safe limit for workers	62. The mean probability of lifting an SNF assembly such that 10 CFR 63.111(a) limits are exceeded shall be less than or equal to 7×10^{-7} per assembly transfer.	WHF-ESD30-FUEL (Seq. 2)	050-SFTM-TOOHIGH-SFT-RTH

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System (continued)	Waste Transfer/Fuel Assembly Transfer (continued)	PWR/ BWR Lifting Grapples (050-HTF0-HEQ-00001) BWR Lifting Grapples (050-HTF0-HEQ-00002)	Protect against[c] drop of an SNF assembly	63. The PWR/BWR grapples are an integral part of the load-bearing path. See Spent Fuel Transfer Machine requirements.	See Spent Fuel Transfer Machine requirements	See Spent Fuel Transfer Machine requirements
Mechanical Handling System (continued)	Waste Transfer/ Canister Transfer	Canister Transfer Machine (050-HTC0-FHM-00001)	Protect against[c] drop	64. The mean probability of dropping a canister from below the two-block height due to the failure of a piece of equipment within the load-bearing path shall be less than or equal to 1×10^{-5} per transfer.	WHF-ESD13-TAD (Seq. 2-3)	CTM-DROP---ALL-HEIGHTS
			Protect against[c] drop	65. The mean probability of drop of a canister from the two-block height due to the failure of a piece of equipment within the load-bearing path shall be less than or equal to 3×10^{-8} per transfer.	WHF-ESD13-TAD (Seq. 3-3)	CTM-2-BLOCK
			Limit drop height	66. The two-block drop height shall not exceed 45 feet from the bottom of a canister to the cavity floor of the cask or aging overpack.	WHF-ESD13-TAD (Seq. 2-3)	This parameter limits the conditional probability of cask breach given a two-block drop to the appropriate value from Table 6.3-7.
			Protect against[c] drop of a load onto a canister	67. The mean probability of dropping a load onto a canister shall be less than or equal to 1×10^{-5} per transfer.	WHF-ESD13-TAD (Seq. 5-3)	CTM-DROP-ONTO-CASK

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Protect against[c] spurious movement	68. The mean probability of a spurious movement of the CTM while a canister is being lifted or lowered shall be less than or equal to 7×10^{-9} per transfer.	WHF-ESD13-TAD (Seq. 6-3)	CTM-SHEAR
			Limit Speed	69. The speed of the CTM trolley and bridge shall be limited to 20 ft/min.	WHF-ESD13-TAD (Seq. 4-3)	This parameter limits the conditional probability of cask breach given a collision to the appropriate value from Table 6.3-7. (2.5 mi/hr, from Table 6.3-7, equals 220 ft/min, which bounds 20 ft/min.)
			Preclude non-flat bottom drop of a DPC or TAD	70. The CTM shall preclude non-flat-bottom drops of DPCs and TADs.	Initiating event does not require further analysis[b]	Table 6.0-2
			Protect against[c] direct exposure to personnel	71. The mean probability of inadvertent radiation streaming resulting from the inadvertent opening of the CTM slide gate, the inadvertent raising of the CTM shield skirt, or an inadvertent motion of the CTM away from an open port shall be less than or equal to 9×10^{-6} per transfer.	WHF-ESD29-TAD (Seq. 3)	ESD29-EXPOSURE-CTM
			Maintain moderator control	72. The mean probability of inadvertent introduction of an oil moderator into a canister shall be less than or equal to 9×10^{-5} over a 720-hour period following the breach of a canister.	WHF-ESD13-TAD (Seq. 2-4)	050-OIL-MODERATOR
			Preclude canister breach	73. Closure of the CTM slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis	Table 6.0-2

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System (continued)	Waste Transfer/ Canister Transfer (continued)	Canister Transfer Machine Grapples (050-HTC0-HEQ-00001)	Protect against[c] drop	74. The CTM grapple is an integral part of the load-bearing path. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements	See Canister Transfer Machine requirements
	TAD Closure	TAD Closure Jib Crane (050-HC00-CRN-00001)	Protect against[c] drop of a load	75. The mean probability of a drop of a load onto a cask containing a TAD shall be less than or equal to 3×10^{-5} per lift.	WHF-ESD25-TAD (Seq. 2-2)	050-JIBCRANE-JIB-DRP
	Dual-Purpose Canister Cutting	DPC Cutting Jib Crane (050-HD00-CRN-00001)	Protect against[c] drop of a load	76. The mean probability of a drop of a load onto a cask containing a DPC shall be less than or equal to 3×10^{-5} per lift.	WHF-ESD18-DPC (Seq. 2-2)	050-JIBCRANE-JIB-DRP
Surface Nuclear Confinement HVAC System	Surface Nuclear Confinement HVAC	Portions of the surface nuclear confinement HVAC system that exhaust from areas with a potential for a breach	Mitigate the consequences of radionuclide release	77. The mean probability that the HVAC system (including HEPA filtration of exhaust air from the WHF confinement areas) becomes unavailable during a 30-day mission time following a radionuclide release shall be less than or equal to 4×10^{-2}. This parameter does not apply in the case of large fires, which may disable the HVAC system	WHF-ESD13-TAD (Seq. 2-5)	CONFINEMENT
				78. The mean probability that the HVAC system (including HEPA filtration of exhaust air from the WHF confinement areas) becomes unavailable during a 1-day mission time following a radionuclide release from the cask sampling and cooling process shall be less than or equal to 1×10^{-3}.	WHF-ESD16-CSNF (Seq. 4-3)	HVAC-PREP

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
		Portions of the surface nuclear confinement HVAC system that support the cooling of ITS electrical equipment and battery rooms	Support ITS electrical function	79. The mean conditional probability of failure of the portions of the surface nuclear confinement HVAC system that support the cooling of ITS electrical equipment and battery rooms in the WHF shall be less than or equal to 2×10^{-2} per ITS electrical train over a period of 720 hours following a radionuclide release.	WHF-ESD13-TAD (Seq. 2-5)	EP-WHF-COOL-1 and EP-WHF-COOL-2
				80. The mean conditional probability of failure of the portions of the surface nuclear confinement HVAC system that support the cooling of ITS electrical equipment and battery rooms in the WHF shall be less than or equal to 5×10^{-4} per ITS electrical train over a period of 24 hours following a cask overpressure or a cooling system line break.	WHF-ESD13-TAD (Seq. 2-5)	EP-WHF-COOL-1-24 and EP-WHF-COOL-2 - 24
Surface Non-Confinement HVAC System	Surface Non-Confinement HVAC	Portions of the surface non-confinement HVAC system that support the cooling of ITS electrical equipment and battery rooms (EDGF)	Support ITS electrical function	81. The mean conditional probability of failure of the portions of the surface non-confinement HVAC system that support the cooling of ITS electrical equipment and battery rooms in the EDGF shall be less than or equal to 2×10^{-2} per ITS electrical train over a period of 720 hours following a radionuclide release.	WHF-ESD13-TAD (Seq. 2-5)	
Wet Handling Facility	Wet Handling Facility (WHF)	Shield Doors (Including Anchorages)	Protect against[c] direct exposure of personnel	82. Equipment shield doors shall have a mean probability of inadvertent opening of less than or equal to 1×10^{-7} per waste container handled.	WHF-ESD29-TAD (Seq. 3)	050-29-SHLDDR-DIRCT-EXP

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Preclude collapse onto waste containers	83. An equipment shield door falling onto a waste container as a result of impact from a conveyance shall be precluded.	Initiating event does not require further analysis[b]	Table 6.0-2
		Cask Port Slide Gate (050-HTC0-HTCH-00002)	Protect against[c] dropping a canister due to a spurious closure of the slide gate	84. The mean probability of a canister drop resulting from a spurious closure of the slide gate shall be less than or equal to 2×10^{-6} per transfer.	WHF-ESD13-TAD (Seq. 2-3)	GATE-36-109 of ESD13-TAD-DROP
			Protect against[c] direct exposure to personnel	85. The mean probability of occurrence of an inadvertent opening of a slide gate shall be less than or equal to 4×10^{-9} per transfer.	WHF-ESD29-TAD (Seq. 3)	050-29-SLIDE-GATE-DIR-EX
			Preclude canister breach	86. Closure of the slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis	Table 6.0-2
		Overpack Port Slide Gate (050-HTC0-HTCH-00001)	Protect against[c] dropping a canister	87. The mean probability of a canister drop resulting from a spurious closure of the slide gate shall be less than or equal to 2×10^{-6} per transfer.	WHF-ESD13-TAD (Seq. 2-3)	GATE-36-109 of ESD13-TAD-DROP
Wet Handling Facility (continued)	Wet Handling Facility (WHF) (continued)	Overpack Port Slide Gate (050-HTC0-HTCH-00001) (continued)	Protect against[c] direct exposure to personnel	88. The mean probability of occurrence of an inadvertent opening of a slide gate shall be less than or equal to 4×10^{-9} per transfer.	WHF-ESD29-TAD (Seq. 3)	050-29-SLIDE-GATE-DIR-EX

Table 6.9-1. Preclosure Nuclear Safety Design Bases for the WHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable)[d]	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Preclude canister breach	89. Closure of the slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis	Table 6.0-2

NOTES: [a] 'Protect against' in this table means either 'reduce the probability of' or 'reduce the frequency of'.
[b] Extremely low probabilities are reported in this table as 1E-9. Increasing the source probability to 1E-9 does not impact the categorization of event sequences.
[c] Design requirement is applied to reduce the frequency of any event sequence that could result in damage to a waste container to beyond Category 2.
[d] The TAD staging racks are not anticipated to be used to stage TAD canisters. The controlling parameters, sequence number, and source are from the DOE Canister Staging Racks requirement to provide protection in the event a DOE standardized canister is inadvertently placed into a TAD staging rack.
[e] Source value bounds the controlling value.

CTM = canister transfer machine; CTT = cask transfer trolley; DOE = U.S. Department of Energy; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; HVAC = heating, ventilation, and air conditioning; ITS = important to safety; SNF = spent nuclear fuel; SSC = structure, system, or component; TAD = transport, aging and disposal; WHF = Wet Handling Facility

Source: Original

6.9.2 Procedural Safety Controls

PSCs are the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. For this analysis, all PSCs were derived to reduce the initiating event sequence to an acceptable level.

Table 6.9-2 lists the PSCs that are required to support the event sequence analysis and categorization. The event sequence column identifies a representative event sequence that relies upon the PSC.

Table 6.9-2. Summary of Procedural Safety Controls for the WHF Facility

Item	SSC	Procedural Safety Controls	Basis	Representative Event Sequence
1	CTT	The CTT is deflated during loading of cask onto trolley, cask preparation activities, and during canister unloading or loading activities.	This control limits the probability of spurious movement of the CTT and resulting canister impact.	WHF-ESD13-TAD, Seq. 6-3
2	Site Transporter Site Prime Mover Cask Tractor	The ST is turned off during, AO bolting and unbolting, and canister unloading or loading activities. The site prime mover and cask tractor are disconnected or secured to prevent motion before waste handling operations begin.	This control limits the probability of spurious movement of the ST, site prime mover, or cask tractor and resulting collision or tipover.	WHF-ESD13-TAD, Seq. 6-3
3	STC TAD canister/ DPC shield ring	Prior to commencing operations that rely upon the TAD canister/DPC shield ring, the operating crew is to verify that the shield ring is installed.	This control limits the probability of operators receiving a direct exposure due to miscommunication between the operator and the crew regarding status of the shield ring. The crew that depends on the shield ring for its own safety will ensure its placement.	WHF-ESD29-TAD, Seq. 2
4	Transportation Cask STC	Whenever a TAD canister or DPC is being moved in a shielded transfer cask or uncanistered SNF is being moved in a transportation cask, the shielded transfer cask or transportation cask will have a lid held in place with a minimum number of installed fasteners such that the stress on the fasteners is less than yield strength for a drop.	This control limits the probability that a drop or tipover of the STC or transportation cask during movement will result in radiological release or criticality.	WHF-ESD19-DPC, Seq. 11-4

Table 6.9-2. Summary of Procedural Safety Controls for the WHF Facility (Continued)

Item	SSC	Procedural Safety Controls	Basis	Representative Event Sequence
5	Surface Nuclear Confinement HVAC, ITS exhaust subsystem serving ITS confinement areas and ITS subsystems serving ITS electrical and battery rooms	One train of HVAC is required to be operating and the second train is required to be in standby before commencing waste handling operations.	HVAC analysis uses this configuration. This control limits the probability that the HVAC system will fail to start when relied upon to mitigate the consequences of an event sequence.	WHF-ESD13-TAD, Seq. 2-5
6	ITS Diesel Generators	Before commencing waste handling operations, two ITS diesel generators are aligned to start on detection of undervoltage. Following the start of the diesel generators, the operator manages the operation of the ITS diesel generators to ensure continuous operation of a train of the Surface Nuclear Confinement HVAC, ITS exhaust subsystem serving ITS confinement areas and ITS subsystems serving ITS electrical and battery rooms in each of the waste handling facilities.	The PCSA reliability analysis models both ITS diesel generators to start and run 720 hours to support the operation of the Surface Nuclear Confinement HVAC System.	WHF-ESD13-TAD, Seq. 2-5
7	Spent fuel pool	With SNF in the pool, the concentration of soluble boron in the WHF pool and transportation cask/DPC fill water is maintained at a minimum of 2,500 mg/l, with the soluble boron enriched to a minimum of 90 wt% in the B-10 isotope.	This control provides the appropriate initial conditions in the WHF pool to ensure that a critical configuration cannot be created in the pool. For wet operations, the minimum required concentration of 2,500 mg/l of soluble boron (enriched to 90 wt % B^{10}) in the WHF pool is sufficient to compensate for the complete omission of fixed neutron absorbers in the analyzed designs.	WHF-ESD21-CSNF, Seq. 2-3
8	ITS SSCs	The amount of time that a waste form spends in each process area or in a given process operation, including total residence time in a facility, is periodically compared against the average exposure times used in the PCSA. Additionally, component failures per demand and component failures per time period are compared against the PCSA. Significant deviations will be analyzed for risk significance.	PCSA uses residence times and reliability data to calculate the probability of an initiating event. This control ensures that the average exposure times and reliability data are maintained consistent with those analyzed in the PCSA.	Applies to all event sequence and fault tree quantification that uses data from Attachment C. Also applies to fire analysis per Section 4.3 and Attachment E.

Table 6.9-2. Summary of Procedural Safety Controls for the WHF Facility (Continued)

Item	SSC	Procedural Safety Controls	Basis	Representative Event Sequence
9	Cask Preparation Platform	Transportation cask lid bolts are independently verified to have been removed prior to moving the cask from the cask preparation area to the unloading room or pool.	This control prevents the CTM from attempting to remove the cask lid with bolts still in place resulting in failure of the bolts and possible drop of the lid or cask.	WHF-ESD13-TAD, Seq. 2-3
10	CTM Port Slide Gates	At completion of a canister transfer operation, the port slide gates are verified to be closed	While the CTM is being used to perform transfer operations, the Operational Radiation Protection Program provides the necessary controls to ensure that workers are not present with the slide gates open. This control limits the probability of workers receiving a direct exposure by entering the transfer room with the CTM away from a port with a waste form container present and the slide gate open.	WHF-ESD29-TAD, Seq. 3
11	CTM	Prior to lifting or lowering a DPC or TAD canister, the CTM guide sleeve is to be verified to have been lowered.	This control limits the probability that a DPC or TAD canister is not in a vertical orientation during transfer such that any potential drops would be flat bottom drops.	WHF-ESD13-TAD, Seq. 2-3
12	WHF Pool	The height of water above the top of the active portions of commercial SNF assemblies in the WHF pool staging rack(s) and open TAD canisters, DPCs, and casks is maintained at or greater than 23 ft.	This control is to ensure that the pool leak path factors presented in the consequence analysis (Ref. 2.2.20, Section 7) are maintained. Additionally, the water level is credited for preservation of shielding for workers.	WHF-ESD30-FUEL, Seq. 2
13	Cask Preparation Room Equipment Confinement Doors	The cask preparation room equipment confinement door is to be closed when waste handling operations are being conducted with a potential for a drop or collision involving a loaded cask or canister outside the WHF pool.	This control is to ensure that the confinement boundary is intact when there is a potential for an event sequence that could result in radiological releases outside the WHF pool.	WHF-ESD05-CSNF, Seq. 5-5
14	Transportation Cask Vestibule and Pool Room Shield Doors	The outer Transportation Cask Vestibule door is to be closed before the Pool Room Shield Door is opened.	This control is to ensure that the confinement boundary is intact during waste handling operations.	WHF-ESD01-CSNF (Seq. 3-5)

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HVAC = heating, ventilation, and air-conditioning; ITS = important to safety; SNF = spent nuclear fuel; STC = shielded transfer cask; TAD = transportation, aging, and disposal; WHF = Wet Handling Facility.

Source: Original

7. RESULTS AND CONCLUSIONS

This analysis report on the WHF and its predecessor companion report, the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37), are part of the PCSA for the GROA that supports the license application. In combination, these documents identify, evaluate, quantify, and categorize event sequences for the GROA facilities and operations. They are part of a collection of analysis reports that encompass all waste handling activities and facilities of the GROA from initial operations to the end of the preclosure period. Probabilistic risk assessment techniques derived from both nuclear power plant and aerospace methods are used to perform the analyses to comply with the risk-informed aspects of 10 CFR 63.111 and 63.112 (Ref. 2.3.2), and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report* (Ref. 2.2.71). The identification and development of the event sequences is limited to those that might lead to direct radiation exposure of workers or onsite members of the public; radiological releases that may affect the workers or public (onsite and offsite); and nuclear criticality.

The results of the analysis are discussed and presented in the logical progression through Section 6 of this document and are not reiterated here. Instead, only key points are highlighted. For the ungrouped event sequence results and the complete grouped event sequence summaries, electronic files are provided due to the large size of hard copy versions (refer to Attachments G and H). In addition, although the results from the SAPHIRE model are used and presented in Section 6 and Attachment B, the model itself is difficult to completely represent in paper form. Therefore, these outputs are also provided electronically (refer to Attachment H). Table 7-1 describes the results and indicates the location within this analysis for each result provided.

Table 7-1. Key to Results

Result	Description	Cross Reference
Grouping of event sequences	Grouping of event sequences and description of event sequence groups	Table G-2
Quantification of event sequences	Calculation of probability distributions for the numbers of occurrences of internal event sequence groups over the preclosure period	Table G-1
Categorization of event sequences	Assignment of frequency categories Category 1, Category 2, or beyond Category 2 to internal event sequence groups based on mean numbers of occurrences	Table 6.8-2 Table 6.8-3 Table G-3
Designation of SSCs as ITS	Identification of SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1
Statement of nuclear safety design bases	Determination of nuclear safety design bases for SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1
Statement of procedural safety controls	Determination of procedural safety controls that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-2

NOTE: ITS = important to safety; SSCs = structures, systems, and components.

Source: Original

Summary of Event Sequences

The analysis concludes that there are no Category 1 event sequences and 22 Category 2 event sequences. Table 7-2 gives the number of Category 2 event sequences by end state for each waste form.

Table 7-2. Summary of Category 2 Event Sequences

End State	Description	Canister Types				Fuel Assembly	Liquid LLW
		DPC	TAD	TAD or DPC[a]	TC		
DE-SHIELD-DEGRADE	Direct exposure due to degradation of shielding				1		
DE-SHIELD-LOSS	Direct exposure due to loss of shielding	2	3		1	1	1[b]
RR-UNFILTERED	Radionuclide release, unfiltered		2		4	1	
RR-FILTERED	Radionuclide release, filtered	2	1		3		
RR-UNFILTERED-ITC	Radionuclide release, unfiltered, also important to criticality						
RR-FILTERED-ITC	Radionuclide release, filtered, also important to criticality						
ITC	Important to criticality						

NOTES: [a]The event sequences counted here are not specific to canister type.
[b]Splash of pool water
DPC = dual-purpose canister; LLW = low-level radioactive waste; TAD = transportation, aging, and disposal canister; TC = transportation cask.

Source: Original

Summary of Conservatisms

It is noted that the event sequence identification and categorization were conducted with conservatisms built into the analysis and inputs, including, but not limited to, the following:

1. Fire frequency and damage analyses are performed without relying on fire suppression. This increases the calculated frequency of large fires and also increases the duration and peak temperature of fires, thereby significantly increasing the calculated probability of waste container failure.

2. If a fire is calculated to propagate out of the initiating location fire zone, the entire building is considered to be involved in the fire.

3. In the PEFA for thermal and fire scenarios, conservatism is built into the boundary conditions, which consider the fire as occurring next to the waste containers instead of only a fraction of the fire occurrence being near the waste form. A fire closer to the target will lead to a higher target failure probability than a fire located further away. By considering all fires to be next to the waste forms, the thermal PEFA yields higher waste form failure probabilities than is likely.

4. For event sequences in which a cask containing a canister is subjected to a drop, slapdown, or in which a load is dropped onto the cask, the calculated containment failure probability pertains to the canister inside without regard to the integrity of the cask. That is, cask containment is not relied upon to reduce probability of containment failure.

5. The structural PEFA uses a conservative failure probability of 1E-5, whereas the actual PEFA assessment indicates values of less than 1E-8 failure probabilities (Table D1.2-7 of Attachment D). This conservatism provides event sequence quantification results of magnitude higher than what they would be if the actual PEFA assessment values are used.

6. The event sequence development for shielding degradation of transportation casks caused by an impact event, considers all casks as if they contained lead gamma shielding that could slump. However, not all transportation casks received at the GROA are lead casks. Because non-lead casks are not affected by this degraded shielding condition, the introduction of this conservatism increases the event sequence quantification value.

7. The structural analyses for drops and collisions of canisters or casks model a rigid, unyielding surface as the target.

8. The structural analysis for drops of loads onto casks or canisters uses a rigid unyielding object for the dropped load.

9. The probabilities of event sequences involving drops of casks and canisters represent a drop height of up to 30 feet for casks and 40 feet for bare canisters. This is much higher than the normal operational lift height but is applied for all lower drop heights. Lower drop heights would result in less structural challenge to casks and canisters.

10. When a canister is inside a waste package, failure of the waste package is considered to fail containment for drop or other mechanical impact events. That is, the canister is not relied upon to reduce the probability of containment failure in those cases. Fire events calculate the probability of canister failure within the waste package without regard to whether or not the waste package fails.

11. Transportation casks are analyzed without impact limiters even for those event sequences in the WHF which impact limiters would be attached.

12. The speed limitation of crane and conveyances within facilities to 20 ft/min and 2.5 mph, respectively, is set to ensure no breach of casks of canisters. The probability of breach at such speeds is calculated to be less than 1E-08 per impact. Speeds could be considerably larger without changing the categorizations of event sequences.

13. The reliability evaluation of the ITS HVAC system, which provides confinement of radioactive material releases following a breach of a waste container, is based a mission time of 720 hrs (30 days). The use of this mission time in the analysis leads to a requirement that the emergency diesel generators provide power to the HVAC for 720 hours following a release. The analysis does not account for the high likelihood of recovering offsite power within the mission time. Recovery of offsite power would reduce the length of time that the diesel generators would be required to run and would thereby reduce the calculated unavailability of the diesel generators. This conservative consideration leads to a lower ITS HVAC availability than is realistically expected.

14. The human reliability analysis preliminary values used for human failure events are typically one or more orders of magnitude higher than values that are obtained through detailed analysis.

15. The probability of failure associated with the structural analysis of mechanical impact loads to casks and canisters is conservatively based on the maximum effective plastic strain of any brick (i.e., finite element mesh) in the modeled structure rather than on evidence of through-wall cracking.

16. Categorization of event sequences is based on the highest category after application of a conservative adjustment to account for the uncertainty in the calculated uncertainties

17. To preserve flexibility in the conduct of operations, the throughput analysis (Ref. 2.2.26) embeds multiple and bounding waste handling scenarios in the throughput numbers. For example, of about 350 DPCs available for transfer in the WHF, the throughput analysis considers 350 DPCs are transferred from vertical transportation casks, another 350 DPCs are transferred from horizontal transportation casks, and another 350 DPCs are transferred from the horizontal aging modules (HAMs) on the aging pad. Including this conservatism in the analysis yields calculated event sequence frequencies that are higher than is realistically expected.

ATTACHMENT A
EVENT TREES

CONTENTS

Page

FIGURES

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

TABLES

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

A1 INTRODUCTION

This attachment presents event trees that are derived from the ESDs in Attachment F of the *Wet Handling Facility Event Sequence Development Analysis* (Ref. 2.2.37). All initiator event trees and system response event trees are located at the end of this attachment. Refer to Table A5-1 for the figure locations of specific event and response trees. The event trees are presented in Figures A5-2 through A5-52 according to ordering rules of hierarchy in SAPHIRE. The first rule is that event trees are presented in ESD order. For example, the event trees associated with WHF-ESD01 appear first, and those associated with WHF-ESD02 appear after that, and so on. The second rule is that the first initiator event tree associated with the ESD appears first and the system response event trees are placed immediately following the first initiator event tree followed by the remaining initiator event trees for the ESD. For example, the first initiator event tree (WHF-ESD01-CSNF) associated with the first ESD (WHF-ESD01) is the first event tree figure. Then the system response event tree (RESPONSE-TCASK-CSNF) appears, followed by the remaining initiator event trees for the ESD (CSNF-ROLLOVER, ESD01-CSNF-COLL). The same kind of ordering is done for each group in turn.

A2 READER'S GUIDE TO THE EVENT TREE DESCRIPTIONS

The following sections are organized by ESD. The event trees that correspond to each ESD are presented as follows:

1. The event trees for the waste forms covered are briefly described and listed (initiator and system-response event trees or self contained event trees, as applicable).

2. The initiating events are described and listed. The listing is provided as a table that includes the assignments of fault trees or basic events to the initiating events. The assignments are made in SAPHIRE using basic rules or by fault-tree construction. The goal of the initiating event table is to provide a link to the underlying system fault tree (covered in Section 6.2 and Attachment B) or basic event (covered in Section 6.3 and Attachment C). In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the system fault tree or basic event level (covered in Attachment B). Note that the initiating event frequencies are defined on a per-unit-handled basis. Thus, when the initiating event frequencies are multiplied by the number of units handled over the preclosure period, the result is an initiating event frequency over the preclosure period.

3. The system-response event tree that corresponds to the initiator event tree or the system response for a self-contained event tree is covered as follows. Each pivotal event used in an event tree is listed in the event tree description section and summarized in Section A3. Each pivotal event is accompanied by a table that provides a link between the name given to the pivotal event in the event tree and the associated system fault tree or basic event. The goal of the pivotal event table is to provide a link to the underlying system fault tree (covered in Section 6.2) or basic event (covered in Section 6.3). Again, in a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the system fault tree or basic event level.

A3 SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES

A self-contained event tree or a system response event tree may include pivotal events of following types:

CELL-DOOR. This pivotal event represents the success or failure of the shield door to not fail and damage waste forms.

TRANSCASK. This pivotal event represents the success or failure of the transportation cask to contain radioactive material after the impact caused by the initiating event. The failure of this pivotal event leads to loss of the cask's containment function. The failure probability for this pivotal event is determined by PEFA, and is given in Table 6.3-2 in Section 6.3.2. In accordance with a simplifying approximation, the same failure probability is used for all casks for the various initiating events.

CANISTER. This pivotal event represents the success or failure of the canister to contain radioactive material after the impact caused by the initiating event. Failure of a containment pivotal event means that a release could occur if the canister containment barrier is breached (along with the cask or waste-package containment, as applicable). In accordance with a simplifying approximation, the conditional probability of canister breach given cask breach is taken to be 1.

SHIELDING. Failure of a shielding pivotal event means that a direct exposure could occur. Casks, some canisters, the cask transfer machine shield bell, and the aging overpack include integral shields that could be pierced or degraded in some impact events. In addition, a breach of a container's seal can also result in a loss of shielding. Thus, this pivotal event represents the success or failure of the shielding function of the cask, canister, or aging overpack after the impact caused by the initiating event. Failure of shielding in these instances refers to an unspecified degree of shielding degradation due to the impact. Failure probabilites are given in Table 6.3-3 in Section 6.3.2.2.

CONFINEMENT. This pivotal event represents the success or failure of the HVAC system in continuing to provide high-efficiency particulate air (HEPA) filtration (radiological confinement) after the initiating event. Success of the pivotal event requires the facility structural integrity as well as the functioning of equipment associated with the HVAC system. Failure results in a potential airborne release that is not mitigated by the HEPA filtration system.

MODERATOR. This pivotal event represents the conditional probability of introducing liquid moderator (water or crane gearbox lubricating oil) into a breached canister, given that a breached canister is present. The conditional probability of failure (introduction of liquid moderator) is the same for all waste forms and all initiating events. Failure of a moderator pivotal event results in an end state that may be susceptible to nuclear criticality. The opportunity for criticality also depends on other pivotal events (e.g., loss of containment which may allow liquid moderator into a breached canister) and physical properties of the waste form.

BORON. This pivotal event represents maintaining adequate Boron concentration in the pool to prevent criticality in the event that spent fuel assemblies are exposed to pool water and reach a critical configuration because of a drop of either a cask or spent fuel assembly drop. If adequate

Boron concentration is not achieved, criticality could occur and an unfiltered gaseous radionuclide release could occur

A4 EVENT TREE DESCRIPTIONS

A4.1 EVENT TREES FOR WHF-ESD01-CSNF

ESD WHF-ESD01-CSNF delineates the event sequences that arise after a structural challenge to a transportation cask with commercial SNF as it is moved from the receipt area into the preparation area. This includes event sequences that arise after the outer vestibule door is closed during movement of a transportation cask into the Cask Preparation Area.

WHF-ESD01-CSNF covers event sequences associated with receipt of a truck trailer. This ESD includes transportation casks containing commercial SNF.

Although the initiator event trees transfer to the same response tree (see Table A4.1-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.1-1. Summary of Event Trees for WHF-ESD01-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD01-CSNF Response: RESPONSE-TCASK-CSNF	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.1.1 Initiating Events for WHF-ESD01-CSNF

The following initiating events are associated with WHF-ESD01-CSNF:

- Truck trailer rollover
- Truck trailer collision.

The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.1-2.

Truck Trailer Rollover. This initiating event accounts for the potential impact to the transportation cask on the truck trailer due to a rollover. The rollover event is modeled as a fault tree and is listed in Section 6.2.2.1.

Truck Trailer Collision.

This initiating event accounts for the potential impact to the transportation cask on the truck trailer due to a collision. The collision event is modeled as a fault tree and is listed in Section 6.2.2.1

Table A4.1-2. Initiating Event Assignments for WHF-ESD01-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Truck trailer rollover	TT-Rollover	ESD01-CSNF-ROLLOVER	050-1-PMTT-ROLLOVER
Truck trailer collision	TT-Collision	ESD01-CSNF-COLL	050-1-PMTT-COLLISION

NOTE: [a] This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.1.2 System Response Event Tree RESPONSE-TCASK-CSNF

The pivotal events that appear in RESPONSE-TCASK-CSNF are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.1-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD01-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD01-CSNF	ESD01-CSNF-ROLLOVER	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD01-CSNF-COLL	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.1-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD01-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD01-CSNF	ESD01-CSNF-ROLLOVER	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD01-CSNF-COLL	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.1-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD01-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD01-CSNF	ESD01-CSNF-ROLLOVER	CONFINEMENT	HVAC
	ESD01-CSNF-COLL	CONFINEMENT	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. The conditional probability of failure (introduction of liquid moderator) is shown in Table A4.1-6.

Table A4.1-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD01-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD01-CSNF	ESD01-CSNF-ROLLOVER	MODERATOR	MODERATOR
	ESD01-CSNF-COLL	MODERATOR	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.2 EVENT TREES FOR WHF-ESD02-DPC

WHF-ESD02-DPC covers event sequences that arise after a structural challenge to a transportation cask (rail cask) loaded with a DPC on a railcar that occurs during transfer from the Transportation Cask Vestibule and movement into the Cask Preparation Area after the outer vestibule door is closed.

This ESD covers transportation casks with DPCs. Although the initiator event trees transfer to the same response tree (see Table A4.2-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.2-1. Summary of Event Trees for WHF-ESD02-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD02-DPC DPC Response: RESPONSE-TCASK-DPC	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.2.1 Initiator Events for WHF-ESD02-DPC

The following initiating events are associated with WHF-ESD02-DPC. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.2-2.

Railcar Derailment. This initiating event accounts for the potential impact to the transportation cask on the railcar due to a derailment. The probability of derailment per railcar received is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree as described in Section 6.2.2.1. The initiating event is specified as a probability of derailment per cask.

Railcar Collision. This initiating event covers the potential impact to the transportation cask on the conveyance due to a collision with another vehicle. The vehicular collision event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of collision per cask.

Table A4.2-2. Initiating Event Assignments for WHF-ESD02-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Railcar derailment	WHF-ESD02-DPC	ESD02-DPC-DERAIL	050-2-PMRC-DERAIL
Railcar collision	WHF-ESD02-DPC	ESD02-DPC-COLL	050-2-PMRC-COLLISION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.2.2 System Response Event Tree RESPONSE-TCASK-DPC

The pivotal events that appear in RESPONSE-TCASK-DPC are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.2-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD02-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD02-DPC	ESD02-DPC-DERAIL	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD02-DPC-COLL	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.2-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-4. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD02-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD1-DPC	ESD02-DPC-DERAIL	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD02-DPC-COLL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.2-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-5. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD02-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD02-DPC	ESD02-DPC-DERAIL	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD02-DPC-COLL	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.2-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD02-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD02-DPC	ESD02-DPC-DERAIL	CONFINEMENT	HVAC
	ESD02-DPC-COLL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.2-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD02-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD02-DPC	ESD02-DPC-DERAIL	MODERATOR	MODERATOR
	ESD02-DPC-COLL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.3 EVENT TREES FOR WHF-ESD03-AODPC

WHF-ESD03-AODPC delineates the event sequences that arise after a structural challenge to an aging overpack loaded with a DPC on a site transporter that occurs during receipt in the Site Transporter Vestibule. This ESD includes activities that occur after the outer vestibule door is closed.

An initiator event tree and a system response event tree represent this ESD (Table A4.3-1). The system response tree is customized within SAPHIRE for the initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.3-1. Summary of Event Trees for WHF-ESD03-AODPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Aging overpack carrying a DPC	Initiator: WHF-ESD03-AODPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.3.1 Initiator Event Trees for WHF-ESD03-AODPC

The following initiating events are associated with WHF-ESD03-AODPC. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.3-2.

Site Transporter Rollover. This initiating event accounts for the potential impact to the DPC due to a rollover of the site transporter. For a site transporter to roll over, the center of mass would have to shift laterally. This could result from traversing a significantly uneven surface or running over a very large object. There are no significantly uneven surfaces in the WHF Entrance Vestibule or Cask Preparation Area. Therefore, this failure mode was omitted from analysis by assignment of guaranteed success in the event tree.

Site Transporter Collision. This initiating event accounts for the potential impact to the DPC due to a collision involving the site transporter. The probability of collision per DPC received is modeled as a fault tree as described in Section 6.2.2.6. The initiating event is specified as a probability of collision per DPC.

Table A4.3-2. Initiating Event Assignments for WHF-ESD03-AODPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Site transporter rollover	WHF-ESD03-AODPC	ESD03-AO-STROLL	050-3-ST-ROLLOVER
Site transporter collision		ESD03-AO-STCOLLIDE	050-3-ST-COLLISION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.3.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.3-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD03-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD03-AO-STROLL	CANISTER-IN-AO	CANISTER-IN-AO-IMPACT
	ESD03-AO-STCOLLIDE	CANISTER-IN-AO	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.3-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD03-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD03-AO-STROLL	AO-SHIELD-DROP	AO-SHIELD-FAIL-DROP
	ESD03-AO-STCOLLIDE	AO-SHIELD-IMPACT	AO-SHIELD-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.3-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD03-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD03-AO-STROLL	HVAC-OFF	HVAC-OFF-STVEST
	ESD03-AO-STCOLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.3-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD03-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD03-AO-STROLL	MODERATOR	MODERATOR
	ESD03-AO-STCOLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.4 EVENT TREES FOR WHF-ESD04-DPC

WHF-ESD04-DPC delineates the event sequences that arise after a structural challenge to a horizontal STC/DPC that occurs during receipt in the Transportation Cask Vestibule and movement of the horizontal STC/DPC into the Cask Preparation Area. This ESD includes activities that occur after the outer vestibule door is closed.

As described in Table A4.4-1, there is one response tree assigned to the initiating event. Although the initiator event trees transfer to the same response tree, the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.4-1. Summary of Event Trees for WHF-ESD04-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks or horizontal shielded transfer casks containing a dual-purpose canister	Initiator: WHF-ESD04-DPC Response: RESPONSE-STC1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26 Table 4)

A4.4.1 Initiating Events for WHF-ESD04-DPC

The following initiating events are associated with WHF-ESD04-DPC:

- Truck trailer rollover

- Truck trailer collision.

The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.4-2.

Cast Transfer Truck Trailer Rollover. This initiating event accounts for the potential impact to the transportation cask on the truck trailer due to a rollover. The rollover event is modeled as a fault tree and is listed in Section 6.2.2.1.

Cast Transfer Truck Trailer Collision

This initiating event accounts for the potential impact to the transportation cask on the truck trailer due to a collision. The collision event is modeled as a fault tree and is listed in Section 6.2.2.1.

Table A4.4-2. Initiating Event Assignments for WHF-ESD04-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
CT Truck Trailer Rollover	WHF-ESD04-DPC	ESD04-HDPC-CTROLL	050-OPTTROLLOVER-HFI-NOD
CT Truck Trailer Collision	WHF-ESD04-DPC	ESD04-HDPC-CTCOLLIDE	050-HCTT-COLLISION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.4.2 System Response Event Tree RESPONSE-STC1

The pivotal events that appear in RESPONSE-STC are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.4-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.4-3. Basic Event Associated with the STC Pivotal Events of WHF-ESD04-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD04-DPC	ESD04-HDPC-CTROLL	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD04-HDPC-CTCOLLIDE	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.4-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.4-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD04-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD04-DPC	ESD04-HDPC-CTROLL	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD04-HDPC-CTCOLLIDE	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.4-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.4-5. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD04-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD04-DPC	ESD04-HDPC-CTROLL	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD04-HDPC-CTCOLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.4-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.4-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD04-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD04-DPC	ESD04-HDPC-CTROLL	CONFINEMENT	HVAC
	ESD04-HDPC-CTCOLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.4-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.4-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD04-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD04-DPC	ESD04-HDPC-CTROLL	MODERATOR	MODERATOR
	ESD04-HDPC-CTCOLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.5 EVENT TREES FOR WHF-ESD05-CSNF

ESD WHF-ESD05 delineates the event sequences that arise after a structural challenge to a transportation cask with commercial SNF resulting from removal of impact limiters, upending, and removal from conveyance and transfer to a preparation station.

Table A4.5-1 summarizes the event trees for WHF-ESD05-CSNF. Although all of the initiating events in the initiator event tree transfer to the same response tree, the response tree is customized within SAPHIRE for each initiating event by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.5-1. Summary of Event Trees for WHF-ESD05-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD05-CSNF Response: RESPONSE-TCASK-CSNF	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.5.1 Initiating Events for WHF-05-CSNF

The following initiating events are associated with WHF-ESD05. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.5-2.

Transportation Cask Tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The tipover event is modeled as a single-event fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of tipover per cask.

Side Impact to Cask. This initiating event covers the potential impact to the transportation cask due to a vehicular collision, unplanned conveyance movement or (for TTCs) a failure of the tilt frame. This event is modeled as fault trees and is listed in Section 6.2.2.1. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Object Dropped onto Transportation Cask/Commercial SNF. This initiating event covers the potential impact to the transportation cask due to the drop of a heavy object, such as an

impact limiter, on the cask. This event is modeled as a fault tree. The initiating event is specified as a probability of object drop per cask.

Cask Drop from Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from the normal operational height during transfer by the cask handling crane. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree. The initiating event is specified as a probability of a drop per cask.

Cask Drop from Above Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from above the normal operational height (for example, due to two-blocking) during transfer by the cask handling crane. The probability of drop per transfer is modeled as a fault tree. The initiating event is specified as a probability of a drop per cask**.**

Unplanned Carrier Movement. This initiating event accounts for the potential impact to the transportation cask due to unplanned carrier movement from either the SPM or site transporter.

Table A4.5-2. Initiating Event Assignments for WHF-ESD05-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Transportation cask tipover	WHF-ESD05-TC	ESD05-UPEND-CASK-TIP	050-OPTIPOVER001-HFI-NOD
Side impact	WHF-ESD05-TC	ESD05-UPEND-SIDE-IMPACT	050-5-CSNF-IMPACT
Object dropped on a cask	WHF-ESD05-TC	ESD05-UPEND-DROPON-CASK	050-5-200T-CRANE-DROPON
Cask drop from operational height	WHF-ESD05-TC	ESD05-UPEND-DROP-OP	050-CHC-CSKDROP-CRN-DRP and 050-TRANSNSCTTLIFTNUMBER
Cask drop from above operational height	WHF-ESD05-TC	ESD05-UPEND-DROP-ABOVE	050-CHC-TWOBLCK-CRN-TBK and 050-TRANSNSCTTLIFTNUMBER
Transportation cask move	WHF-ESD05-TC	ESD05-UPEND-MOVE	ESD05-UPEND-MOVE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.5.2 System Response Event Tree RESPONSE-TCASK-CSNF

The pivotal events that appear in RESPONSE-TCASK-CSNF are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.5-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.5-3. Basic Event Associated with the CASK Pivotal Events for WHF-ESD05-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD05-CSNF	ESD05-UPEND-CASK-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD05-UPEND-SIDE-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD05-UPEND-DROPON-CASK	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD05-UPEND-DROP-OP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD05-UPEND-DROP-ABOVE	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.5-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.5-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD05-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD05-CSNF	ESD05-UPEND-CASK-TIP	SHIEL-CASK-DROP	CASK-SHIELDING-DROP
	ESD05-UPEND-SIDE-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD05-UPEND-DROPON-CASK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD05-UPEND-DROP-OP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD05-UPEND-DROP-ABOVE	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.5-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.5-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD05-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD05-CSNF	ESD05-UPEND-CASK-TIP	CONFINEMENT	HVAC
	ESD05-UPEND-SIDE-IMPACT		
	ESD05-UPEND-DROPON-CASK		
	ESD05-UPEND-DROP-OP		
	ESD05-UPEND-DROP-ABOVE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.5-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.5-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD05-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD05-CSNF	ESD05-UPEND-CASK-TIP	MODERATOR	MODERATOR
	ESD05-UPEND-SIDE-IMPACT		
	ESD05-UPEND-DROPON-CASK		
	ESD05-UPEND-DROP-OP		
	ESD05-UPEND-DROP-ABOVE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.6 EVENT TREES FOR WHF-ESD06-VTC AND TTC

ESD WHF-ESD06 delineates the event sequences that arise after a structural challenge to a transportation cask/DPC that occurs during removal of impact limiters, upending, and removal of transportation cask from conveyance and transfer to CTT. For casks with trunnions that can be uprighted on the conveyance, this ESD applies to the following waste forms:

- Commercial SNF in DPCs contained in rail casks (railcar to CTT)
- Commercial SNF in DPCs contained in horizontal STCs (cask tractor trailer to CTT).

For casks without trunnions that must be uprighted with a lifting frame, this ESD applies to commercial SNF in DPCs contained in transportation casks that are upended with a tilting frame (TTC) (railcar, cask stand then to CTT).

This ESD covers transportation casks with DPCs with and without trunnions. Although the initiator event trees transfer to the same response tree (see Table A4.6-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.6-1. Summary of Event Trees for WHF-ESD06

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC (casks contain Trunnions)	Initiator: WHF-ESD06-TTC DPC Response: RESPONSE-TCASK	346
Transportation cask containing a DPC (casks do not contain Trunnions)	Initiator: WHF-ESD06-VTC DPC Response: RESPONSE-TCASK	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.6.1 Initiating Events for WHF-ESD06 VTC and TTC

The following initiating events are associated with WHF-ESD06 for the two types of transportation tasks discussed above. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.6-2.

Cask Drop from Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from the normal operational height during transfer by the cask handling crane. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree. The initiating event is specified as a probability of a drop per cask.

Cask Drop from Above Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from above the normal operational height (for example, due to two-blocking) during transfer by the cask handling crane. The probability of drop per transfer is modeled as a fault tree. The initiating event is specified as a probability of a drop per cask.

Transportation Cask Tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The tipover event is modeled as a single-event fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of tipover per cask.

Side Impact to Cask. This initiating event covers the potential impact to the transportation cask due to a vehicular collision, unplanned conveyance movement or (for TTCs) a failure of the tilt frame. This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Object Dropped onto Transportation Cask/DPC. This initiating event covers the potential impact to the transportation cask due to the drop of a heavy object, such as an impact limiter, on

the cask. This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of object drop per cask.

Table A4.6-2. Initiating Event Assignments for WHF-ESD06 TTC and VTC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of Cask from Operational Height	WHF-ESD06-TTC	ESD06-TTC-UP-DROP	050-6-HS-CRANE-DROP
Drop of Cask Above Operational Height		ESD06-TTC-UP-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and 050-TRANSCTTLIFTNUMBER
TC Tips Over		ESD06-TTC-UP-TIP	050-OPTIPOVER001-HFI-NOD
Side Impact		ESD06-TTC-UP-IMPACT	050-6-HS-TC-IMPACT
Drop on Cask		ESD06-TTC-UP-DROPON	050-6-200T-CRANE-DROPON
Transportation Cask Moves		ESD06-TTC-UP-MOVE	ESD06-TTC-UP-MOVE
Drop of Cask from Operational Height	WHF-ESD06-VTC	ESD06-VTC-UP-DROP	050-CHC-CSKDROP-CRN-DROP and 050-TRANSCTTLIFTNUMBER
Drop of Cask above Operational Height		ESD06-VTC-UP-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and 050-TRANSCTTLIFTNUMBER
TC Tips Over		ESD06-VTC-UP-TIP	050-OPTIPOVER001-HFI-NOD
Side Impact		ESD06-VTC-UP-IMPACT	050-6-VTC-IMPACT
Drop on Cask		ESD06-VTC-UP-DROPON	050-6-200T-CRANE-DROPON
Transportation Cask Moves		ESD06-VTC-UP-MOVE	ESD06-VTC-UP-MOVE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.6.2 System Response Event Tree RESPONSE-TCASK

The pivotal events that appear in RESPONSE-TCASK are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.6-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-3. Basic Event Associated with the CASK Pivotal Events for WHF-ESD06 TTC and VTC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD06-TTC	ESD06-TTC-UP-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-TTC-UP-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD06-TTC-UP-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-TTC-UP-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD06-TTC-UP-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-TTC-UP-MOVE	CASK-DROP	CASK-DROP-OPERATIONAL
WHF-ESD06-VTC	ESD06-VTC-UP-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-VTC-UP-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD06-VTC-UP-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-VTC-UP-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD06-VTC-UP-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD06-VTC-UP-MOVE	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.6-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD06 TTC and VTC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD06-TTC	ESD06-TTC-UP-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-TTC-UP-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-TTC-UP-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-TTC-UP-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD06-TTC-UP-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-TTC-UP-MOVE	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
WHF-ESD06-VTC	ESD06-VTC-UP-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-VTC-UP-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-VTC-UP-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-VTC-UP-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD06-VTC-UP-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD06-VTC-UP-MOVE	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source Original

CANISTER. Table A4.6-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-5. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD06 TTC and VTC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD06-TTC	ESD06-TTC-UP-DROP	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD06-TTC-UP-TWOBLOCK		
	ESD06-TTC-UP-TIP		
	ESD06-TTC-UP-IMPACT		
	ESD06-TTC-UP-DROPON		
	ESD06-TTC-UP-MOVE		
	ESD06-VTC-UP-DROP		
	ESD06-VTC-UP-TWOBLOCK		
	ESD06-VTC-UP-TIP		
	ESD06-VTC-UP-IMPACT		
	ESD06-VTC-UP-DROPON		
	ESD06-VTC-UP-MOVE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.6-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD06 TTC and VTC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD06-TTC	ESD06-TTC-UP-DROP	CONFINEMENT	HVAC
	ESD06-TTC-UP-TWOBLOCK		
	ESD06-TTC-UP-TIP		
	ESD06-TTC-UP-IMPACT		
	ESD06-TTC-UP-DROPON		
	ESD06-TTC-UP-MOVE		
WHF-ESD06-VTC	ESD06-VTC-UP-DROP		
	ESD06-VTC-UP-TWOBLOCK		
	ESD06-VTC-UP-TIP		
	ESD06-VTC-UP-IMPACT		
	ESD06-VTC-UP-DROPON		
	ESD06-VTC-UP-MOVE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.6-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD06 TTC and VTC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD06-TTC	ESD06-TTC-UP-DROP	MODERATOR	MODERATOR
	ESD06-TTC-UP-TWOBLOCK		
	ESD06-TTC-UP-TIP		
	ESD06-TTC-UP-IMPACT		
	ESD06-TTC-UP-DROPON		
	ESD06-TTC-UP-MOVE		
WHF-ESD06-VTC	ESD06-VTC-UP-DROP		
	ESD06-VTC-UP-TWOBLOCK		
	ESD06-VTC-UP-TIP		
	ESD06-VTC-UP-IMPACT		
	ESD06-VTC-UP-DROPON		
	ESD06-VTC-UP-MOVE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.7 EVENT TREES FOR WHF-ESD07-DPC

ESD WHF-ESD07 delineates the event sequences that arise after a structural challenge to a transportation cask with DPC or STC with DPC associated with cask preparation activities (i.e., installation of cask lid lift fixture). This ESD applies to the following waste forms:

- Commercial SNF in DPCs contained in STCs on CTT
- Commercial SNF in DPCs contained in a transportation cask on CTT.

This ESD covers transportation casks with DPCs. Although the initiator event trees transfer to the same response tree (see Table A4.7-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.7-1 Summary of Event Trees for WHF-ESD07-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD07-DPC DPC Response: RESPONSE-TCASK	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.7.1 Initiating Events for WHF-ESD07-DPC

The following initiating events are associated with WHF-ESD07-DPC for transportation tasks with DPCs. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.7-2.

Transportation Cask Tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The tipover event is modeled as a single-event fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of tipover per cask.

Side Impact to Cask. This initiating event covers the potential impact to the transportation cask due to a vehicular collision, unplanned conveyance movement or (for TTCs) a failure of the tilt frame. This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Object Dropped onto Transportation Cask/DPC. This initiating event covers the potential impact to the transportation cask due to the drop of a heavy object such as the lid lift fixture on the cask. This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of object drop per cask.

Cask Drop from Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from the normal operational height during transfer by the cask handling crane. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree. The initiating event is specified as a probability of a drop per cask.

Table A4.7-2. Initiating Event Assignments for WHF-ESD07-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Transportation cask tipover	WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	ESD07-CPREP-CASKTIP
Side impact		ESD07-CPREP-SIMPACT	ESD07-CPREP-SIMPACT
Object dropped on a cask		ESD07-CPREP-DROPON	050-JIBCRANE-CRJ-DRP AND 050-DPCPREPLIFTNUMBER
Cask drop from operational height		ESD07-CPREP-CASKDROP	050-OPCASKDROP01-HFI-NOD
Transportation cask tipover		ESD07-CPREP-CASKTIP	ESD07-CPREP-CASKTIP
Side impact		ESD07-CPREP-SIMPACT	050-FL-SC001-SC-FOH
Object dropped on a cask		ESD07-CPREP-DROPON	ESD08-CPREP-DROPON

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.7.2 System Response Event Tree RESPONSE-TCASK

The pivotal events that appear in RESPONSE-TCASK are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.7-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.7-3. Basic Event Associated with the CASK Pivotal Events for WHF-ESD07-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD07-CPREP-SIMPACT	CASK-IMPACT	CASK- FAIL-IMPACT
	ESD07-CPREP-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD07-CPREP-CASKDROP	CASK- DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.7-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.7-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD07-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELD	Associated Fault Tree or Basic Event[a]
WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD07-CPREP-SIMPACT		CASK-SHIELDING-IMPACT
	ESD07-CPREP-DROPON		CASK-SHIELDING-DROP
	ESD07-CPREP-CASKDROP		CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.7-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.7-5. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD06-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD07-CPREP-SIMPACT		
	ESD07-CPREP-DROPON		
	ESD07-CPREP-CASKDROP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.7-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.7-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD07-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	CONFINEMENT	HVAC
	ESD07-CPREP-SIMPACT		
	ESD07-CPREP-DROPON		
	ESD07-CPREP-CASKDROP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.7-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.7-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD07-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD07-DPC	ESD07-CPREP-CASKTIP	MODERATOR	MODERATOR
	ESD07-CPREP-SIMPACT		
	ESD07-CPREP-DROPON		
	ESD07-CPREP-CASKDROP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.8 EVENT TREES FOR WHF-ESD08-CSNF

ESD WHF-ESD08-CSNF delineates the event sequences that arise from structural challenges associated with the installation of lid lift fixture on transportation cask/commercial SNF. This ESD applies to uncanistered commercial SNF in a transportation cask or truck trailer.

Although the initiator event trees transfer to the same response tree (see Table A4.8-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.8-1. Summary of Event Trees for WHF-ESD08-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD08-CSNF Response: RESPONSE-TCASK-CSNF	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.8.1 Initiating Events for WHF-ESD08-CSNF

The individual initiating events that were identified in the MLD are indicated on the ESD by their initiating event identifiers and, for quantification purposes, are collected into one of five groups. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.8-2.

Side Impact to Cask. This initiating event covers the potential impact to the transportation cask due to a vehicular collision, unplanned conveyance movement or (for TTCs) a failure of the tilt frame. This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Object Dropped onto Transportation Cask/Commercial SNF. This initiating event covers the potential impact to the transportation cask due to the drop of a heavy object, such on the cask.

This event is modeled as a fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of object drop per cask.

Cask Drop from Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from the normal operational height during transfer by the cask handling crane. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree. The initiating event is specified as a probability of a drop per cask.

Transportation Cask Tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The tipover event is modeled as a single-event fault tree and is listed in Section 6.2.2.1. The initiating event is specified as a probability of tipover per cask.

Table A4.8-2. Initiating Event Assignments for WHF-ESD08-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Impact to cask	WHF-ESD08-CSNF	ESD08-CPREP-IMPACT	ESD08-CPREP-IMPACT
Object dropped on a cask	WHF-ESD08-CSNF	ESD08-CPREP-DROPON	050-JIBCRANE-CRJ-DRP and 050-DPCPREPLIFTNUMBER
Cask drop from operational height	WHF-ESD08-CSNF	ESD08-CPREP-DROP	050-OPCASKDROP01-HFI-NOD
Transportation cask tipover	WHF-ESD08-CSNF	ESD08-CPREP-TIP	ESD08-CPREP-TIP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source:

A4.8.2 System Response Event Tree RESPONSE-TCASK-CSNF

The pivotal events that appear in RESPONSE-TCASK-CSNF are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.8-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.8-3. Basic Event Associated with the CASK Pivotal Events for WHF-ESD08-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD08-CSNF	ESD08-CPREP-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD08-CPREP-DROPON	CASK- DROP	CASK-DROP-OPERATIONAL
	ESD08-CPREP-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD08-CPREP-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.8-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.8-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD08-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD08-CSNF	ESD08-CPREP-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD08-CPREP-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD08-CPREP-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD08-CPREP-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.8-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.8-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD08-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD08-CSNF	ESD08-CPREP-IMPACT	CONFINEMENT	HVAC
	ESD08-CPREP-DROPON		
	ESD08-CPREP-DROP		
	ESD08-CPREP-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.8-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.8-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD08-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD08-CSNF	ESD08-CPREP-IMPACT	MODERATOR	MODERATOR
	ESD08-CPREP-DROPON		
	ESD08-CPREP-DROP		
	ESD08-CPREP-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.9 EVENT TREES FOR WHF-ESD09-DPC

ESD WHF-ESD09-DPC delineates the event sequences that arise after a structural challenge to a transportation cask with DPC or STC with DPC associated with cask preparation activities (i.e., installation of cask lid lift fixture). This ESD applies to the following waste forms:

- Commercial SNF in DPCs contained in STCs on CTT
- Commercial SNF in DPCs contained in a transportation cask on CTT.

With the lid removed, the cask provides no containment or shielding.

This ESD covers transportation casks or STCs with DPCs. Although the initiator event trees transfer to the same response tree (see Table A4.9-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.9-1. Summary of Event Trees for WHF-ESD09-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD09-DPC DPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.9.1 Initiating Events for WHF-ESD09-DPC

The following initiating events are associated with WHF-ESD09-DPC for transportation tasks with DPCs. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.9-2.

Cask Drop from Operational Height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from the normal operational height during transfer by the cask handling crane. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree. The initiating event is specified as a probability of a drop per cask.

Side Impact to STC. This initiating event covers the potential impact to the STC due to collision between the CTT and another moving vehicle, facility structures, or facility equipment. This event is modeled as a fault tree and is listed in Section 6.2.2.4. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE

Object Dropped onto DPC. This initiating event covers the potential impact to the transportation cask due to the drop of a heavy object such as the lid lift fixture on the cask. This event is modeled as a fault tree. The initiating event is specified as a probability of object drop per cask.

Table A4.9-2. Initiating Event Assignments for WHF-ESD09-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of Cask	WHF-ESD09-DPC	ESD09-DPREP-CASKDROP	050-OPCASKDROP01-HFI-NOD
Impact to cask	WHF-ESD09-DPC	ESD09-DPREP-IMPACT	ESD09-DPREP-IMPACT
Object dropped on cask	WHF-ESD09-DPC	ESD09-DPREP-DROPON	050-JIBCRANE-CRJ-DRP and 050-DPCPREPLIFTNUMBER

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.9.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.9-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.9-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD09-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD09-DPC	ESD09-DPREP-CASKDROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD09-DPREP-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD09-DPREP-CASKDROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.9-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.9-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD09-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD09-DPC	ESD09-DPREP-CASKDROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD09-DPREP-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD09-DPREP-CASKDROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.9-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.9-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD09-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD09-DPC	ESD09-DPREP-CASKDROP	CONFINEMENT	HVAC
	ESD09-DPREP-IMPACT		
	ESD09-DPREP-CASKDROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.9-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.9-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD09-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD09-DPC	ESD09-DPREP-CASKDROP	MODERATOR	MODERATOR
	ESD09-DPREP-IMPACT		
	ESD09-DPREP-CASKDROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.10 EVENT TREES FOR WHF-ESD10-DPC

ESD WHF-ESD10-DPC delineates the event sequences that arise after a structural challenge to a transportation cask that contains a DPC. This includes transfer of the transportation cask/DPC from Cask Preparation Area to Cask Unloading Room. With the lid lifting fixture on, the transportation cask provides shielding but does not provide containment since the transportation

cask lid is unbolted. This ESD applies to commercial SNF in DPCs contained in transportation casks on CTT.

This ESD covers transportation casks with DPCs. Although the initiator event trees transfer to the same response tree (see Table A4.10-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.10-1. Summary of Event Trees for WHF-ESD10-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD10-DPC DPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.10.1 Initiating Events for WHF-ESD10-DPC

The following initiating events are associated with WHF-ESD10-DPC for transportation tasks with DPCs. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.10-2 and listed below.

- CTT collision with facility structures or equipment
- CTT or cask catches crane hook/rigging resulting in impact.

The initiating event is specified as a probability of object drop per cask is modeled as a fault tree as described in Section 6.2.2.2.

Table A4.10-2. Initiating Event Assignments for WHF-ESD10-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
CTT impact	WHF-ESD10-DPC	ESD10-CTT-IMPACT	050-OPIMPACT0000-HFI-NOD
CTT collision	WHF-ESD10-DPC	ESD10-CTT-COLLIDE	050-CTT-COLLIDE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.10.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.10-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.10-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD10-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD10-DPC	ESD10-CTT-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD10-CTT-COLLIDE	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.10-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.10-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD10-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD10-DPC	ESD10-CTT-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD10-CTT-COLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.10-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.10-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD10-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD10-DPC	ESD10-CTT-IMPACT	CONFINEMENT	HVAC
	ESD10-CTT-COLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.10-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.10-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD10-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD10-DPC	ESD10-CTT-IMPACT	MODERATOR	MODERATOR
	ESD10-CTT-COLLIDE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.11 EVENT TREES FOR WHF-ESD11-AODPC

A4.11.1 Event Trees for WHF-ESD11 (Site Transporter with Aging Overpack/DPC)

This ESD delineates the event sequences that arise after a structural challenge to an aging overpack during transfer of an aging overpack/DPC or aging overpack/TAD canister on a site transporter, through the Site Transporter Vestibule, aging overpack access platform, and Loading Room (receipt or export). This ESD applies to commercial SNF in DPCs contained in aging overpacks on site transporters.

An initiator event tree and a system response event tree represent this ESD (Table A4.11-1). The system response tree is customized within SAPHIRE for the initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.11-1. Summary of Event Trees for WHF-ESD11-AODPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Aging overpack carrying a DPC	Initiator: WHF-ESD11-AODPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.11.1.1 Initiator Event Trees for WHF-ESD11 (Site Transporter with Aging Overpack/DPC)

The following initiating events are associated with WHF-ESD11-AODPC. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.11-2.

Site Transporter Collision. This initiating event accounts for the potential impact to the DPC due to a collision involving the site transporter. The probability of collision per DPC received is modeled as a fault tree as described in Section 6.2.2.6. The initiating event is specified as a probability of collision per DPC.

Object Dropped onto Aging Overpack/DPC. This initiating event covers the potential impact to the DPC due to the drop of a heavy object on the aging overpack. This event is modeled as a fault tree. The initiating event is specified as a probability of object drop per cask.

Aging Overpack/DPC Tipover. This initiating event covers the potential impact to the DPC due to a site transporter tipover. The tipover event is modeled as a single-event fault tree. The initiating event is specified as a probability of tipover per cask.

Table A4.11-2. Initiating Event Assignments for WHF-ESD11-AODPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Site transporter collision	WHF-ESD11-AODPC	ESD11-DPC-COLLIDE	050-11-ST-COLLISION
Drop on aging overpack		ESD11-DPC-DROP	050-JIBCRANE-CRJ-DRP
AO/DPC tip over		ESD11-DPC-TIP	050-11-ST-ROLLOVER
Side impact		ESD11-DPC-IMPACT	ESD11-DPC-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.11.1.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.11-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD11-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AODPC	ESD11-DPC-COLLIDE	CANISTER-AO-IMPACT	CANISTER-AO-IMPACT-FAIL
	ESD11-DPC-DROP	CANISTER-AO-DROP	CANISTER-AO-DROP-FAIL
	ESD11-DPC-TIP	CANISTER-AO-DROP	CANISTER-AO-DROP-FAIL
	ESD11-DPC-IMPACT	CANISTER-AO-IMPACT	CANISTER-AO-IMPACT-FAIL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.11-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD11-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AODPC	ESD11-DPC-COLLIDE	AO-SHIELD-IMPACT	AO-SHIELD-FAIL-IMPACT
	ESD11-DPC-DROP	AO-SHIELD-DROP	AO-SHIELD-FAIL-DROP
	ESD11-DPC-TIP	AO-SHIELD-DROP	AO-SHIELD-FAIL-DROP
	ESD11-DPC-IMPACT	AO-SHIELD-IMPACT	AO-SHIELD-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.11-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD11-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD11-DPC-COLLIDE	CONFINEMENT	HVAC
	ESD11-DPC-DROP		
	ESD11-DPC-TIP		
	ESD11-DPC-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.11-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD11-AODPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD03-AODPC	ESD11-DPC-COLLIDE	MODERATOR	MODERATOR
	ESD11-DPC-DROP		
	ESD11-DPC-TIP		
	ESD11-DPC-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.11.2 Event Trees for WHF-ESD11-AOTAD (Site Transporter with Aging Overpack/TAD Canister)

This ESD delineates the event sequences that arise after a structural challenge to an aging overpack during transfer aging overpack/TAD canister on a site transporter, through the Site

Transporter Vestibule, aging overpack access platform, and Loading Room (receipt or export). This ESD applies to commercial SNF in TAD canisters contained in aging overpacks on site transporters.

An initiator event tree and a system response event tree represent this ESD (Table A4.11-7). The system response tree is customized within SAPHIRE for the initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.11-7. Summary of Event Trees for WHF-ESD11-AOTAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Aging overpacks containing a TAD canister	Initiator: WHF-ESD11-AOTAD Response: RESPONSE-CANISTER1	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.11.2.1 Initiator Event Trees for WHF-ESD11 (Site Transporter with Aging Overpack/DPC)

The following initiating events are associated with WHF-ESD11. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.11-8.

Site Transporter Collision. This initiating event accounts for the potential impact to the TAD canister due to a collision involving the site transporter. The probability of collision per TAD canister received is modeled as a fault tree as described in Section 6.2.2.6. The initiating event is specified as a probability of collision per DPC.

Object Dropped onto Aging Overpack/TAD Canister. This initiating event covers the potential impact to the TAD canister due to the drop of a heavy object on the aging overpack. This event is modeled as a fault tree. The initiating event is specified as a probability of object drop per cask.

Aging Overpack/TAD Canister Tipover. This initiating event covers the potential impact to the TAD canister due to a site transporter tipover. The tipover event is modeled as a single-event fault tree. The initiating event is specified as a probability of tipover per cask.

Table A4.11-8. Initiating Event Assignments for WHF-ESD11-AOTAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Site transporter collision	WHF-ESD11-AOTAD	ESD11-TAD-COLLIDE	050-11-ST-COLLISION
Drop on aging overpack		ESD11-TAD-DROP	050-JIBCRANE-CRJ-DRP
AO/TAD canister tip over		ESD11-TAD-TIP	050-11-ST-ROLLOVER
Side Impact		ESD11-TAD-IMPACT	ESD11-TAD-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.11.2.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.11-9 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-9. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD11-AOTAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AOTAD	ESD11-TAD-COLLIDE	CANISTER-AO-IMPACT	CANISTER-AO-IMPACT-FAIL
	ESD11-TAD-DROP	CANISTER-AO-DROP	CANISTER-AO-DROP-FAIL
	ESD11-TAD-TIP	CANISTER-AO-DROP	CANISTER-AO-DROP-FAIL
	ESD11-TAD-IMPACT	CANISTER-AO-IMPACT	CANISTER-AO-IMPACT-FAIL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.11-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-10. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD11-AOTAD

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AOTAD	ESD11-TAD-COLLIDE	AO-SHIELD-IMPACT	AO-SHIELD-FAIL-IMPACT
	ESD11-TAD-DROP	AO-SHIELD-DROP	AO-SHIELD-FAIL-DROP
	ESD11-TAD-TIP	AO-SHIELD-DROP	AO-SHIELD-FAIL-DROP
	ESD11-TAD-IMPACT	AO-SHIELD-IMPACT	AO-SHIELD-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.11-11 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-11. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD11-AOTAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AOTAD	ESD11-TAD-COLLIDE	CONFINEMENT	HVAC
	ESD11-TAD-DROP		
	ESD11-TAD-TIP		
	ESD11-TAD-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.11-12 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.11-12. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD11-AOTAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD11-AOTAD	ESD11-TAD-COLLIDE	MODERATOR	MODERATOR
	ESD11-TAD-DROP		
	ESD11-TAD-TIP		
	ESD11-TAD-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.12 EVENT TREES FOR WHF-ESD12-DPC

A4.12.1 Event Trees for WHF-ESD12 (Aging Overpack/DPC on Site Transporter)

This ESD delineates the event sequences that arise after a structural challenge from an aging overpack/DPC collision with Cask Loading Room shield door.

The initiating event and number of waste forms is given in Table A4.12-1.

Table A4.12-1. Summary of Event Trees for WHF-ESD12-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Aging overpack carrying a DPC	Initiator: WHF-ESD12-DPC	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.12.1.1 Initiator Event Trees for WHF-ESD12 (Site Transporter with Aging Overpack/DPC/DPC)

There is one initiating event associated with WHF-ESD12 described below and the SAPHIRE assignments are given in Table A4.12-2.

Collision with Cask Loading Shield Door. This initiating event describes collision with the cask loading room shield door while the AO/DPC is on the site transporter.

Table A4.12-2. Initiating Event Assignments for WHF-ESD12-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Site transporter collision with shield door	WHF-ESD12-DPC	ESD12-DPC-DOOR	ESD12-DPC-DOOR

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.12.1.2 Pivotal Events

The pivotal events for site transporter collision with the shield door are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CELL DOOR. Table A4.12-3 indicates the basic event that is associated with this pivotal event for the initiating event as described in Section 6.2.2.3.

Table A4.12-3. Basic Event Associated with the CELL DOOR pivotal event for WHF-ESD12-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CELL DOOR	Associated Fault Tree or Basic Event[a]
WHF-ESD12-DPC	ESD12-DPC-DOOR	CELL-DOOR	SHIELD-DOOR-FAILURE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CASK. Table A4.12-4 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-4. Basic Event Associated with the CASK pivotal event for WHF-ESD12-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD12-DPC	ESD12-DPC-DOOR	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.12-5 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-5. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD12-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD12-DPC	ESD12-DPC-DOOR	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.12-6 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD12-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD12-DPC	ESD12-DPC-DOOR	CONFINEMENT	HVAC

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.12-7 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD12-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD12-DPC	ESD12-DPC-DOOR	MODERATOR	MODERATOR

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.12.2 Event Trees for WHF-ESD12-TAD (Aging Overpack/Site Transporter or STC/CTT containing a TAD Canister)

This ESD delineates the event sequences that arise after a structural challenge from aging overpack/site transporter containing a TAD canister colliding with the cask loading shield door or the STC/CTT containing a TAD canister colliding with the cask unloading door.

Table A4.12-8. Summary of Event Trees for WHF-ESD12-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Aging overpacks or STCs containing a TAD canister	Initiator: WHF-ESD12-TAD	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.12.2.1 Initiator Event Trees for WHF-ESD12 (Aging Overpack/Site Transporter or STC/CTT containing a TAD Canister)

There is one initiating event associated with WHF-ESD12-TAD described below and the SAPHIRE assignments are given in Table A4.12-9.

Collision with Cask Loading or Cask Unloading Shield Door. This initiating event describes aging overpack/site transporter collision with the cask unloading shield door or the STC/CTT collision with the cask unloading shield door as described in Section 6.2.2.3.

Table A4.12-9. Initiating Event Assignments for WHF-ESD12-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Site transporter or CTT collision with shield door	WHF-ESD12-TAD	ESD12-TAD-DOOR	ESD12-TAD-DOOR

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.12.2.2 Pivotal Events

The pivotal events for site transporter collision with the shield door are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CELL DOOR. Table A4.12-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.12-10. Basic Event Associated with the CELL DOOR pivotal event for WHF-ESD12-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CELL DOOR	Associated Fault Tree or Basic Event[a]
WHF-ESD12-TAD	ESD12-TAD-DOOR	CELL-DOOR	SHIELD-DOOR-FAILURE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CASK. Table A4.12-11 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-11. Basic Events Associated with the CASK Pivotal Events of WHF-ESD12-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD12-TAD	ESD12-TAD-DOOR	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.12-12 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-12. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD12-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD12-TAD	ESD12-TAD-DOOR	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.12-13 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-13. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD12-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD12-TAD	ESD12-TAD-DOOR	CONFINEMENT	HVAC

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.12-14 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.12-14. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD12-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD12-TAD	ESD12-TAD-DOOR	MODERATOR	MODERATOR

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.13 EVENT TREES FOR WHF-ESD13

A4.13.1 Event Trees for WHF-ESD13 (DPC Transfer with CTM)

This ESD delineates the event sequences that arise after a structural challenge resulting from transfer of a DPC from a transportation cask to STC within the CTM.

Although the initiator event trees transfer to the same response tree (see Table A4.13-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.13-1. Summary of Event Trees for WHF-ESD13-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD13-DPC DPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.13.1 Initiating Events for WHF-ESD13-DPC

The following initiating events are associated with WHF-ESD13-DPC involving CTM operation. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.13-2.

Canister Drop from Operational Height. This initiating event accounts for the potential impact to the DPC due to having been dropped from the normal operational height during transfer by the CTM. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree as described in Section 6.2.2.4. The initiating event is specified as a probability of a drop per cask.

Canister Drop from Above Operational Height. This initiating event accounts for the potential impact to the DPC due to having been dropped from above the normal operational height (for example, due to two-blocking) during transfer by the CTM. The probability of drop per transfer is modeled as a fault tree as described in Section 6.2.2.4. The initiating event is specified as a probability of a drop per cask.

Side Impact to Canister. This initiating event covers the potential side impact to the DPC as it being lifted and transferred by the CTM. This event is modeled as a fault tree and is listed in Section 6.2.2.4. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Drop on Canister. This initiating event covers the potential impact to the DPC due to the drop of a heavy object such as the CTM bell. This event is modeled as a fault tree and is listed in Section 6.2.2.4. The initiating event is specified as a probability of object drop per cask.

Spurious movement of DPC. This initiating event results from spurious site transporter movement or CTM bell movement.

Canister Drop Inside Bell. This initiating event describes a drop inside the STM bell due to either human or mechanical failures.

Table A4.13-2 Initiating Event Assignments for WHF-ESD13-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of cask from operational height	WHF-ESD13-DPC	ESD13-DPC-DROP	CTM-DROP---ALL-HEIGHTS and 050-LIFTS-PER-DPC-CAN
Drop of cask above operational height	WHF-ESD13-DPC	ESD13-DPC-TWOBLOCK	CTM-2-BLOCK and 050-LIFTS-PER-DPC-CAN
Side impact of canister	WHF-ESD13-DPC	ESD13-DPC-SIDEIMPACT	ESD13-DPC-SIDEIMPACT
Drop on canister	WHF-ESD13-DPC	ESD13-DPC-DROPON	CTM-DROP-ONTO-CASK and 050-CTMOBJLIFTNUMBERD
Spurious movement	WHF-ESD13-DPC	ESD13-DPC-SPURMOVE	ESD13-DPC-SPURMOVE
Canister drop inside bell	WHF-ESD13-DPC	ESD13-DPC-DROPBELL	CTM-DROP-IN-SHIELD-BELL and 050-LIFTS-PER-DPC-CAN

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.13.1.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.13-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD13-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD13-DPC	ESD13-DPC-DROP	CANISTER-DROP	CANISTER-FAILS-DROP
	ESD13-DPC-TWOBLOCK	CANISTER-TWOBLOCK	CANISTER-FAIL-TWOBLOCK
	ESD13-DPC-SIDEIMPACT	CANISTER-IMPACT	CANISTER-FAIL-IMPACT
	ESD13-DPC-DROPON	CANISTER-DROP	CANISTER-FAILS-DROP
	ESD13-DPC-SPURMOVE	CANISTER-SHEAR	CANISTER-SHEAR-CTM
	ESD13-DPC-DROPBELL	CANISTER-DROP	CANISTER-FAILS-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.13-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD13-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD13-DPC	ESD13-DPC-DROP	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-DPC-TWOBLOCK	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-DPC-SIDEIMPACT	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-DPC-DROPON	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-DPC-SPURMOVE	SHIELD-LOSS	SHIELD-TOTAL-LOSS
	ESD13-DPC-DROPBELL	SHIELD-CTM	SHIELD-FAIL-CTM

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.13-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD13-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD13-DPC	ESD13-DPC-DROP	CONFINEMENT	HVAC
	ESD13-DPC-TWOBLOCK		
	ESD13-DPC-SIDEIMPACT		
	ESD13-DPC-DROPON		
	ESD13-DPC-SPURMOVE		
	ESD13-DPC-DROPBELL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.13-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD13-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD13-DPC	ESD13-DPC-DROP	MODERATOR	MODERATOR
	ESD13-DPC-TWOBLOCK		
	ESD13-DPC-SIDEIMPACT		
	ESD13-DPC-DROPON		
	ESD13-DPC-SPURMOVE		
	ESD13-DPC-DROPBELL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.13.2 Event Trees for WHF-ESD13 (TAD Canister Transfer with CTM)

This ESD delineates the event sequences that arise after a structural challenge resulting from transfer of a TAD canister from a STC to aging overpack within the CTM.

Although the initiator event trees transfer to the same response tree (see Table A4.13-7), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.13-7. Summary of Event Trees for WHF-ESD13-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a TAD canister	Initiator: WHF-ESD13-TAD TAD Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.13.2.1 Initiating Events for WHF-ESD13-TAD

The following initiating events are associated with WHF-ESD13-TAD involving CTM operation. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.13-8.

Canister Drop from Operational Height. This initiating event accounts for the potential impact to the TAD canister due to having been dropped from the normal operational height during transfer by the CTM. The probability of drop per transfer is derived from empirical data in Section 6.3 and is modeled as a single-event fault tree as described in Section 6.2.2.4. The initiating event is specified as a probability of a drop per cask.

Canister Drop from Above Operational Height. This initiating event accounts for the potential impact to the TAD canister due to having been dropped from above the normal operational height (for example, due to two-blocking) during transfer by the CTM. The probability of drop per transfer is modeled as a fault tree as described in Section 6.2.2.4. The initiating event is specified as a probability of a drop per cask.

Side Impact to Canister. This initiating event covers the potential side impact to the TAD canister as it being lifted and transferred by the CTM. This event is modeled as a fault tree and is listed in Section 6.2.2.4. The initiating event is specified as a probability of impact per cask. The following initiating event name is assigned in the SAPHIRE rules file associated with the initiating event. The following two fault trees are linked to the initiating event with an OR gate at the fault-tree level in SAPHIRE.

Canister Drop inside CTM Shielding Bell. This initiating event covers the potential impact to the TAD canister due to the drop of a heavy object such as the CTM bell. This event is modeled as a fault tree and is listed in Section 6.2.2.4. The initiating event is specified as a probability of object drop per cask.

Spurious Movement of TAD Canister. This initiating event results from spurious site transporter movement or CTM bell movement.

Canister Drop Inside Bell. This initiating event describes a drop inside the CTM bell due to either human or mechanical failures.

Table A4.13-8. Initiating Event Assignments for WHF-ESD13-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of Cask From Operational Height	WHF-ESD13-TAD	ESD13-TAD-DROP	CTM-DROP---ALL-HEIGHTS and 050-LIFTS-PER-TAD-CAN
Drop of Cask Above Operational Height	WHF-ESD13-TAD	ESD13-TAD-TWOBLOCK	CTM-2-BLOCK and 050-LIFTS-PER-TAD-CAN
Side Impact of Canister	WHF-ESD13-TAD	ESD13-TAD-SIDEIMPACT	ESD13-TAD-SIDEIMPACT
Drop on Canister	WHF-ESD13-TAD	ESD13-TAD-DROPON	CTM-DROP-ONTO-CASK and 050-CTMOBJLIFTNUMBERD
Spurious Movement	WHF-ESD13-TAD	ESD13-TAD-SPURMOVE	ESD13-TAD-SPURMOVE
Canister Drop Inside Bell	WHF-ESD13-TAD	ESD13-TAD-DROPBELL	CTM-DROP-IN-SHIELD-BELL and 050-LIFTS-PER-TAD-CAN

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.13.2.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.13-9 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-9. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD13-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD13-TAD	ESD13-TAD-DROP	CANISTER-DROP	CANISTER-FAILS-DROP
	ESD13-TAD-TWOBLOCK	CANISTER-TWOBLOCK	CANISTER-FAIL-TWOBLOCK
	ESD13-TAD-SIDEIMPACT	CANISTER-IMPACT	CANISTER-FAIL-IMPACT
	ESD13-TAD-DROPON	CANISTER-DROP	CANISTER-FAILS-DROP
	ESD13-TAD-SPURMOVE	CANISTER-SHEAR	CANISTER-SHEAR-CTM
	ESD13-TAD-DROPBELL	CANISTER-DROP	CANISTER-FAILS-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.13-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-10. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD13-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD13-TAD	ESD13-TAD-DROP	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-TAD-TWOBLOCK	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-TAD-SIDEIMPACT	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-TAD-DROPON	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD13-TAD-SPURMOVE	SHIELD-LOSS	SHIELD-TOTAL-LOSS
	ESD13-TAD-DROPBELL	SHIELD-CTM	SHIELD-FAIL-CTM

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.13-11 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-11. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD13-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD13-TAD	ESD13-TAD-DROP	CONFINEMENT	HVAC
	ESD13-TAD-TWOBLOCK		
	ESD13-TAD-SIDEIMPACT		
	ESD13-TAD-DROPON		
	ESD13-TAD-SPURMOVE		
	ESD13-TAD-DROPBELL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.13-12 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.13-12. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD13-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD13-TAD	ESD13-TAD-DROP	MODERATOR	MODERATOR
	ESD13-TAD-TWOBLOCK		
	ESD13-TAD-SIDEIMPACT		
	ESD13-TAD-DROPON		
	ESD13-TAD-SPURMOVE		
	ESD13-TAD-DROPBELL		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.14 EVENT TREES FOR WHF-ESD14-DPC

This ESD delineates the event sequences that arise after a structural challenge during movement of transportation cask/DPC on CTT from the Cask Unloading Room to the preparation station.

The STC is bolted and provides confinement.

Although the initiator event trees transfer to the same response tree (see Table A4.14-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.14-1. Summary of Event Trees for WHF-ESD14-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD14-DPC TAD Response: RESPONSE-STC1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.14.1 Initiating Events for WHF-ESD14-DPC

The following initiating events are associated with WHF-ESD14-DPC involving movement from the cask unloading room to the preparation station. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.14-2.

Side Impact to CTT-Transportation Cask/DPC. This initiating event describes a collision of the CTT with a WHF structure as described in Section 6.2.2.2.

CTT or Transportation Cask/DPC Catches Crane Hook/Rigging Leading to Tip Over. This initiating event describes CTT tipover due to a human error event as described in Section 6.2.2.2.

Table A4.14-2. Initiating Event Assignments for WHF-ESD14

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to CTT-transportation cask/DPC	WHF-ESD14-DPC	ESD14-DPC-IMPACT	050-CTT-COLLIDE
CTT or transportation cask/DPC catches crane hook/rigging leading to tip over	WHF-ESD14-DPC	ESD14-DPC-TIP	050-OPTIPOVER3-HFI-NOD

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.14.2 System Response Event Tree RESPONSE-STC1

The pivotal events that appear in RESPONSE-STC1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.14-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.14-3. Basic Event Associated with the STC Pivotal Events of WHF-ESD14-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD14-DPC	ESD14-DPC-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD14-DPC-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.14-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.14-4. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD14-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD14-DPC	ESD14-DPC-IMPACT	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD14-DPC-TIP	CANISTER-FAIL	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.11-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.14-5. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD14-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD14-DPC	ESD14-DPC-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD14-DPC-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.14-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.14-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD14-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD14-DPC	ESD14-DPC-IMPACT	CONFINEMENT	HVAC
	ESD14-DPC-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.14-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.14-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD14-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD14-DPC	ESD14-DPC-IMPACT	MODERATOR	MODERATOR
	ESD14-DPC-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.15 EVENT TREES FOR WHF-ESD15-DPC

This ESD delineates the event sequences that arise from structural challenges during movement of STC/DPC from the preparation station to the DPC cutting station.

The STC is bolted and provides confinement.

Although the initiator event trees transfer to the same response tree (see Table A4.15-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.15-1. Summary of Event Trees for WHF-ESD15-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD15-DPC STC Response: RESPONSE-STC1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.15.1 Initiating Events for WHF-ESD15-DPC

The following initiating events are associated with WHF-ESD15-DPC involving movement from the cask unloading room to the preparation station. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.15-2.

Table A4.15-2. Initiating Event Assignments for WHF-ESD15-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to STC/DPC	WHF-ESD15-DPC	ESD15-PREP-SIMPACT	050-OPCTCOLLIDE3-HFI-NOD
Drop of heavy load on STC/DPC	WHF-ESD15-DPC	ESD15-PREP-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-DPC-CUT-TRAN
Drop of STC/DPC at operational height	WHF-ESD15-DPC	ESD15-PREP-DROP	050-CHC-CSKDROP-CRN-DRP and 050-STCLIFTS-DPC-CUT
Drop of STC/DPC above operational height	WHF-ESD15-DPC	ESD15-PREP-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and 050-STCLIFTS-DPC-CUT
STC/DPC tips over after being in placed in DPC cutting station	WHF-ESD15-DPC	ESD15-PREP-TIP	050-OPTIPOVER006-HFI-NOD

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.15.2 System Response Event Tree RESPONSE-STC1

The pivotal events that appear in RESPONSE-STC1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.15-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.15-3. Basic Event Associated with the STC Pivotal Events of WHF-ESD15-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD15-DPC	ESD15-PREP-SIMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD15-PREP-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD15-PREP-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD15-PREP-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD15-PREP-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.15-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.15-4. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD15-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD15-DPC	ESD15-PREP-SIMPACT	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD15-PREP-DROPON		
	ESD15-PREP-DROP		
	ESD15-PREP-TWOBLOCK		
	ESD15-PREP-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.15-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.15-5. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD15-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD15-DPC	ESD15-PREP-SIMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD15-PREP-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD15-PREP-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD15-PREP-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD15-PREP-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.15-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.15-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD15-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD15-DPC	ESD15-PREP-SIMPACT	CONFINEMENT	HVAC
	ESD15-PREP-DROPON		
	ESD15-PREP-DROP		
	ESD15-PREP-TWOBLOCK		
	ESD15-PREP-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.15-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.15-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD15-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD15-DPC	ESD15-PREP-SIMPACT	MODERATOR	MODERATOR
	ESD15-PREP-DROPON		
	ESD15-PREP-DROP		
	ESD15-PREP-TWOBLOCK		
	ESD15-PREP-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.16 EVENT TREES FOR WHF-ESD16-CSNF

This ESD delineates the event sequences that arise after a structural challenge during transportation cask/commercial SNF preparation activities prior to moving to pool.

Although the initiator event trees transfer to the same response tree (see Table A4.16-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.16-1. Summary of Event Trees for WHF-ESD16-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD16-CSNF STC Response: RESPONSE-PREPSTATION	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.16.1 Initiating Events for WHF-ESD16-CSNF

The following initiating events are associated with WHF-ESD16 involving movement from the cask unloading room to the preparation station. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.16-2.

Table A4.16-2. Initiating Event Assignments for WHF-ESD16-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Impact to transportation cask valve	WHF-ESD16-CSNF	ESD16-PREP-VALVEIMP	ESD16-PREP-VALVEIMP
Sampling line break	WHF-ESD16-CSNF	ESD16-PREP-SAMPLE	ESD16-PREP-SAMPLE
Cask overpressure	WHF-ESD16-CSNF	ESD16-PREP-OVERPRESSURE	OVERPRESSURIZATION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.16.2 System Response Event Tree PREPSTATION

The pivotal events that appear in PREPSTATION are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CONFINEMENT. Table A4.16-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.16-3. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD16-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD16-CSNF	ESD16-PREP-VAVEIMP	HVAC-PREP	HVAC-FAIL-DURING-PREP
	ESD16-PREP-SAMPLE		
	ESD16-PREP-OVERPRESSURE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.16-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.16-4. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD16-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD16-CSNF	ESD16-PREP-SIMPACT	MODERATOR-SAMPLING	MODERATOR-NONE
	ESD16-PREP-DROPON		
	ESD16-PREP-OVERPRESSURE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.17 EVENT TREES FOR WHF-ESD17-DPC

This ESD delineates the event sequences that arise from structural challenges during transportation cask/DPC preparation activities prior to DPC lid cutting.

Although the initiator event trees transfer to the same response tree (see Table A4.17-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.17-1. Summary of Event Trees for WHF-ESD17-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD17-DPC STC Response: RESPONSE-PREPSTATION	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.17.1 Initiating Events for WHF-ESD17-DPC

The following initiating events are associated with WHF-ESD17-DPC involving movement from the cask unloading room to the preparation station. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.17-2 and are described in Section 6.2.2.10.

Table A4.17-2. Initiating Event Assignments for WHF-ESD17-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Impact to canister valves	WHF-ESD17-DPC	ESD17-PREP-VALVEIMP	ESD17-PREP-VALVEIMP
Sampling line break	WHF-ESD17-DPC	ESD17-PREP-SAMPLE	ESD17-PREP-SAMPLE
Overpressurization of canister	WHF-ESD17-DPC	ESD17-PREP-OVERPRESSURE	OVERPRESURIZATION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.17.2 System Response Event Tree PREPSTATION

The pivotal events that appear in PREPSTATION are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CONFINEMENT. Table A4.17-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.17-3. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD17-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD17-DPC	ESD17-PREP-VALVEIMP	HVAC-PREP	HVAC-FAIL-DURING-PREP
	ESD17-PREP-SAMPLE		
	ESD17-PREP-OVERPRESSURE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.17-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.17-4. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD17-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD17-DPC	ESD17-PREP-SIMPACT	MODERATOR-SAMPLING	MODERATOR-NONE
	ESD17-PREP-DROPON		
	ESD17-PREP-OVERPRESSURE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.18 EVENT TREES FOR WHF-ESD18-DPC

This ESD delineates the event sequences that arise from structural challenges with the STC/DPC preparation activities at the DPC cutting station.

Although the initiator event trees transfer to the same response tree (see Table A4.18-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.18-1. Summary of Event Trees for WHF-ESD18-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD18-DPC STC Response: RESPONSE-PREPSTATION	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.18.1 Initiating Events for WHF-ESD18-DPC

The following one initiating event is associated with WHF-ESD18-DPC involving STC/DPC preparation activities at the DPC cutting station. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.18-2.

Table A4.18-2. Initiating Event Assignments for WHF-ESD18-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of heavy load on canister vent or port line	WHF-ESD18-DPC	ESD18-DPC-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-DPC-CUT-TRAN

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.18.2 System Response Event Tree PREPSTATION

The pivotal events that appear in PREPSTATION are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CONFINEMENT. Table A4.18-3 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.18-3. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD18-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD18-DPC	ESD18-DPC-DROPON	HVAC-PREP	HVAC-FAIL-DURING-PREP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.18-3 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.18-3. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD18-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD18-DPC	ESD18-DPC-DROPON	MODERATOR-SAMPLING	MODERATOR-NONE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.19 EVENT TREES FOR WHF-ESD19-DPC

A4.19.1 Event Trees for WHF-ESD19 (Drop in Pool)

This ESD delineates the event sequences that arise after a structural challenge to a STC with a DPC during the transfer from the DPC cutting station to the pool ledge. This ESD considers drops in the pool.

Although the initiator event trees transfer to the same response tree (see Table A4.19-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.19-1. Summary of Event Trees for WHF-ESD19-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD19-DPC STC Response: RESPONSE-POOLMOVE	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.19.1.1 Initiating Events for WHF-ESD19 (Drop in Pool)

The following initiating events are associated with WHF-ESD19-DPC involving transfer of STC/DPC from the DPC cutting station to the pool ledge that lead to a drop in the pool. The

assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.19-2.

Table A4.19-2. Initiating Event Assignments for WHF-ESD19-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to cask	WHF-ESD19-DPC	ESD19-POOL-IMPACT	050-OPTCIMPACT06-HFI-NOD and TIME-OVER-POOL-TO-POOL
Drop of heavy load on cask	WHF-ESD19-DPC	ESD19-POOL-DROPON	POOL-OBJDROPON
Drop of cask at operational height	WHF-ESD19-DPC	ESD19-POOL-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-POOL-TO-POOL
Drop of cask above operational height	WHF-ESD19-DPC	ESD19-POOL-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-POOL-TO-POOL
Cask tips over	WHF-ESD19-DPC	ESD19-POOL-TIP	050-OPTIPOVER007-HFI-NOD and TIME-OVER-POOL-TO-POOL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.19.1.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.19-3 indicates the basic event that is associated with this pivotal event for the initiating event.

Table A4.19-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-POOL-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
WHF-ESD19-DPC	ESD19-POOL-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
WHF-ESD19-DPC	ESD19-POOL-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
WHF-ESD19-DPC	ESD19-POOL-TWOBLOCK	CASK-FAIL	CASK-FAILS
WHF-ESD19-DPC	ESD19-POOL-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

Source: Original

BORON. Table A4.19-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-4. Basic Event Associated with the BORON Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-POOL-IMPACT	BORON	BORON-SYSTEM-FAILS
WHF-ESD19-DPC	ESD19-POOL-DROPON	BORON	
WHF-ESD19-DPC	ESD19-POOL-DROP	BORON	
WHF-ESD19-DPC	ESD19-POOL-TWOBLOCK	BORON	
WHF-ESD19-DPC	ESD19-POOL-TIP	BORON	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.19.2 Event Trees for WHF-ESD19-DPC (Drop on Floor)

This ESD delineates the event sequences that arise after a structural challenge to a STC with a DPC during the transfer from the DPC cutting station to the pool ledge. This ESD considers drops on WHF floor.

Although the initiator event trees transfer to the same response tree (see Table A4.19-5 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.19-5. Summary of Event Trees for WHF-ESD19-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD19-DPC STC Response: RESPONSE-STC1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.19.2.1 Initiating Events for WHF-ESD19 (Drop on Floor)

The following initiating events are associated with WHF-ESD19-DPC involving transfer of the STC/DPC from the DPC cutting station to the pool ledge that lead to a drop on the floor. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.19-6.

Table A4.19-6. Initiating Event Assignments for WHF-ESD19-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to cask	WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	050-OPTCIMPACT06-HFI-NOD and TIME-OVER-FLOOR-TO-POOL
Drop of heavy load on cask	WHF-ESD19-DPC	ESD19-FLOOR-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-POOL-TRANS
Drop of cask at operational height	WHF-ESD19-DPC	ESD19-FLOOR-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-FLOOR-TO-POOL
Drop of cask above operational height	WHF-ESD19-DPC	ESD19-FLOOR-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-FLOOR-TO-POOL
Cask tips over	WHF-ESD19-DPC	ESD19-FLOOR-TIP	050-OPTIPOVER007-HFI-NOD and TIME-OVER-FLOOR-TO-POOL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.19.2.2 System Response Event Tree RESPONSE-STC1

The pivotal events that appear in RESPONSE-STC1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.19-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-7. Basic Event Associated with the CASK Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD19-FLOOR-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD19-FLOOR-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD19-FLOOR-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD19-FLOOR-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.19-8 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-8. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD19-FLOOR-DROPON		
	ESD19-FLOOR-DROP		
	ESD19-FLOOR-TWOBLOCK		
	ESD19-FLOOR-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.19-9 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-9. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD19-FLOOR-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD19-FLOOR-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD19-FLOOR-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD19-FLOOR-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.19-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-10. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	CONFINEMENT	HVAC
	ESD19-FLOOR-DROPON		
	ESD19-FLOOR-DROP		
	ESD19-FLOOR-TWOBLOCK		
	ESD19-FLOOR-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.19-11 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.19-11. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD19-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD19-DPC	ESD19-FLOOR-IMPACT	MODERATOR	MODERATOR
	ESD19-FLOOR-DROPON		
	ESD19-FLOOR-DROP		
	ESD19-FLOOR-TWOBLOCK		
	ESD19-FLOOR-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.20 EVENT TREES FOR WHF-ESD20

A4.20.1 Event Trees for WHF-ESD20-CSNF (Drop in Pool)

This ESD delineates the event sequences that arise after a structural challenge to a transportation cask with bare commercial SNF during the transfer from the preparation station to the pool ledge. This ESD considers drops in the pool.

Although the initiator event trees transfer to the same response tree (see Table A4.20-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.20-1. Summary of Event Trees for WHF-ESD20-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD20-CSNF Response: RESPONSE-POOLMOVE	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.226, Table 4)

A4.20.1.1 Initiating Events for WHF-ESD20-CSNF

The following initiating events shown in Table A4.20-2 are associated with WHF-ESD20-CSNF involving transportation cask with bare commercial SNF during the transfer from the preparation station to the pool ledge.

Table A4.20-2. Initiating Event Assignments for WHF-ESD20-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to cask	WHF-ESD20-DPC	ESD20-POOL-IMPACT	050-OPTCIMPACT06-HFI-NOD and TIME-OVER-POOL-TO-POOL
Drop of cask at operational height		ESD20-POOL-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-POOL-TO-POOL
Drop of cask above operational height		ESD20-POOL-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-POOL-TO-POOL
Cask tips over		ESD20-POOL-TIP	050-OPTIPOVER007-HFI-NOD and TIME-OVER-POOL-TO-POOL
Drop of heavy load on cask		ESD20-POOL-DROPON	POOL-OBJDROPON

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.20.1.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.20-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.20-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD20- CSNF	ESD20-POOL-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD20-POOL-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD20-POOL-TWOBLOCK	CASK-FAIL	CASK-FAILS
	ESD20-POOL-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD20-POOL-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

BORON. Table A4.20-4 indicates the basic event that is associated with this pivotal event for each initiating event t.

Table A4.20-4. Basic Event Associated with the BORON Pivotal Events of WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD20- CSNF	ESD20-POOL-IMPACT	BORON	BORON-SYSTEM-FAILS
	ESD20-POOL-DROP		
	ESD20-POOL-TWOBLOCK		
	ESD20-POOL-TIP		
	ESD20-POOL-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.20.2 Event Trees for WHF-ESD20 (Drop on Floor)

This ESD delineates the event sequences that arise after a structural challenge to a transportation cask with bare commercial SNF during the transfer from the preparation station to the pool ledge. This ESD considers drops in the pool.

Although the initiator event trees transfer to the same response tree (see Table A4.20-5 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.20-5. Summary of Event Trees for WHF-ESD20-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD20-CSNF Response: RESPONSE-TCASK-CSNF	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.20.2.1 Initiating Events for WHF-ESD20-CSNF

The following initiating events shown in Table A4.20-6 are associated with WHF-ESD20 involving transfer transportation cask with bare commercial SNF during the transfer from the preparation station to the pool ledge.

Table A4.20-6. Initiating Event Assignments for WHF-ESD20-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Side impact to cask	WHF-ESD20-CSNF	ESD20-FLOOR-IMPACT	050-OPTCIMPACT06-HFI-NOD and TIME-OVER-FLOOR-TO-POOL
Drop of cask at operational height		ESD20-FLOOR-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-FLOOR-TO-POOL
Drop of cask above operational height		ESD20-FLOOR-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-FLOOR-TO-POOL
Cask tips over		ESD20-FLOOR-TIP	050-OPTIPOVER007-HFI-NOD and TIME-OVER-FLOOR-TO-POOL
Drop of heavy load on cask		ESD20-FLOOR-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-POOL-TRANS

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.20.2.2 System Response Event Tree RESPONSE-TCASK-CSNF

The pivotal events that appear in RESPONSE-TCASK-CSNF are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.20-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.20-7. Basic Event Associated with the CASK Pivotal Events for WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD20-CSNF	ESD20-FLOOR-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD20-FLOOR-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD20-FLOOR-TWOBLOCK	CASK- TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD20-FLOOR-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD20-FLOOR-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.20-8 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.20-8. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD20-CSNF	ESD20-FLOOR-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD20-FLOOR-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD20-FLOOR-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD20-FLOOR-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD20-FLOOR-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.20-9 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.20-9. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD20-CSNF	ESD20-FLOOR-IMPACT	CONFINEMENT	HVAC
	ESD20-FLOOR-DROP		
	ESD20-FLOOR-TWOBLOCK		
	ESD20-FLOOR-TIP		
	ESD20-FLOOR-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.20-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.20-10. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD20-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD20-CSNF	ESD20-FLOOR-IMPACT	MODERATOR	MODERATOR
	ESD20-FLOOR-DROP		
	ESD20-FLOOR-TWOBLOCK		
	ESD20-FLOOR-TIP		
	ESD20-FLOOR-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21 EVENT TREES FOR WHF-ESD21

This ESD delineates the event sequences that arise after a structural challenge to a cask that occurs during lowering of the cask to the pool floor. This ESD applies to uncanistered commercial SNF in a transportation cask.

Release into the pool is considered a filtered release. Because of the potential drop height, the ability of the cask to maintain integrity is not included in this event sequence. In effect, this means that the cask is modeled as failing open in this ESD.

Although the initiator event trees transfer to the same response tree (see Table A4.21-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.21-1. Summary of Event Trees for WHF-ESD21-CSNF

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation casks containing bare SNF assemblies (9 BWR or 4 PWR SNF assemblies per cask)	Initiator: WHF-ESD21-CSNF Response: RESPONSE-POOLMOVE	3,775

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.21.1 Event Trees for WHF-ESD21-TC/CSNF

A4.21.1.1 Initiating Events for WHF-ESD21-CSNF

The following initiating events shown in Table A4.21-2 are associated with WHF-ESD21-CSNF involving transportation cask with bare commercial SNF to the pool floor.

Table A4.21-2. Initiating Event Assignments for WHF-ESD21-CSNF

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of transportation cask	WHF-ESD21-CSNF	ESD21-CSNF-LOWER-DROP	050-CHC-CSKDROP-CRN-DRP
Impact to transportation cask		ESD21-CSNF-LOWER-IMPACT	050-OPTCIMPACT07-HFI-NOD
Tipover of transportation cask		ESD21-CSNF-LOWER-TIP	050-OPTIPOVER-HFI-NOD
Drop onto transportation cask		ESD21-CSNF-LOWER-DROPON	ESD21-CSNF-LOWER-DROPON

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21.1.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in RESPONSE-POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.21-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD21-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD21-CSNF	ESD21-CSNF-LOWER-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-CSNF-LOWER-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD21-CSNF-LOWER-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-CSNF-LOWER-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

BORON. Table A4.21-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-4. Basic Event Associated with the BORON Pivotal Events of WHF-ESD21-CSNF

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD21-CSNF	ESD21-CSNF-LOWER-DROP	BORON	BORON-SYSTEM-FAILS
	ESD21-CSNF-LOWER-IMPACT		
	ESD21-CSNF-LOWER-TIP		
	ESD21-CSNF-LOWER-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21.2 Event Trees for WHF-ESD21 (STC/DPC)

This ESD delineates the event sequences that arise after a structural challenge to a cask that occurs during lowering of the cask to the pool floor. This ESD applies to DPCs contained in STCs.

Release into the pool is considered a filtered release. Because of the potential drop height, the ability of the cask to maintain integrity is not included in this event sequence. In effect, this means that the cask is modeled as failing open in this ESD.

Although the initiator event trees transfer to the same response tree (see Table A4.21-5), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.21-5. Summary of Event Trees for WHF-ESD21-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
STC containing a DPC	Initiator: WHF-ESD21-DPC STC Response: RESPONSE-POOLMOVE	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.21.2.1 Initiating Events for WHF-ESD21-DPC

The following initiating events shown in Table A4.21-6 are associated with WHF-ESD21-DPC involving transfer of an STC containing a DPC to the pool floor.

Table A4.21-6. Initiating Event Assignments for WHF-ESD21-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of shielded transfer cask	WHF-ESD21-DPC	ESD21-DPC-LOWER-DROP	050-CHC-CSKDROP-CRN-DRP
Impact to shielded transfer cask		ESD21-DPC-LOWER-IMPACT	050-OPTCIMPACT07-HFI-NOD
Drop onto shielded transfer cask		ESD21-DPC-LOWER-DROPON	ESD21-DPC-LOWER-DROPON
Tipover of shielded transfer cask		ESD21-DPC-LOWER-TIP	050-OPTIPOVER008-HFI-NOD

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21.2.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in RESPONSE-POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.21-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-7. Basic Event Associated with the CASK Pivotal Events of WHF-ESD21-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD21-DPC	ESD21-DPC-LOWER-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-DPC-LOWER-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD21-DPC-LOWER-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-DPC-LOWER-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

BORON. Table A4.21-8 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-8. Basic Event Associated with the BORON Pivotal Events of WHF-ESD21-DPC

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD21-DPC	ESD21-DPC-LOWER-DROP	BORON	BORON-SYSTEM-FAILS
WHF-ESD21-DPC	ESD21-DPC-LOWER-IMPACT	BORON	
WHF-ESD21-DPC	ESD21-DPC-LOWER-TIP	BORON	
WHF-ESD21-DPC	ESD21-DPC-LOWER-DROPON	BORON	

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21.3 Event Trees for WHF-ESD21-TAD

This sequence represents a structural challenge to a TAD canister resulting in an unfiltered radionuclide release due to an impact to a cask, a drop of a heavy object onto the cask a tip over, or a cask drop. In this sequence the TAD canister falls on the pool floor. The TAD canister is contained in an STC that is bolted.

Release into the pool is considered a filtered release. Because of the potential drop height in the pool, drop of the cask into the bottom of the pool is believed to have a probability of one.

Although the initiator event trees transfer to the same response tree (see Table A4.21-9 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.21-9. Summary of Event Trees for WHF-ESD21-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD21-TAD STC Response: RESPONSE-POOLMOVE	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.21.3.1 Initiating Events for WHF-ESD21-TAD

The following initiating events shown in Table A5.21-10 are associated with WHF-ESD21-TAD involving transfer of an STC containing a TAD canister out of the pool.

Table A4.21-10. Initiating Event Assignments for WHF-ESD21-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop of STC	WHF-ESD21-TAD	ESD21-TAD-LOWER-DROP	050-CHC-CSKDROP-CRN-DRP
Impact to STC	WHF-ESD21-TAD	ESD21-TAD-LOWER-IMPACT	050-OPTCIMPACT08-HFI-COD
Drop onto STC	WHF-ESD21-TAD	ESD21-TAD-LOWER-DROPON	050-PHC-OBJDROP-CRN-DRP and 050-OBJLIFT-POOL-FLOOR
Tipover of STC	WHF-ESD21-TAD	ESD21-TAD-LOWER-TIP	050-OPTIPOVER009-HFI-COD

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.21.3.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in RESPONSE-POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.21-11 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-11. Basic Event Associated with the CASK Pivotal Events of WHF-ESD21-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD21-TAD	ESD21-TAD-LOWER-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-TAD-LOWER-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD21-TAD-LOWER-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD21-TAD-LOWER-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

BORON. Table A4.21-12 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.21-12. Basic Event Associated with the BORON Pivotal Events of WHF-ESD21-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD21-TAD	ESD21-TAD-LOWER-DROP	BORON	BORON-SYSTEM-FAILS
	ESD21-TAD-LOWER-IMPACT		
	ESD21-TAD-LOWER-TIP		
	ESD21-TAD-LOWER-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.22 EVENT TREES FOR WHF-ESD22-FUEL

This sequence represents a structural challenge to a fuel assembly in the pool resulting in an unfiltered gaseous radionuclide release due to a drop of the assembly at the operational height.

Although the initiator event trees transfer to the same response tree (see Table A4.22-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.22-1. Summary of Event Trees for WHF-ESD22-FUEL

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
	Initiator: WHF-ESD22-FUEL STC Response: RESPONSE-POOLCONFINE	

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.22.1 Initiating Events for WHF-ESD22-FUEL

The following initiating events shown in Table A4.22-2 are associated with WHF-ESD22-FUEL involving transfer of spent fuel assemblies to either a TAD canister or staging rack.

Table A4.22-2. Initiating Event Assignments for WHF-ESD22-FUEL

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop on Rack	WHF-ESD22-FUEL	ESD22-FUEL-DROPRACK	050-SFTM-FUELDRP-RACK
Drop of Bundle		ESD22-FUEL- DROP	050-SFTM-FUELDRP-SFT-DPR

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.22.2 System Response Event Tree RESPONSE-POOLCONFINE

The pivotal events that appear in RESPONSE-POOLMOVE are summarized below. With drop of the spent fuel assembly, the only issue is whether Boron concentration is maintained.

BORON. Table A4.22-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.22-3. Basic Event Associated with the BORON Pivotal Events of WHF-ESD22-FUEL

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD22-FUEL	ESD22-FUEL-DROPRACK	BORON	BORON-SYSTEM-FAILS
	ESD22-FUEL-DROP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.23 EVENT TREES FOR WHF-ESD23-POOL

This ESD delineates the event sequences that arise after a spill of contaminated water due to a mishandling of low level liquid waste during pool operations.

The assignment for initiating events for this sequence is given in Table A4.23-4.

Table A4.23-4. Summary of Event Trees for WHF-ESD23-POOL

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
	Initiator: WHF-ESD23-POOL	Low Level Liquid Waste

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.23.1 Initiating Events for WHF-ESD23-POOL

The following initiating events shown in Table A4.23-5 are associated with WHF-ESD23-POOL involving mishandling of low level liquid waste during pool operations. All end states result in direct exposure.

Table A4.23-5. Initiating Event Assignments for WHF-ESD23-POOL

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Mishap in pool cleanup	WHF-ESD23-POOL	ESD23-LLW-CLEANUP	050-LLW-CLEANUP
Mishap in pool recirculation		ESD23-LLW-RECIRC	050-LLW-RECIRC-PPM-RUP
Drop of pool filters		ESD23-LLW-DROP	050-OP-FILTER-EXPOSE and FILTER-NUMBER
Improper decontamination of DPC/STC		ESD23-LLW-DECON	050-LLW-DECON-FAIL
Spill of pool water from collision		ESD23-LLW-COLLISION	050-LLW-COLLISION

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.23.2 System Response Event Tree

There is no response tree since the above events result in direct exposure.

A4.24 EVENT TREES FOR WHF-ESD24-TAD

A4.24.1 Event Trees for WHF-ESD24-TAD (Drop in Pool)

This ESD delineates the event sequences that arise after a structural challenge resulting from collisions of the STC/TAD canister with structure or equipment. This includes events that occur while the TAD canister is not closed and the STC/TAD canister being transferred from the pool ledge to the TAD canister closure station. The STC is bolted. This ESD considers drops in the pool.

Although the initiator event trees transfer to the same response tree (see Table A4.24-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.24-1. Summary of Event Trees for WHF-ESD24-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD24-TAD STC Response: RESPONSE-POOLMOVE	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.24.1.1 Initiating Events for WHF-ESD24-TAD

The following initiating events are associated with WHF-ESD24-TAD involving transfer of the STC/TAD canister being transferred from the pool ledge to the TAD canister closure station that lead to a drop in the pool. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.24-2.

Table A4.24-2. Initiating Event Assignments for WHF-ESD24-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Impact of STC/TAD - pool	WHF-ESD24-TAD	ESD24-POOL-IMPACT	050-OPTCIMPACT09-HFI-NOD and TIME-OVER-POOL-TO-CLOSE
Drop at operational height - pool		ESD24-POOL-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-POOL-TO-CLOSE
Drop above operational height - pool		ESD24-POOL-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-POOL-TO-CLOSE
Tip over of STC/TAD - pool		ESD24-POOL-TIP	050-OPTIPOVER010-HFI-NOD and TIME-OVER-POOL-TO-CLOSE
Drop on STC/TAD - pool		ESD24-POOL-DROPON	POOL-OBJDROPON

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.24.1.2 System Response Event Tree RESPONSE-POOLMOVE

The pivotal events that appear in POOLMOVE are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CASK. Table A4.24-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-3. Basic Event Associated with the CASK Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CASK	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-POOL-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD24-POOL-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD24-POOL-TWOBLOCK	CASK-FAIL	CASK-FAILS
	ESD24-POOL-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD24-POOL-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

BORON. Table A4.24-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-4. Basic Event Associated with the BORON Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to BORON	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-POOL-IMPACT	BORON	BORON-SYSTEM-FAILS
WHF-ESD24-TAD	ESD24-POOL-DROP		
WHF-ESD24-TAD	ESD24-POOL-TWOBLOCK		
WHF-ESD24-TAD	ESD24-POOL-TIP		
WHF-ESD24-TAD	ESD24-POOL-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.24.2 Event Trees for WHF-ESD24-TAD (Drop on Floor)

This ESD delineates the event sequences that arise after a structural challenge resulting from collisions of the STC/TAD canister with structure or equipment. This includes events that occur while the TAD canister is not closed and the STC/TAD canister being transferred from the pool ledge to the TAD canister closure station. This ESD considers drops on floor.

Although the initiator event trees transfer to the same response tree (see Table A4.24-5), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.24-5. Summary of Event Trees for WHF-ESD24-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD24-TAD STC Response: RESPONSE-STC1	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.24.2.1 Initiating Events for WHF-ESD24-TAD

The following initiating events are associated with WHF-ESD24-TAD involving transfer of the STC/TAD canister being transferred from the pool ledge to the TAD canister closure station that lead to a drop on the floor. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.24-6.

Table A4.24-6. Initiating Event Assignments for WHF-ESD24-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Impact of STC/TAD - pool	WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	050-OPTCIMPACT09-HFI-NOD AND TIME-OVER-FLOOR-TO-CLOSE
Drop at operational height - pool	WHF-ESD24-TAD	ESD24-FLOOR-DROP	050-CHC-CSKDROP-CRN-DRP and TIME-OVER-FLOOR-TO-CLOSE
Drop above operational height - pool	WHF-ESD24-TAD	ESD24-FLOOR-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and TIME-OVER-FLOOR-TO-CLOSE
Tip over of STC/TAD - pool	WHF-ESD24-TAD	ESD24-FLOOR-TIP	050-OPTIPOVER010-HFI-NOD AND TIME-OVER-FLOOR-TO-CLOSE
Drop on STC/TAD - pool	WHF-ESD24-TAD	ESD24-FLOOR-DROPON	050-JIBCRANE-CRJ-DRP and TIME-OVER-FLOOR-TO-CLOSE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.24.2.2 System Response Event Tree RESPONSE-STC1

The pivotal events that appear in RESPONSE-STC1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.24-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-7. Basic Event Associated with the STC Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to STC	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT
	ESD24-FLOOR-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD24-FLOOR-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD24-FLOOR-TIP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD24-FLOOR-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.24-8 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-8. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD24-FLOOR-DROP		
	ESD24-FLOOR-TWOBLOCK		
	ESD24-FLOOR-TIP		
	ESD24-FLOOR-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.24-9 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-9. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD24-FLOOR-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD24-FLOOR-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD24-FLOOR-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD24-FLOOR-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.24-10 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-10. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	CONFINEMENT	HVAC
	ESD24-FLOOR-DROP		
	ESD24-FLOOR-TWOBLOCK		
	ESD24-FLOOR-TIP		
	ESD24-FLOOR-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.24-11 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.24-11. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD24-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD24-TAD	ESD24-FLOOR-IMPACT	MODERATOR	MODERATOR
	ESD24-FLOOR-DROP		
	ESD24-FLOOR-TWOBLOCK		
	ESD24-FLOOR-TIP		
	ESD24-FLOOR-DROPON		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.25 EVENT TREES FOR WHF-ESD25-TAD

This ESD delineates the event sequences that arise after a structural challenge that occurs during the assembly and closure of the STC/TAD canister.

Although the initiator event trees transfer to the same response tree (see Table A4.25-1 below), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.25-1. Summary of Event Trees for WHF-ESD25-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD25-TAD STC Response: RESPONSE-TAD	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.25.1 Initiating Events for WHF-ESD25-TAD

The following initiating events are associated with WHF-ESD25-TAD involving assembly and closure of the STC/TAD. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.25-2.

Table A4.25-2. Initiating Event Assignments for WHF-ESD25-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Object dropped onto TAD	WHF-ESD25-TAD	ESD25-TAD-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-TAD-CLOSE
Side Impact to TAD	WHF-ESD25-TAD	ESD25-TAD-IMPACT	ESD25-TAD-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.25.2 System Response Event Tree RESPONSE-TAD

The pivotal events that appear in RESPONSE-TAD are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

TAD. Table A4.25-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.25-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD25-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD25-TAD	ESD25-TAD-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD25-TAD-IMPACT	CASK-IMPACT	CASK-FAIL-IMPACT

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.25-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.25-4. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD25-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD25-TAD	ESD25-TAD-DROPON	CONFINEMENT	HVAC
	ESD25-TAD-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.25-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.25-5. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD25-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD25-TAD	ESD25-TAD-DROPON	MODERATOR	MODERATOR
	ESD25-TAD-IMPACT		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.26 EVENT TREES FOR WHF-ESD26-TAD

This ESD delineates the event sequences that arise after a structural challenge that occurs during the assembly and closure of the STC/TAD canister.

Although the initiator event trees transfer to the same response tree (see Table A4.26-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.26-1. Summary of Event Trees for WHF-ESD26-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD26-TAD STC Response: RESPONSE-TADDRY	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.26.1 Initiating Events for WHF-ESD26-TAD

The following initiating events are associated with WHF-ESD26-TAD involving TAD canister drying and inerting. The assignments made within SAPHIRE for quantification of one initiating event is indicated in Table A4.26-2.

Table A4.26-2. Initiating Event Assignments for WHF-ESD26-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Failure to dry TAD	WHF-ESD26-TAD	ESD26-TAD-DRYFAIL	050-TADDRY-FAIL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.26.2 System Response Event Tree RESPONSE-TAD

The pivotal events that appear in RESPONSE-TAD are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

DRYING. Table A4.26-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.26-3. Basic Events Associated with the DRYING Pivotal Events of WHF-ESD26-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to DRYING	Associated Fault Tree or Basic Event[a]
WHF-ESD26-TAD	ESD26-TAD-DRYFAIL	050-TADDRY-FAIL	050-TADDRY-FAIL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

OVERPRESSURE. Table A4.26-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.26-4. Basic Event Associated with the OVERPRESSURE Pivotal Events of WHF-ESD26-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to OVERPRESSURE	Associated Fault Tree or Basic Event[a]
WHF-ESD26-TAD	ESD26-TAD-DRYFAIL	OVERPRESSURE	050-OVERPRESSURE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.27 EVENT TREES FOR WHF-ESD27-TAD

This ESD delineates the event sequences that arise after a structural challenge resulting from the welding, drying, and inerting activities associated with TAD canister closure.

Although the initiator event trees transfer to the same response tree (see Table A4.27-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.27-1. Summary of Event Trees for WHF-ESD27-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
TAD canisters produced at repository (44 BWR or 21 PWR SNF assemblies per canister)	Initiator: WHF-ESD27-TAD STC Response: RESPONSE-PREPSTATION	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.27.1 Initiating Events for WHF-ESD27-TAD

The following initiating events are associated with WHF-ESD27-TAD involving TAD canister drying and inerting. The assignments made within SAPHIRE for quantification of one initiating event is indicated in Table A4.27-2.

Table A4.27-2. Initiating Event Assignments for WHF-ESD27-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Bad weld – improper or cracked	WHF-ESD27-TAD	ESD27-TAD-BADWELD	050-OPWELDDETECT-FAIL
Line break	WHF-ESD27-TAD	ESD27-TAD-LINE	050-TADDRY-HOS-RUP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.27.2 System Response Event Tree RESPONSE-PREPSTATION

The pivotal events that appear in PREPSTATION are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CONFINEMENT. Table A4.27-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.27-3. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD27-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD27-TAD	ESD27-TAD-BADWELD	HVAC-PREP	HVAC-FAIL-DURING-PREP
	ESD27-TAD-LINE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.27-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.27-4. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD27-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD27-TAD	ESD27-TAD-BADWELD	MODERATOR-SAMPLING	MODERATOR-NONE
	ESD27-TAD-LINE		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.28 EVENT TREES FOR WHF-ESD28-TAD

This ESD delineates the event sequences that arise after a structural challenge to a STC that contains a TAD canister during exporting activities.

Although the initiator event trees transfer to the same response tree (see Table A4.28-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic

rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.28-1. Summary of Event Trees for WHF-ESD28-TAD

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD28-TAD DPC Response: RESPONSE-CANISTER1	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.28.1 Initiating Events for WHF-ESD28

The following initiating events are associated with WHF-ESD28-TAD during TAD canister exporting activities. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.28-2.

Table A4.28-2. Initiating Event Assignments for WHF-ESD28-TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Drop on TAD canister	WHF-ESD28-TAD	ESD28-TAD-DROPON	050-JIBCRANE-CRJ-DRP and 050-OBJLIFT-TAD-EXPORT
Drop at operational height		ESD28-TAD-DROP	050-CHC-CSKDROP-CRN-DRP and 050-TADLIFT-TAD-EXPORT
Drop above operational height		ESD28-TAD-TWOBLOCK	050-CHC-TWOBLCK-CRN-TBK and 050-TADLIFT-TAD-EXPORT
Impact to TAD canister		ESD28-TAD-IMPACT	050-OPCTCOLLIDE4-HFI-NOD
TAD canister tipover		ESD28-TAD-TIP	050-OPTIPOVER011-HFI-NOD

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.28.2 System Response Event Tree RESPONSE-CANISTER1

The pivotal events that appear in RESPONSE-CANISTER1 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

STC. Table A4.28-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.28-3. Basic Events Associated with the STC Pivotal Events of WHF-ESD28-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to STC	Associated Fault Tree or Basic Event[a]
WHF-ESD28-TAD	ESD28-TAD-DROPON	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD28-TAD-DROP	CASK-DROP	CASK-DROP-OPERATIONAL
	ESD28-TAD-TWOBLOCK	CASK-TWOBLOCK	CASK-DROP-TWOBLOCK
	ESD28-TAD-IMPACT	CAST-IMPACT	CASK-FAIL-IMPACT
	ESD28-TAD-TIP	CASK-DROP	CASK-DROP-OPERATIONAL

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.28-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.28-4. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD28-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD28-TAD	ESD28-TAD-DROPON	CANISTER-FAIL	CANISTER-IN-CASK-FAIL
	ESD28-TAD-DROP		
	ESD28-TAD-TWOBLOCK		
	ESD28-TAD-IMPACT		
	ESD28-TAD-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.28-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.28-5. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD28-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD28-TAD	ESD28-TAD-DROPON	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD28-TAD-DROP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD28-TAD-TWOBLOCK	SHIELD-CASK-DROP	CASK-SHIELDING-DROP
	ESD28-TAD-IMPACT	SHIELD-CASK-IMPACT	CASK-SHIELDING-IMPACT
	ESD28-TAD-TIP	SHIELD-CASK-DROP	CASK-SHIELDING-DROP

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.28-6 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.28-6. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD28-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD28-TAD	ESD28-TAD-DROPON	CONFINEMENT	HVAC
	ESD28-TAD-DROP		
	ESD28-TAD-TWOBLOCK		
	ESD28-TAD-IMPACT		
	ESD28-TAD-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.28-7 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.28-7. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD28-TAD

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD28-TAD	ESD28-TAD-DROPON	MODERATOR	MODERATOR
	ESD28-TAD-DROP		
	ESD28-TAD-TWOBLOCK		
	ESD28-TAD-IMPACT		
	ESD28-TAD-TIP		

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.29 EVENT TREES FOR WHF-ESD29-DPC

This ESD delineates the event sequences that result in direct exposures from cask preparation activities and CTM movement. The initiating event assigned in SAPHIRE is assigned in Table A4.29-1.

Table A4.29-1. Summary of Event Trees for WHF-ESD29-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD29-DPC	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.29.1 Initiating Events for WHF-ESD29

The following initiating events are associated with WHF-ESD29-DPC during cask preparation activities and CTM movement. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.29-2.

Table A4.29-2. Initiating Event Assignments for WHF-ESD29-DPC and -TAD

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Failure to install shield ring	WHF-ESD29-DPC	ESD29-EXPOSURE-RING	050-OPDPCSHIELD2-HFI-NOW
Loss of CTM shielding during lift	WHF-ESD29-DPC	ESD29-EXPOSURE-CTM	ESD29-EXPOSURE-CTM
DPC lift fixture installed properly	WHF-ESD29-DPC	ESD29-EXPOSURE-LIFT	050-LIDDISPLACE1-HFI-NOD OR 050-OPDPCSHIELD1-HFI-NOW or 050-OPDPCSHIELD3-HFI-NOW
Failure to install shield ring	WHF-ESD29-TAD	ESD29-TAD-RING	050-OPSTCSHIELD1-HFI-COD
Loss of CTM shielding during lift	WHF-ESD29-TAD	ESD29-TAD-CTM	ESD29-TAD-CTM

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.29.2 System Response Event Tree

There is no response tree since the above events result in direct exposure.

A4.30 EVENT TREES FOR WHF-ESD30 (POOL ACTIVITIES)

A4.30.1 Event Trees for WHF-ESD30-DPC

This ESD delineates the event sequences that result in direct exposures due to pool operations. The initiating event assigned in SAPHIRE is assigned in Table A4.30-1.

Table A4.30-1. Summary of Event Trees for WHF-ESD30-DPC

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD30-DPC	346

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.30.1.1 Initiating Events for WHF-ESD30-DPC

The following initiating events are associated with WHF-ESD30-DPC during pool operations. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.30-2.

Table A4.30-2. Initiating Event Assignments for WHF-ESD30-DPC

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Exposure to pool splash	WHF-ESD30-DPC	ESD30-EXPOSURE-SPLASH	ESD30-EXPOSURE-SPLASH
Improper decontamination	WHF-ESD30-DPC	ESD30-EXPOSURE-DECON	050-OPEXPOSE-DECON

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.30.1.2 System Response Event Tree

There is no response tree since the above events result in direct exposure.

A4.30.2 Event Trees for WHF-ESD30-FUEL (SFTM Lifted Too High)

This ESD delineates the event sequences that result in direct exposures due to pool operations by lifting the SFTM too high. As described in *Shielding Requirements and Dose Rate Calculations for WHF and LLW* (Ref. 2.2.90, Section 7.1.11, p. 103), the maximum lift height of the spent fuel is approximately 10 feet from the top of the pool. The initiating event assigned in SAPHIRE is assigned in Table A4.30-3.

Table A4.30-3. Summary of Event Trees for WHF-ESD30-FUEL

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing a DPC	Initiator: WHF-ESD30-FUEL	346

NOTE: DPC = dual-purpose canister.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.30.2.1 Initiating Events for WHF-ESD30-FUEL

The following initiating events are associated with WHF-ESD30-FUEL during pool operations. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.30-4.

Table A4.30-4. Initiating Event Assignments for WHF-ESD30-FUEL

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Fuel assembly lifted too high	WHF-ESD30-FUEL	ESD30-EXPOSURE-FUELHIGH	50-SFTM-TOOHIGH-SFT-RTH

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.30.2.2 System Response Event Tree

There is no response tree since the above events result in direct exposure.

A4.31 Event Trees for WHF-ESD31

This ESD delineates the event sequences that arise from fires that occur in the facility.

Although the initiator event trees transfer to the same response tree (see Table A4.31-1), the response tree is customized within SAPHIRE for each initiator event tree by the use of basic rules. The rules instruct SAPHIRE where to look for the fault tree that models each pivotal event. The assignments made in the rules files are indicated in this section.

Table A4.31-1. Summary of Event Trees for WHF-ESD31

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing bare commercial SNF	Initiator: WHF-ESD31-CSNF Response: RESPONSE-FIRE	3,775
Rail car, STC, or aging overpack containing a DPC	Initiator: WHF-ESD31-DPC Response: RESPONSE-FIRE	346
STC or aging overpack containing a TAD canister	Initiator: WHF-ESD31-TAD Response: RESPONSE-FIRE	1,165

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.26, Table 4)

A4.31.1 Initiating Events for WHF-ESD31

The following initiating events are associated with WHF-ESD31 for the waste forms listed in Table A4.31-1 for that occur in the WHF. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.31-2.

Localized Fire Affects Transportation Cask in the Transportation Cask Vestibule. This initiating event accounts for the fires occurring in the transportation cask vestibule that affect transportation casks. The probability of a fire in that room is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a cask in the Transportation Cask Vestibule per cask.

Localized Fire Affects Transportation Cask or STC in the Preparation Area. This initiating event accounts for the fires occurring in the preparation area that affect transportation casks or STCs. The probability of a fire in that room is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a cask in the preparation area per cask.

Localized Fire Affects Transportation Cask or STC in the Cask Unloading Room. This initiating event accounts for the fires occurring in the Cask Unloading Room that affect transportation casks or STCs. The probability of a fire in that room is derived from fire analysis,

which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a cask in the Cask Unloading Room per cask.

Localized Fire Affects DPC or TAD Canister in the Cask Transfer Machine. This initiating event accounts for the fires occurring in the CTM that affect DPCs or TAD canisters. The probability of a fire in the CTM is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a DPC or TAD canister in the CTM per container.

Localized Fire Affects DPC at the DPC Cutting Station. This initiating event accounts for the fires occurring at the DPC Cutting Station that affect DPCs. The probability of a fire at the DPC cutting station is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a DPC at the DPC cutting station per container.

Localized Fire Affects TAD Canister at the TAD Canister Closure Station. This initiating event accounts for the fires occurring at the TAD Canister Closure Station that affect TADs. The probability of a fire at the TAD canister closure station is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a TAD canister at the TAD canister closure station per container.

Localized Fire Affects STC or TAD Canister in the Site Transporter Vestibule or Loading Room. This initiating event accounts for the fires occurring in the Site Transporter Vestibule or Loading Room that affect STCs or TAD canisters. The probability of a fire in the Site Transporter Vestibule or Loading Room is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a fire that affects a STC or TAD canister at the Site Transporter Vestibule or Loading Room per container.

Large Fire Affects Any Waste Form in the WHF. This initiating event accounts for large fires occurring in the WHF that affect all waste forms, including commercial SNF, TAD canisters, and DPCs in any configuration. The probability of a large fire in the WHF is derived from fire analysis, which is shown in Attachment F and is modeled as a single-event fault tree as described in Section 6.2.2.10. The initiating event is specified as a probability of a large fire that affects any waste form per container.

Table A4.31-2. Initiating Event Assignments for WHF-ESD31

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level[a]
Localized fire affects transportation cask in the Transportation Cask Vestibule	WHF-ESD31-CSNF	ESD31-CSNF-TCVEST	050-FIRE-CSNF-VEST
Localized fire affects transportation cask or STC in the Preparation Area	WHF-ESD31-CSNF	ESD31-CSNF-PREP	050-FIRE-CSNF-PREP
Large fire affects any waste form in the WHF	WHF-ESD31-CSNF	ESD31-CSNF-LARGE	050-FIRE-LARGE-CSNF
Localized fire affects transportation cask in the Transportation Cask Vestibule	WHF-ESD31-DPC	ESD31-DPC-TCVEST	050-FIRE-DPC-VEST
Localized fire affects transportation cask or STC in the Preparation Area	WHF-ESD31-DPC	ESD31-DPC-PREP	050-FIRE-DPC-PREP
Localized fire affects transportation cask or STC in the Cask Unloading Room	WHF-ESD31-DPC	ESD31-DPC-UNLOAD	050-FIRE-DPC-UNLOAD
Localized fire affects DPC or TAD in the cask transfer machine	WHF-ESD31-DPC	ESD31-DPC-CTM	050-FIRE-DPC-CTM
Localized fire affects DPC at the DPC cutting station	WHF-ESD31-DPC	ESD31-DPC-DPCCUT	050-FIRE-DPC-DPCCUT
Large fire affects any waste form in the WHF	WHF-ESD31-DPC	ESD31-DPC-LARGE	050-FIRE-DPC-LARGE
Localized fire affects TAD canister at the TAD canister closure station	WHF-ESD31-TAD	ESD31-TAD-CLOSURE	050-FIRE-TAD-CLOSE
Localized fire affects STC or TAD canister in the Site Transporter Vestibule	WHF-ESD31-TAD	ESD31-TAD-STVEST	050-FIRE-TAD-VEST
Localized fire affects STC or TAD canister in the Loading Room	WHF-ESD31-TAD	ESD31-TAD-LOAD	050-FIRE-TAD-LOAD
Localized fire affects DPC or TAD canister in the cask transfer machine	WHF-ESD31-TAD	ESD31-TAD-CTM	050-FIRE-TAD-CTM
Large fire affects any waste form in the WHF	WHF-ESD31-TAD	ESD31-TAD-LARGE	050-FIRE-TAD-LARGE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.31.2 System Response Event Tree FIRE

The pivotal events that appear in PREP-STATION are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. This pivotal event represents the success or failure of the canister to contain radioactive material after the thermal impact caused by the initiating event. Due to the unique nature of thermal failures of canister contained within a cask, the conditional probability of cask breach given canister breach in a fire is taken to be 1. Details on the thermal failure analysis for cask-canister systems is outlined in Attachment x. Table A4.31-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.31-3. Basic Events Associated with the CANISTER Pivotal Events of WHF-ESD31

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event[a]
WHF-ESD31-CSNF	ESD31-CSNF-TCVEST	BARE-FUEL-FIRE	BARE-FUEL-FAIL-FIRE
	ESD31-CSNF-PREP		
	ESD31-CSNF-LARGE		
WHF-ESD31-DPC	ESD31-DPC-TCVEST	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
	ESD31-DPC-PREP	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
	ESD31-DPC-UNLOAD	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
	ESD31-DPC-CTM	CANISTER-FIRE-CTM	CANISTER-FIRE-FAIL-CTM
	ESD31-DPC-DPCCUT	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
	ESD31-DPC-LARGE	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
WHF-ESD31-TAD	ESD31-TAD-CLOSURE	CANISTER-FIRE	CANISTER-IN-CASK-FIRE
	ESD31-TAD-STVEST	CANISTER-FIRE-AO	CANISTER-FAIL-FIRE-AO
	ESD31-TAD-LOAD	CANISTER-FIRE-AO	CANISTER-FAIL-FIRE-AO
	ESD31-TAD-CTM	CANISTER-FIRE-CTM	CANISTER-FIRE-FAIL-CTM
	ESD31-TAD-LARGE	CANISTER-FIRE	CANISTER-IN-CASK-FIRE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. This pivotal event represents the success or failure of the aging overpack to continue to provide its shielding function after the impact caused by the initiating event. For fire event sequences, the shielding always fails. Table A4.31-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.31-4. Basic Event Associated with the SHIELDING Pivotal Events of WHF-ESD31

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event[a]
WHF-ESD31-CSNF	ESD31-CSNF-TCVEST	SHIELD-FIRE	SHIELD-FAIL-FIRE
	ESD31-CSNF-PREP		
	ESD31-CSNF-LARGE		
WHF-ESD31-DPC	ESD31-DPC-TCVEST		
	ESD31-DPC-PREP		
	ESD31-DPC-UNLOAD		
	ESD31-DPC-CTM	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD31-DPC-DPCCUT	SHIELD-FIRE	SHIELD-FAIL-FIRE
	ESD31-DPC-LARGE	SHIELD-FIRE	SHIELD-FAIL-FIRE
WHF-ESD31-TAD	ESD31-TAD-CLOSURE	SHIELD-FIRE	SHIELD-FAIL-FIRE
	ESD31-TAD-STVEST	SHIELD-FIRE-AO	SHIELD-FIRE-AO-FAILS
	ESD31-TAD-LOAD	SHIELD-FIRE-AO	SHIELD-FIRE-AO-FAILS
	ESD31-TAD-CTM	SHIELD-CTM	SHIELD-FAIL-CTM
	ESD31-TAD-LARGE	SHIELD-FIRE	SHIELD-FAIL-FIRE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. This pivotal event represents the success or failure of the HVAC system in continuing to provide radiological confinement after the initiating event. During fire event sequences, the HVAC system is always believed to fail due to damage to the system caused by the fire. Table A4.31-5 specifies the fault tree that is associated with this pivotal event for each initiating event.

Table A4.31-5. Basic Event Associated with the CONFINEMENT Pivotal Events of WHF-ESD31

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event[a]
WHF-ESD31-CSNF	ESD31-CSNF-TCVEST	CONFINEMENT	HVAC-FAILS-FIRE
	ESD31-CSNF-PREP	HVAC-FIRE	HVAC-FAILS-FIRE
	ESD31-CSNF-LARGE	HVAC-FIRE	HVAC-FAILS-FIRE
WHF-ESD31-DPC	ESD31-DPC-TCVEST	CONFINEMENT	HVAC
	ESD31-DPC-PREP	HVAC-FIRE	HVAC-FAILS-FIRE
	ESD31-DPC-UNLOAD	CONFINEMENT	HVAC
	ESD31-DPC-CTM	CONFINEMENT	HVAC
	ESD31-DPC-DPCCUT	HVAC-FIRE	HVAC-FAILS-FIRE
	ESD31-DPC-LARGE	HVAC-FIRE	HVAC-FAILS-FIRE
WHF-ESD31-TAD	ESD31-TAD-CLOSURE	HVAC-FIRE	HVAC-FAILS-FIRE
	ESD31-TAD-STVEST	CONFINEMENT	HVAC
	ESD31-TAD-LOAD	CONFINEMENT	HVAC
	ESD31-TAD-CTM	CONFINEMENT	HVAC
	ESD31-TAD-LARGE	HVAC-FIRE	HVAC-FAILS-FIRE

NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. This pivotal event represents the conditional probability of introducing liquid moderator (water or crane gearbox lubricating oil) into a breached canister, given that a breached canister is present. This pivotal event is modeled as a fault tree as discussed in Section 6.2.2.10. The conditional probability of failure (introduction of liquid moderator) is the same for all waste forms. Table A4.31-6 specifies the fault tree that is associated with this pivotal event for each initiating event.

Table A4.31-6. Basic Event Associated with the MODERATOR Pivotal Events of WHF-ESD31

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event[a]
WHF-ESD31-CSNF	ESD31-CSNF-TCVEST	MODERATOR-BARE-FUEL	MODERATOR-BARE-FUEL-FIRE
	ESD31-CSNF-PREP		
	ESD31-CSNF-LARGE		
WHF-ESD31-DPC	ESD31-DPC-TCVEST	MODERATOR-FIRE	050-WATER-MOD-FIRE
	ESD31-DPC-PREP		
	ESD31-DPC-UNLOAD		
	ESD31-DPC-CTM		
	ESD31-DPC-DPCCUT		
	ESD31-DPC-LARGE		
WHF-ESD31-TAD	ESD31-TAD-CLOSURE	MODERATOR-FIRE	050-WATER-MOD-FIRE
	ESD31-TAD-STVEST		
	ESD31-TAD-LOAD		
	ESD31-TAD-CTM		
	ESD31-TAD-LARGE		

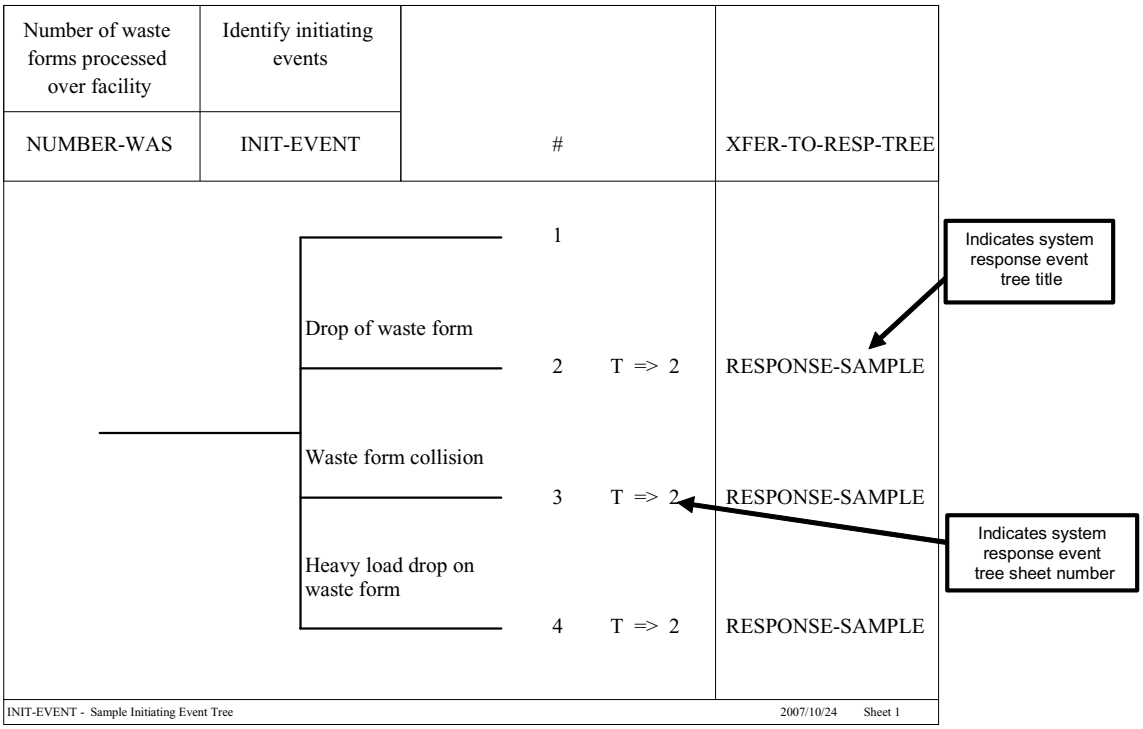
NOTE: [a]This column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A5. EVENT TREES

Navigation from an initiator event tree to the corresponding response event tree is assisted by the rightmost two columns on the initiator event trees as shown in Figure A5-1. The numbers under the "#" symbol may be used by the reader to refer to a particular branch of an event tree, but it is not used elsewhere in this analysis.

Refer to Table A5-1 for the relationship between the ESDs, initiating event trees and system response event trees.



Source: Original

Figure A5-1. Example Initiator Event Tree Showing Navigation Aids

Table A5-1. ESDs to Event Trees

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD01	Event Sequences for Activities Associated with Receipt of Transportation Cask with Spent Nuclear Fuel in the Transportation Cask Vestibule and Movement into Cask Preparation Area	WHF-ESD01-CSNF	Figure A5-2	RESPONSE-TCASK-CSNF	Figure A5-3
WHF-ESD02	Event Sequences for Activities Associated with Receipt of Transportation Cask with DPC in the Transportation Cask Vestibule and Movement into Cask Preparation Area	WHF-ESD02-DPC	Figure A5-4	RESPONSE-TCASK-DPC	Figure A5-5
WHF-ESD03	Event Sequences for Activities Associated with Receipt of Aging Overpack in the Site Transporter Vestibule	WHF-ESD03-AODPC	Figure A5-6	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD04	Event Sequences for Activities Associated with Receipt of Horizontal STC/DPC in the Transportation Cask Vestibule and Movement into the Cask Preparation Area	WHF-ESD04-DPC	Figure A5-8	RESPONSE-STC1	Figure A5-9

Table A5-1. ESDs to Event Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD05	Event Sequences for Activities Associated with TC/CSNF Removal of Impact Limiters, Upending, and Removal from Conveyance and Transfer to Preparation Station	WHF-ESD05-CSNF	Figure A5-10	RESPONSE-TCASK-CSNF	Figure A5-3
WHF-ESD06	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending, and Removal of Transportation Cask from Conveyance and Transfer to CTT	WHF-ESD06-VTC WHF-ESD06-TTC	Figure A5-11 Figure A5-13	RESPONSE-TCASK	Figure A5-12
WHF-ESD07	Event Sequences for Associated Cask Preparation Activities (i.e., Installation of Lid Lift Fixture on Transportation Cask/DPC)	WHF-ESD07-DPC	Figure A5-14	RESPONSE-TCASK	Figure A5-12
WHF-ESD08	Event Sequences for Associated Cask Preparation Activities (i.e., Installation of Cask Lid Lift Fixture on Transportation Cask/CSNF)	WHF-ESD08-CSNF	Figure A5-15	RESPONSE-TCASK-CSNF	Figure A5-3
WHF-ESD09	Event Sequences for Associated Cask Preparation Activities (i.e., Lid Removal, or Installation of DPC Lid Lift Fixture, STC/DPC or Transportation Cask/DPC)	WHF-ESD09-DPC	Figure A5-16	RESPONSE-CANISTER1	Figure A5-7

Table A5-1. ESDs to Event Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD10	Event Sequences for Associated with Transfer of Cask on CTT from Preparation Area to Cask Unloading Room	WHF-ESD10-DPC	Figure A5-17	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD11	Event Sequences Associated with Transfer of an Aging Overpack/DPC or Aging Overpack/TAD on Site Transporter, through Site Transporter Vestibule, Aging Overpack Access Platform, and Loading Room (Receipt or Export)	WHF-ESD11-AODPC WHF-ESD11-AOTAD	Figure A5-18 Figure A5-19	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD12	Event Sequences Associated with Aging Overpack (DPC or TAD) on Site Transporter or STC/TAD on CTT Colliding with Cask Loading Shield Door	WHF-ESD12-DPC WHF-ESD12-TAD	Figure A5-20 Figure A5-21	N/A	N/A
WHF-ESD13	Event Sequences for Activities Associated with the Transfer of a Canister to or from an Aging Overpack, STC, or Transportation Cask with the CTM	WHF-ESD13-DPC WHF-ESD13-TAD	Figure A5-22 Figure A5-23	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD14	Event Sequences for Activities Associated with the Transfer of STC/DPC from the Cask Unloading Room to the Preparation Station	WHF-ESD14-DPC	Figure A5-24	RESPONSE-STC1	Figure A5-9

Table A5-1. ESDs to Event Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD15	Event Sequences for Activities Associated with the Transfer of STC/DPC from the Preparation Station to the DPC Cutting Station	WHF-ESD15-DPC	Figure A5-25	RESPONSE-STC1	Figure A5-9
WHF-ESD16	Event Sequences for Activities Associated with the STC/DPC Preparation at the Preparation Station	WHF-ESD16-CSNF	Figure A5-26	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD17	Event Sequences for Activities Assoicated with the STC/DPC Preparation Activities at the DPC Cutting Station	WHF-ESD17-DPC	Figure A5-28	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD18	Event Sequences for Activities Associated with the STC/DPC Preparation Activities – DPC Cutting at DPC Cutting Station	WHF-ESD18-DPC	Figure A5-29	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD19	Event Sequences Associated with Transfer of STC/DPC from DPC Cutting Station to Pool Ledge	WHF-ESD19-DPC	Figure A5-30	RESPONSE-POOLMOVE RESPONSE-STC1	Figure A5-31 Figure A5-9
WHF-ESD20	Event Sequences Associated with Transfer of Transportation Cask/CSNF from Preparation Station to Pool Ledge	WHF-ESD20-CSNF	Figure A5-32	RESPONSE-POOLMOVE RESPONSE-TCASK-CSNF	Figure A5-31 Figure A5-3

Table A5-1. ESDs to Event Trees (Continued)

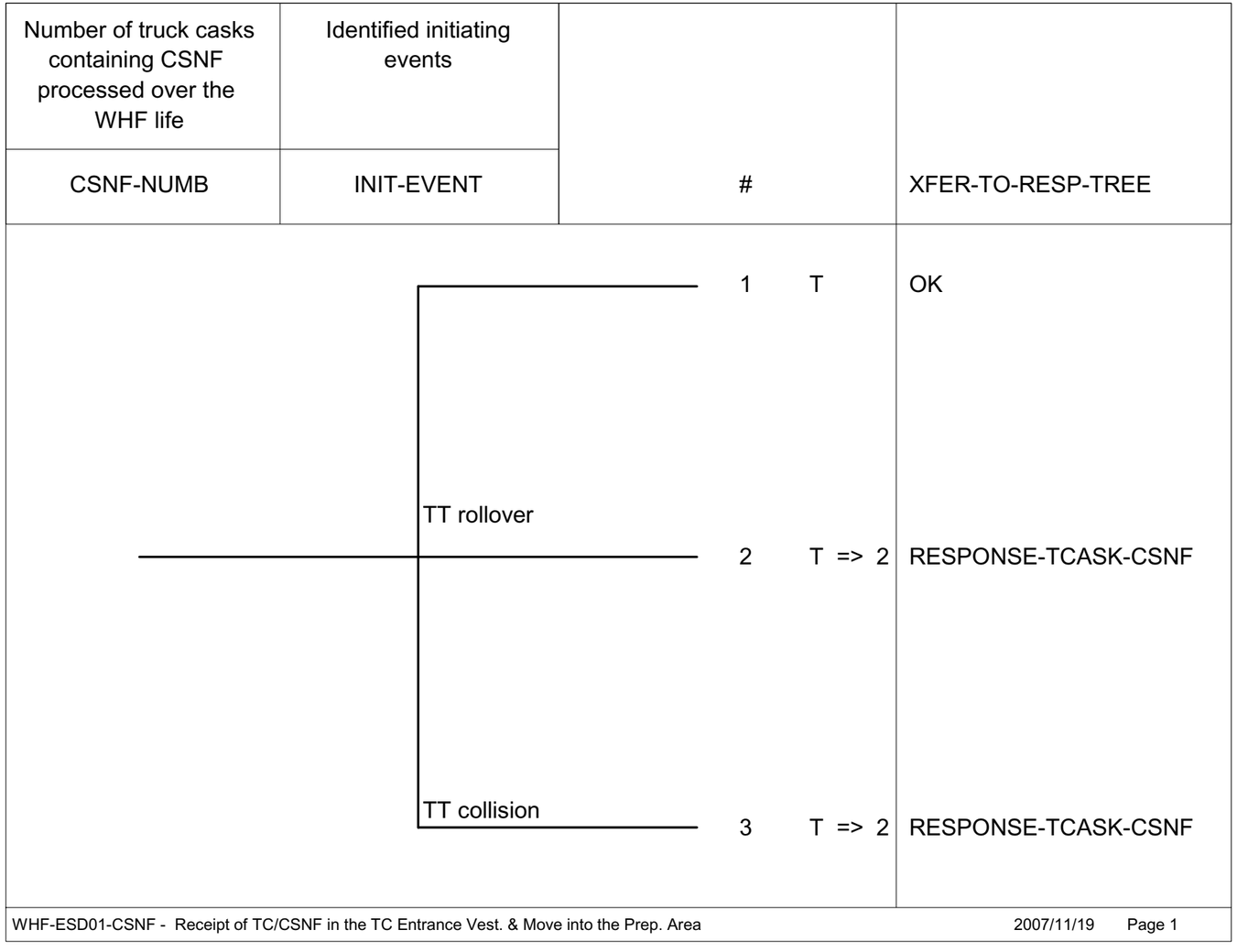
ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD21	Event Sequences for Activities Involving Lowering STC/DPC or Transportation Cask/CSNF to the Pool Floor	WHF-ESD21-CSNF WHF-ESD21-DPC WHF-ESD21-TAD	Figure A5-33 Figure A5-34 Figure A5-35	RESPONSE-POOLMOVE	Figure A5-31
WHF-ESD22	Event Sequences for Pool Activities Involving Transfer of Fuel Assembly to TAD Canister or Fuel Staging Rack	WHF-ESD22-FUEL	Figure A5-36	RESPONSE-POOLCONFINE	Figure A5-37
WHF-ESD23	Event Sequences for Activities Associated with Handling of Low Level Liquid Waste	WHF-ESD23-POOL	Figure A5-38	DE-SHIELD-LOSS	N/A
WHF-ESD24	Event Sequences for Activities Associated with the Transfer of STC/TAD from the Pool Ledge to the TAD Canister Closure Station	WHF-ESD24-TAD	Figure A5-39	RESPONSE-POOLMOVE RESPONSE-STC1	Figure A5-31 Figure A5-9
WHF-ESD25	Event Sequences for Activities Associated with Preparation of STC/TAD and Closure of TAD Canister	WHF-ESD25-TAD	Figure A5-40	RESPONSE-TAD	Figure A5-41
WHF-ESD26	Event Sequences for Activities Associated with Closure of TAD Canister – TAD Drying and Inerting Process	WHF-ESD26-TAD	Figure A5-42	N/A	N/A

Table A5-1. ESDs to Event Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
WHF-ESD27	Event Sequences for Activities Associated with TAD Closure – Welding, Drying, and Inerting Process	WHF-ESD27-TAD	Figure A5-43	RESPONSE-PREPSTATION	Figure A5-27
WHF-ESD28	Event Sequences for Activities Associated with Transfer of STC/TAD from TAD Closure Station to CTT in the Preparation Station	WHF-ESD28-TAD	Figure A5-44	RESPONSE-CANISTER1	Figure A5-7
WHF-ESD29	Direct Expsoure Event Sequences for Activities Associated with Cask Preparation or CTM Movement	WHF-ESD29-DPC WHF-ESD29-TAD	Figure A5-45 Figure A5-46	N/A	N/A
WHF-ESD30	Direct Exposure Event Sequences for Activities Associated with Pool Operations	WHF-ESD30-DPC WHF-ESD30-FUEL	Figure A5-47 Figure A5-48	N/A	N/A
WHF-ESD31	Event Sequences for Activities Associated with Fires Occurring in the WHF	WHF-ESD31-CSNF WHF-ESD31-DPC WHF-ESD31-TAD	Figure A5-49 Figure A5-51 Figure A5-52	RESPONSE-FIRE	Figure A5-50

NOTE: CSNF = commercial spent nuclear fuel; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; STC = shielded transportation cask; TAD = Transportation, aging, and disposal canister; TC = transportation cask.

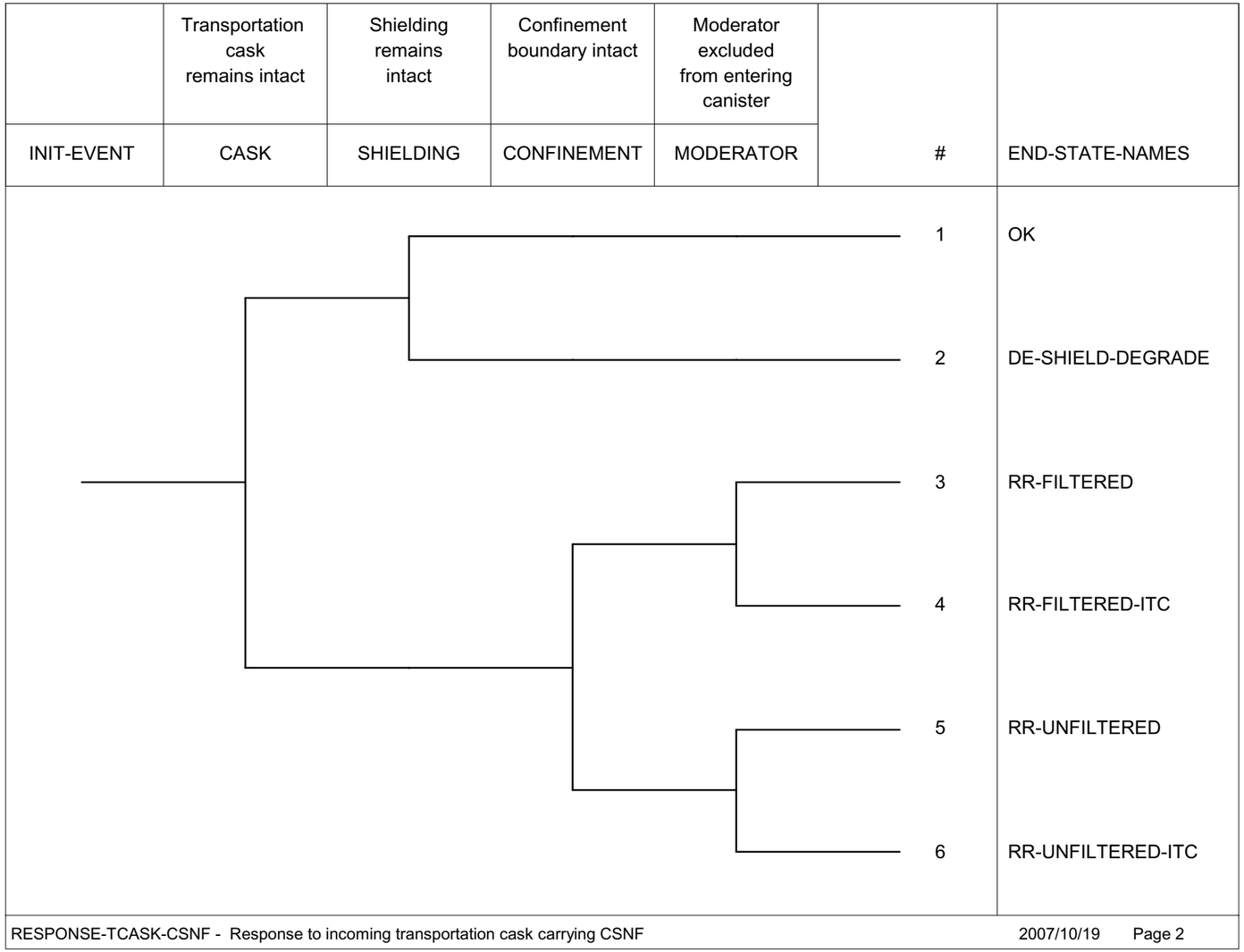
Source: Original



NOTE: CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; TT = tractor trailer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

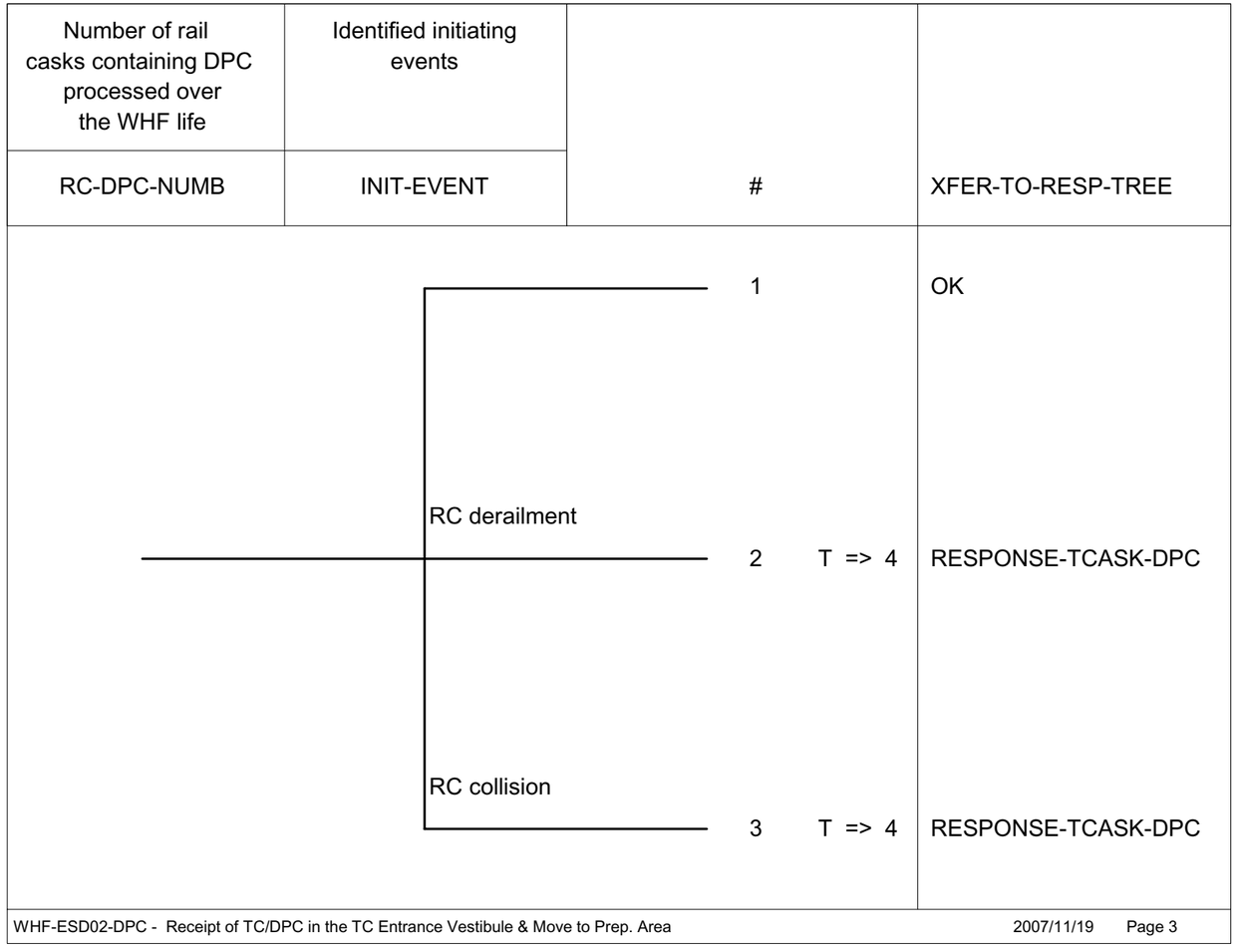
Figure A5-2. Event Tree WHF-ESD01-CSNF – Receipt of Transportation Cask with Commercial SNF in the Transportation Cask Entrance Vestibule and Move into the Preparation Area



NOTE: CSNF = commercial spent nuclear fuel; DE = direct exposure; ESD = event sequence diagram; INIT = initiating; ITC = important to criticality; RR = radionuclide release; STC = shielded transfer cask; WHF = Wet Handling Facility.

Source: Original

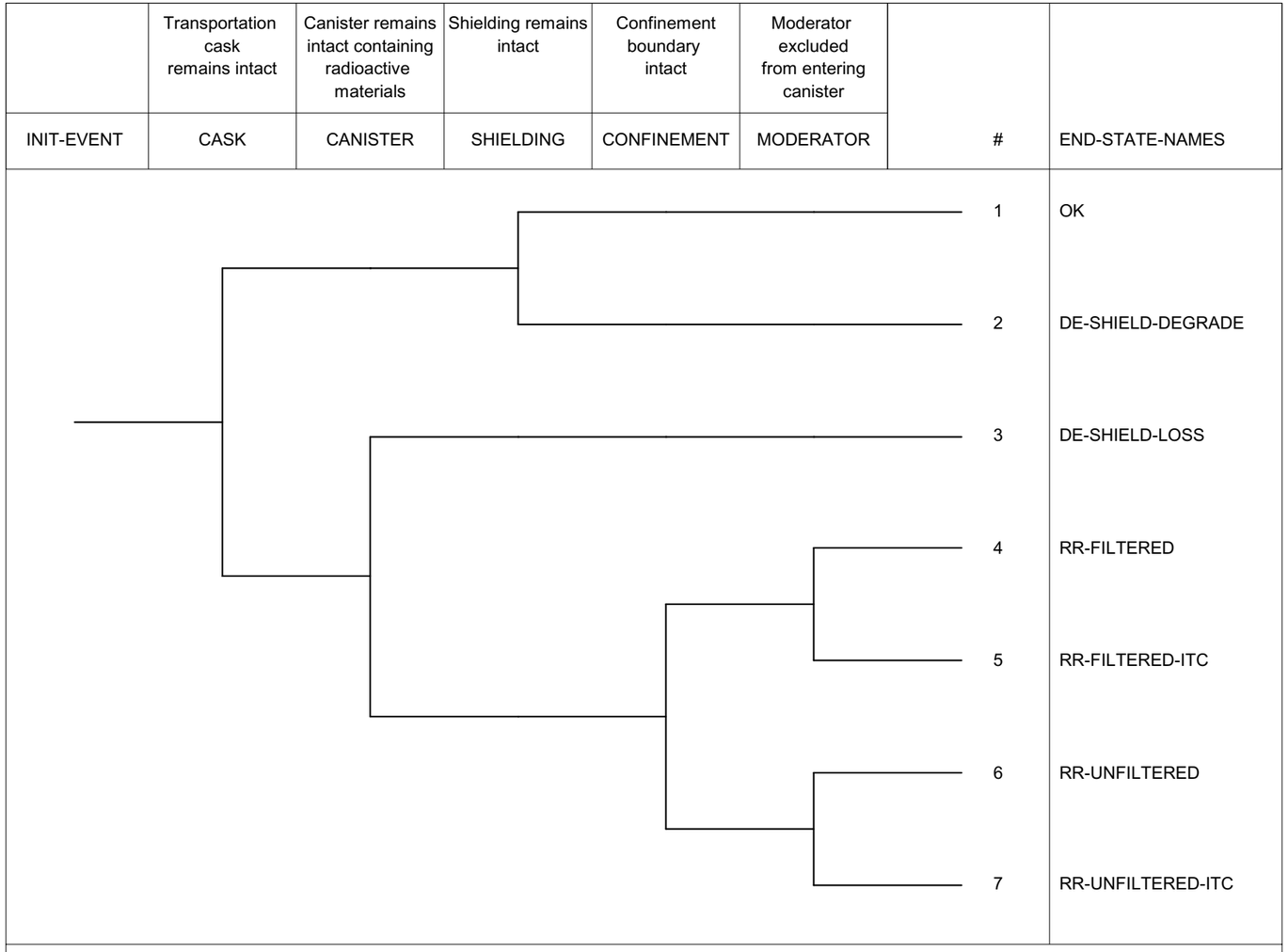
Figure A5-3. Event Tree RESPONSE-TCASK-CSNF – Response to Incoming Transportation Cask Carrying Commercial SNF



NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RC = railcar; RESP = response; T = transfer; TC = transportation cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-4. Event Tree WHF-ESD02-DPC – Receipt of Transportation Cask with DPC in the Transportation Cask Entrance Vestibule and Move into the Preparation Area



NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating; ITC = important to criticality; RR = radionuclide release; STC = shielded transfer cask; WHF = Wet Handling Facility.

Source: Original

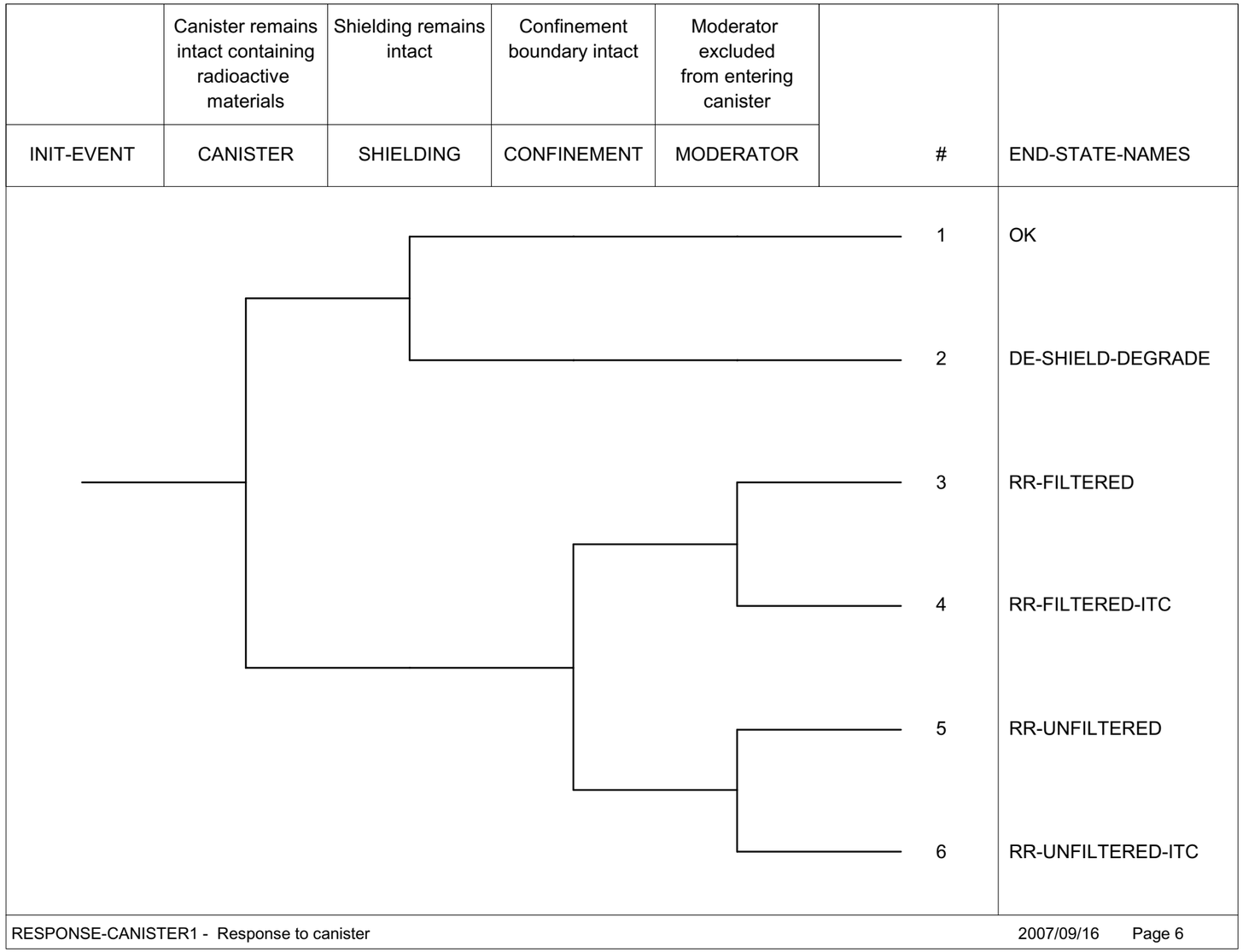
Figure A5-5. Event Tree RESPONSE-TCASK-DPC – Response to Incoming Transportation Cask Carrying DPC

Number of AO/ DPC processed over the WHF life	Identified initiating events		
AO-DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	ST rollover	2 T => 6	RESPONSE-CANISTER1
	ST collision	3 T => 6	RESPONSE-CANISTER1
WHF-ESD03-AODPC - Receipt of Aging Overpack/DPC in the Site Transporter Vestibule		2007/11/02	Page 5

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; ST = site transporter; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-6. Event Tree WHF-ESD03-AODPC – Receipt of Aging Overpack with DPC in the Site Transporter Vestibule



NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating; ITC = important to criticality; RR = radionuclide release; WHF = Wet Handling Facility.

Source: Original

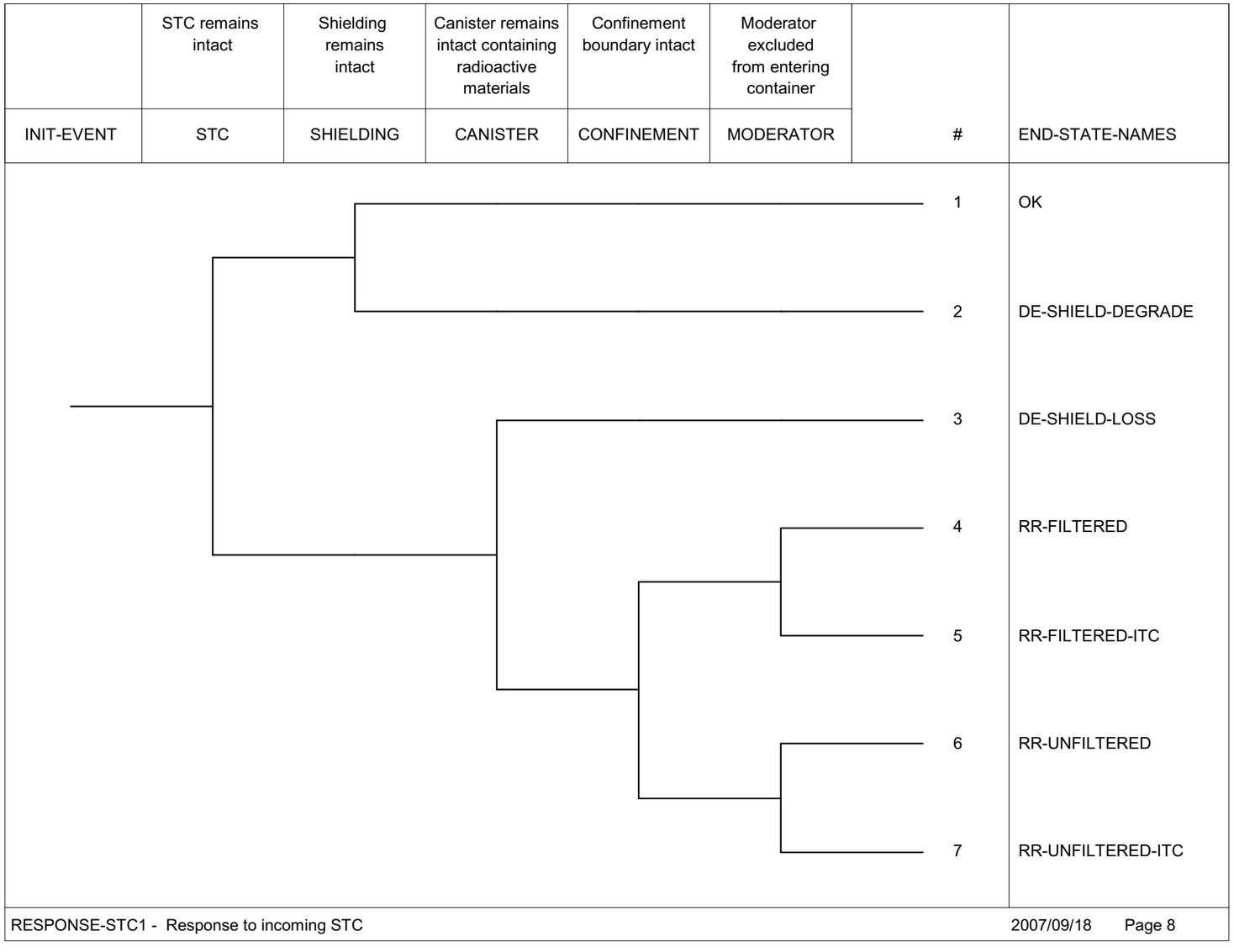
Figure A5-7. Event Tree RESPONSE-TCASK-CANISTER1 – Response to Canister

Number of DPCs processed over the WHF life	Identified initiating events	#	
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	CT trailer rollover	2 T => 8	RESPONSE-STC1
	CT trailer collision	3 T => 8	RESPONSE-STC1
WHF-ESD04-DPC - Receipt of STC/DPC in the RC Entrance Vestibule and Movement into the Prep Area		2007/11/02	Page 7

NOTE: CT = cask transfer; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; STC = shielded transfer cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

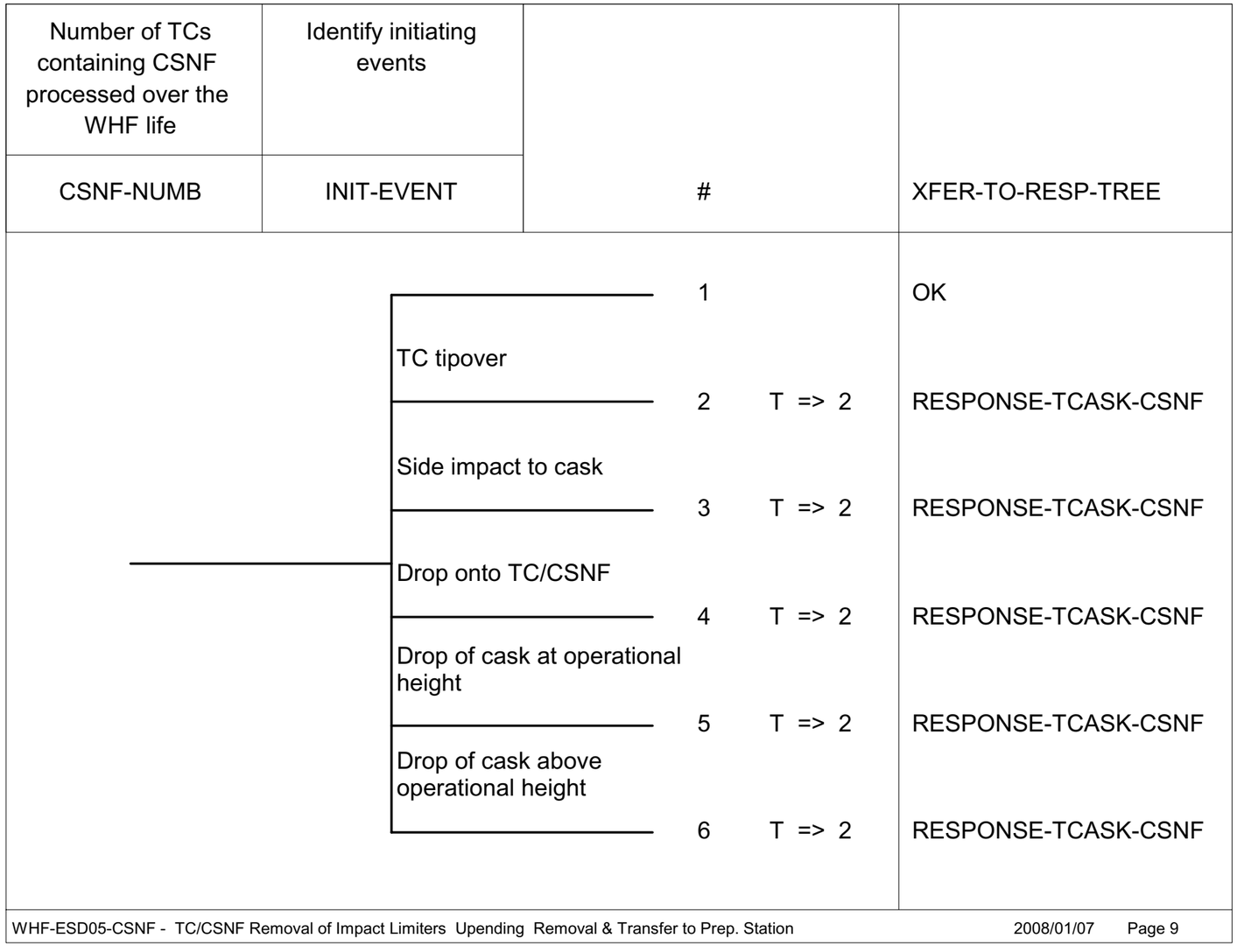
Figure A5-8. Event Tree WHF-ESD04-DPC – Receipt of STC with DPC in the Railcar Entrance Vestibule and Movement into the Preparation Area



NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating; ITC = important to criticality; RR = radionuclide release; STC = shielded transfer cask; WHF = Wet Handling Facility.

Source: Original

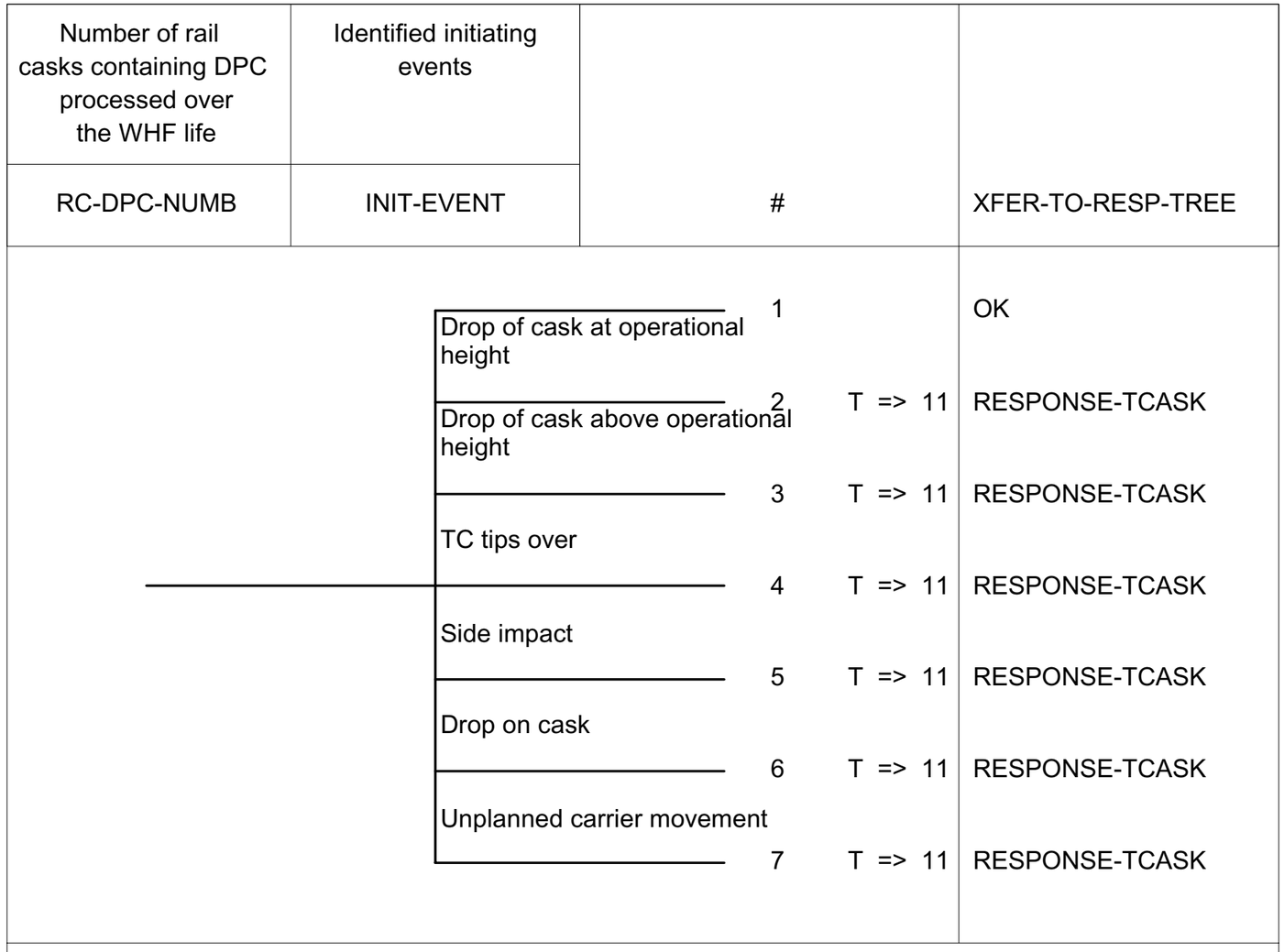
Figure A5-9. Event Tree RESPONSE-STC1 – Response to Incoming STC



NOTE: CSNF = commercial spent nuclear fuel; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; TC = transportation cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

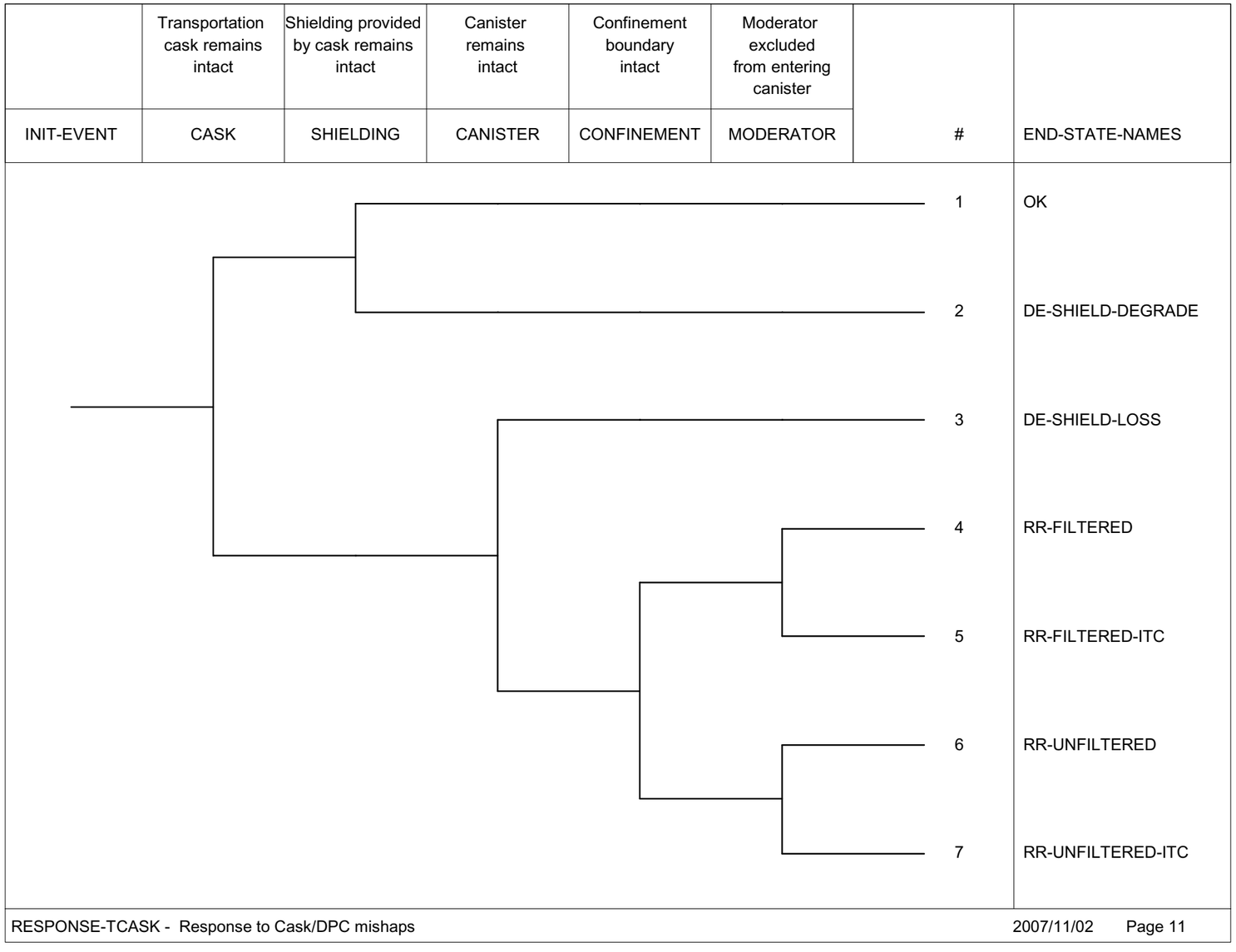
Figure A5-10. Event Tree WHF-ESD05-CSNF – Transportation Cask with Commercial SNF Removal of Impact Limiters, Upending, Removal, and Transfer to Preparation Station



NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RC = railcar; RESP = response; T = transfer; TC = transportation cask; VTC = vertical transportation cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-11. Event Tree WHF-ESD06-VTC– Railcar with DPC Upright and Removal from Conveyance



NOTE: DE = direct exposure; DPC = dual-purpose canister; INIT = initiating; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-12. Event Tree RESPONSE-TCASK – Response to Cask/DPC Mishaps

Number of horizontal STC/ DPC processed over the WHF life	Identified initiating events	#		XFER-TO-RESP-TREE
HSTC-DPC-NUMB	INIT-EVENT	#		XFER-TO-RESP-TREE
	Drop of cask at operational height	1		OK
	Drop of cask above operational height	2	T => 11	RESPONSE-TCASK
	TC tips over	3	T => 11	RESPONSE-TCASK
	Side impact	4	T => 11	RESPONSE-TCASK
	Drop on cask	5	T => 11	RESPONSE-TCASK
	Unplanned carrier movement	6	T => 11	RESPONSE-TCASK
		7	T => 11	RESPONSE-TCASK
WHF-ESD06-TTC - HS/DPC Uprighting and Removal from Conveyance			2007/12/05	Page 10

NOTE: CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; INIT = initiating; NUMB = number; PREP = preparation; RESP = response; STC = shielded transfer cask; T = transfer; TC = transportation cask; TTC = a transportation cask that is upended using a tilt frame; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

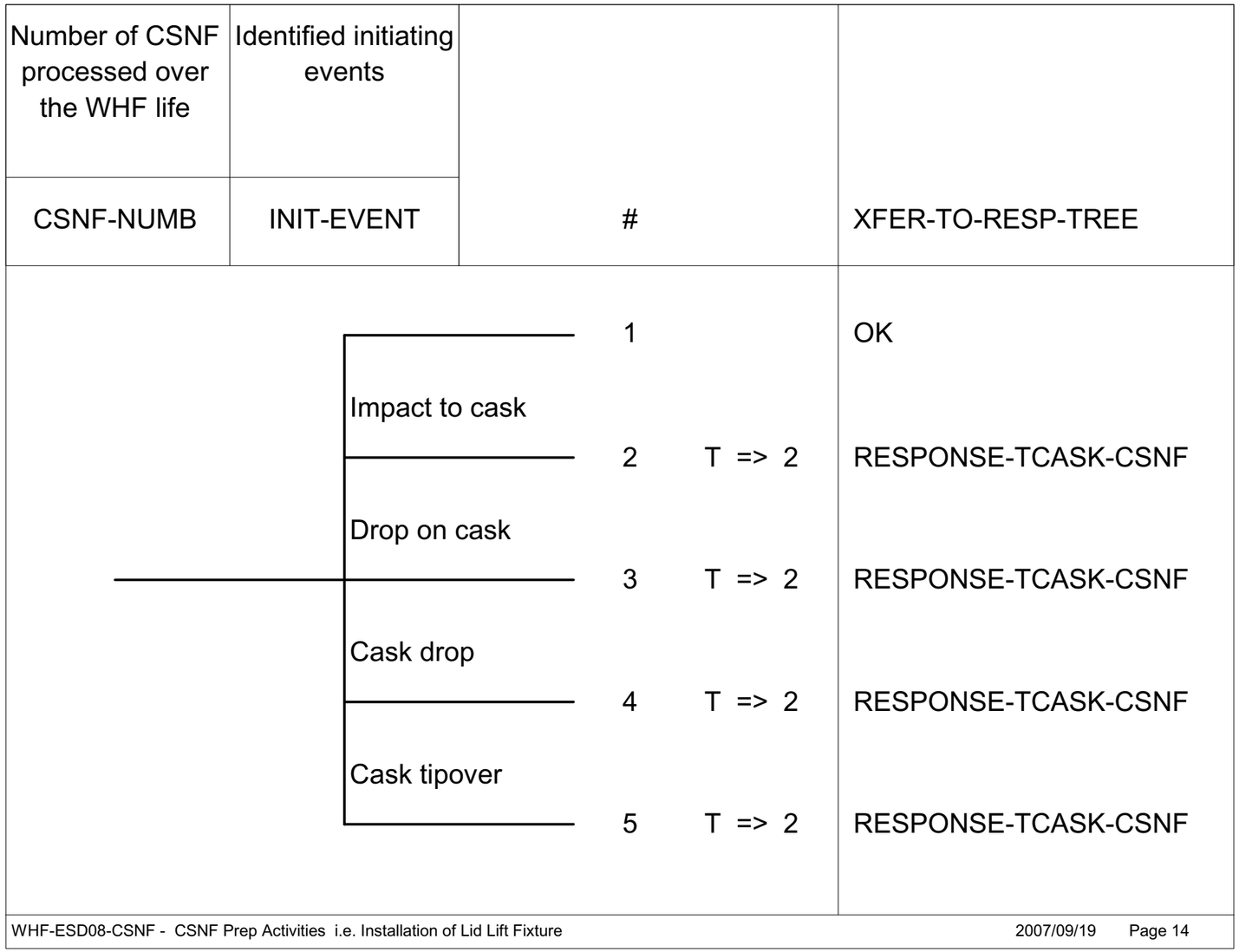
Figure A5-13. Event Tree WHF-ESD06-TTC – HISTAR/DPC Upright and Removal from Conveyance

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Cask tips over	2 T => 11	RESPONSE-TCASK
	Impact to cask	3 T => 11	RESPONSE-TCASK
	Drop on cask	4 T => 11	RESPONSE-TCASK
	Cask drop	5 T => 11	RESPONSE-TCASK
WHF-ESD07-DPC - Transportation Cask/DPC Preparation Activities i.e. Installation of Lid Lift Fixture		2007/11/02	Page 13

NOTE: DPC = dual-purpose canister; INIT = initiating; NUMB = number; RESP = response; T = transfer; XFER = transfer.

Source: Original

Figure A5-14. Event Tree WHF-ESD07-DPC – Transportation Cask/DPC Preparation Activities (i.e., Installation of Lid-Lift Fixture)



NOTE: CSNF = commercial spent nuclear fuel; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-15. Event Tree WHF-ESD08-CSNF – Commercial SNF Preparation Activities (i.e., Installation of Lid-Lift Fixture)

Number of DPCs processed over the WHF life	Identified initiating events	#		XFER-TO-RESP-TREE
DPC-NUMB	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	Drop of cask	2	T => 6	RESPONSE-CANISTER1
	Impact to cask	3	T => 6	RESPONSE-CANISTER1
	Drop on cask	4	T => 6	RESPONSE-CANISTER1
WHF-ESD09-DPC - DPC Prep Activities i.e. Sampling Lid Removal or Installation of Lid Removal Fixture (Lid off)			2007/09/19	Page 15

NOTE: DPC = dual-purpose canister; INIT = initiating; RESP = response; WHF = Wet Handling Facility.

Source: Original

Figure A5-16. Event WHF-ESD09-DPC – DPC Preparation Activities (i.e., Sampling Lid Removal or Installation of Lid-Lift Fixture (Lid Off))

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	CTT tipover	2 T => 6	RESPONSE-CANISTER1
	CTT Collision	3 T => 6	RESPONSE-CANISTER1
WHF-ESD10-DPC - Transfer of DPC on Cask Transfer Trolley from Prep Area to Cask Unloading Room		2007/11/02	Page 16

NOTE: CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-17. Event Tree WHF-ESD10-DPC – Transfer of DPC on CTT from Preparation Area to Cask Unloading Room

Number of AO/ DPC processed over the WHF life	Identified initiating events	#		XFER-TO-RESP-TREE
AO-DPC-NUMB	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	ST Collision	2	T => 6	RESPONSE-CANISTER1
	Drop on AO	3	T => 6	RESPONSE-CANISTER1
	AO/DPC tip over	4	T => 6	RESPONSE-CANISTER1
	AO/DPC side impact	5	T => 6	RESPONSE-CANISTER1
WHF-ESD11-AODPC - Transfer of AO/DPC on ST from ST Entrance Vestibule to Cask Loading Room			2008/02/25	Page 17

NOTE: AO = aging overpack; DPC = dual-purpose canister; INIT = initiating; NUMB = number; RESP = response; ST = site transporter; T = transfer; XFER = transfer.

Source: Original

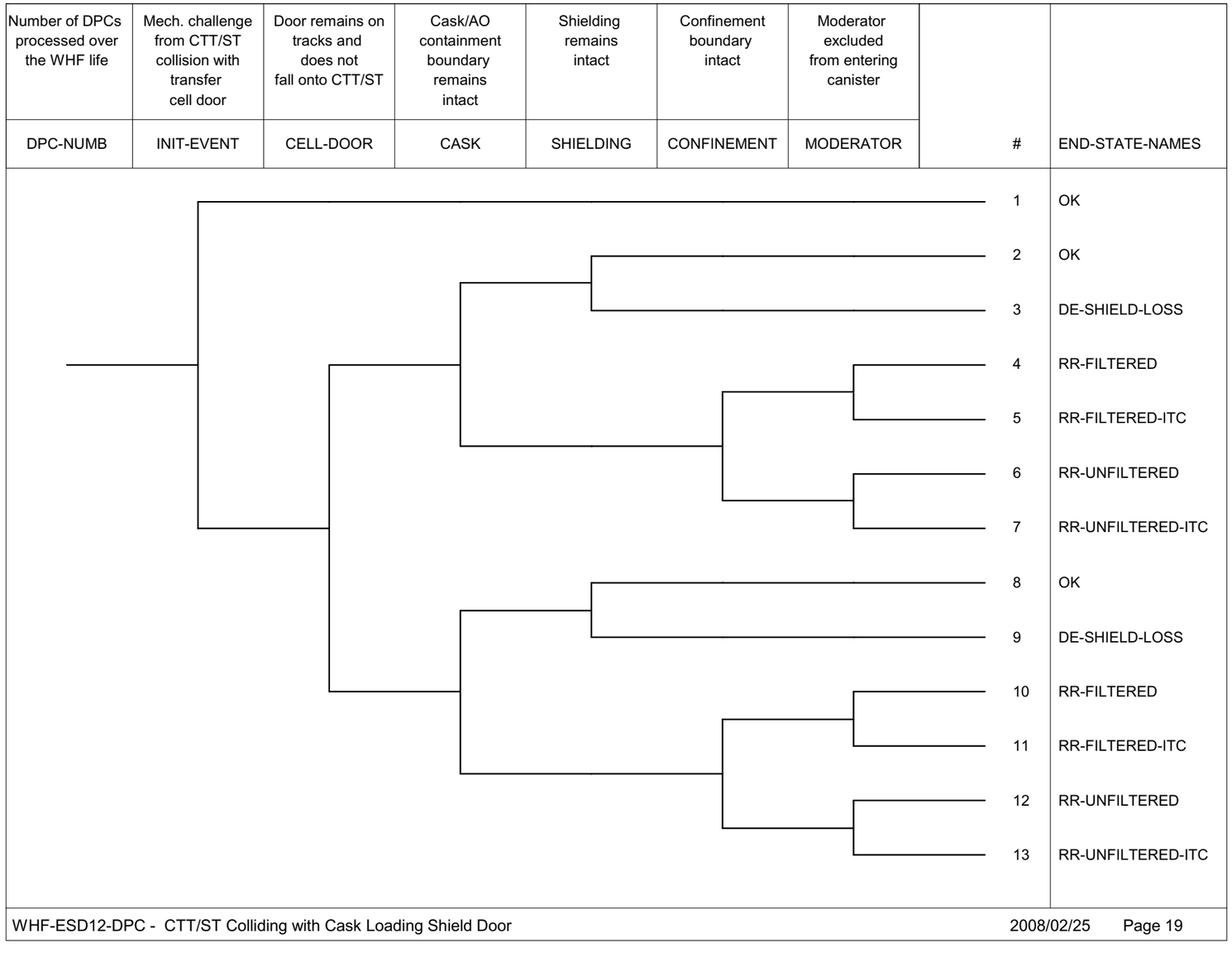
Figure A5-18. Event Tree WHF-ESD11-AO-DPC – Transfer of Aging Overpack/DPC on Site Transporter from Site Transporter Vestibule to Cask Loading Room

Number of TADs processed over the WHF life	Identified initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	ST Collision	2 T => 6	RESPONSE-CANISTER1
	Drop on AO	3 T => 6	RESPONSE-CANISTER1
	AO/TAD tip over	4 T => 6	RESPONSE-CANISTER1
	Side impact	5 T => 6	RESPONSE-CANISTER1
WHF-ESD11-AOTAD - Transfer of AO/DPC on ST from ST Entrance Vestibule to Cask Loading Room		2008/01/07	Page 18

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; ST = site transporter; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

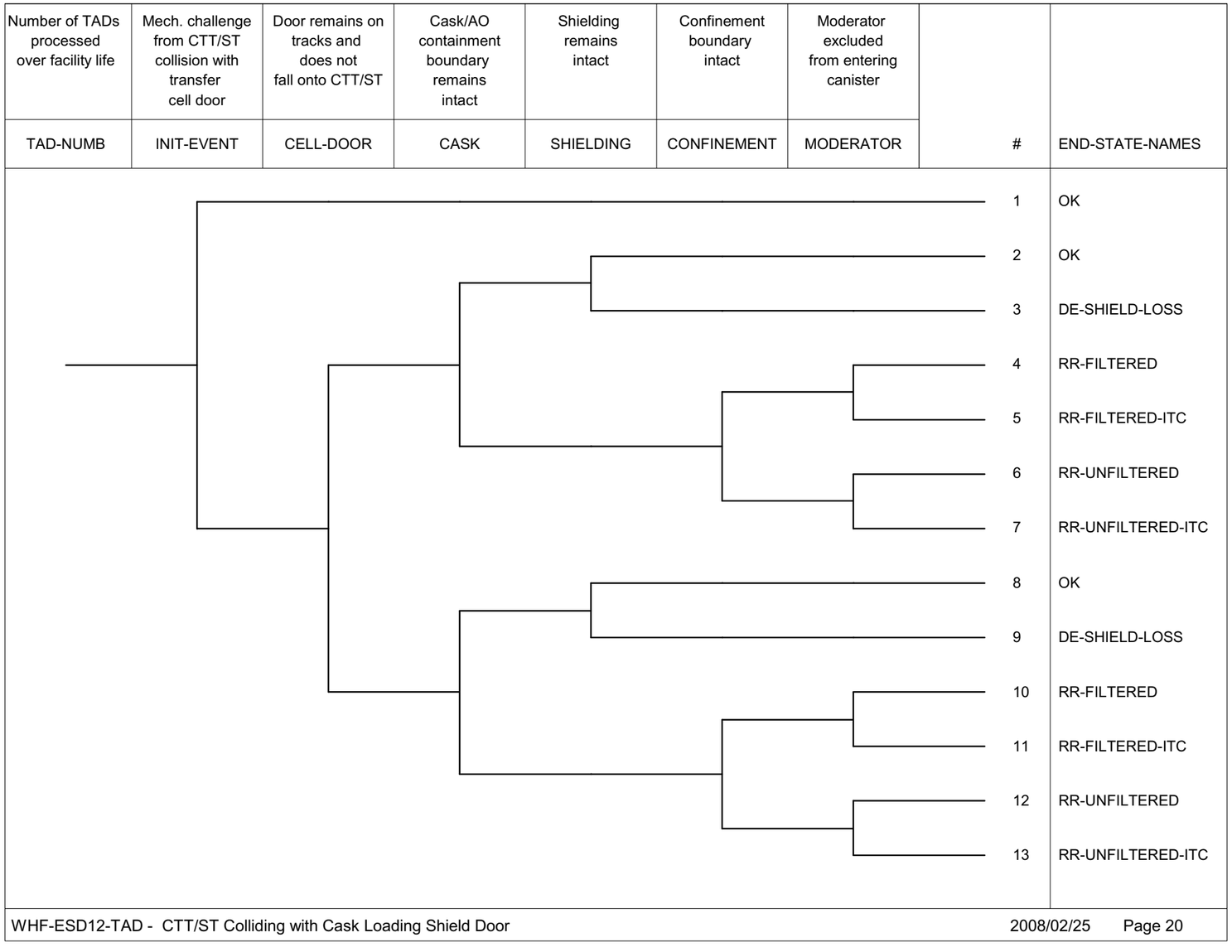
Figure A5-19. Event Tree WHF-ESD11-AO-TAD – Transfer of Aging Overpack/DPC on Site Transporter from Site Transporter Entrance Vestibule to Cask Loading Room



NOTE: AO = aging overpack; CTT = cask transfer trolley; DE = direct exposure; DPC = dual-purpose canister; INIT = initiating; ITC = important to criticality; NUMB = number; RR = radionuclide release; ST = site transporter; WHF = Wet Handling Facility.

Source: Original

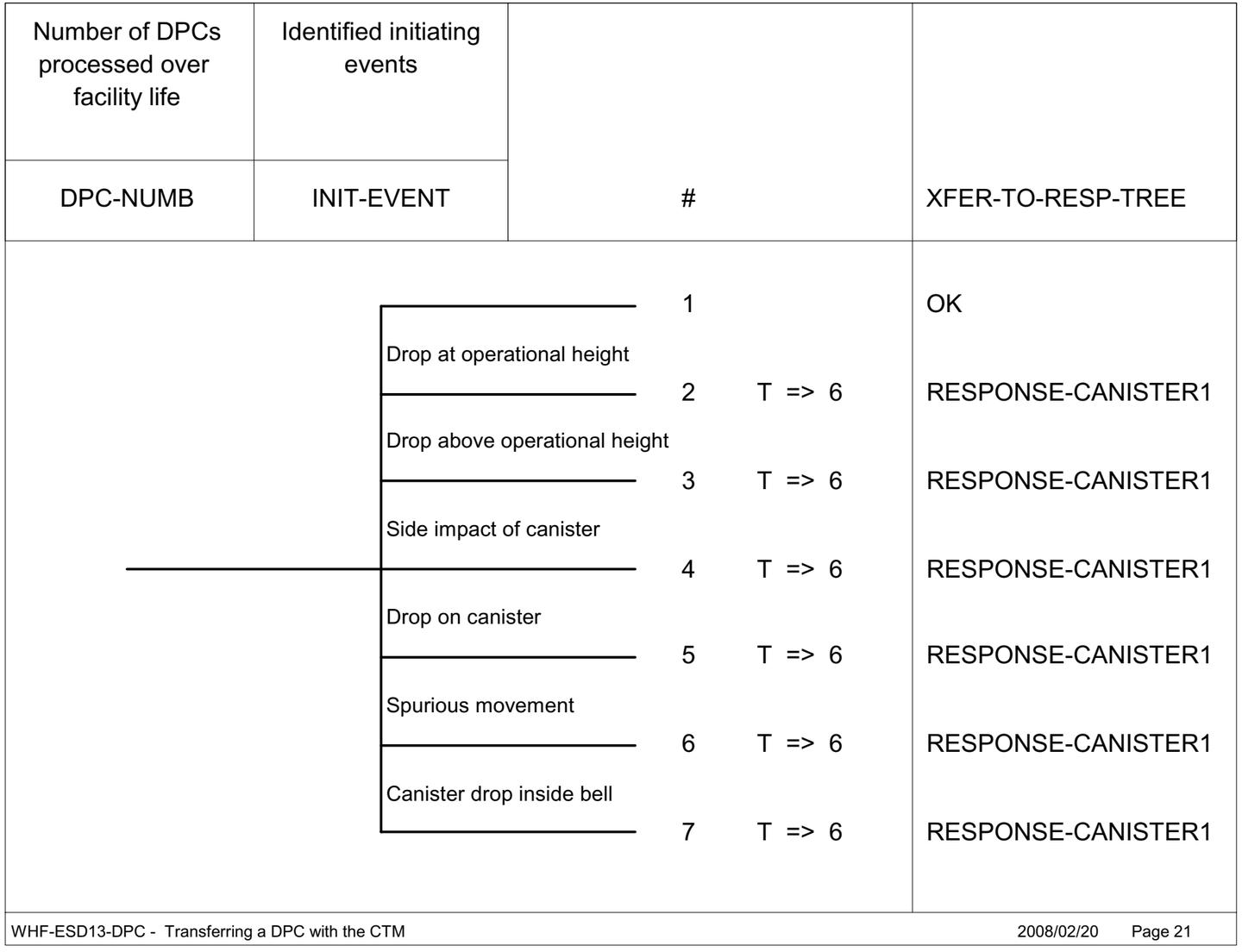
Figure A5-20. Event Tree WHF-ESD12-DPC – CTT/Site Transporter Colliding with Cask Loading Shield Door



NOTE: AO = aging overpack; CTT = cask transfer trolley; DE = direct exposure; ESD = event sequence diagram; INIT = initiating; ITC = important to criticality; NUMB = number; RR = radionuclide release; ST = site transporter; TAD = transportation, aging, and disposal canister.

Source: Original

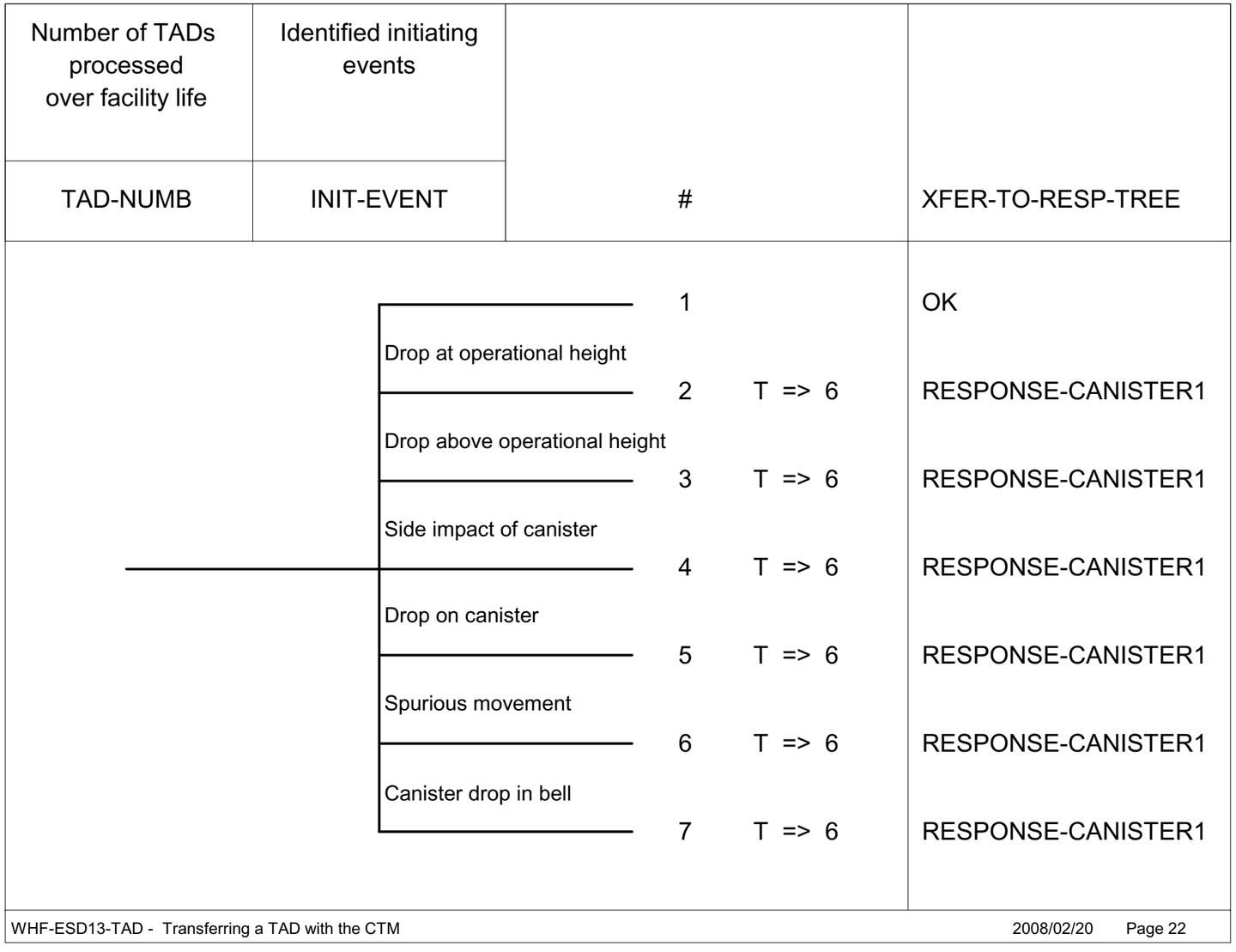
Figure A5-21. Event Tree WHF-ESD12-TAD– CTT/Site Transporter Colliding with Cask Loading Shield Door



NOTE: CTM = canister transfer machine; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-22. Event Tree WHF-ESD13-DPC – Transferring a DPC with the CTM



NOTE: CTM = canister transfer machine; DPC = dual-purpose canister; INIT = initiating; NUMB = number; RR = radionuclide release; T = transfer; TAD = transportation, aging, and disposal canister; XFER = transfer.

Source: Original

Figure A5-23. Event Tree WHF-ESD13-TAD – Transferring a DPC with the CTM

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Impact to Cask	2 T => 8	RESPONSE-STC1
	Cask tipover	3 T => 8	RESPONSE-STC1
WHF-ESD14-DPC - Transfer of a STC/DPC from Cask Unload Room to Preparation Station		2007/11/02	Page 23

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; STC = shielded transfer cask; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-24. Event Tree WHF-ESD14-DPC – Transfer of a STC/DPC from Cask Unload Room to Preparation Station

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Side impact	2 T => 8	RESPONSE-STC1
	Drop on cask	3 T => 8	RESPONSE-STC1
	~~Drop at operational~~ height	4 T => 8	RESPONSE-STC1
	~~Drop above~~ operational height	5 T => 8	RESPONSE-STC1
	STC/DPC tip over	6 T => 8	RESPONSE-STC1
WHF-ESD15-DPC - Transfer of STC/DPC from Prep Station to Cutting Station		2007/11/02	Page 24

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; STC = shielded transfer cask; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-25. Event Tree WHF-ESD15-DPC – Transfer of STC/DPC from Preparation Station to Cutting Station

Number of CSNF processed over the WHF life	Identify initiating events		
CSNF-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Impact to cask valves	2 T => 26	RESPONSE-PREPSTATION
	Sample line break	3 T => 26	RESPONSE-PREPSTATION
	Cask overpressure	4 T => 26	RESPONSE-PREPSTATION
WHF-ESD16-CSNF - Transportation Cask/CSNF Preparation at Preparation Station		2008/02/20	Page 25

NOTE: CSNF = commercial spent nuclear fuel; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-26. Event Tree WHF-ESD16-CSNF – Transportation Cask/Commercial SNF Preparation at Preparation Station

	Confinement boundary intact	Moderator excluded from entering cask		
INIT-EVENT	CONFINEMENT	MODERATOR	#	END-STATE-NAMES
			1	RR-FILTERED
			2	RR-FILTERED-ITC
			3	RR-UNFILTERED
			4	RR-UNFILTERED-ITC
RESPONSE-PREPSTATION - Response to preparation activites at Cask Preparation Area			2007/12/06	Page 26

NOTE: INIT = initiating; ITC = important to criticality; NUMB = number; PREP = preparation; RR = radionuclide release; RESP = response.

Source: Original

Figure A5-27. Event Tree RESPONSE – PREP STATION – Response to Preparation Activities at Cask Preparation Area

Number of DPCs processed over the WHF life	Identified initiating events	#		XFER-TO-RESP-TREE
DPC-NUMB	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	Impact to canister valves	2	T => 26	RESPONSE-PREPSTATION
	Sampling line break	3	T => 26	RESPONSE-PREPSTATION
	Overpressurization of canister	4	T => 26	RESPONSE-PREPSTATION
WHF-ESD17-DPC - Preparation of STC/DPC at the DPC Cutting Station			2007/12/10	Page 27

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; PREP = preparation; RESP = response; STC = shielded transfer cask; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-28. Event Tree WHF-ESD17-DPC – Preparation of STC/DPC at the DPC Cutting Station

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Drop on canister vent lines	2 T => 26	RESPONSE-PREPSTATION
WHF-ESD18-DPC - DPC Cutting at the DPC Cutting Station		2007/11/02	Page 28

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

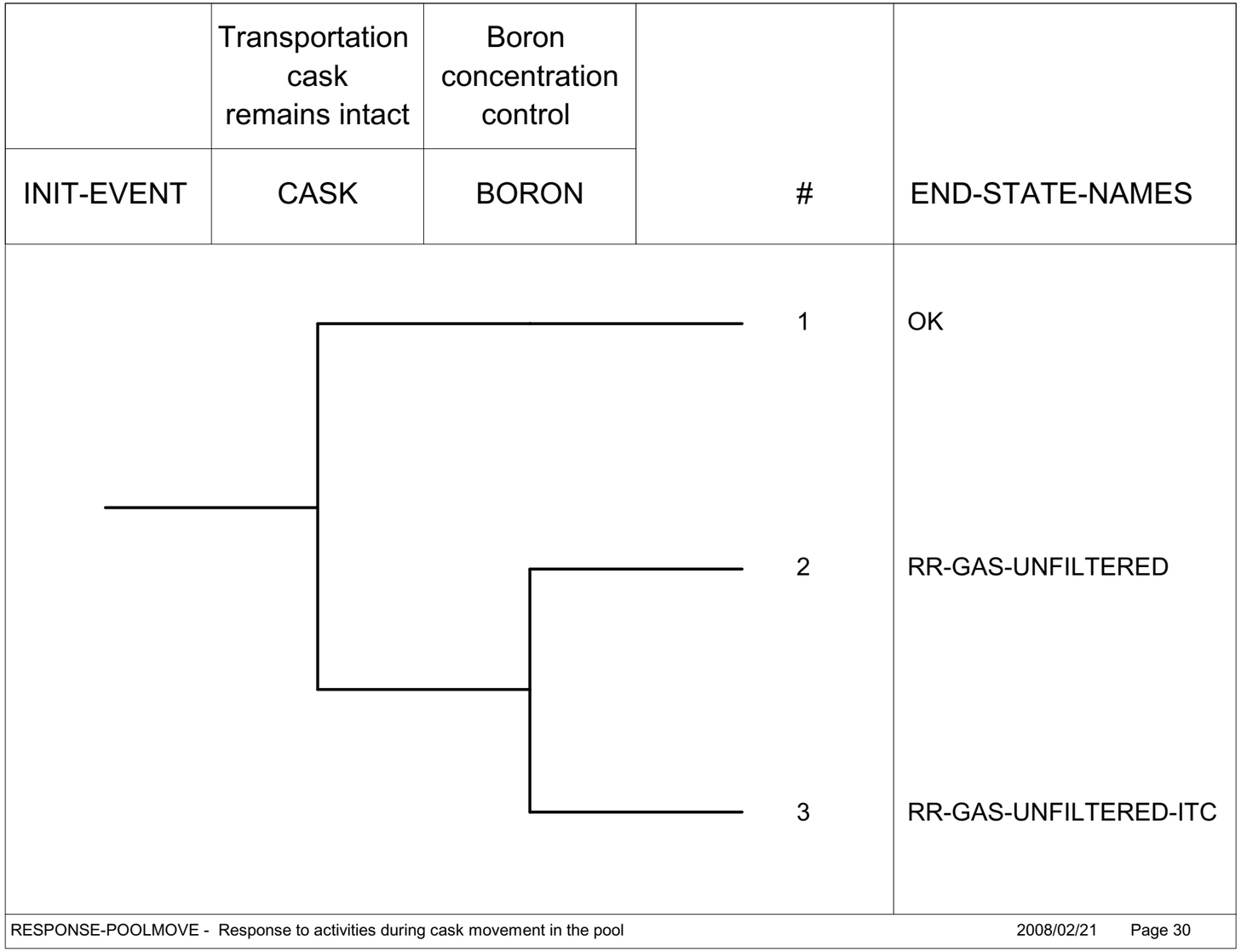
Figure A5-29. Event Tree WHF-ESD18-DPC – DPC Cutting at the DPC Cutting Station

Number of DPCs processed over the WHF life	Identified initiating events		
DPC-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
	Impact to Cask - Pool	1	OK
	Drop on Cask - Pool	2 T => 30	RESPONSE-POOLMOVE
	Drop at Operation Height - Pool	3 T => 30	RESPONSE-POOLMOVE
	Drop Above Operation Height - Pool	4 T => 30	RESPONSE-POOLMOVE
	Cask Tips Over - Pool	5 T => 30	RESPONSE-POOLMOVE
	Impact to Cask - Floor	6 T => 30	RESPONSE-POOLMOVE
	Drop on Cask - Floor	7 T => 8	RESPONSE-STC1
	Drop at Operation Height - Floor	8 T => 8	RESPONSE-STC1
	Drop Above Operation Height - Floor	9 T => 8	RESPONSE-STC1
	Cask Tips Over - Floor	10 T => 8	RESPONSE-STC1
		11 T => 8	RESPONSE-STC1
WHF-ESD19-DPC - Transfer of STC/DPC from Prep Station to Pool Ledge		2008/01/04	Page 29

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; PREP = preparation; RESP = response; STC = shielded transfer cask; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

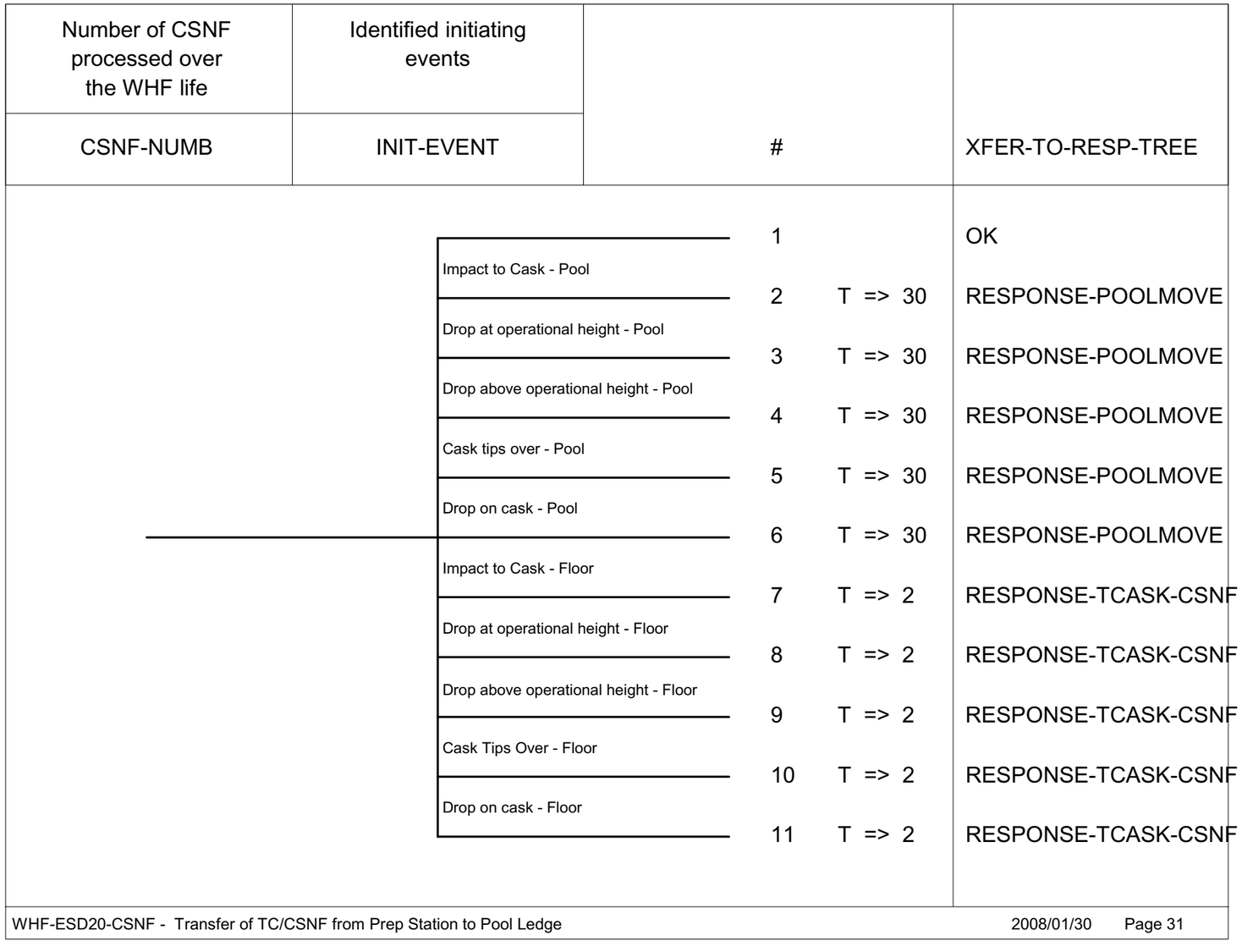
Figure A5-30. Event Tree WHF-ESD19-DPC – Transfer of STC/DPC from Preparation Station to Pool Ledge



NOTE: INIT = initiating; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-31 Event Tree RESPONSE-POOLMOVE – Response to Activities during Cask Movement in the Pool



NOTE: CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

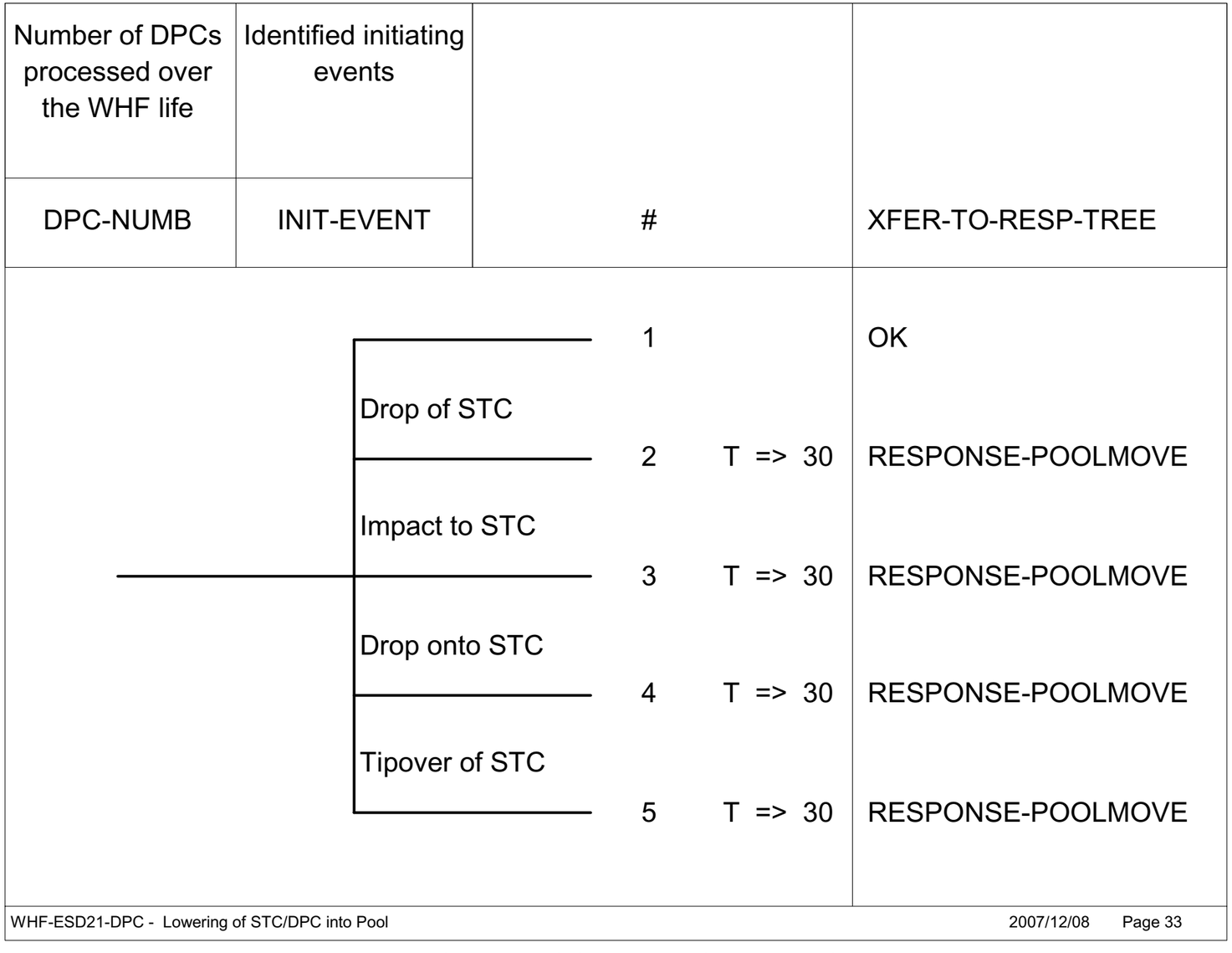
Figure A5-32. Event Tree WHF-ESD20-CSNF – Transfer of Transportation Cask/CSNF from Preparation Station to Pool Ledge

Number of CSNF processed over the WHF life	Identified initiating events		
CSNF-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
	Drop of TC	1	OK
		2 T => 30	RESPONSE-POOLMOVE
	Impact to TC	3 T => 30	RESPONSE-POOLMOVE
	Tipover of TC	4 T => 30	RESPONSE-POOLMOVE
	Drop onto TC	5 T => 30	RESPONSE-POOLMOVE
WHF-ESD21-CSNF - Lowering of TC/CSNF into Pool		2007/12/08	Page 32

NOTE: CSNF = commercial spent nuclear fuel; INIT = initiating; RESP = response; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-33. Event Tree WHF-ESD21-CSNF – Lowering of Transportation Cask/Commercial SNF into Pool



NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; STC = shielded transfer cask; T = transfer; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-34. Event Tree WHF-ESD21-DPC – Lowering of STC/DPC into Pool

Number of TADs processed over facility life	Identified initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Drop of STC	2 T => 30	RESPONSE-POOLMOVE
	Impact to STC	3 T => 30	RESPONSE-POOLMOVE
	Drop onto STC	4 T => 30	RESPONSE-POOLMOVE
	Tipover of STC	5 T => 30	RESPONSE-POOLMOVE
WHF-ESD21-TAD - Removing TAD from Pool Bottom		2007/12/08	Page 34

NOTE: ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; STC = shielded transfer cask; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-35. Event Tree WHF-ESD21-TAD – Removing TAD from Pool Bottom

Number of fuel assemblies processed over facility life	Identified initiating events		
FUEL-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Drop onto rack	2 T => 36	RESPONSE-POOLCONFINE
	Drop of bundle	3 T => 36	RESPONSE-POOLCONFINE
WHF-ESD22-FUEL - Transfer of Fuel Assembly to TAD		2007/12/10	Page 35

NOTE: INIT = initiating; NUMB = number; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility.

Source: Original

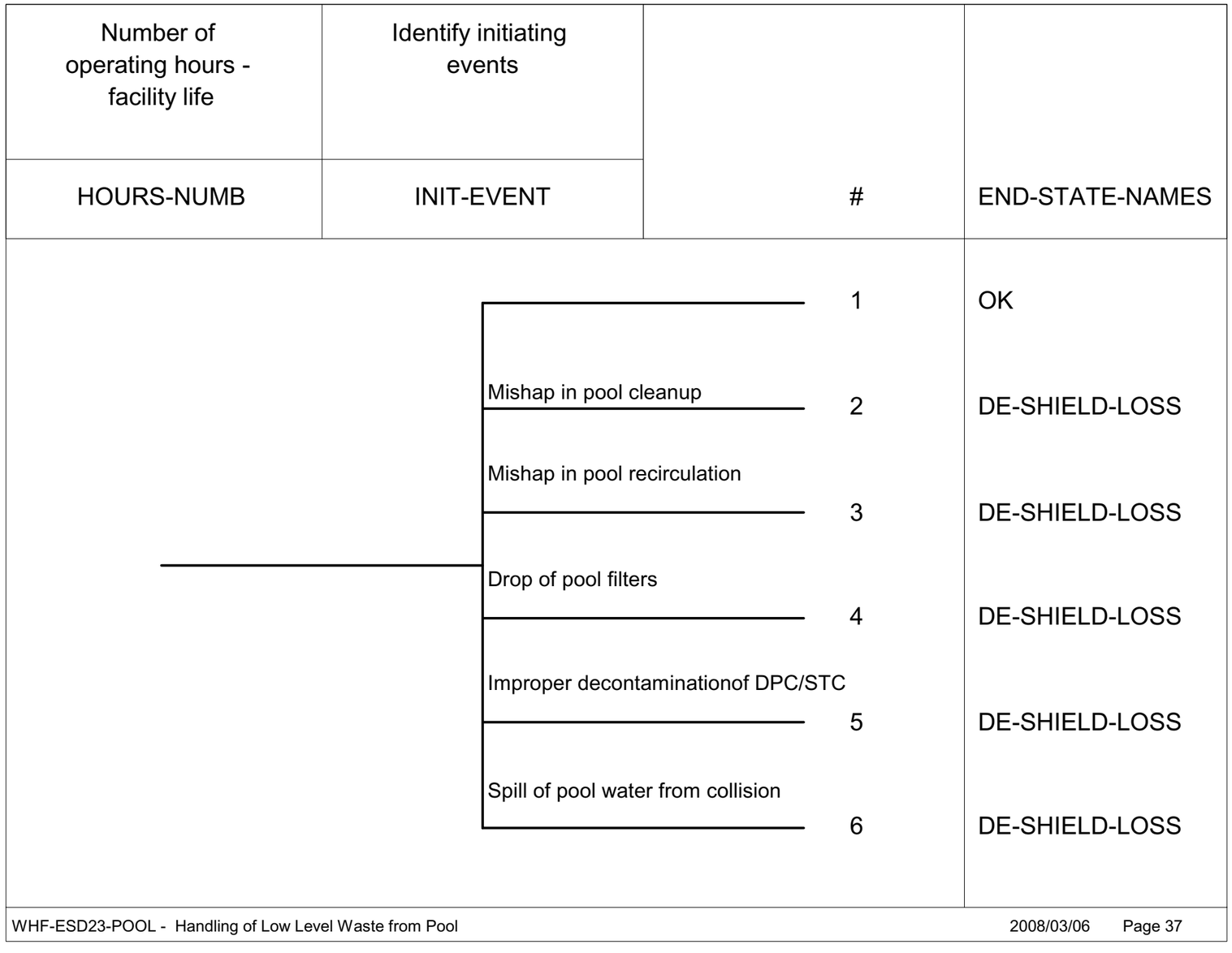
Figure A5-36. Event Tree WHF-ESD22-FUEL – Transfer of Fuel Assembly to TAD Canister

	Boron concentration control maintained		
INIT-EVENT	BORON	#	END-STATE-NAMES
		1	RR-GAS-UNFILTERED
		2	RR-GAS-UNFILTERED-ITC
RESPONSE-POOLCONFINE - Pool confinement failures		2008/02/21	Page 36

NOTE: INIT = initiating; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-37 Event Tree RESPONSE-POOLCONFINE – Pool Confinement Failures



NOTE: DE = direct exposure; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; NUMB = number; STC = shielded transfer cask; WHF = Wet Handling Facility.

Source: Original

Figure A5-38. Event Tree WHF-ESD23-POOL – Handling of Low-Level Waste from Pool

Number of TADs processed over the WHF life	Identified initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
	Impact of STC/TAD - Pool	1	OK
	Drop at operational height - Pool	2 T => 30	RESPONSE-POOLMOVE
	Drop above operational height - Pool	3 T => 30	RESPONSE-POOLMOVE
	Tip over of STC/TAD - Pool	4 T => 30	RESPONSE-POOLMOVE
	Drop on STC/TAD - Pool	5 T => 30	RESPONSE-POOLMOVE
	Impact of STC/TAD - Floor	6 T => 30	RESPONSE-POOLMOVE
	Drop at operational height - Floor	7 T => 8	RESPONSE-STC1
	Drop above operational height - Floor	8 T => 8	RESPONSE-STC1
	Tip over of STC/TAD - Floor	9 T => 8	RESPONSE-STC1
	Drop on STC/TAD - Floor	10 T => 8	RESPONSE-STC1
		11 T => 8	RESPONSE-STC1
WHF-ESD24-TAD - Transfer of STC/TAD from Pool Ledge to Prep Area		2007/12/08 Page 38	

NOTE: ESD = event sequence diagram; INIT = initiating; PREP = preparation; RESP = response; STC = shielded transfer cask; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-39. Event Tree WHF-ESD24-TAD – Transfer of STC/TAD from Pool Ledge to Preparation Area

Number of TADs processed over the WHF life	Identified initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Object dropped onto TAD	2 T => 40	RESPONSE-TAD
	Side impact to cask	3 T => 40	RESPONSE-TAD

WHF-ESD25-TAD - Assembly and Closure of STC/TAD 2007/12/10 Page 39

NOTE: ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; STC = shielded transfer cask; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-40. Event Tree WHF-ESD25-TAD – Assembly and Closure of STC/TAD

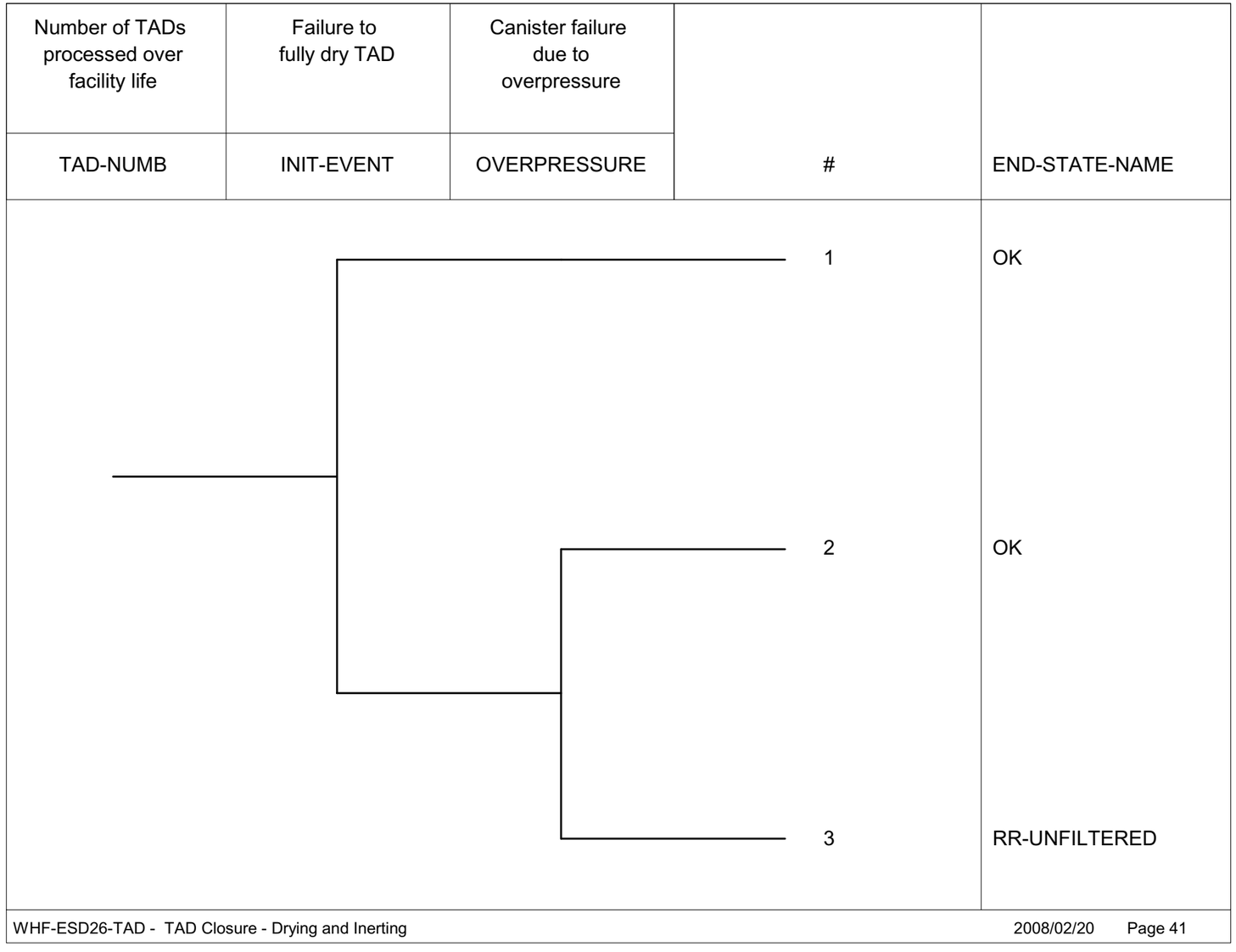
	TAD remains intact	Confinement boundary intact	Moderator excluded from entering canister		
INIT-EVENT	TAD	CONFINEMENT	MODERATOR	#	END-STATE-NAMES
				1	OK
				2	RR-FILTERED
				3	RR-FILTERED-ITC
				4	RR-UNFILTERED
				5	RR-UNFILTERED-ITC

RESPONSE-TAD - Response to TAD closure 2007/11/02 Page 40

NOTE: INIT = initiating; ITC = important to criticality; RR = radionuclide release; TAD = transportation, aging, and disposal canister.

Source: Original

Figure A5-41. Event Tree RESPONSE-TAD – Response to TAD Closure



NOTE: ESD = event sequence diagram; INIT = initiating; RESP = response; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-42. Event Tree WHF-ESD26-TAD – TAD Closure - Drying and Inerting

Number of TADs processed over facility life	Identify initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Bad weld - improper or cracked	2 T => 26	RESPONSE-PREPSTATION
	Line break	3 T => 26	RESPONSE-PREPSTATION

NOTE: INIT = initiating; NUMB = number; RESP = response; T = transfer; TAD = transportation, aging, and disposal canister; XFER = transfer.

Source: Original

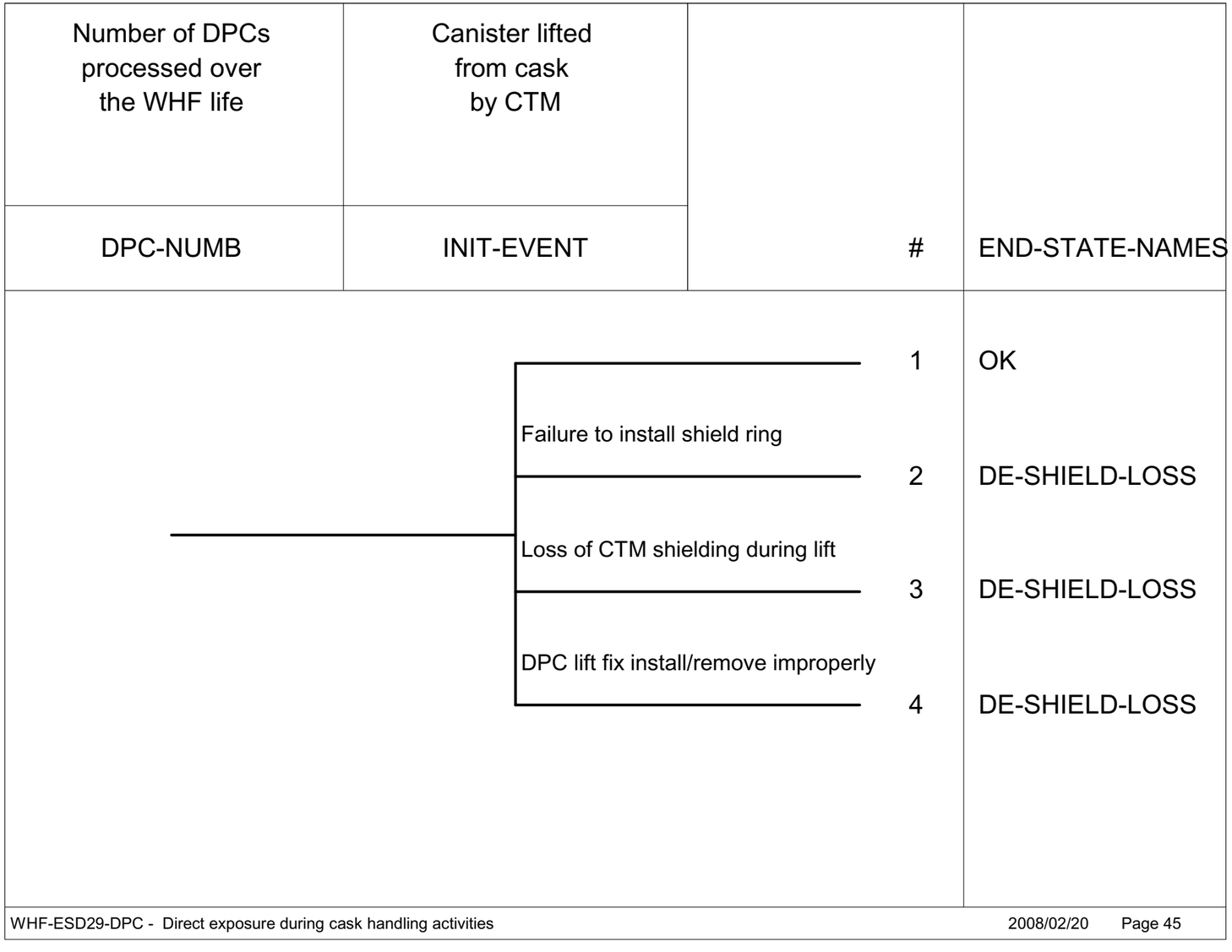
Figure A5-43. Event Tree WHF-ESD27-TAD– TAD Canister Closure Process

Number of TADs processed over facility life	Identified initiating events		
TAD-NUMB	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Drop on TAD	2 T => 8	RESPONSE-STC1
	Drop at operational height	3 T => 8	RESPONSE-STC1
	Drop above operational height	4 T => 8	RESPONSE-STC1
	Impact to TAD	5 T => 8	RESPONSE-STC1
	TAD tip over	6 T => 8	RESPONSE-STC1
WHF-ESD28-TAD - Transfer of TAD from TAD Closure Station to CTT		2008/02/22	Page 44

NOTE: CTT = cask transfer trolley; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

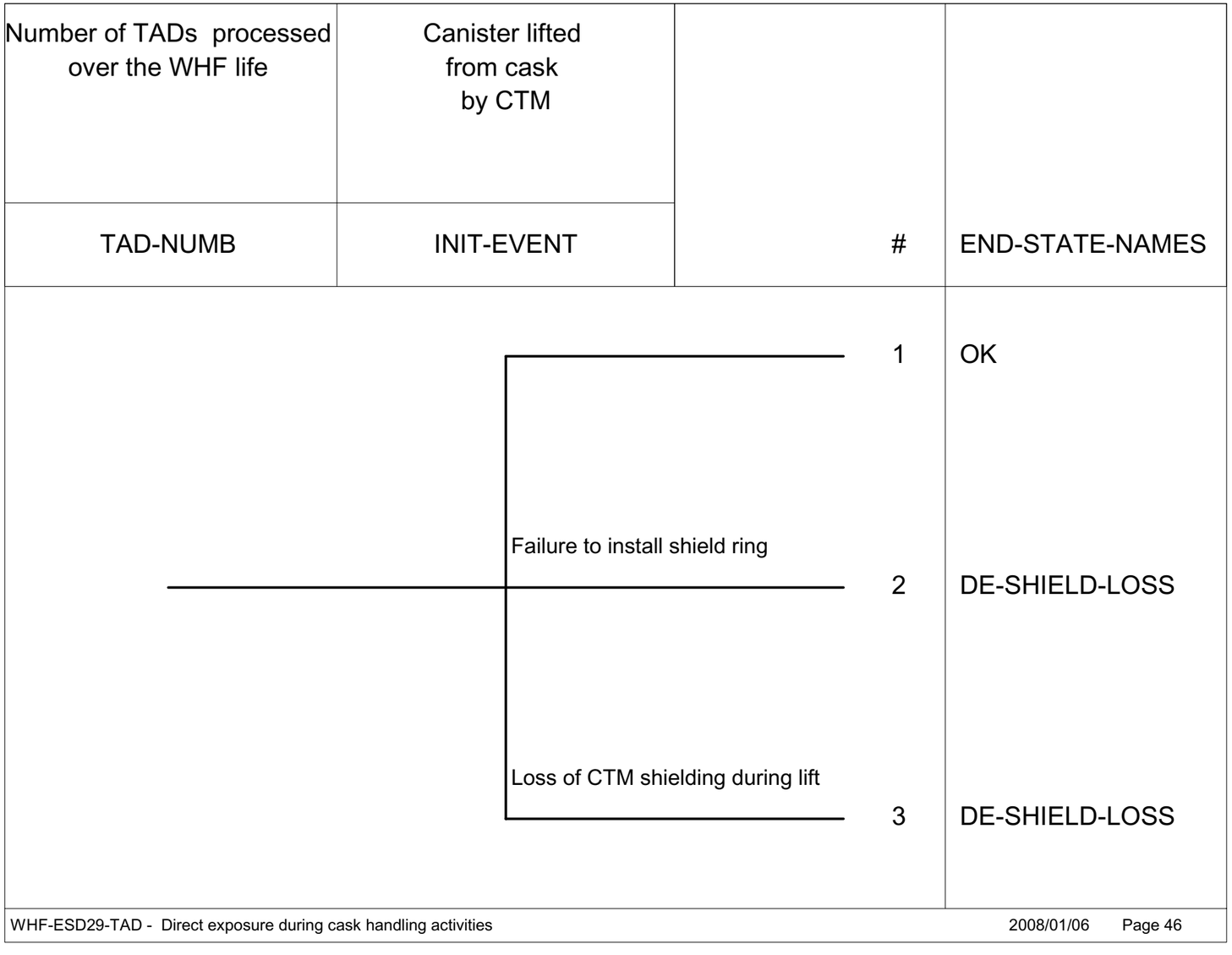
Figure A5-44. Event Tree WHF-ESD28-TAD – Transfer of TAD from TAD Closure Station to CTT



NOTE: CTM = canister transfer machine; DE = direct exposure; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; WHF = Wet Handling Facility.

Source: Original

Figure A5-45. Event Tree WHF-ESD29-DPC – Direct Exposure During Cask Handling Activities



NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility.

Source Original

Figure A5-46. Event Tree WHF-ESD29-TAD – Direct Exposure During Cask Handling Activities

Number of DPCs processed over the WHF life	Identify initiating events		
DPC-NUMB	INIT-EVENT	#	END-STATE-NAMES
		1	OK
	Exposure to pool splash	2	DE-SHIELD-LOSS
	Improper decontamination	3	DE-SHIELD-LOSS
WHF-ESD30-DPC - Direct exposure during pool activities		2007/11/02	Page 47

NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating; NUMB = number; WHF = Wet Handling Facility.

Source: Original

Figure A5-47. Event Tree WHF-ESD30-DPC – Direct Exposure During Pool Activities

Number of fuel assemblies transferred during facility life	Identify initiating events		
FUEL-NUMB	INIT-EVENT	#	END-STATE-NAMES
		1	OK
	Fuel assembly lifted too high	2	DE-SHIELD-LOSS
WHF-ESD30-FUEL - Direct exposure during pool activities		2007/11/02	Page 48

NOTE: DE = direct exposure; ESD = event sequence diagram; INIT = initiating NUMB = number; WHF = Wet Handling Facility.

Source: Original

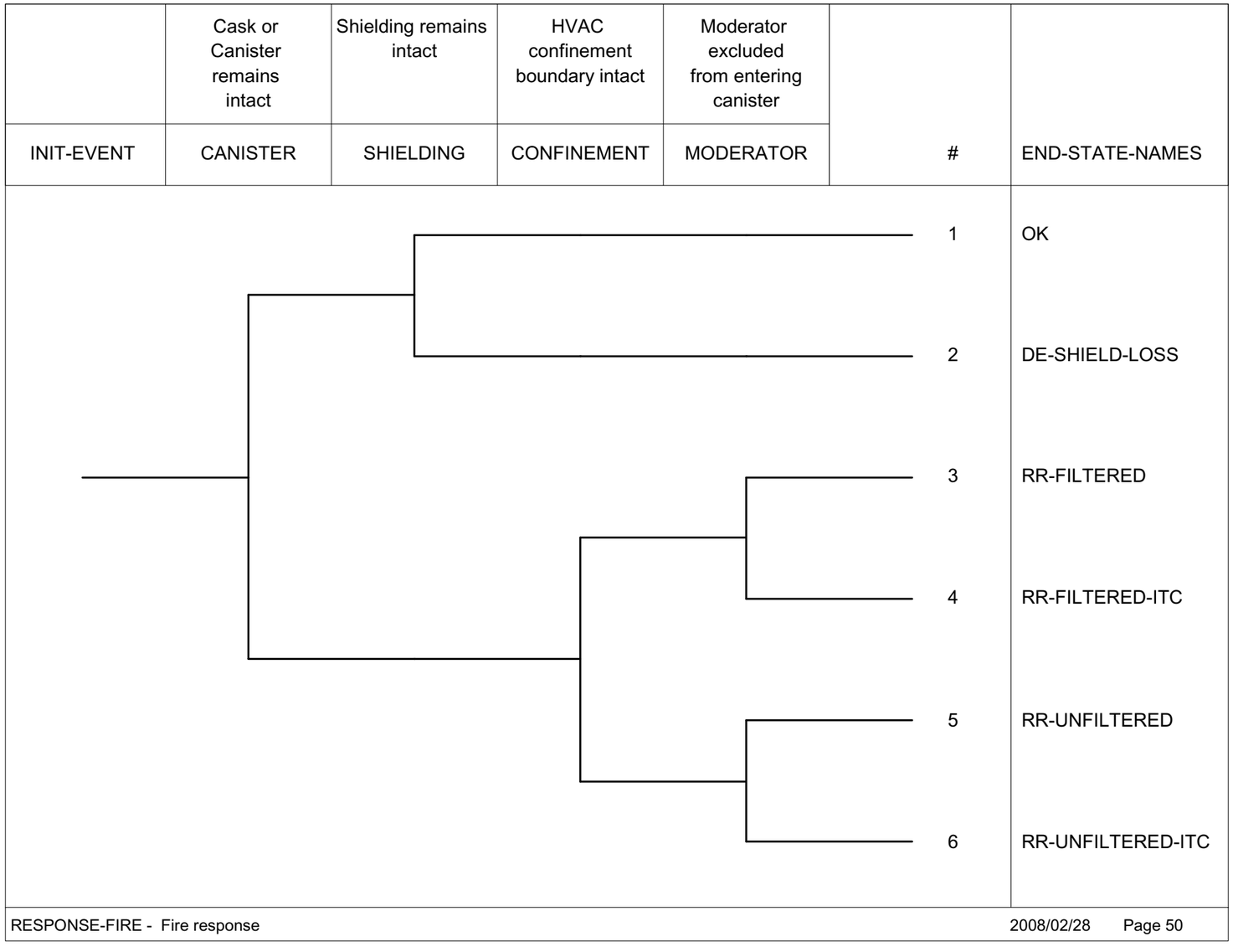
Figure A5-48. Event Tree WHF-ESD30-FUEL – Direct Exposure During Pool Activities

Number of CSNF processed over the WHF life	Identified initiating events	#	XFER-to-RESP-TREE
CSNF-NUMB	INIT-EVENT	#	XFER-to-RESP-TREE
		1	OK
	Local Fire - TC Vestibule	2 T => 50	REPONSE-FIRE
	Local Fire - Preparation Area	3 T => 50	REPONSE-FIRE
	Large fire affects CSNF	4 T => 50	REPONSE-FIRE
WHF-ESD31-CSNF - Fire occurring in the WHF - CSNF		2007/11/02 Page 49	

NOTE: CSNF = commercial spent nuclear fuel; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; T = transfer; TC = transportation cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

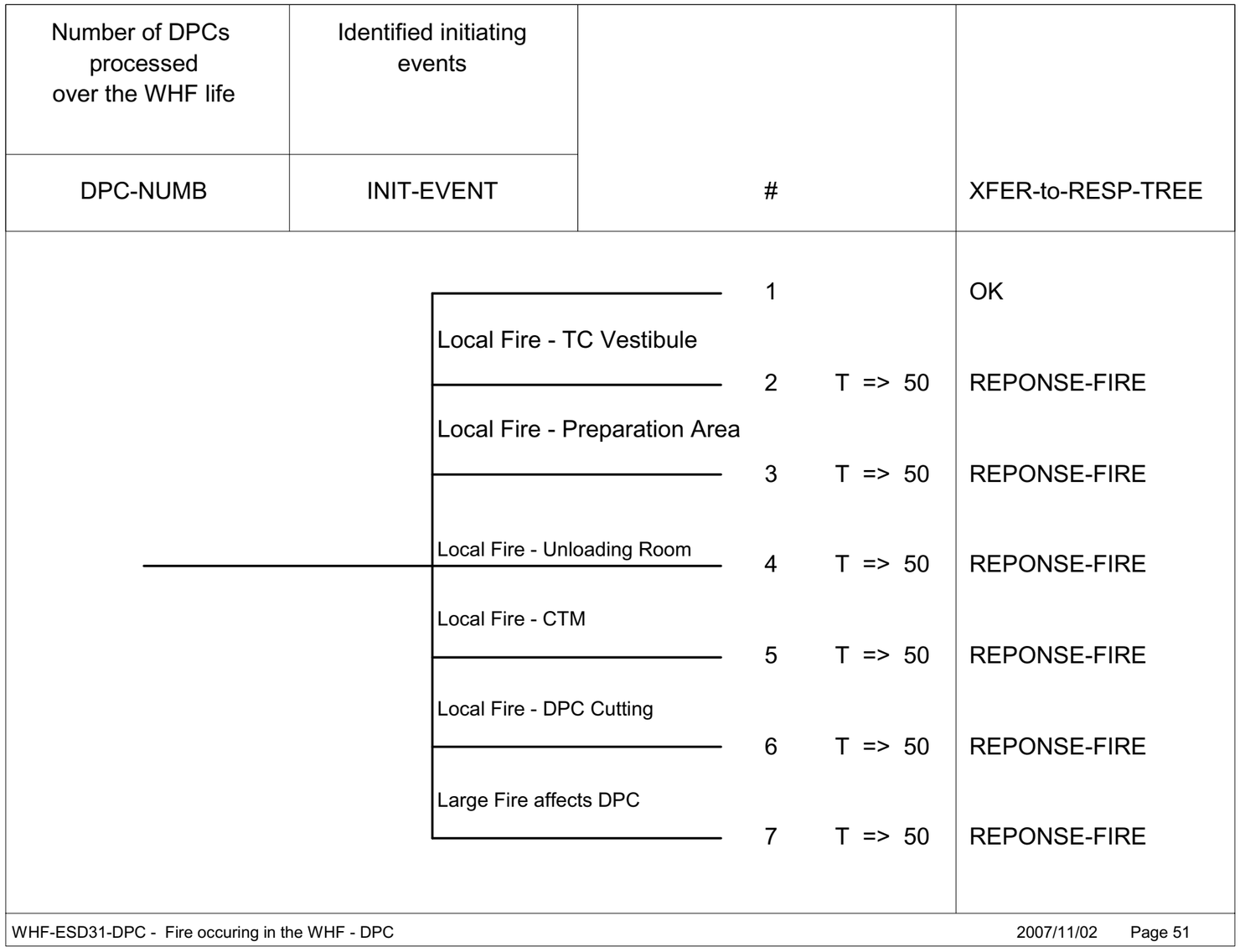
Figure A5-49. Event Tree WHF-ESD31-CSNF – Fire Occurring in the WHF-Commercial SNF



NOTE: HVAC = heating, ventilation, and air conditioning; INIT = initiating; ITC = important to criticality; RR = radionuclide release.

Source: Original

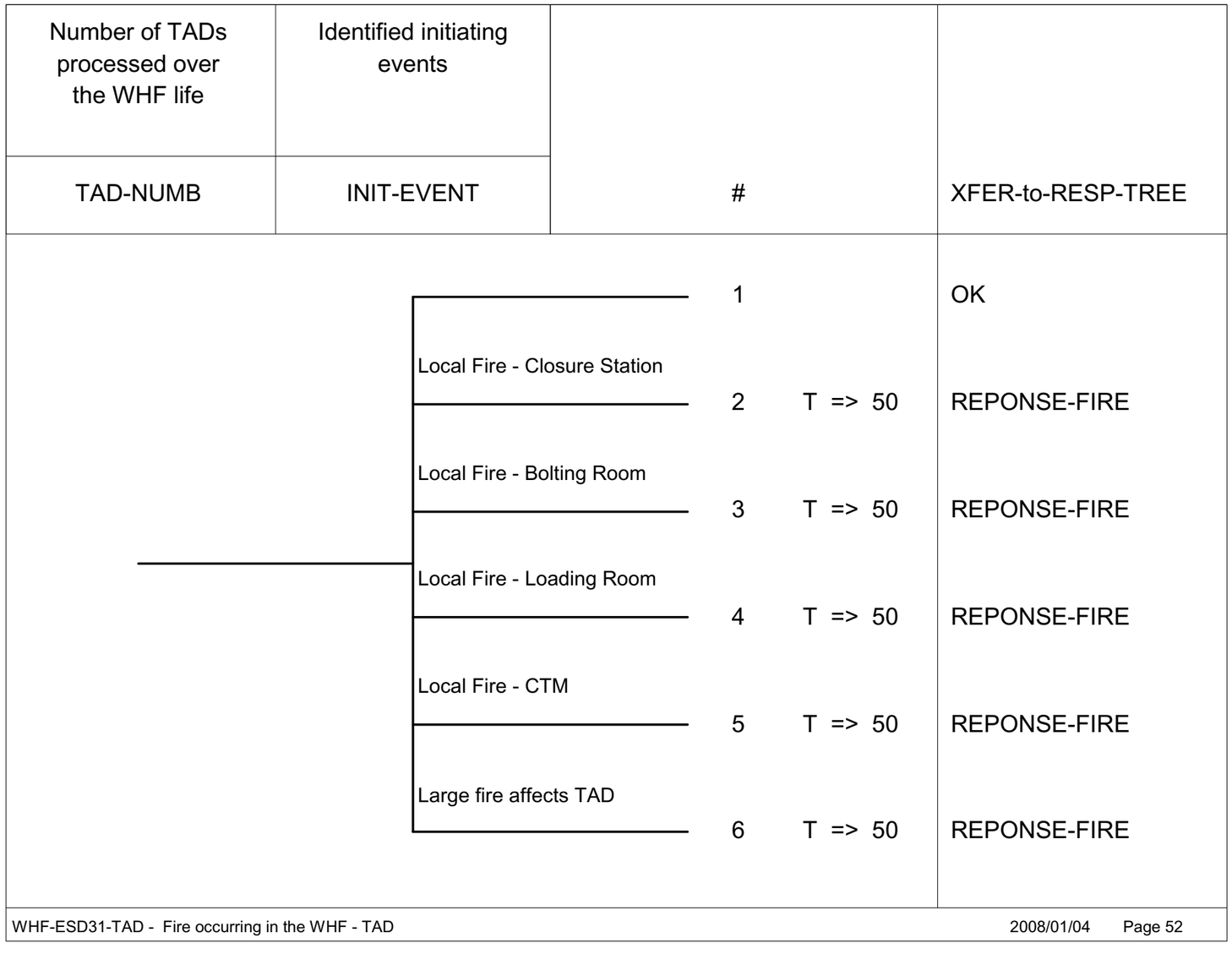
Figure A5-50. Event Tree RESPONSE-FIRE – Fire Response



NOTE: CTM = canister transfer machine; DPC = dual-purpose canister; ESD = event sequence diagram; INIT = initiating; RESP = response; T = transfer; TC = transportation cask; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-51. Event Tree WHF-ESD31-DPC – Fire Occurring in the WHF-DPC



NOTE: CTM = cask transfer machine; ESD = event sequence diagram; INIT = initiating; NUMB = number; RESP = response; ST = site transporter; T = transfer; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility; XFER = transfer.

Source: Original

Figure A5-52. Event Tree WHF-ESD31-TAD – Fire Occurring in the WHF-TAD

ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

CONTENTS

Page

CONTENTS (Continued)

Page

FIGURES

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

TABLES

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

ACRONYMS AND ABBREVIATIONS

Acronyms

AAR	Association of American Railroads
ASD	adjustable speed drive
AHU	air handling unit
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
CTT	cask transfer trolley
CTM	canister transfer machine
DOE	U.S. Department of Energy
ESD	event sequence diagram
FRA	Federal Railroad Administration
HLW	high-level radioactive waste
IHF	Initial Handling Facility
ITS	important to safety
MCO	multicanister overpack
NHTSA	National Highway Traffic Safety Administration
PLC	programmable logic controller
RF	Receipt Facility
RHS	remote handling system
SFP	single failure point
SNF	spent nuclear fuel
SPM	site prime mover
SPMRC	site prime mover railcar
SPMTT	site prime mover truck trailer
TEV	transport and emplacement vehicle
WHF	Wet Handling Facility
WPTT	waste package transfer trolley

ACRONYMS AND ABBREVIATIONS (Continued)

Abbreviations

AC	alternating current
DC	direct current
fpm	foot per minute
psi	pound per square inch
scfm	standard cubic foot per minute

ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

This attachment presents system and pivotal event fault trees that are used in the event trees described in Attachment A. The system fault trees are presented and described in Section B1 through B10, on a system basis. For the most part, the pivotal events link to a basic event and these are presented in tables. In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the system fault tree or basic event level. These supplemental fault trees are presented and described.

B1 SITE PRIME MOVER ANALYSIS – FAULT TREES

B1.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B1.1.1 *AAR S-2043. 2003. *Performance Specification for Trains Used to Carry High-Level Radioactive Material.* Washington, D.C.: Association of American Railroads. TIC: 257585.

Design Constraints

B1.1.2 49 CFR 571 2007. Transportation: Federal Motor Vehicle Safety Standards.

B1.1.3 Motor Vehicle Safety. 49 U.S.C. 301.

B1.2 SITE PRIME MOVER DESCRIPTION

B1.2.1 Overview

The site prime mover (SPM) is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs during Intra-Site Operations and within the Canister Receipt and Closure Facility (CRCF), the Wet Handling Facility (WHF), the Initial Handling Facility (IHF) and the Receipt Facility (RF).

Movement of the site prime mover railcar or site prime mover truck trailer within the WHF is limited to the entry vestibule and the Cask Preparation Area. The SPM arrives at the WHF with a transportation cask that may contain:

- Commercial spent nuclear fuel (SNF) canisters
- Dual-purpose canisters (DPCs).

DPCs may also arrive in aging overpacks on a site transporter and Hi-Star DPCs arrive on a horizontal cask transfer trailer. These conveyances are described in later sections of this attachment.

B1.2.2 System Description

B1.2.2.1 Site Prime Mover

The SPM is a commercially available vehicle that has the capability of moving both railcars and truck trailers loaded with transportation casks. Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations.

The driving and braking power comes directly from the road tires, as they are in contact with the rails. Weight sharing between the flanged rail and regular road wheels is automatically varied to achieve the required power transmission needs. More weight can be distributed on the rail wheels when moving, or more on the road wheels when braking, accelerating and negotiating inclines. The SPM has speed limiters that set the maximum speed of the vehicle to less than 9.0 miles per hour for Intrasite movements.

During Intrasite activities, the diesel engine drives the generator, which provides the required 480V, 3-phase, 60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480V, 3-phase, 60 Hz power is supplied to the generator. The diesel engine is not used to move the railcar or truck trailer inside the facility

The SPM is equipped with both an automatic wagon coupling system for railcars and a fifth wheel coupling device for truck trailers. In addition, the SPM is equipped with high-performance compressors, priority filling system, and an electronic regulating valve with filling speed adjustments and a 100-gallon diesel fuel tank.

B1.2.2.2 Railcars

Railcars used for movement of transportation casks are designed in accordance with the Federal Railroad Administration (FRA) requirements under authority delegated by the Secretary of Transportation. The FRA administers a safety program that oversees the movement of nuclear shipments throughout the Nation's rail transportation system. Performance standards are addressed in the Association of American Railroads Standard S-2043 Draft (Ref. B1.1.1).

B1.2.2.3 Truck Trailers

The U.S. Department of Transportation (DOT) has the primary responsibility for regulating the safe transport of radioactive materials in the United States. It sets the standards for packaging,

transporting, and handling radioactive materials, including labeling, shipping papers, loading, and unloading requirements.

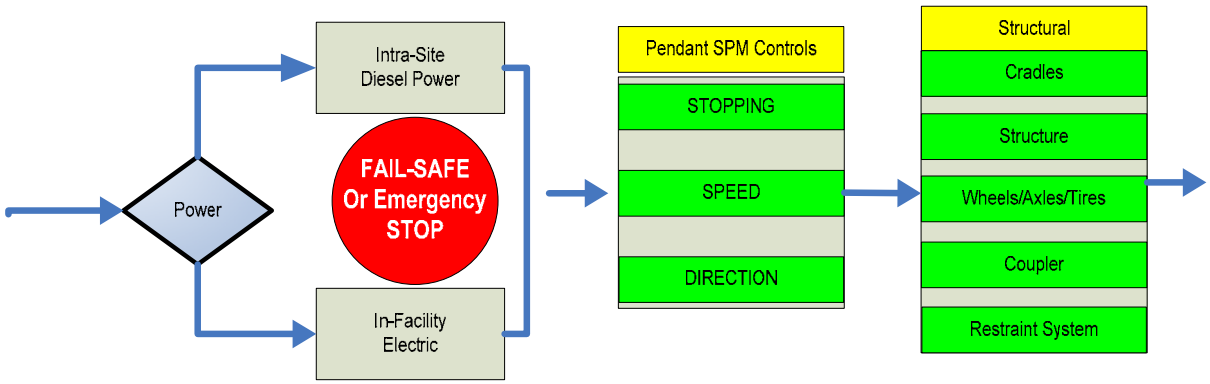
Trailers used for the movement of transportation casks are designed in accordance with the National Highway Traffic Safety Administration (NHTSA) requirements as authorized by 49 USC Part 301 (Motor Vehicle Safety: Standards and Compliance, Section 30111(Ref. B1.1.3)). The requirements are delineated in 49 CFR Part 571 (Ref. B1.1.2).

B1.2.2.4 Sub-Systems

The SPM railcar and SPM truck trailer systems are composed of four subsystems:

- Power plant—a diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all Intra-Site Operations. For operations conducted inside facilities, the SPM is connected to facility 480V, 3-phase, 60 Hz power.
- Vehicle controls—during Intra-Site Operations, the operator controls the SPM at the operator's console inside the SPM. For all operations inside of the WHF, the operator controls the SPM with either a remote (wireless) controller or through a pendant connected to the vehicle.
- Structural controls-these subsystems include restraints for securing the transportation casks to the railcar/truck trailer; automatic coupler hardware; cradles for supporting the transportation cask; and wheels/tires and axles.
- Brakes—for the railcar comply with FRA requirements and for the truck trailer the braking system complies with 49 CFR Part 571 (Ref. B1.1.2).

A simplified schematic of the functional components on the SPM railcar/truck trailer is shown in Figure B1.2-1.



Source: Original

Figure B1.2-1. Site Prime Mover Simplified Schematic Intra-Site and In-Facility

B1.2.3 Operations

B1.2.3.1 Normal Operations

In-facility SPM operations begin when the SPM has positioned the railcar/truck trailer outside the entry vestibule at the facility such that the railcar/truck trailer is pushed into the facility. The SPM diesel engine is shut down and the outer and inner vestibule door is opened. Facility 480V, 3-phase, 60 Hz power is connected to the SPM for all operations inside the facility. The SPM is never operated inside a facility using the diesel engine.

The operator connects the pendant controller or uses a remote (wireless) controller to move the railcar/truck trailer into the Transportation Cask Vestibule and Transportation Cask Vestibule Annex. Once inside, the outer vestibule door is closed. The Cask Preparation Room Annex door is then opened and the SPM moves the railcar/truck trailer into position in the Cask Preparation Area. Once in position, the SPM is disconnected from the railcar/truck trailer and returns to the Transportation Cask Vestibule. The Cask Preparation Room Annex door is then closed. The outer vestibule door can then be opened and the SPM exits the facility. Once outside, the SPM is shut down and the facility power is removed and the inner and outer vestibule doors are closed.

B1.2.3.2 Site Prime Mover Off-Normal Operations

In the event of loss of power, the SPM is designed to stop, retain control of the railcar/truck trailer, and enter a locked mode. Upon the restoration of power the SPM stays in the locked mode until operator action is taken to return to normal operations.

B1.2.3.3 Site Prime Mover Testing and Maintenance

Testing and maintenance of the SPM is done on a periodic basis and does not affect the normal operations of the SPM. Testing and/or maintenance are not performed on a SPM when it is coupled with a railcar/truck trailer. A SPM that has malfunctioned or has a warning light lit on the SPM will be deemed unserviceable and turned in for maintenance. Unserviceable vehicles will not be used.

If an unserviceable state is identified during movement, the operator puts the SPM in a safe state (as quickly as possible) and recovery actions for the SPM are invoked.

B1.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with system, structures, and components. The five areas considered are addressed in Table B1.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B1.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Structural	Material failure Coupler Wheels/tires/axle	—	—	—	—
Brakes	Material failure	—	—	Failure to engage (set)	—
Power plant	Governor fails Safe state on	—	—	Failure to stop	—
Remote control	Spurious commands	—	—	Improper command	Collide with end stops

Source: Original

B1.4 SITE PRIME MOVER RELATED FAILURE SCENARIOS

There are various top events for the SPM operating inside the WHF. Table B1.4-1 provides a cross reference between the Event Sequence Diagram (ESD) and the SPM fault trees that support them.

Table B1.4-1. ESD Cross Reference with SPM Railcar/Truck Trailer Fault Trees

WHF ESD Number	SPMTT Collision	SPMRC Collision	SPMRC Derailment	SPMTT Rollover
ESD01-CSNF	X	-	-	X
ESD02-DPC		X	X	

NOTE: ESD = event sequence diagram; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.

Source: Original

There are three basic SPM fault trees developed for the WHF. The top events for these fault trees and the variations are:

- Prime mover with railcar or truck trailer collides with WHF structures
  - SPM truck trailer with commercial SNF collides with WHF structures
  - SPM railcar with DPC collides with WHF structures
- Site prime mover with railcar derails during movement
  - SPM railcar with DPC derails
- Site prime mover with truck trailer rolls over
  - SPM truck trailer with commercial SNF rollover.

B1.4.1 SPM Railcar Collides with WHF Structures

B1.4.1.1 Description

SPM railcar collision within the WHF can occur as a result of human error or mechanical failures. Mechanical failures leading to a collision consist of the SPM failure to stop with commanded, the SPM exceeding a safe speed or the SPM moving in a wrong direction.

B1.4.1.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the SPM for mechanical failures and the SPM operator maintains situational awareness and proper control of the movement of the SPM. To avoid collisions, the SPM must stop when commanded, be prevented from entering a runaway situation or respond correctly to a SPM movement command.

The SPM is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the SPM by either commanding a stop from the start/stop button or by releasing the palm switch which initiates an emergency stop. At anytime there is a loss of power detected, the SPM will immediately stop all movement and enter into a "lock mode" safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a speed limiter on the diesel engine for outside movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. Simultaneous operation of the railroad wheels and the road tires is prevented by design of the SPM.

B1.4.1.3 Design Requirements and Features

Requirements

Since the dominant contributor to the SPMRC collision in the facility is human error, no priority is given to either the remote or the pendant controllers. The SPM is operated on electrical power when inside the building. The SPM is disconnected from the railcar or truck trailer in the Cask Preparation Room and moved out of the building before cask preparation activities begin.

Design Features

The SPM has two off-equipment control devices that have complete control over the SPM. The drive system limits the maximum speed of the SPM to 9.0 mph.

System Configuration and Operating Conditions

Requirements

Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a "deadman

switch." On the loss of AC power derived from the facility, the SPM immediately enters the "lock mode" safe state. The "lock mode" safe state is not reversible without specific operator action

Design Features and Inputs

Stopping the SPM is accomplished by pushing the "stop" button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source immediately respond by removing power from the propulsion system on the SPM.

Testing and Maintenance

Requirements

There is no maintenance or testing permitted on a SPM loaded with a transportation cask.

Design Feature

None.

B1.4.1.4 Fault Tree Model

The fault tree model for "SPM Railcar Collision in WHF" accounts for both human errors and/or SPM railcar hardware problems that could result in a collision. There is only one movement within the WHF. Once the SPM railcar has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the railcar and it is moved out of the facility.

The fault tree for SPM railcar and SPM truck trailer are identical; the fault tree for the SPM truck trailer is discussed in the next section.

The top event is a collision of the SPM railcar in the WHF and is shown in Figure B1.4-3. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop (Figure B1.4-4) or exceeding a safe speed (Figure B1.4-5). Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

B1.4.1.5 Basic Event Data

Table B1.4-2 contains a list of basic events used in the SPM railcar collision fault trees. The mission time has been set at one hour, which is conservative, because it will not require one hour to disconnect the SPM from the railcar and to remove it from the facility.

Table B1.4-2. Basic Event Probability for SPM Railcar Collision

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-OPRCCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000
050-OPRCINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-OPRCINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-PWR-LOSS	1	4.100E-006	4.100E-006	0.000E+000	0.000E+000
050-SPMRC-BRP000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
050-SPMRC-BRK001-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
050-SPMRC-CBP001-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
050-SPMRC-CBP001-CBP-SHC	3	1.880E-008	0.000E+000	1.880E-008	1.000E+000
050-SPMRC-CPL000-CPL-FOH	3	1.910E-006	0.000E+000	1.910E-006	1.000E+000
050-SPMRC-CT000--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-SPMRC--CT001--CT-FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-SPMRC-CT002--CT--FOH	3	6.880E-005	0.000E+000	6.880E-005	1.000E+000
050-SPMRC-CT003-CT-SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
050-SPMRC-G65000-G65-FOH	3	1.160E-005	0.000E+000	1.160E-005	1.000E+000
050-SPMRC-HC001--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
050-SPMRC-HC001--HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
050-SPMRC-IEL011-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-SPMRC-MOE000-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
050-SPMRC-SC021--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
050-SPMRC-SEL021-SEL-FOH	3	4.160E-006	0.000E+000	4.160E-006	1.000E+000
050-SPMRC-STU001-STU-FOH	3	2.107E-004	0.000E+000	4.810E-008	4.380E+003

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc = calculation; Prob = probability; Miss = mission

Source: Original

B1.4.1.5.1 Human Failure Events

Three human errors have been identified for this fault tree. Two of these failure modes have been assigned a failure probability of 1.00E+00. These human errors are:

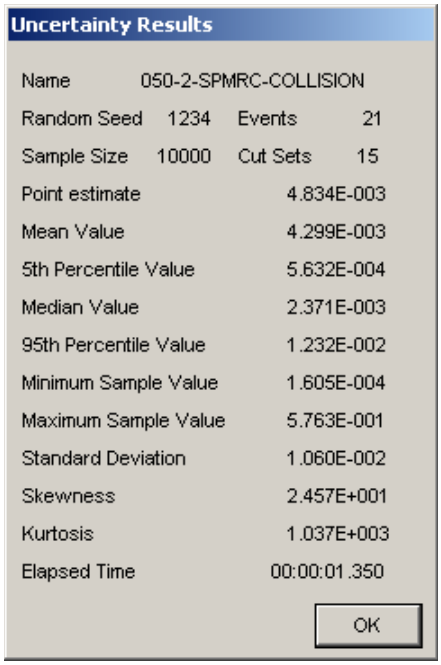
- Operator causes collision (050-OPRCCOLLIDE1-HFI-NOD)
- Operator initiates runaway (050-OPRCINTCOL01-HFI-NOD)
- Operator causes SPMTT collision with mobile platform (050-OPRCINTCOL02-HFI-NOD).

B1.4.1.5.2 Common-Cause Failures

There are no common-cause failures (CCFs) identified for this fault tree.

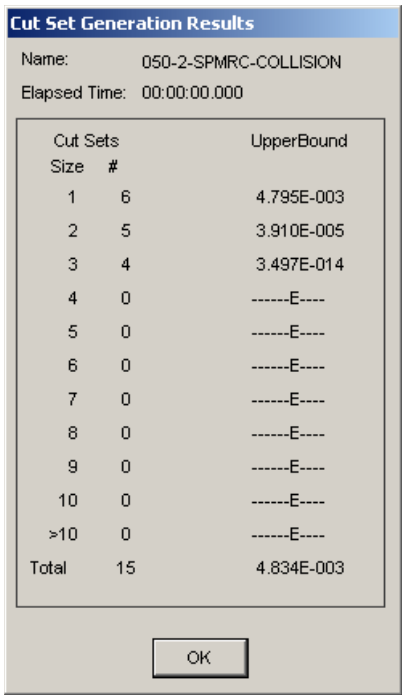
B1.4.1.6 Uncertainty and Cut Set Generation Results

Figure B1.4-1 contains the uncertainty results obtained from running the fault tree for "SPM Railcar Collision in WHF" using a cutoff probability of 1E-12. Figure B1.4-2 provides the cut set generation results for the "SPM Railcar Collision in WHF" fault tree.



Source: Original

Figure B1.4-1. Uncertainty Results of the "SPM Railcar Collision in WHF" Fault Tree



Source: Original

Figure B1.4-2. Cut Set Generation Results for the "SPM Railcar Collision in WHF" Fault Tree

B1.4.1.7 Cut Sets

Table B1.4-3 contains the cut sets for the "SPM Railcar Collision in WHF" fault tree. The probability of failure is 4.834E-3.

Table B1.4-3. Cut Sets for SPM Railcar Collision

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-2-SPMRC-COLLISION	62.07	3.000E-003	050-OPRCCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	050-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	050-SPMRC-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand Brake (Pneumatic) Failure on Demand PMRC Fails to Stop on Loss of Power	5.0E-005
	0.57	2.750E-005	050-OPRCINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000
			050-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.8E-005

Table B1.4-3. Cut Sets for PMRC Collision (Continued)

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
	0.24	1.160E-005	050-OPRCINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			050-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	050-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	050-SPMRC-CT0001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	050-SPMRC-CPL00-CPL-FOH	Railcar Automatic Coupler System Fails	1.9E-006
	0.00	7.275E-013	050-SPMRC-BRK001-BRP-FOD	SPMRC Brake (Pneumatic) Failure on Demand	5.0E-005
			050-SPMRC-CT002--CT--FOH	Pendant Direction Controller Fails	6.9E-005
			050-SPMRC-STU001-STU-FOH	SPMRC End Stops Fail	2.1E-004
	0.00	5.535E-014	050-PWR-LOSS	Loss of Site Power	4.1E-006
			050-SPMRC-MOE000-MOE-FSO	SPMRC Lock Mode State Fails on Loss of Power	1.4E-008
	0.00	3.370E-014	050-SPMRC-CT003-CT-SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			050-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
			050-SPMRC-SC021--SC--FOH	Speed Controller on SPMRC Pendant Fails	1.3E-004
	0.00	5.531E-015	050-SPMRC-BRP001-BRP-FOD	SPMRC Brake (Pneumatic) Failure on Demand	5.0E-005
			050-SPMRC-HC001--HC--SPO	Spurious Command from Pendant Controller	5.2E-007
			050-SPMRC-STU001-STU-FOH	SPMRC End Stops Fail	2.1E-004
	0.00	1.233E-015	050-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	9.1E-008
			050-SPMRC-MOE000-MOE-FSO	PMRC Lock Mode State Fails on Loss of Power	1.4E-008
	0.00	1.095E-015	050-SPMRC-CT003-CT-SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			050-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
			050-SPMRC-SEL021-SEL-FOH	Speed Selector on PMRC Pendant Fails	4.2E-006
	0.00	2.538E-016	050-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable - Short Circuit	1.9E-008

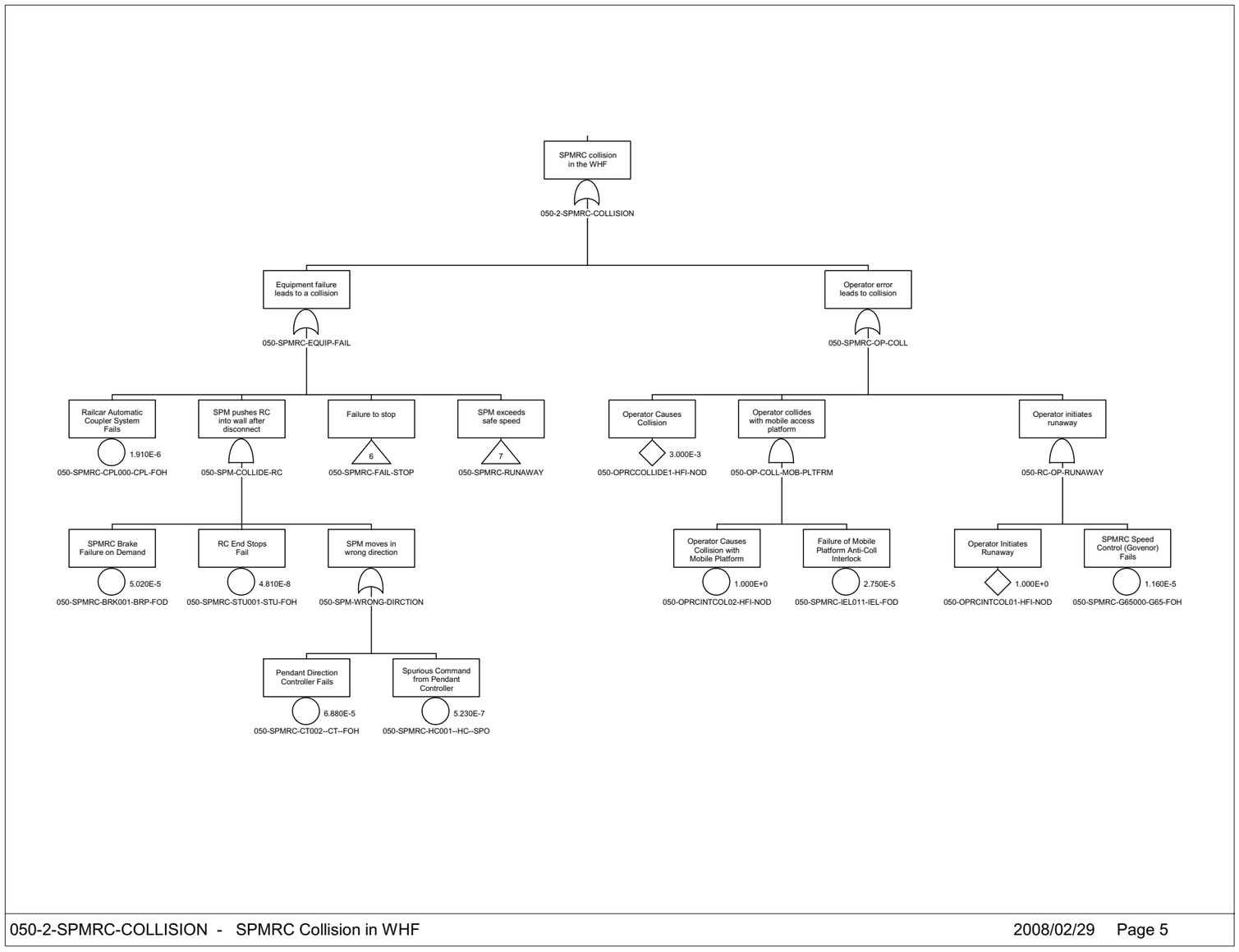
Table B1.4-3. Cut Sets for PMRC Collision (Continued)

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
			050-SPMRC-MOE000-MOE-FSO	PMRC Lock Mode State Fails on Loss of Power	1.4E-008
4.834E-003 = Total					

NOTE: PMRC = prime mover railcar; SPMRC = Site prime mover railcar

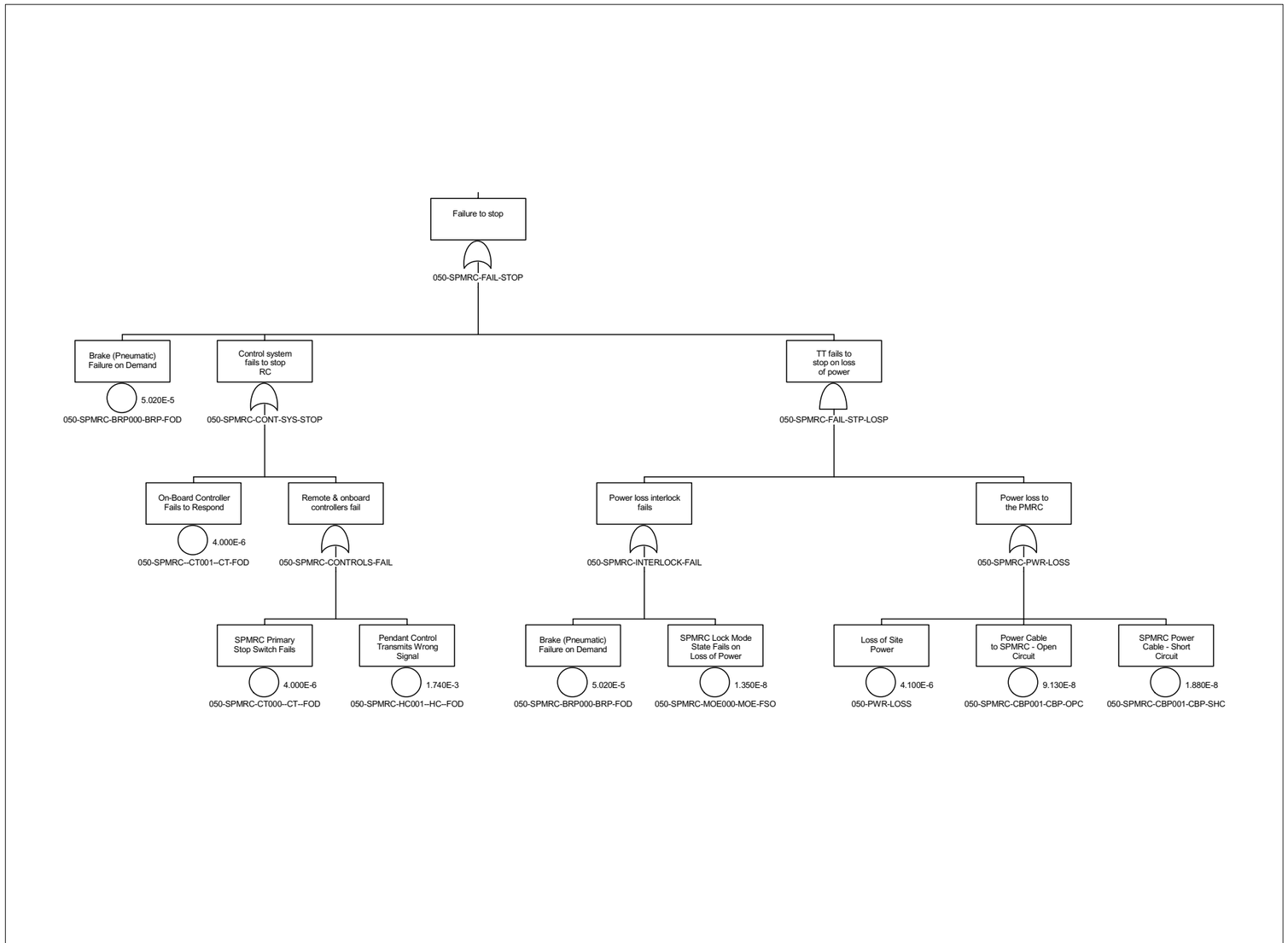
Source: Original

B1.4.1.8 Fault Trees



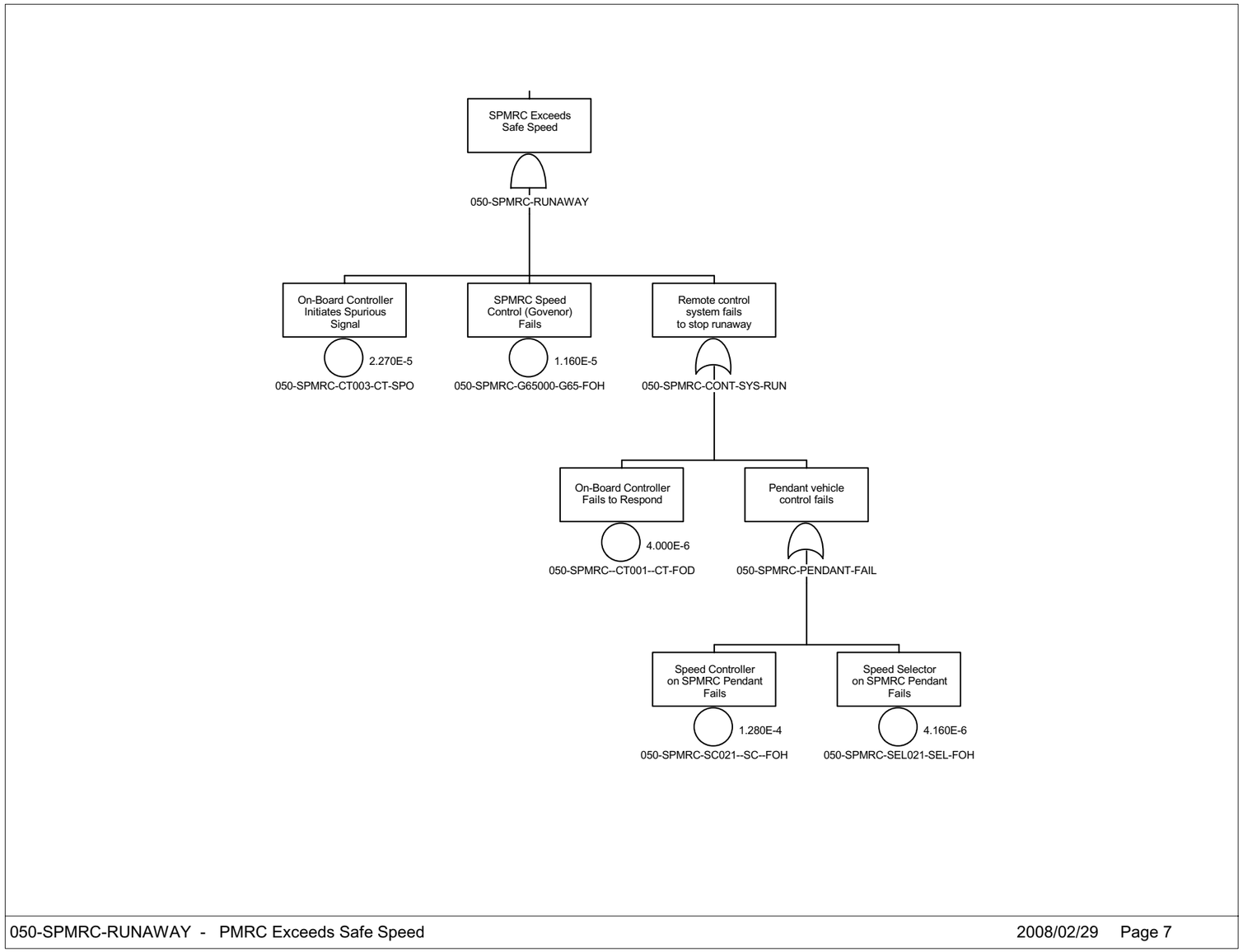
Source: Original

Figure B1.4-3. SPM Railcar Collision in WHF



Source: Original

Figure B1.4-4. SPM Railcar Fail to Stop



Source: Original

Figure B1.4-5. SPM Railcar Exceeds Safe Speed

B1.4.2 SPM Truck Trailer Collides with WHF Structures

B1.4.2.1 Description

The collision fault tree for SPMTT collision within the WHF is identical for each type of transportation cask that is processed at the WHF. SPM truck trailer collision within the WHF can occur as a result of human error or mechanical failures. Mechanical failures leading to a collision consist of the SPM failure to stop with command, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

B1.4.2.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the SPM for mechanical failures and the SPM operator maintains situational awareness and proper control of the movement of the SPM. To avoid collisions, the SPM must stop when commanded, be prevented from entering a runaway situation, or respond correctly to a SPM movement command.

The SPM is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the SPM by either commanding a "stop" from the start/stop button or by releasing the palm switch which initiates an emergency stop. If at anytime there is a loss of power detected, the SPM will immediately stop all movement and enter into "lock mode" safe state. The SPM will remain in this "lock mode" safe state until power is returned and the operator restarts the SPM.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a governor on the diesel engine for outside movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

B1.4.2.3 Design Requirements and Features

Requirements

Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a "deadman switch." On the loss of AC power derived from the facility, the SPM immediately enters the "lock mode" safe state. The "lock mode" safe state is not reversible without specific operator action

Since the dominant contributor to the SPMTT collision in the facility is human error, no priority is given to either the remote or the pendant controllers. The SPM is operated on electrical power when inside the building. The SPM is disconnected from the railcar or truck trailer in the Cask Preparation Room and moved out of the building before cask preparation activities begin.

Features

Stopping the SPM is accomplished by pushing the "stop" button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source immediately respond by removing power from the propulsion system on the SPM.

The SPM has two off-equipment control devices that have complete control over the SPM. The drive system limits the maximum speed of the SPM to 9.0 mph.

Testing and Maintenance

Requirements

No maintenance or testing permitted on a SPM loaded with a transportation cask.

Feature

None.

B1.4.2.4 Fault Tree Model

The fault tree model for "SPM Truck Trailer Collision in WHF" accounts for both human errors and/or SPM truck trailer hardware problems that could result in collision. There is only one movement within the WHF. Once the SPM truck trailer has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the truck trailer and is moved out of the facility.

The top event is a collision of the SPM truck trailer in the WHF and is shown in Figure B1.4-8. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop (Figure B1.4-9), or exceeding a safe speed (Figure B1.4-10). Failure to stop may occur due to mechanical failure of brakes or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

B1.4.2.5 Basic Event Data

Table B1.4-4 contains a list of basic events used in the "SPM Truck Trailer Collision in WHF" fault trees. The mission time has been set at one hour which is conservative because it will not require one hour to disconnect the SPM from the railcar and to remove it from the facility.

Table B1.4-4. Basic Event Probability for SPM Truck Trailer Collision

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-OPTTCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000
050-OPTTINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-OPTTINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-PWR-LOSS	1	4.100E-006	4.100E-006	0.000E+000	0.000E+000
050-SPMTT-BRP000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
050-SPMTT-BRK001-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
050-SPMTT-CBP001-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
050-SPMTT-CBP001-CBP-SHC	3	1.880E-008	0.000E+000	1.880E-008	1.000E+000
050-SPMTT-CPL000-CPL-FOH	3	1.910E-006	0.000E+000	1.910E-006	1.000E+000
050-SPMRC-CT000--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-SPMTT--CT001--CT-FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-SPMTT-CT001--CT-FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-SPMTT-CT002--CT--FOH	3	6.880E-005	0.000E+000	6.880E-005	1.000E+000
050-SPMTT--CT001-CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
050-SPMTT-G65000-G65-FOH	3	1.160E-005	0.000E+000	1.160E-005	1.000E+000
050-SPMTT-HC002--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
050-SPMRC-HC001-HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
050-SPMTT-IEL102-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-SPMTT-MOE000-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
050-SPMTT-SC021--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
050-SPMTT-SEL021-SEL-FOH	3	4.160E-006	0.000E+000	4.160E-006	1.000E+000
050-SPMTT-STU001-STU-FOH	3	2.107E-004	0.000E+000	4.810E-008	4.380E+003

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; SPMTT = site prime mover truck trailer.

Source: Original

B1.4.2.5.1 Human Failure Events

Three human errors have been identified for this fault tree. Two of these failure modes have been assigned a failure probability of 1.00E+00. These human errors are:

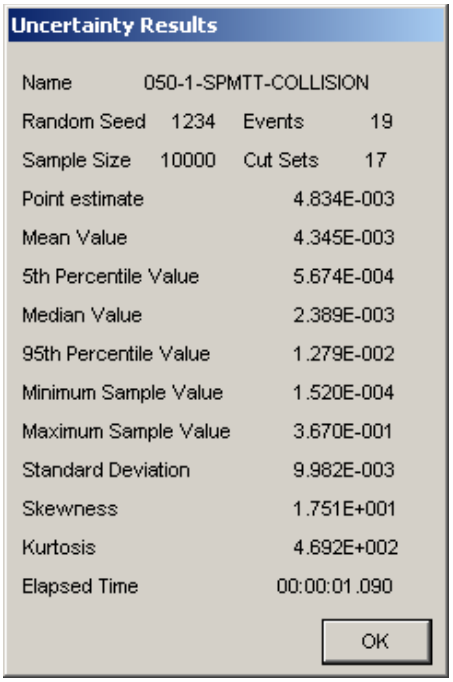
1. Operator causes collision (050-OPTTCOLLIDE1-HFI-NOD)
2. Operator initiates runaway (050-OPTTINTCOL01-HFI-NOD)
3. Operator causes SPMRC collision with mobile platform (050-OTTCINTCOL02-HFI-NOD).

B1.4.2.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

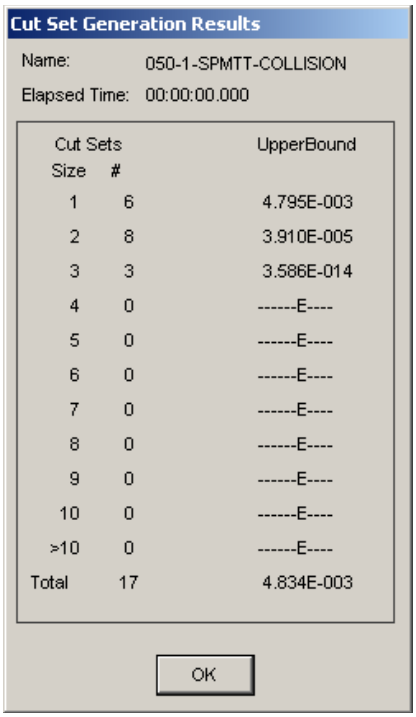
B1.4.2.6 Uncertainty and Cut Set Generation Results

Figure B1.4-6 contains the uncertainty results obtained from running the fault tree for "SPM Truck Trailer Collision in WHF" using a cutoff probability of 1E-12. Figure B1.4-7 provides the cut set generation results for the "SPM Truck Trailer Collision in WHF" fault tree.



Source: Original

Figure B1.4-6. Uncertainty Results of the "SPM Truck Trailer Collision in WHF" Fault Tree



Source: Original

Figure B1.4-7. Cut Set Generation Results for the "SPM Truck Trailer Collision in WHF" Fault Tree

B1.4.2.7 Cut Sets

Table B1.4-5 contains the cut sets for "SPM Truck Trailer Collision in WHF" fault tree. The probability of failure is 4.83E-03.

Table B1.4-5. Cut Sets for SPM Truck Trailer Collision

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
050-1-SPMTT-COLLISION	62.07	3.000E-003	050-OPRCCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	050-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	050-SPMTT-BRK001-BRP-FOD	Brake (Pneumatic) Failure on Demand Brake (Pneumatic) Failure on Demand PMRC Fails to Stop on Loss of Power	5.0E-005
	0.57	2.750E-005	050-OPTTINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000
			050-SPMTT-IEL102-IEL-FOD	Failure of Mobile Platform Anti-Coll Interlock	2.8E-005

Table B1.4-5. Cut Sets for SPM Truck Trailer Collision (Continued)

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
	0.24	1.160E-005	050-OPTTINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			050-SPMTT-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	050-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	050-SPMTT-CT0001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	050-SPMTT-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	1.9E-006
	0.00	2.058E-10	050-PWR-LOSS	Loss of Site Power	4.1E-06
			050-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.0E-05
	0.00	4.583E-12	050-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.0E-05
			050-SPMTT-CBP001-CBP-OPC	Power cable to SPMTT - open circuit	9.1E-08
	0.00	9.438E-13	050-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.0E-05
			050-SPMTT-CBP001-CBP-SHC	SPMTT Power Cable - Short Circuit	1.9E-08
	0.00	5.535E-14	050-PWR-LOSS	Loss of Site Power	4.1E-06
			050-SPMTT-MOE000-MOE-FSO	SPMTT lock mode state fails on loss of power	1.4E-08
	0.00	3.370E-14	050-SPMTT--CT001-CT--SPO	On-Board Controller Spurious Operation	2.3E-05
			050-SPMTT-G65000-G65-FOH	PMTT Speed Control (Govenor) Fails	1.2E-05
			050-SPMTT-SC021--SC--FOH	Speed Controller on SPMTT Pendant Fails	1.3E-04
	0.00	1.233E-15	050-SPMTT-CBP001-CBP-OPC	Power cable to SPMTT - open circuit	9.1E-08
			050-SPMTT-MOE000-MOE-FSO	SPMTT lock mode state fails on loss of power	1.4E-08
	0.00	1.095E-15	050-SPMTT--CT001-CT--SPO	On-Board Controller Spurious Operation	2.3E-05
			050-SPMTT-G65000-G65-FOH	PMTT Speed Control (Govenor) Fails	1.2E-05
			050-SPMTT-SEL021-SEL-FOH	Speed Selector on SPMTT Pendant Fails	4.2E-06
	0.00	1.053E-15	050-SPMTT--CT001-CT--SPO	On-Board Controller Spurious Operation	2.3E-05

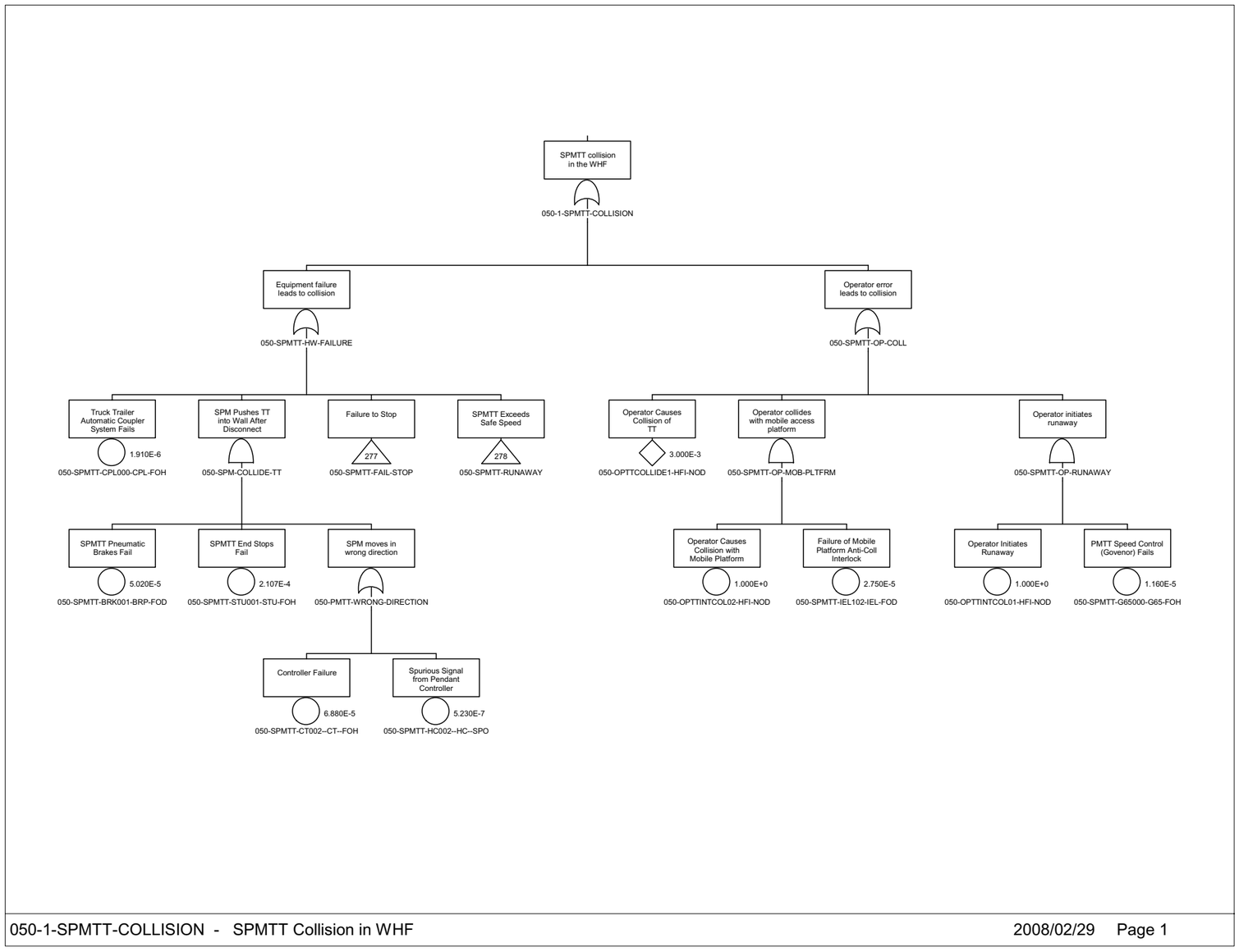
Table B1.4-5. Cut Sets for SPM Truck Trailer Collision (Continued)

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
			050-SPMTT-CT001--CT-FOD	On-Board Controller Fails to Respond	4.0E-06
			050-SPMTT-G65000-G65-FOH	PMTT Speed Control (Govenor) Fails	1.2E-05
4.834E-003 = Total					

NOTE: PMTT = prime mover truck trailer; SPMTT = site prime mover truck trailer; TT = truck trailer.

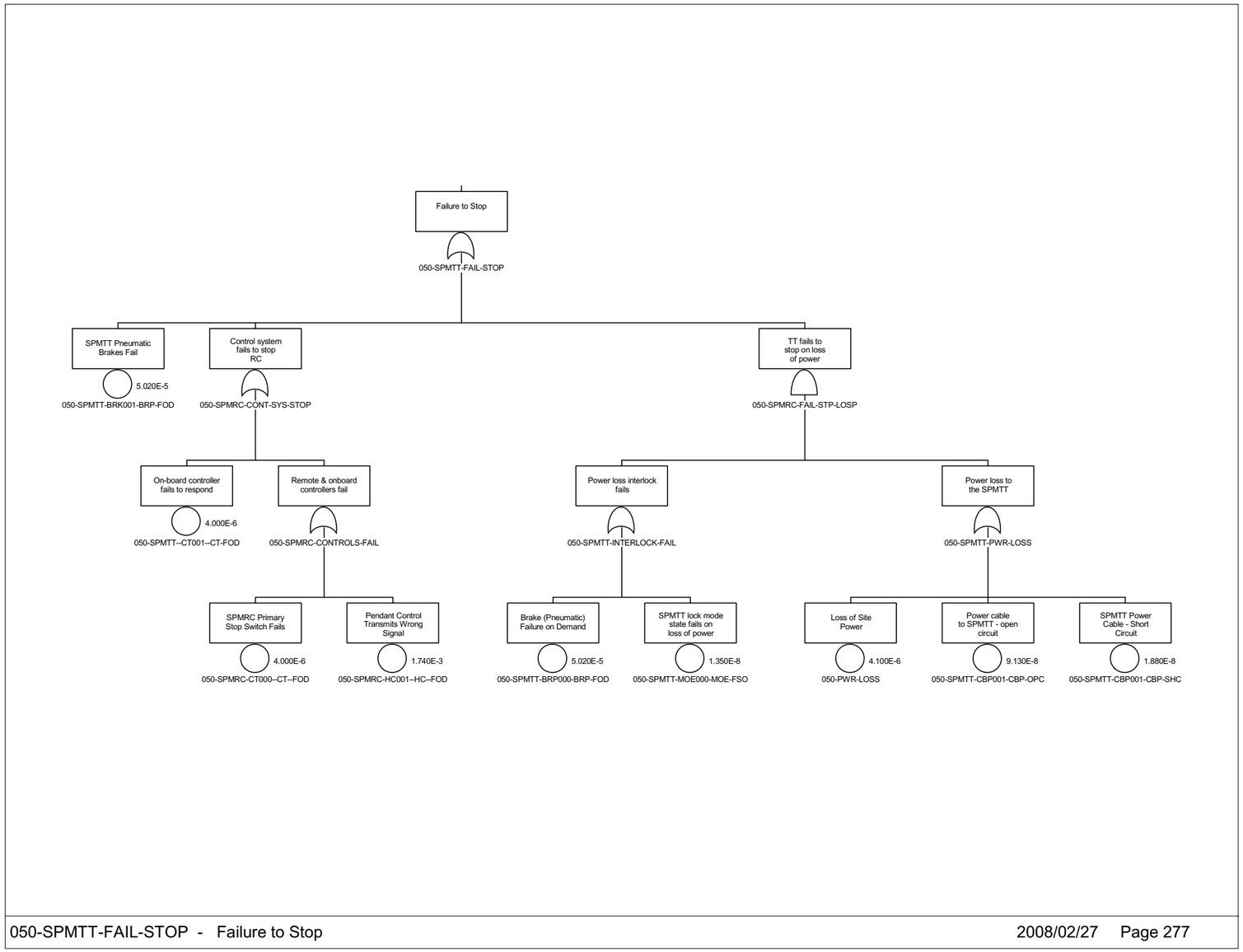
Source: Original

B1.4.2.8 Fault Trees



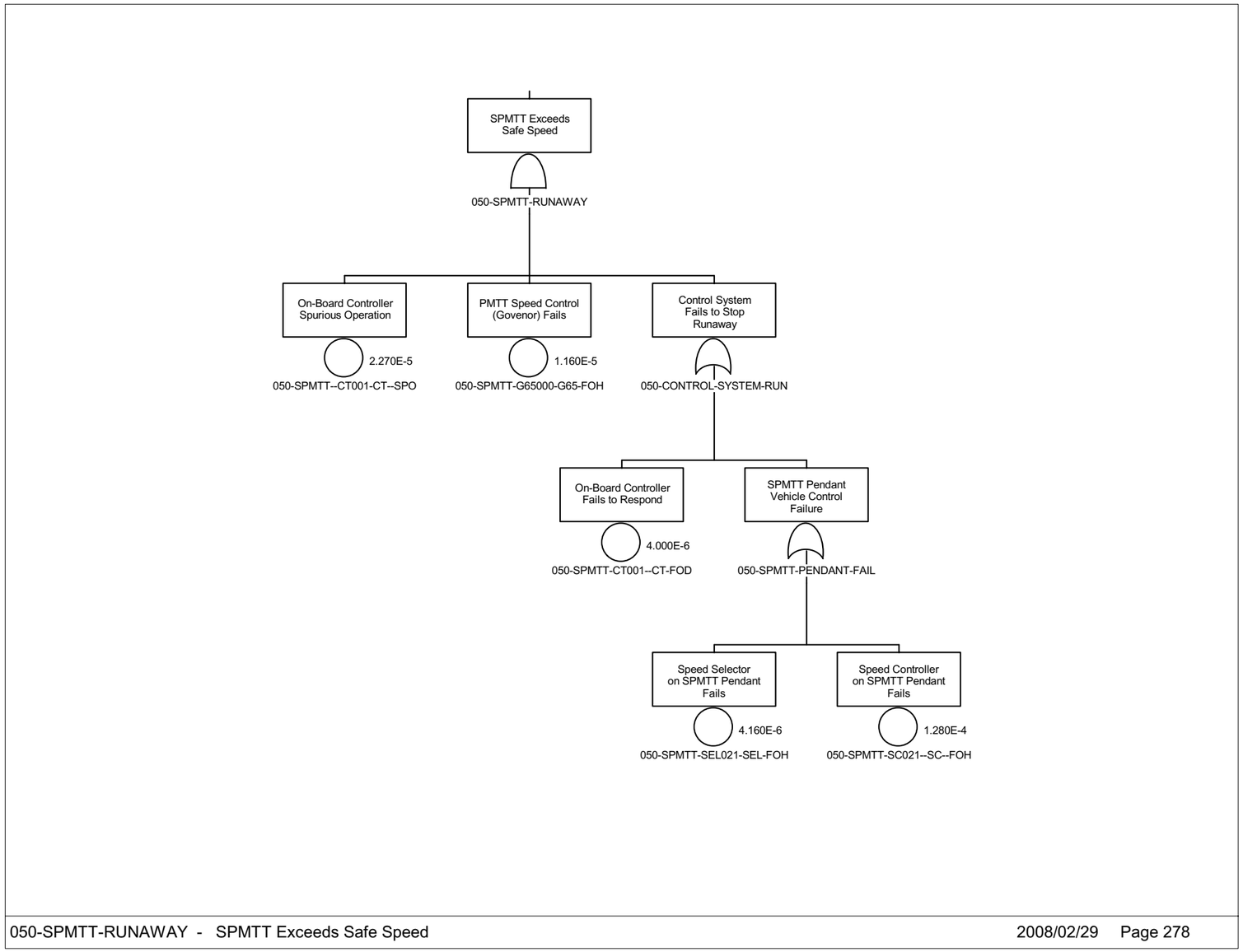
Source: Original

Figure B1.4-8. SPM Truck Trailer Collision in WHF



Source: Original

Figure B1.4-9. SPM Truck Trailer Failure to Stop



Source: Original

Figure B1.4-10. SPM Truck Trailer Exceeds Safe Speed

B1.4.3 SPMRC Derailment

B1.4.3.1 Description

The fault tree for "SPM Railcar Derailment" with the WHF is identical for each type of transportation cask. Derailment is characterized by a basic event that accounts for the probability of a railcar derailment per mile of travel with in the WHF.

This fault tree considers the potential for the SPM to derail during movement of the railcar to the Preparation Area. The top event is "Derailment of the SPMRC." This fault tree is shown in Figure B1.4-13.

The probability of derailment is based on historical data for train derailment at low speeds and is discussed in the section on data development. The probability of derailment per mile is multiplied by the number of miles the SPM travels from the vestibule to the preparation area (approximately 4E-2 miles). Detailed analysis for this basic event is contained in Attachment C.

B1.4.3.2 Success Criteria

The success criterion is that the SPM railcar does not derail during the transport process.

B1.4.3.3 Design Requirements and Features

Requirements

The railcar design requirements comply with Association of American Railroads Standard S-2043 (Ref. B1.1.1).

Features

The design features of the railcar are in compliance with Association of American Railroads Standard S-2043 (Ref. B1.1.1).

Testing and Maintenance

Requirements

No maintenance or testing permitted on a railcar loaded with a transportation cask.

Feature

None.

B1.4.3.4 Fault Tree Model

The fault tree model for "SPM Railcar Derailment" consists of the probability for a railcar derailment per mile of travel times the number of occurrences for each type of transportation cask.

B1.4.3.5 Basic Event Data

Table B1.4-6 contains a list of basic events used in the "SPM Railcar Derailment" fault trees.

Table B1.4-6. Basic Event Probability for SPM Railcar Derailment

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-SPMRC-DERAIL-PERMILE	3	1.180E-005	0.000E+000	1.180E-005	1.000E+000
050-SPMRC-MILES-IN-WHF	V	4.000E-002	4.000E-002	0.000E+000	0.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc = calculation; Fail = failure; Prob = probability; Miss = mission

Source: Original

The calculated probability of a derailment inside the WHF is the probability of a railcar derailing per mile of travel times the distance travelled within the facility.

B1.4.3.5.1 Human Failure Events

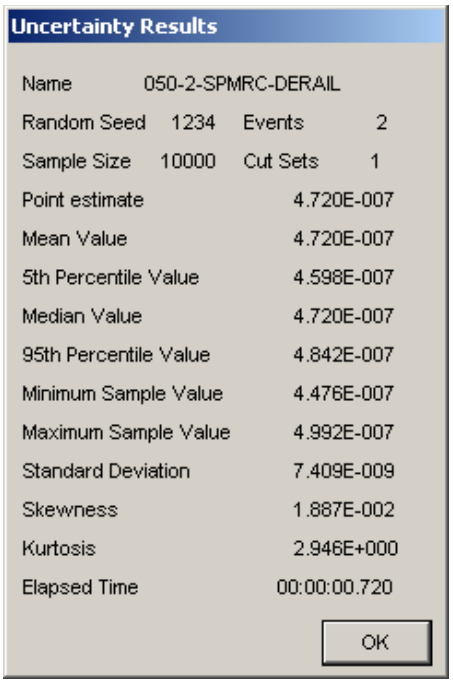
There are no human errors identified for this fault tree.

B1.4.3.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

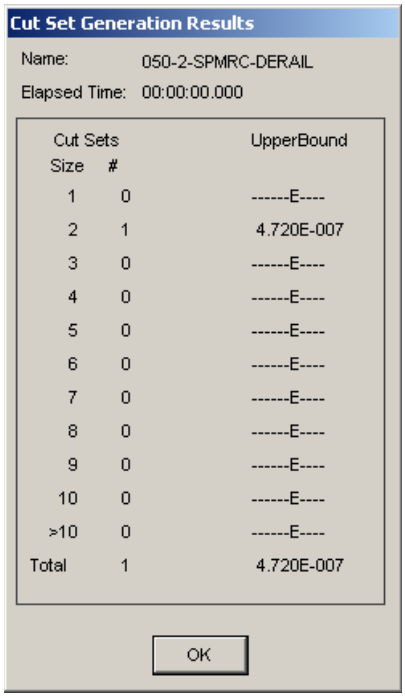
B1.4.3.6 Uncertainty and Cut Set Generation Results

Figure B1.4-11 contains the uncertainty results obtained from running the fault tree for "SPM Railcar Derailment" using a cutoff probability of 1E-12. Figure B1.4-12 provides the cut set generation results for the "SPMRC Derailment" fault tree.



Source: Original

Figure B1.4-11. Uncertainty Results of the "SPM Railcar Derailment" Fault Tree



Source: Original

Figure B1.4-12. Cut Set Generation Results for the "SPM Railcar Derailment: Fault Tree

B1.4.3.7 Cut Sets

Tables B1.4-7 contains the cut sets for "SPM Railcar Derailment" fault tree. The probability of derailment per cask is 4.72E-7.

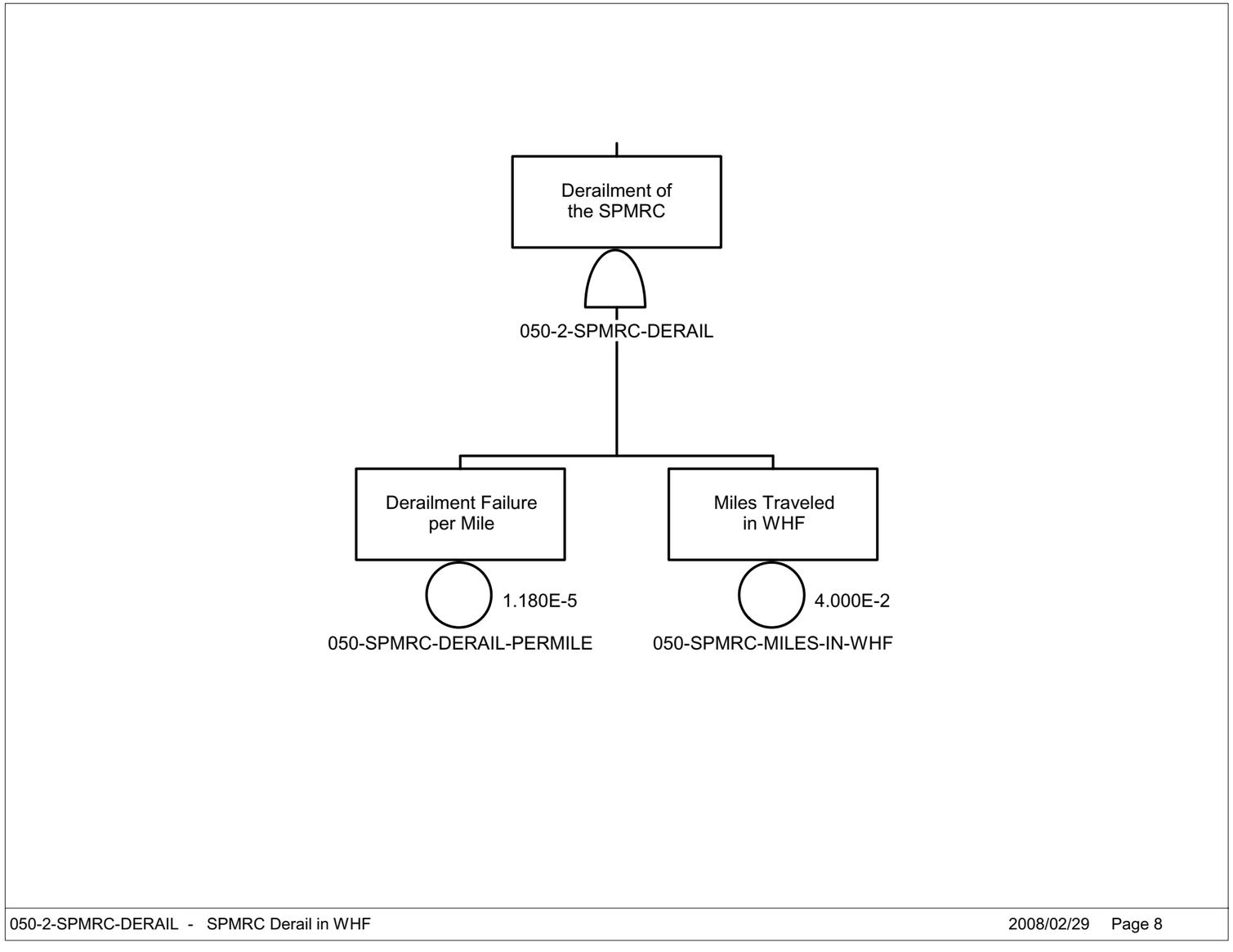
Table B1.4-7. Cut Sets for SPM Railcar Derailment

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
050-2-SPMRC-DERAIL	100.00	4.720E-007	050-PMRC-DERAIL-PERMILE	Derailment of a railcar per mile	1.2E-005
			050-PMRC-MILES-IN-WHF	Miles Traveled in WHF	4.0E-002
4.720E-007 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B1.4.3.8 Fault Trees



Source: Original

Figure B1.4-13. SPM Railcar Derailment in WHF

B1.4.4 SPMTT Rollover in WHF

B1.4.4.1 Description

The fault trees for "SPM Truck Trailer Rollover in the WHF" are identical for each type of transportation cask. Rollover is characterized by a human error basic event that accounts for the probability of an operator jackknifing the truck trailer while backing through the WHF vestibule areas into the Cask Preparation Room.

During movement, a rail track failure, obstacle on the track, or a structural failure on the railcar could potentially lead to a rollover. For the truck trailer, an obstacle on the road or a structural failure on the trailer could potentially lead to a rollover. There are no design constraints for these types of failures; to prevent this situation relies on an operator response to initiate an emergency stop command. Since this is a recovery action, no credit is taken for the operator response.

B1.4.4.2 Success Criteria

The design of the SPM prevents the majority of scenarios that could potentially cause a SPM rollover. A low center of gravity and a wide footprint of the railcar/truck trailer results in a stable platform during movements. In addition, the WHF vestibule is too small in length and width for a jack-knife to occur resulting in a roll over

The success criterion is that no rollover occurs while transferring the trailer into the WHF with the SPM.

B1.4.4.3 Design Features and Requirements

System Configuration and Operating Conditions

The design of the SPM prevents the majority of scenarios that could potentially cause a SPM rollover. A low center of gravity and a wide footprint of the railcar/truck trailer results in a stable platform during movements.

Requirements

Trailers used for the movement of transportation casks are designed in accordance with the requirements contained in NHTSA requirements as authorized by 49 USC Part 301, Motor Vehicle Safety (Ref. B1.1.3). The requirements are delineated in 49 CFR Part 571, Transportation: Federal Motor Vehicle Safety Standards (Ref. B1.1.2).

While backing the SPMTT through the Entry Vestibule and to the Cask Preparation Room, at a minimum one walker-spotter is required to ensure no objects are in the path of the SPMTT and to stop the driver from continuing to back up if a jackknife situation with the trailer begins to occur.

Design Features

Not applicable.

B1.4.4.4 Fault Tree Model

The fault tree model for SPM truck trailer rollover (Figure B1.4-14) consists of a single human error associated with the operator jackknifing the truck trailer when positioning it in the WHF.

B1.4.4.5 Basic Event Data

A rollover within the WHF can only occur if the driver of the SPMTT jackknifes the truck trailer.

There is only one basic event consisting of a human error causing a jackknife of the trailer shown in Figure B1.4-14. The human reliability analysis assesses a 0.000E+00 probability of this occurring.

B1.4.4.5.1 Human Failure Events

The human error probability of causing a jackknife of the trailer has been assessed as zero due to presence of a walker/spotter (see Section 6.4 and Attachment E).

B1.4.4.5.2 Common-Cause Failures

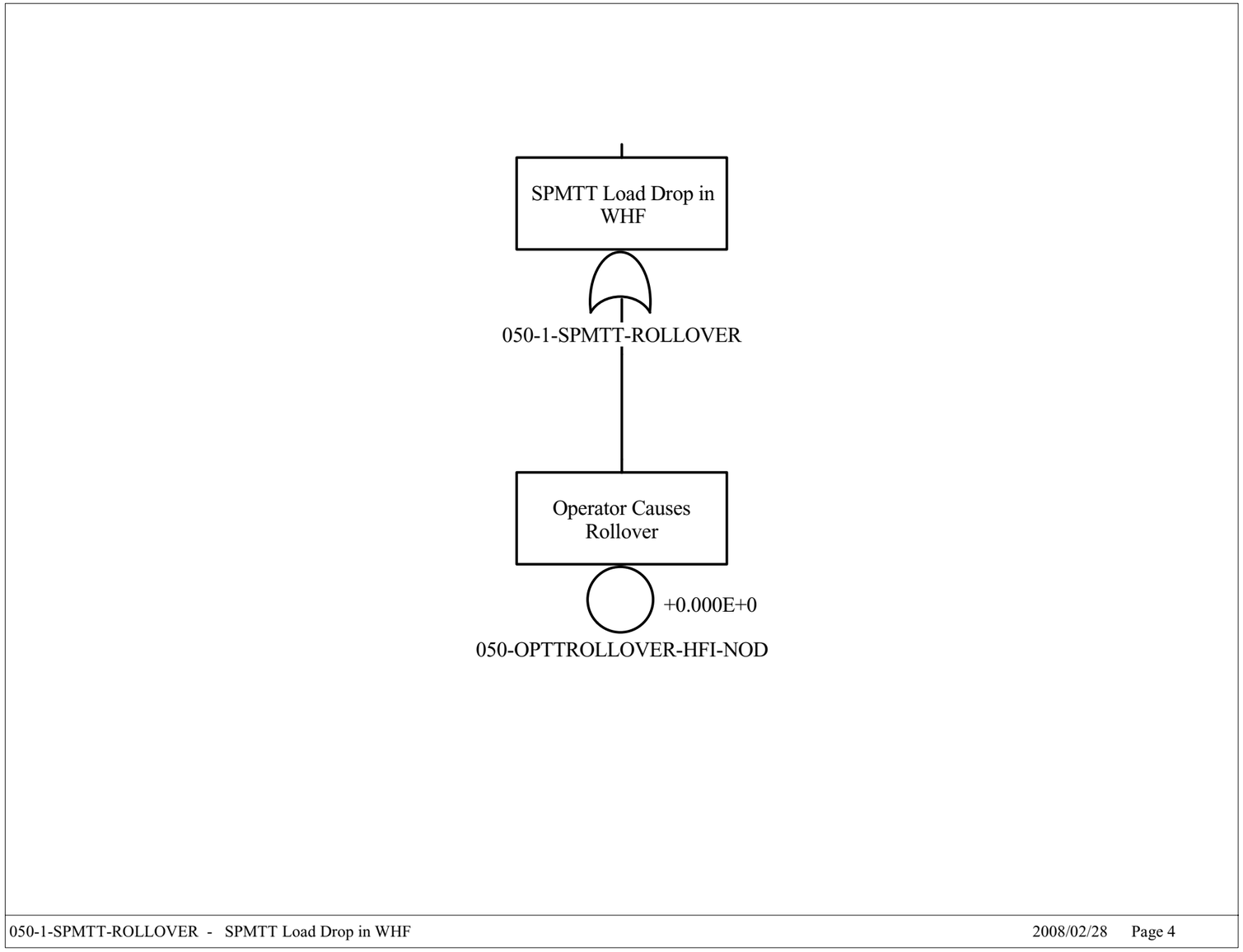
No CCFs were identified for this fault tree.

B1.4.4.6 Uncertainty and Cut Set Generation Results

Because there is only a single basic event assessed as having zero probability of occurrence, there are no uncertainty values or cut sets to be calculated.

B1.4.4.7 Fault Tree

The fault tree model for SPMTT rollover is shown in Figure B1.4-14.



Source: Original

Figure B1.4-14. SPM Truck Trailer Rollover in WHF

B2 CASK TRANSFER TROLLEY FAULT TREE ANALYSIS

B2.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B2.1.1 BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report for Cask Transfer Trolley.* 000-30R-HM00-00200-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071219.0001.

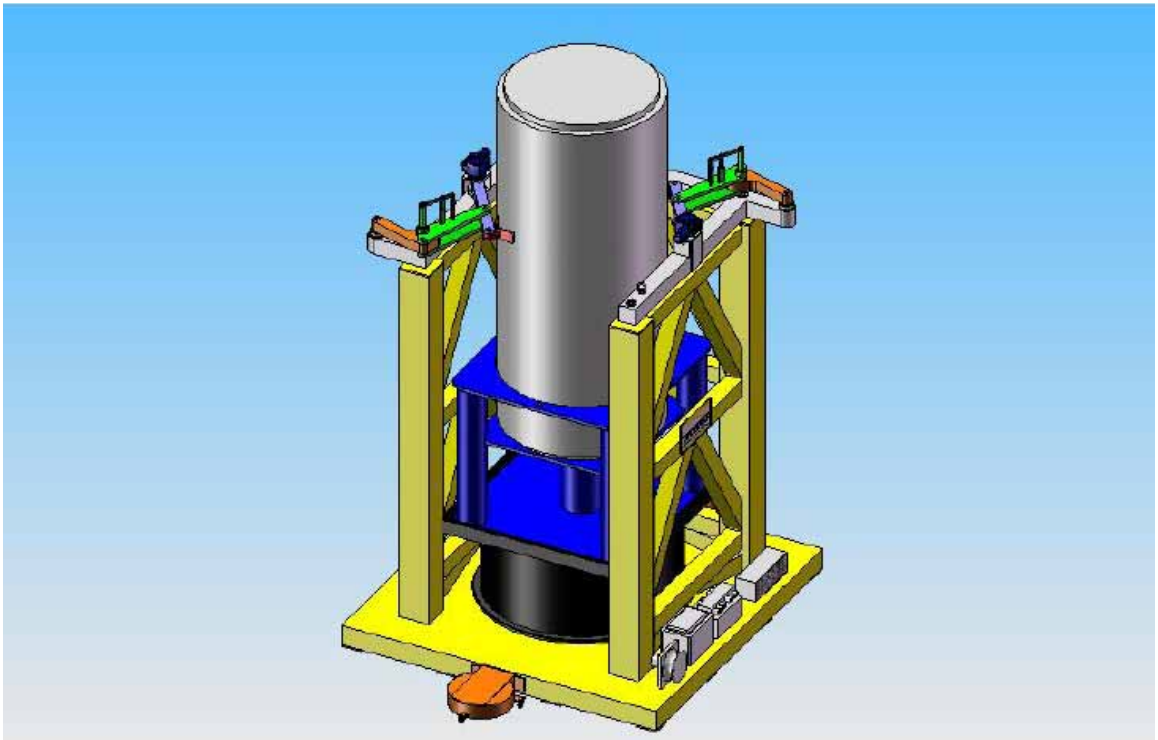
B2.1.2 *BSC (Bechtel SAIC Company) 2007. *Preliminary Throughput Study for the Initial Handling Facility.* 51A-30R-IH00-00100-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0021.

B2.1.3 *Morris Material Handling 2007. *P&ID – Cask Transfer Trolley*. V0-CY05-QHC4-00459-00029-001 Rev. 005. Oak Creek, Wisconsin: Morris Material Handling. ACC: ENG.20071019.0003.

B2.2 CASK TRANSFER TROLLEY DESCRIPTION

B2.2.1 Physical Description

The cask transfer trolley (CTT) is an air powered machine that will be used to transport various vertically oriented transportation casks from the Cask Preparation Area to the Canister Transfer Room. The trolley consists of a platform, a cask support assembly, a pedestal assembly, a seismic restraint system, and an air system as illustrated in Figure B2.2-1.



Source: Modified from Ref. B2.1.1

Figure B2.2-1. Cask Transfer Trolley

The platform, or main deck, is the main support structure for the trolley. The structure is designed to hold the air bearings under the deck and simultaneously support the cask support assembly and cask. The cask support assembly is the truss work that is welded to the platform and cradles three sides of the cask. The cask support assembly provides the structural support for the seismic restraint system and pedestal assembly to hold the cask during an earthquake or collision event.

The CTT must handle a number of different types of casks; consequently several different pedestals are used to properly position the cask height at 27 ft-3 in. from the floor. Each pedestal sub-component is designed for its respective cask to sit down in a "cavity." The depth of the cavity is a minimum of 6 inches which is sufficient to prevent the cask from exiting from the pedestal due to uplift during the worst case seismic event. In addition, the cask is restrained in the longitudinal and transverse directions by the cavity walls and restrained in the vertical down direction by the pedestal itself.

This design also ensures the cask is positioned in the correct position in the trolley. The trolley is positioned within a set tolerance under the cask transfer port in the Cask Unloading Room using bumpers and stops that are bolted to the floor with bolts that will shear to allow the CTT to slide during a significant seismic event.

In addition to the cask being restrained at the bottom by the pedestal assembly, the upper section of the cask is restrained to prevent side motions during a seismic event. The system is made up of two linkage systems that are mounted on opposite corners of the cask support assembly. An electric motor extends and retracts the restraint brackets to predetermined positions. Different cask diameters are handled by bolting unique interface clamps onto the seismic restraints.

When the restraint system is properly positioned next to the cask, a locking pin is air actuated to secure the system. This solid, high strength alloy locking pin can withstand the shear stresses that would be experienced during a seismic event. Both locking pins are monitored by proximity switches (or limit switches) that are hard wired to the control system to verify the pins are in place. If the locking pins are not secured properly, the CTT will not be able to power up and move/levitate.

The facility compressed air supply inflates nine 54-inch diameter air casters beneath the trolley platform. Each air caster consists of a urethane torus-shaped bag with a chamber inside the torus. The air film is produced when air is distributed to each air caster causing the air bags to inflate. The inflated bags create a seal against the floor surface and confine the air within the chambers of the bags until the air pressure is sufficient to offset the weight of the loaded trolley. The air bearings allow the CTT to rise above the steel floor approximately 1/2 in. to 7/8 in. The air bearings are supplied with facility air (between 75 to 100 psi optimal) and consume from 500 to 700 scfm. A hose reel for the 1-1/2 in. diameter air hose is mounted on the platform. The reel is equipped with an air-powered return, a ball valve shut-off, quick disconnect fittings, and a safety air fuse.

A main “off/on” control valve and separate flow control/monitoring valve for each air bearing allows adjustment and verification of pressure/flow for each individual bearing. There are two interlocks for the air; one pressure monitor verifies that the main incoming pressure is not too high, and a second set of monitors verifies that all bearings have sufficient air pressure. This air monitoring system for the air bearings is not important to safety and therefore has not been analyzed.

End mounted turtle-style drive units that are 360-degree steerable, are used to steer the CTT. Traction is produced by down-pressure on the wheels provided by a small air bag on each drive unit. Air is supplied from facility air to a high speed pneumatic motor in combination with a reducer to limit the wheel speed of the turtle drives. The maximum speed of the system is less than or equal to 10 fpm at the maximum air pressure available from the facility compressed air supply.

The CTT speed is controlled in two ways. First, the electrical control system is designed to provide a control signal to the air valve that produces a speed range of 0 to10 fpm. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, restricts the air flow to prevent a “run-away” condition.

B2.2.2 Control System

The control system is relay-based and includes a pendant station for its operator interface.

No programmable logic controllers (PLCs) are used—all interlocks are hard wired. The pendant is a standard crane pendant that has all of the controls for the unit including:

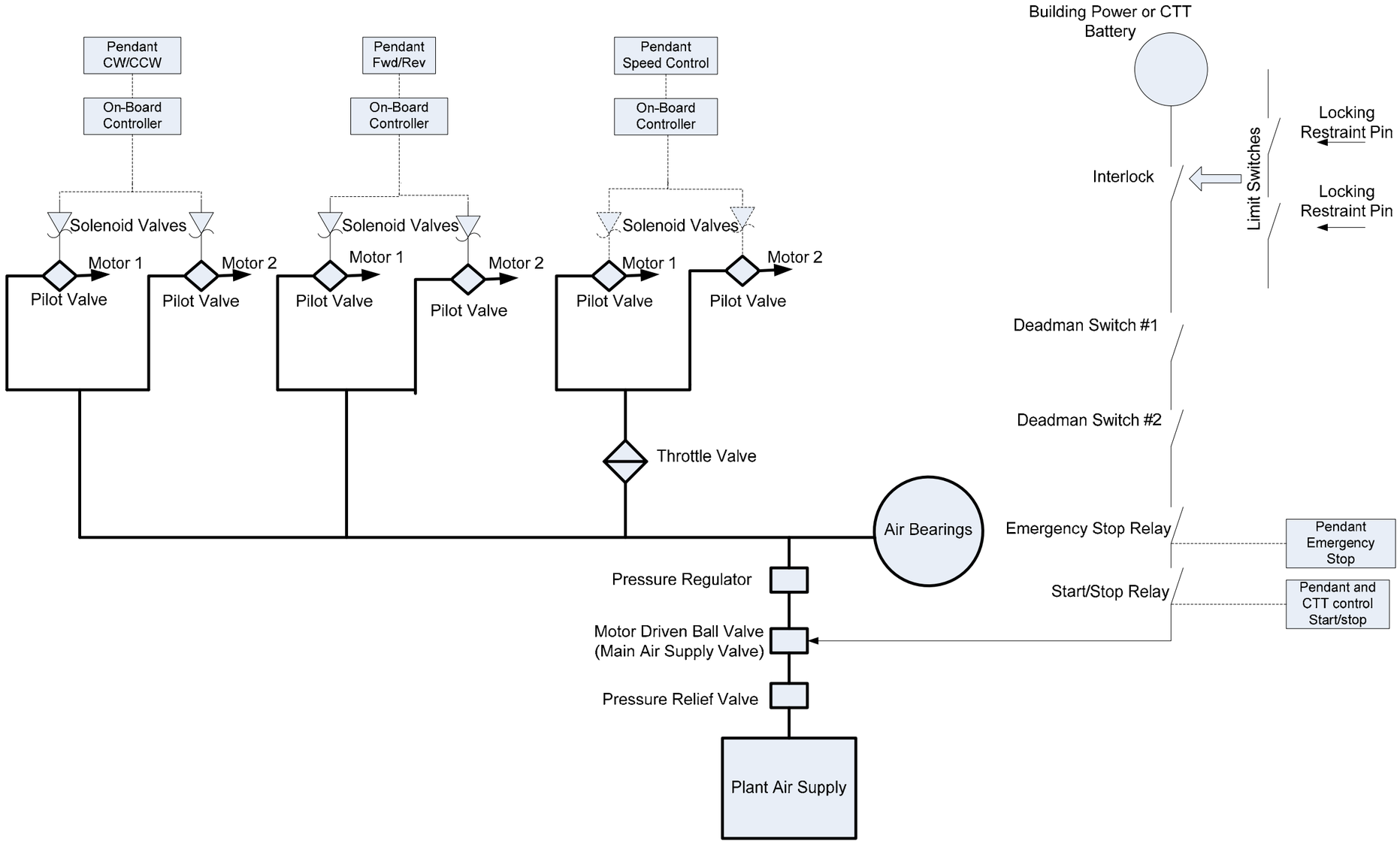
- Deadman Handle—the operator must press both handles to allow air to flow to the CTT to levitate and move horizontally.
- Emergency-stop button–The operator presses the emergency stop button on the pendant control or on the CTT to stop the CTT.
- Clockwise/counterclockwise momentary switch–The operator turns this switch to turn the drive units for horizontal movement. This rotational characteristic is used to move the CTT to the storage or maintenance location after it leaves the Cask Preparation Area.
- Forward/reverse switch–The operator uses the forward/reverse switch to determine the direction of the drive units
- Variable speed control switch–The operator uses the variable speed control switch to adjust the CTT drive speed.
- Cask restraint–The operator uses the selector switch to actuate the motor to close the restraints and automatically engage the locking pin.

During normal operations, the controls operate off a battery system contained on the CTT. Only one operator is needed to move the CTT since it only travels in one direction when it is carrying a cask. The CTT moves forward and reverse between the Cask Unloading Room and the Cask Preparation Area and is restrained from side to side by removable barriers that are mounted to the building floor.

A schematic of the control system is shown in Figure B2.2-2.

The main air supply valve is a solenoid operated pilot valve that is fail safe (i.e., it is a spring valve that closes upon loss of electrical power or loss of air pressure). The air supply valve opens when the locking restraint pins actuate the limit switches and the pendant deadman switches are actuated.

The controls on the pendant are clockwise/counterclockwise, forward/reverse and drive speed to control the valves for the motor drives. These valves are also fail safe solenoid operated pilot valves.



Source: Modified from Ref. B2.1.3.

Figure B2.2-2. Schematic of the CTT Control System

Releasing the deadman switches or pressing the emergency-stop or start/stop buttons on the pendant control or the emergency-stop button on the CTT opens a relay to interrupt power to the main air supply valve, causing it to close. Upon closing the main supply valve, the air pressure levitating the CTT and driving the motors is reduced and the CTT lowers to the floor.

B2.2.3 Operation

B2.2.3.1 Initial Conditions

The CTT is initially located in the Cask Preparation Area with the battery fully charged, the seismic restraints retracted, and with no air hose connected. Based on the next planned cask to be loaded onto the trolley, the corresponding pedestal components are installed into the base and bumpers are bolted onto the seismic restraints and supports. The air hose is then connected to the CTT.

The overhead crane moves a cask onto the pedestal. With the cask still attached to the crane, the operator remotely operates the seismic restraints and secures the cask to the CTT by extending the electric motor driven actuators. When the restraints are in place, the locking pins are pneumatically inserted. With the cask secured to the trolley, the overhead crane is disengaged from the cask.

When the locking pins are inserted properly (thus locking the seismic restraints in place), a pair of proximity switches (limit switches) de-activates the interlock and the main air supply valve can be opened to allow the main air bearings and drive motors can be operated. Once all preparations of the cask are complete, the trolley can be moved to the Transfer Area using the pendant controls.

B2.2.3.2 Cask Movement

When all steps are properly completed, air is introduced to the CTT. The operator actuates the air bearings, levitating the CTT with the load. The system continuously and automatically checks the flow and pressure to each air bearing; if a problem is detected, the air supply to all bearings is stopped and the system lowers to the ground.

Once the trolley is raised, the operator drives the CTT into the Cask Unloading Room. By moving forward and reverse, the CTT is driven through the door way. Guides bolted to the floor ensure that the CTT can only move forward and back, and in addition, will ensure that the CTT is properly positioned directly below the transfer port. Once in position, the air flow to the bearings is stopped and the CTT lowers to the ground and rests in position. The operator disconnects the quick-disconnect air hose and rewinds the hose onto the trolley. The shield doors that separate the Cask Preparation Area from the Cask Unloading Room are then closed.

B2.2.3.3 System/Pivotal Event Success Criteria

Success criteria for loading a cask onto the CTT at the Cask Preparation Area, and unloading the canisters from the cask in the Cask Unloading Room, require the CTT to remain stationary during these operations with no spurious movement. Success criteria for moving the CTT with

cask from the Cask Preparation Area to the transfer area requires the CTT to travel at an allowable speed, and the operator to be able to control the CTT movement.

During cask loading at the Cask Preparation Area, compressed air must be available to the CTT to remotely insert the locking pins into the restraint system. Both pin interlocks must function before the main air supply valve can be opened, thereby preventing movement of the CTT until the cask has been loaded and restrained. Once the locking pins are in place, the crane is removed from the cask. During the time the crane is being removed from the cask, the air supply valve is closed and the valves that control the air to the air bags and motors are closed. Movement is not initiated until both deadman switches on the remote pendant control are pressed to allow air to the air bags to levitate the CTT.

Upon the CTT reaching the Cask Unloading Room, procedures require that the air supply hose to be disconnected and removed from the CTT to prevent any movement while unloading the canisters from the cask. This is accomplished by locating the air supply unit outside the Cask Unloading Room. An interlock prevents the transfer port slide gate from opening until the shield door to the transfer room is closed. Thus, because the air supply is external to the Cask Unloading Room, the air hose must be removed from the CTT before the shield door can be closed, and the shield door must be closed before the port slide gate can be opened allowing canister transfer from the cask. Therefore, the location of the air supply unit and the shield door interlock requires removal of the air supply from the CTT before canister transfer can begin.

When moving the cask between the Cask Preparation Area and the Cask Unloading Room, movement in the wrong direction is prevented by the guide rails bolted to the floor along the path of the CTT. This forces the CTT to move only in a straight line forward and back between the two areas. Runaway of the CTT is prevented by the throttle valve which is set at the factory such that the maximum speed is 10 fpm at the maximum facility air pressure.

The CTT is stopped to prevent a collision into a closed shield door or the end stops in the Cask Unloading Room by the operator speed controls on the pendant, by the deadman switches on the pendant or the CTT, or by the emergency stop buttons on the pendant and on the CTT. The speed controls slow down and stop the CTT by controlling the drive speed valve, and the deadman switches and emergency stop buttons remove power to the main air supply valve causing it to close. Because the emergency stop function is a recovery action performed by the operator and requires operator intervention, these functions were not modeled in the analysis.

On loss of electrical power from the battery, the air valves all fail closed, and no air will pass through to the air bearings or drive units and the CTT settles to the floor. If the air pressure and flow is lost, the unit can not levitate or move horizontally and the CTT again lowers to the floor and no other action will occur. A separate sustained signal is needed to actuate the air valves to raise the load (positive operator action.) Thus, although a spurious signal may cause air to flow momentarily, additional controls need to actuate to cause the unit to levitate or move horizontally.

B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B2.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B2.3-1. Dependencies and Interactions Analysis

Systems, Structures, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Air supply	Provides levitation and motive force	—	—	Fail to disconnect air hose	—
Locking pin limit switches	Prevents spurious movement	—	—	—	—
Guide rails	Prevents movement in wrong direction	—	—	—	Shear during seismic event allows CTT to slide
Pendant control	Controls direction and speed and initiates movement	—	—	Wrong instructions	—
Deadman switch	Allows operation	—	—	Fail to release	—
Emergency stop	Stops CTT	—	—	Fail to energize	—
Throttle valve	Limits maximum speed	—	—	—	—
Structure	Constrains and supports cask	—	—	—	Seismic causes impact
Shield door	Opens for CTT to pass through	—	—	Close door inadvertently	Closes on CTT

NOTE: CTT = cask transfer trolley

Source: Original

B2.4 CTT-RELATED FAILURE SCENARIOS

There are four fault trees associated with the CTT:

1. Spurious movement of the CTT in the Cask Preparation Area during cask loading.
2. Spurious movement of the CTT in the Cask Preparation Area during cask preparation.
3. Collision of the CTT during cask transfer.
4. Spurious movement of the CTT in the Cask Loading Room.

An additional fault tree involving the CTT is closing of the shield door on the CTT as the CTT moves a cask from the Cask Preparation Area to the Canister Transfer Room. This fault tree is

described in a separate section involving inadvertent shield door closure that satisfies ESD-12, pivotal event "Collision with Cask Unloading Room Shield Door."

In all cases a conservative mission time of one hour per cask transfer was used for each fault tree. The time required to move a cask to the trolley and disconnect the crane is approximately 55 minutes, while the time required moving the trolley from the Cask Preparation Area to the Cask Unloading Room is approximately 15 minutes. The time required to extract the canister from the cask is approximately 20 minutes (Ref. B2.1.2). Therefore, a one hour mission time is considered a conservative value.

B2.4.1 Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading

B2.4.1.1 Description

This fault tree describes spurious movement of the CTT during cask loading to satisfy ESD-5 and ESD-6, pivotal event "Spurious Movement." The top event is "Spurious Movement of the CTT during Cask Loading" which is defined as unplanned movement of the CTT while the cask is being loaded onto the CTT. This fault tree is shown in Figures B2.4-3 and B2.4-4.

Spurious movement can be caused by equipment failures, or by a combination of equipment failure and operator error. For equipment failures to cause spurious movement the main air supply valve must open to supply air to the air bags to levitate the CTT. This can occur if the main air supply valve fails open or the locking pin limit switches and control system fail causing the valve to open. For the operator to initiate spurious movement, the locking pin limit switches must fail allowing the operator to open the main air supply valve.

B2.4.1.2 Success Criteria

A success criterion is that the CTT remains motionless during loading of the transportation cask. Movement of the CTT during this operation could cause impact and damage to the transportation cask.

B2.4.1.3 Design Requirements and Features

Requirements

There are no additional design requirements.

Features

The design feature is the locking restraint pin system that prevents power to the main air supply valve until the pins are in place and the limit switches are activated to allow power to the air supply valve.

B2.4.1.4 Fault Tree Model

The top event is "Spurious Movement of the CTT during Cask Loading in the Cask Preparation Area" (Figure B2.4-3). This can occur if the control system initiates a spurious signal and both of the pin limit switches fail, or the operator initiates a command to move the CTT and both of the pin limit switches fail. A third failure mode is the mechanical failure of the main supply valve in conjunction with a spurious signal from the control system to initiate movement or failures of the control valves or the valve to the air bags.

A conservative mission time for this operation has been set at one hour.

B2.4.1.5 Basic Event Data

Table B2.4-1 contains a list of basic events used in the fault tree (Figures B2.4-3 and B2.4-4) for the "Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading.

Table B2.4-1. Basic Event Probabilities for Spurious Movement of the CTT during Cask Loading

Name	Calculation Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050--CTT--SV401--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
050-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
050-CTT--SV301---SV--SPO	3	4.090E-007	0.000E+000	4.090E-007	1.000E+000
050-CTT--ZS301---ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
050-CTT--ZS302---ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
050-CTT-FWDREVM1-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-FWDREVM2-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM1--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM2--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-OPSPURMOV-HFI-NOD	1	1.000E-004	1.000E-004	0.000E+000	0.000E+000
050-PIN-LIMIT-ZS-CCF	1	1.380E-005	1.380E-005	0.000E+000	0.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B2.4.1.5.1 Human Failure Events

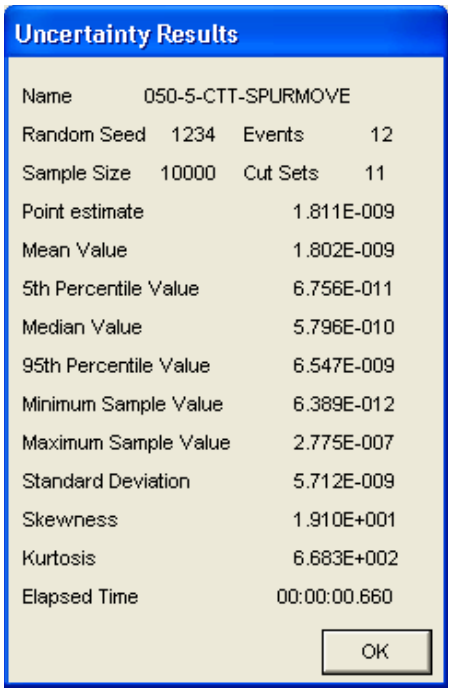
One operator error involves initiation of spurious movement. The operator error is 050-OPSPURMOVE01-HFI-NOD.

B2.4.1.5.2 Common-Cause Failures

One common-cause failure was added to the tree to account for failure of both restraint pin limit switches. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the success criteria (Table C3-1, CCCG = 2). The common-cause failure is 050-PIN-LIMIT-SW-CCF.

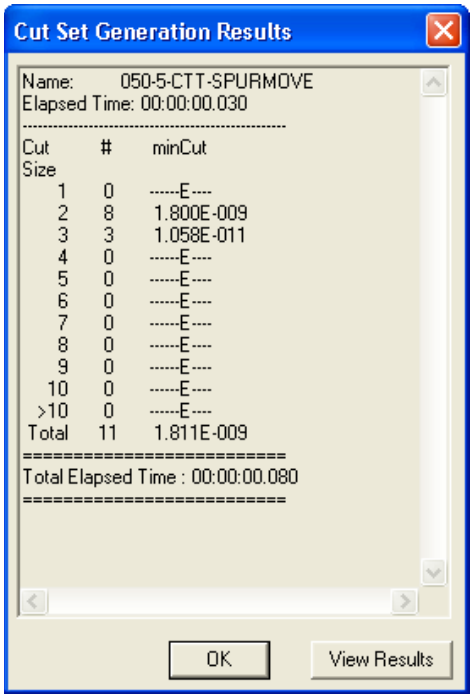
B2.4.1.6 Uncertainty and Cut Set Generation Results

Figure B2.4-1 contains the uncertainty results obtained from running the fault tree for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading" using a cutoff probability of 1E-15. Figure B2.4-2 provides the cut set generation results for "Spurious movement of the CTT in the Cask Preparation Area during Cask Loading."



Source: Original

Figure B2.4-1. Uncertainty Results of the Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading Fault Tree



Source: Original

Figure B2.4-2. Cut Set Generation Results for the Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading Fault Tree

B2.4.1.7 Cut Sets

Table B2.4-2 contains the cut sets for spurious movement of the CTT in the Cask Preparation Area during cask loading. The total probability per cask loading is 1.81E-9.

Table B2.4-2. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading and for CTT Air Supply Failure

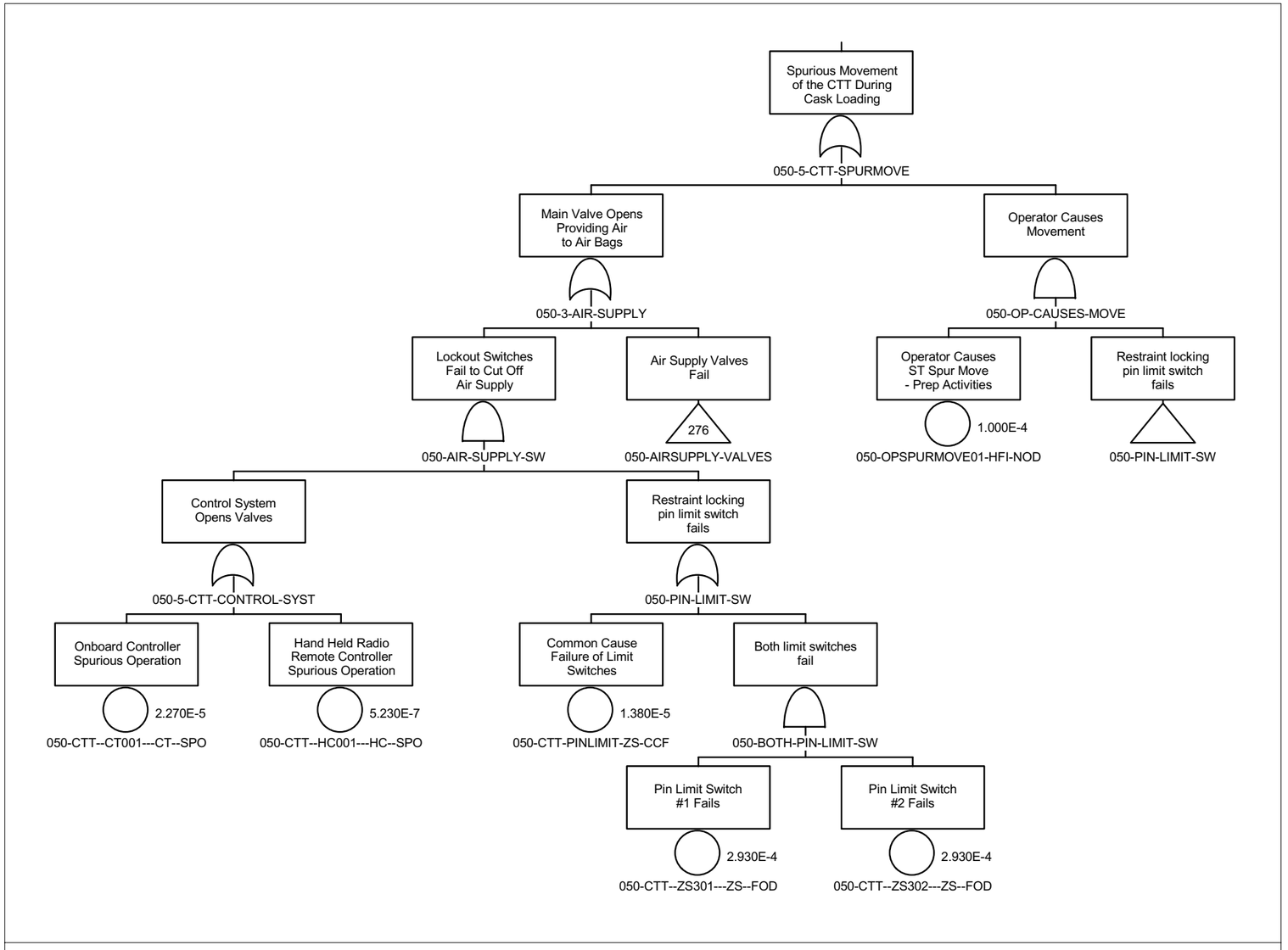
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
050-5-CTT-SPURMOVE	76.22	1.380E-009	050-CTT-PINLIMIT-ZS-CCF	Common Cause Failure of Limit Switches	1.380E-005
			050-OPSPURMOVE01-HFI-NOD	Operator Causes ST Spur Move - Prep Activities	1.000E-004
	17.30	3.133E-010	050-CTT--CT001---CT--SPO	Onboard Controller Spurious Operation	2.270E-005
			050-CTT-PINLIMIT-ZS-CCF	Common Cause Failure of Limit Switches	1.380E-005
	1.10	1.992E-011	050--CTT--SV401--SV--FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.870E-005
			050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
	1.10	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007

Table B2.4-2. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
			050-CTT-FWDREVM2-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.870E-005
	1.10	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-FWDREVM1-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.870E-005
	1.10	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-SVROTM2--SV--FOH	Failure of SV Providing Rotation to Motor 2	4.870E-005
	1.10	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-SVROTM1--SV--FOH	Failure of SV Providing Rotation to Motor 1	4.870E-005
	0.47	8.585E-012	050-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.930E-004
			050-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.930E-004
			050-OPSPURMOVE01-HFI-NOD	Operator Causes ST Spur Move - Prep Activities	1.000E-004
	0.40	7.217E-012	050-CTT--HC001---HC--SPO	Hand Held Radio Remote Controller Spurious Operation	5.230E-007
			050-CTT-PINLIMIT-ZS-CCF	Common Cause Failure of Limit Switches	1.380E-005
	0.11	1.949E-012	050-CTT--CT001---CT--SPO	Onboard Controller Spurious Operation	2.270E-005
			050-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.930E-004
			050-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.930E-004
	0.00	4.490E-014	050-CTT--HC001---HC--SPO	Hand Held Radio Remote Controller Spurious Operation	5.230E-007
			050-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.930E-004
			050-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.930E-004
1.811E-009 = Total					

B2.4.1.8 Fault Trees

The fault trees for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading" are shown in Figures B2.4-3 and B2.4-4.



Source: Original

Figure B2.4-3. Fault Tree for Spurious Movement of the CTT in the Cask Preparation Area During Cask Loading

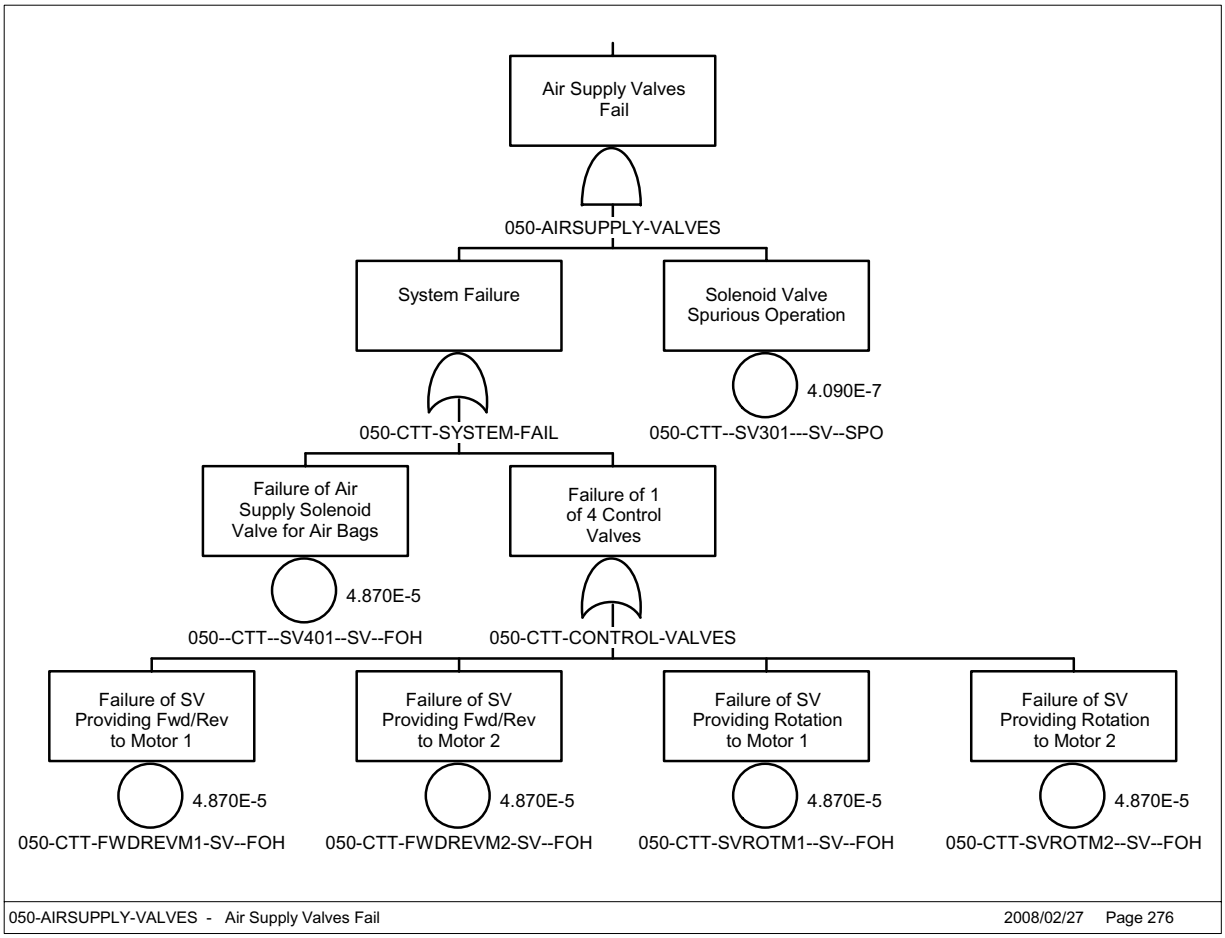


Figure B2.4-4. Fault Tree for CTT Air Supply Valve Failure

B2.4.2 Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation

B2.4.2.1 Description

This fault tree describes spurious movement of the CTT during cask preparation to satisfy ESD-7, 8 and 9, pivotal event "Side Impact to Cask." The top event is "Spurious Movement of the CTT during Cask Prep" which is defined as unplanned movement of the CTT while the cask is being prepared for movement to the Cask Unloading Room by unbolting the lid and installing the lid adapter. This fault tree is shown in Figure B2.4-7.

During this operation, the locking pins have been installed and the limit switches are closed. Spurious movement can be caused by multiple equipment failures, or by operator error. For equipment failures to cause spurious movement the main air supply valve must open to supply air to the air bags to levitate the CTT. This can occur through failure of the main air supply valve coupled with spurious commands from the control system or failure of the control valves. Alternatively, the operator can initiate spurious movement since at this stage of the operation there are no preventive interlocks.

B2.4.2.2 Success Criteria

Success criterion is that the CTT remain motionless during cask preparation. Movement of the CTT during this operation could cause an impact to occur resulting in damage to the transportation cask.

B2.4.2.3 Design Features and Requirements

There are no design features or requirements for this operation.

B2.4.2.4 Fault Tree Model

The top event in this fault tree is spurious movement of the CTT during cask preparation (Figure B2.4-7). This can occur through spurious signals from the control system, spurious operation of the main air supply valve, failure of the control valves, or operator error initiating CTT movement.

B2.4.2.5 Basic Event Data Inputs

Table B2.4-3 contains a list of basic events used in the fault tree (Figures B2.4-7) for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Preparation".

Table B2.4-3. Basic Event Probabilities for Spurious Movement of the CTT During Cask Preparation

Name	Calc. Type	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
050-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
050-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
050-OPSPURMOVE01-HFI-NOD	1	1.000E-004	1.000E-004	0.000E+000	0.000E+000
050--CTT--SV401--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT--SV301---SV--SPO	3	4.090E-007	0.000E+000	4.090E-007	1.000E+000
050-CTT-FWDREVM1-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-FWDREVM2-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM1--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM2--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000

NOTE: a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B2.4.2.5.1 Human Failure Events

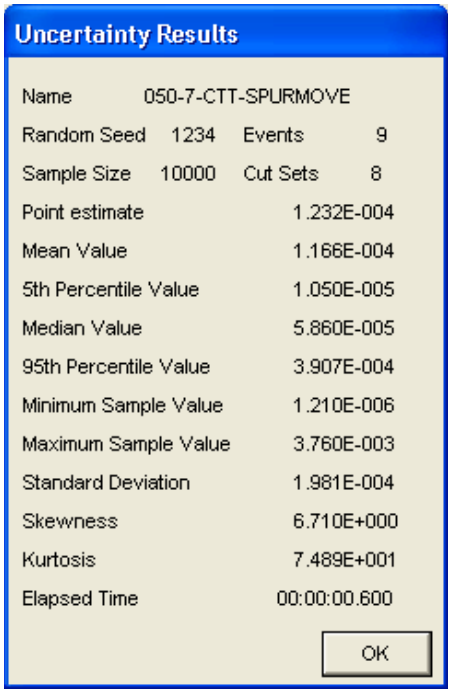
One operator error (050-OPSPURMOVE01-HFI-NOD) involves initiation of spurious movement.

B2.4.2.5.2 Common-Cause Failures

There is no CCF associated with this fault tree.

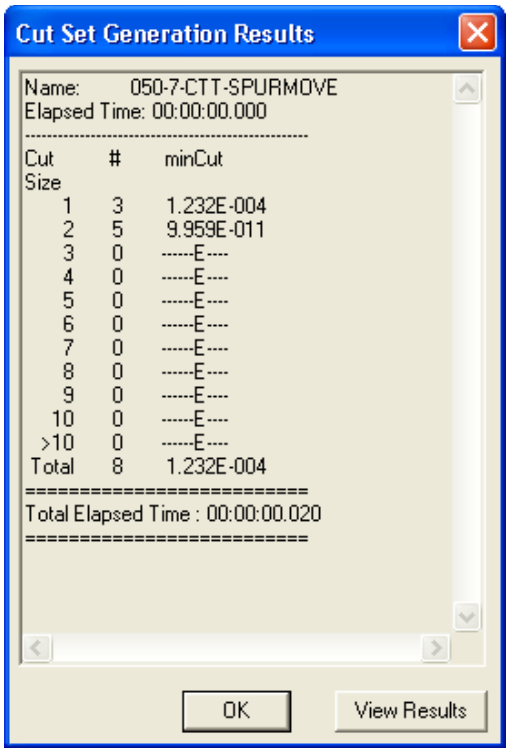
B2.4.2.6 Uncertainty and Cut Set Generation Results

Figure B2.4-5 contains the uncertainty results obtained from running the fault tree for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Preparation". Figure B2.4-6 provides the cut set generation results for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Preparation" fault Tree.



Source: Original

Figure B2.4-5. Uncertainty Results of the CTT Spurious During Cask Preparation



Source: Original

Figure B2.4-6. Cut Set Generation Results for CTT Spurious Movement during Cask Preparation

B2.4.2.7 Cut Sets

Table B2.4-4 contains the cut sets for spurious movement of the CTT in the Cask Preparation Area during cask preparation. The total probability per cask is 1.23E-4 with operator initiation of spurious movement the dominant cause of movement during cask preparation.

Table B2.4-4. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation

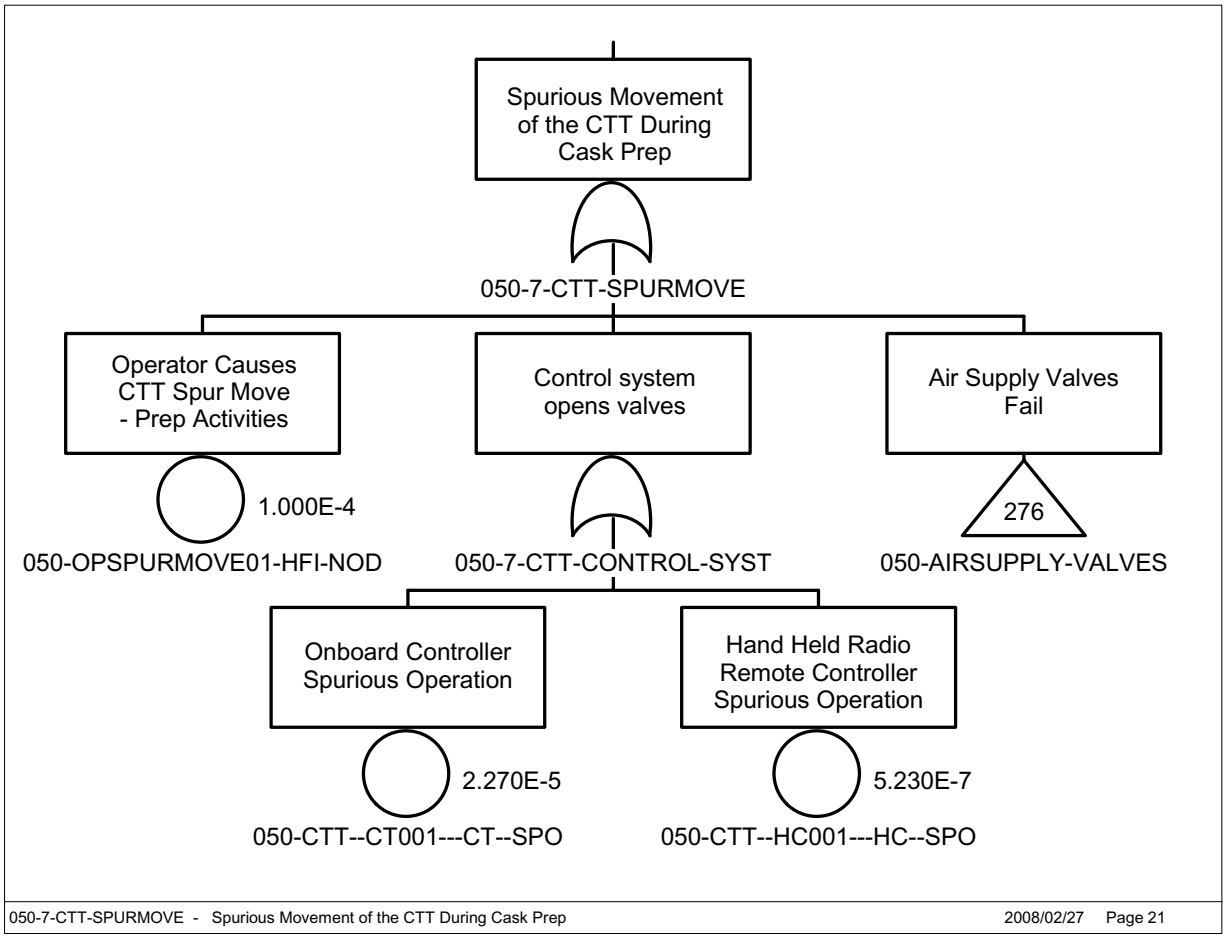
Fault Tree	% Cut Set	Prob./Freq.	Basic Event	Description	Probability
050-7-CTT-SPURMOVE	81.16	1.000E-004	050-OPSPURMOVE01-HFI-NOD	Operator Causes CTT Spur Move - Prep Activities	1.000E-004
	18.42	2.270E-005	050-CTT--CT001---CT--SPO	Onboard Controller Spurious Operation	2.270E-005
	0.42	5.230E-007	050-CTT--HC001---HC--SPO	Hand Held Radio Remote Controller Spurious Operation	5.230E-007
	0.00	1.992E-011	050--CTT--SV401--SV--FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.870E-005
			050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
	0.00	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-SVROTM1--SV--FOH	Failure of SV Providing Rotation to Motor 1	4.870E-005
	0.00	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-FWDREVM1-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.870E-005
	0.00	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-SVROTM2--SV--FOH	Failure of SV Providing Rotation to Motor 2	4.870E-005
	0.00	1.992E-011	050-CTT--SV301---SV--SPO	Solenoid Valve Spurious Operation	4.090E-007
			050-CTT-FWDREVM2-SV--FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.870E-005
1.232E-004 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B2.4.2.8 Fault Trees

The fault trees for "Spurious Movement of the CTT in the Cask Preparation Area during Cask Preparation" are shown in Figure B2.4-7. Note that the transfer gate 276 in Figure B2.4-7 refers to the fault tree in Figure B2.4-4.



Source: Original

Figure B2.4-7. Fault Tree for Spurious Movement of the CTT During Cask Preparation

B2.4.3 Collision of CTT during Cask Transfer

B2.4.3.1 Description

This fault tree considers the potential for the CTT to collide into a structure or object while moving a cask from the Cask Preparation Area to the Cask Unloading Room to satisfy ESD10 and ESD14, pivotal event "CTT Collision" and "Impact to Cask," respectively The top event is "CTT Collision into Structure." This fault tree is shown in Figure B2.4-10 and Figure B2.4-11.

Two primary causes of a collision are operator initiated (possibly through inattention) or failure of the CTT to stop. Movement in the wrong direction as a contributing factor is negated by the use of guide rails forcing the CTT to only move forward and back. A runaway condition is prevented by the control system, designed to give a proportional signal to the air valve that produces a speed range of only 0 to 10 fpm, and an in-line factory-set mechanical throttle valve that limits the speed to 10 fps in the event the control system fails. In the event both of these devices fail, the stop functions must also fail. Since all three functions must fail for a runaway condition, the primary events leading to a collision are operator error or failure to stop.

Failure to stop the CTT requires that failure of the normal stop function, deadman switches, and the air supply valve all fail to close on demand. The emergency stop buttons, one on the pendant and one on the CTT, must also fail; however, because these are recovery actions to be taken by the operator, the emergency stop functions are not credited in the fault tree.

B2.4.3.2 Success Criteria

The success criterion for this event is that the CTT does not experience collision with any object, including the shield door, during transfer of a cask from the Cask Preparation Area to the Cask Unloading Room. A collision of the CTT could cause damage to the transportation cask.

B2.4.3.3 Design Requirements and Features

The design feature is the deadman switches on the pendant control that must be pressed for air to be supplied to the CTT to provide motive power. There are no requirements for this operation.

B2.4.3.4 Fault Tree Model

The top event of the fault tree is a collision of the CTT into an object or structure during transfer of a cask from the Cask Preparation Area to the Cask unloading Room. This may occur through operator error or equipment failure of the normal or emergency stop functions. A conservative mission time for this operation has been set at one hour.

B2.4.3.5 Basic Event Data

Table B2.4-5 contains a list of basic events used in the CTT collision fault tree (Figures B2.4-10 and B2.4-11) for "Collision of the CTT during Cask Transfer.

Table B2.4-5. Basic Event Probability for CTT Collision during Cask Transfer

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-CTT--DSW000--ESC-CCF	1	1.180E-005	1.180E-005	0.000E+000	0.000E+000
050-CTT--DSW001--ESC-FOD	1	2.500E-004	2.500E-004	0.000E+000	0.000E+000
050-CTT--DSW002--ESC-FOD	1	2.500E-004	2.500E-004	0.000E+000	0.000E+000
050-CTT--HC021---HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
050-CTT--SV601---SV--FOD	1	6.280E-004	6.280E-004	0.000E+000	0.000E+000
050-CTT--SV602---SV--FOD	1	6.280E-004	6.280E-004	0.000E+000	0.000E+000
050-OPCTTCOLLID2-HFI-NOD	1	1.000E-003	1.000E-003	0.000E+000	0.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.
Source: Original

B2.4.3.5.1 Human Failure Events

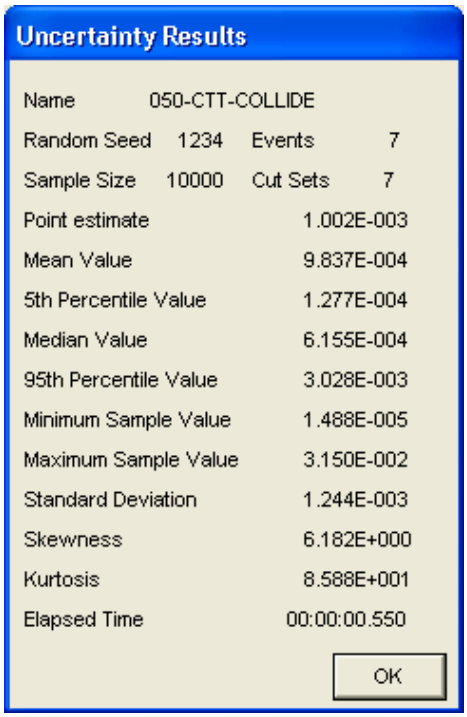
A collision may be caused by an operator error (050-OPCTTCOLLID2-HFI-NOD) failing to stop the CTT.

B2.4.3.5.2 Common-Cause Failures

One common-cause failure (050-CTT--DSW000--ESC-CCF) involves failure of both deadman switches, both of which must be pressed for the main air supply valve to open. An alpha factor of 0.047 was used to determine the CCF value using two of two as the success criteria (Table C3-1, CCCG = 2).

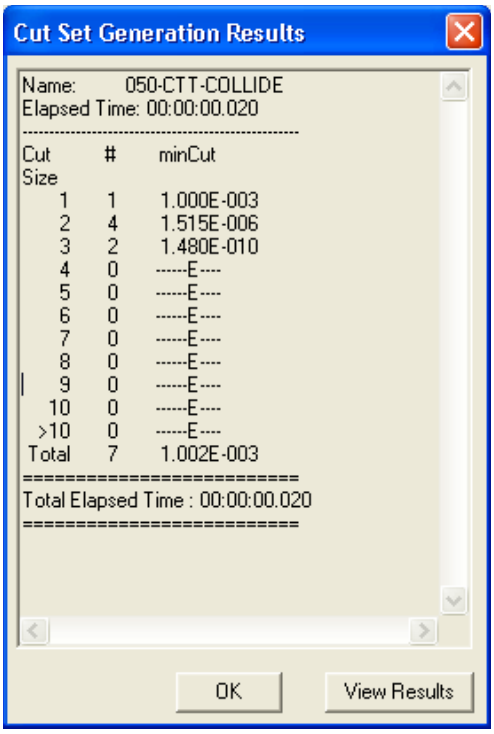
B2.4.3.6 Uncertainty and Cut Set Generation Results

Figure B2.4-8 contains the uncertainty results obtained from running the fault trees for "Collision of the CTT during Cask Transfer" using a cutoff probability of 1E-12. Figure B2.4-9 provides the cut set generation results for the "Collision of the CTT during Cask Transfer" fault tree.



Source: Original

Figure B2.4-8. Uncertainty Results for the Collision of the CTT during Cask Transfer Fault Tree



Source: Original

Figure B2.4-9. Cut Set Generation Results for the Collision of the CTT during Cask Transfer Fault Tree

B2.4.3.7 Cut Sets

Table B2.4-6 contains the cut sets for "Collision of the CTT during cask Transfer" from the Cask Preparation Area to the Canister Transfer Area. The total frequency per cask is 1.00E-03 with operator error the dominant cause of collision.

Table B2.4-6. Cut Sets for Collision of the CTT during Cask Transfer and CTT Fail to Stop

Fault Tree	% Cut Set	Probability/ Frequency	Basic Event	Description	Probability
050-CTT-COLLIDE	99.85	1.000E-003	050-OPCTCOLLIDE2-HFI-NOD	Operator causes CTT collision	1.000E-003
	0.11	1.093E-006	050-CTT--HC021---HC--FOD	Remote stop control transmits wrong instruction	1.740E-003
			050-CTT--SV601---SV--FOD	Main air supply valve on CTT fails to close	6.280E-004
	0.04	3.944E-007	050-CTT--SV601---SV--FOD	Main air supply valve on CTT fails to close	6.280E-004
			050-CTT--SV602---SV--FOD	Solenoid valve fails to close	6.280E-004
	0.00	2.053E-008	050-CTT--DSW000--ESC-CCF	Common cause failure of deadman switches	1.180E-005
			050-CTT--HC021---HC--FOD	Remote stop control	1.740E-003

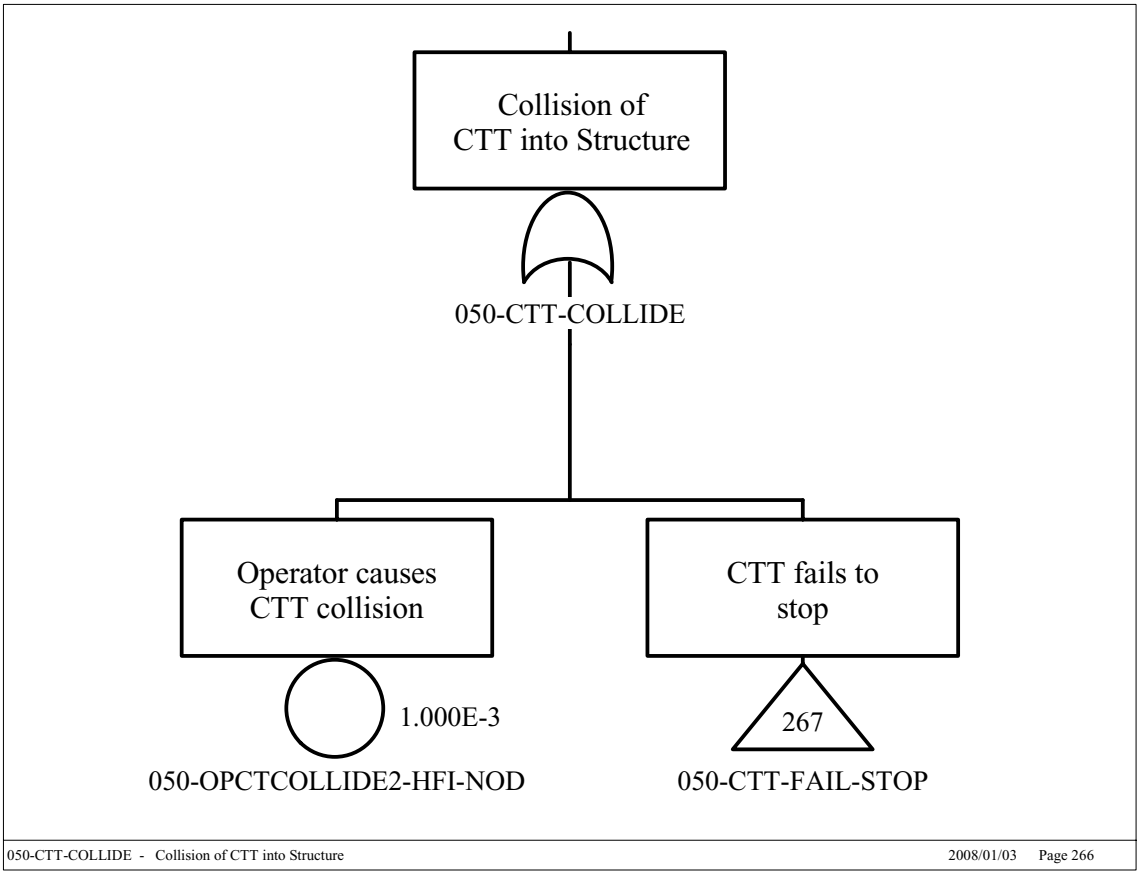
Table B2.4-6. Cut Sets for Collision of the CTT During Cask Transfer (Continued)

Fault Tree	% Cut Set	Probability/ Frequency	Basic Event	Description	Probability
				transmits wrong instruction	
	0.00	7.410E-009	050-CTT--DSW000--ESC-CCF	Common cause failure of deadman switches	1.180E-005
			050-CTT--SV602---SV--FOD	Solenoid valve fails to close	6.280E-004
	0.00	1.088E-010	050-CTT--DSW001--ESC-FOD	Deadman switch 1 fails closed	2.500E-004
			050-CTT--DSW002--ESC-FOD	Deadman switch 2 fails closed	2.500E-004
			050-CTT--HC021---HC--FOD	Remote stop control transmits wrong instruction	1.740E-003
	0.00	3.925E-011	050-CTT--DSW001--ESC-FOD	Deadman switch 1 fails closed	2.500E-004
			050-CTT--DSW002--ESC-FOD	Deadman switch 2 fails closed	2.500E-004
			050-CTT--SV602---SV--FOD	Solenoid valve fails to close	6.280E-004
1.002E-003 = Total					

NOTE: Freq. = frequency; Prob. = probability.

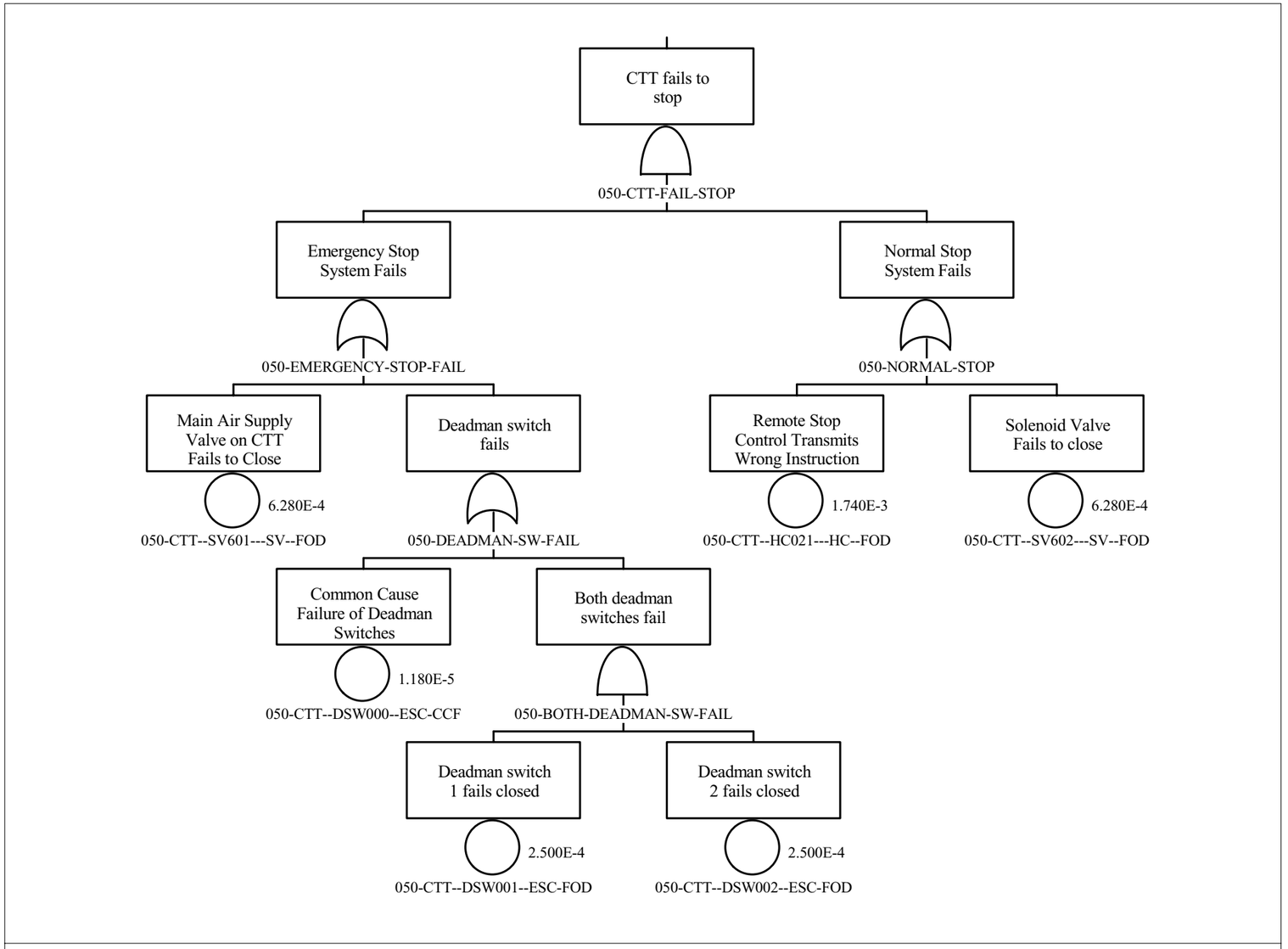
Source: Original

B2.4.3.8 Fault Trees



Source: Original

Figure B2.4-10. Fault Tree for Collision of the CTT During Cask Transfer (Page 1)



Source: Original

Figure B2.4-11. Fault Tree for CTT Fail to Stop

B2.4.4 Spurious Movement of the CTT in the Canister Transfer Room

B2.4.4.1 Description

This fault tree describes spurious movement of the CTT during extraction, or unloading, of the canister from the transportation cask on the CTT to satisfy ESD13, the pivotal event "CTT Spurious Movement." The top event is "Spurious Movement during Canister Transfer" which is defined as unplanned movement of the CTT while the canister is being removed from the transportation cask. This fault tree is shown in Figure B2.4-14.

Spurious movement is prevented in the Canister Transfer Room by disconnecting the air supply hose from the CTT. The shield door interlock (external to the CTT) must be closed to allow the port slide gate to open and canister extraction to begin. Thus, if the shield door is not closed the slide gate cannot open and extraction of the canister cannot begin. With the air supply located outside the Canister Transfer Room, the operator must disconnect the air supply hose to the CTT for the shield door to be closed, or the shield door will cut through the hose upon closing. If the operator fails to disconnect the hose, movement may be initiated by failure of the door interlocks and the control system causing the main air supply valve to open, or the main air supply valve to "fail open" in conjunction with failure of the controls or the control valves. During this transfer process the operator is not in the Canister Transfer Room and cannot access the controls to initiate spurious movement.

B2.4.4.2 Success Criteria

Success criterion is that the CTT remain motionless during canister extraction from the transportation cask. Movement of the CTT during this operation could cause impact to occur and/or shear and damage to the canister.

B2.4.4.3 Design Requirements and Features

The design feature is the shield door interlocks that prevent the extraction operation until the shield door is closed. Requirements include locating the air supply outside the Canister Transfer Room, and for the operator to disconnect the air supply to the CTT prior to unloading.

B2.4.4.4 Fault Tree Model

The top event is the spurious movement of the CTT during extraction of the canister from the transportation cask on the CTT. This may occur through failure to disconnect the air supply resulting in operation of the main air supply valve. The air supply valve may fail through spurious operation of the valve or spurious signals generated by the control system. Compressed air may be available to the CTT through failure of the operator to disconnect the air hose, or failure of the shield door interlocks. A conservative mission time for this operation has been set at one hour.

B2.4.4.5 Basic Event Data Input

Table B2.4-7 contains a list of basic events used in the fault tree (Figures B2.4-14) for "Spurious Movement during Canister Transfer" in the canister Transfer Area.

Table B2.4-7. Basic Event Probability for Spurious Movement during Canister Transfer

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-CR---IEL001--IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-CR---IEL002--IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-CR---IELCCF--IEL-CCF	1	1.290E-006	1.290E-006	0.000E+000	0.000E+000
050-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
050-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
050-OPNODISCOAIR-HFI-NOD	1	1.000E-003	1.000E-003	0.000E+000	0.000E+000
050-CTT--SV301---SV--SPO	3	4.090E-007	0.000E+000	4.090E-007	1.000E+000
050--CTT--SV401--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-FWDREVM1-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-FWDREVM2-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM1--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
050-CTT-SVROTM2--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B2.4.4.5.1 Human Failure Events

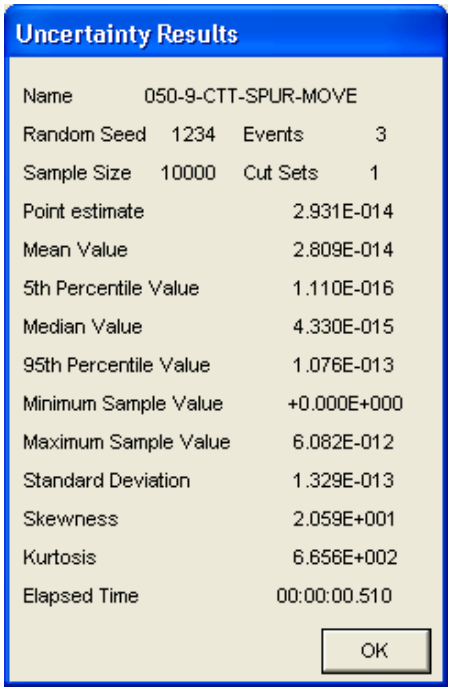
One operator error involves failure to disconnect the air supply (050-OPNODISCOAIR-HFI-NOD).

B2.4.4.5.2 Common-Cause Failures

One common-cause failure (050-CR---IELCCF--IEL-CCF) involves failure of both shield door interlocks allowing the shield door to close and the slide port gate to open. An alpha factor of 0.047 was used to determine the CCF value using two of two as the success criteria (Table C3-1, CCCG = 2).

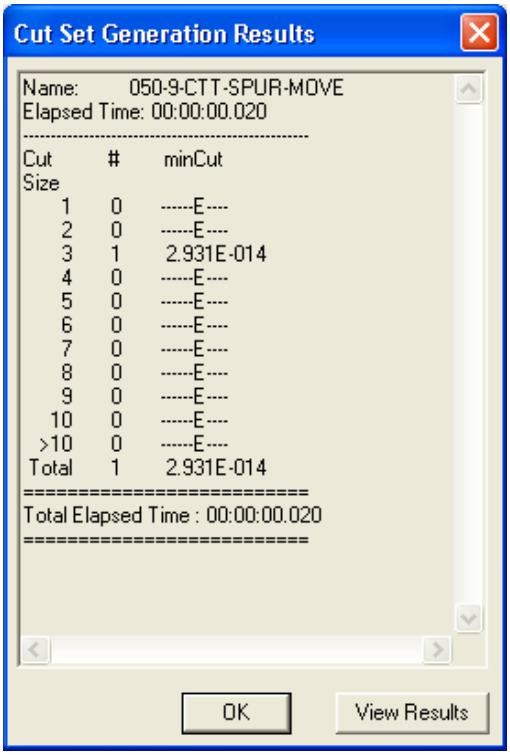
B2.4.4.6 Uncertainty and Cut Set Generation Results

Figure B2.4-12 contains the uncertainty results obtained from running the fault trees for "Spurious Movement during Canister Transfer" while extracting the canister from the transportation cask in the unloading area. Figure B2.4-13 provides the cut set generation results for "Spurious Movement during Canister Transfer" fault tree.



Source: Original

Figure B2.4-12. Uncertainty Results for the Spurious Movement during Canister Transfer Fault Tree



Source: Original

Figure B2.4-13. Cut Set Generation Results for the Spurious Movement during Canister Transfer Fault Tree

B2.4.4.7 Cut Sets

Table B2.4-8 contains the cut sets for "Spurious Movement during Canister Transfer" in the canister unloading area. The total frequency per cask is 2.93E-014.

Table B2.4-8. Cut Sets for Spurious Movement during Canister Transfer and Collision of CTT during Cask Transfer

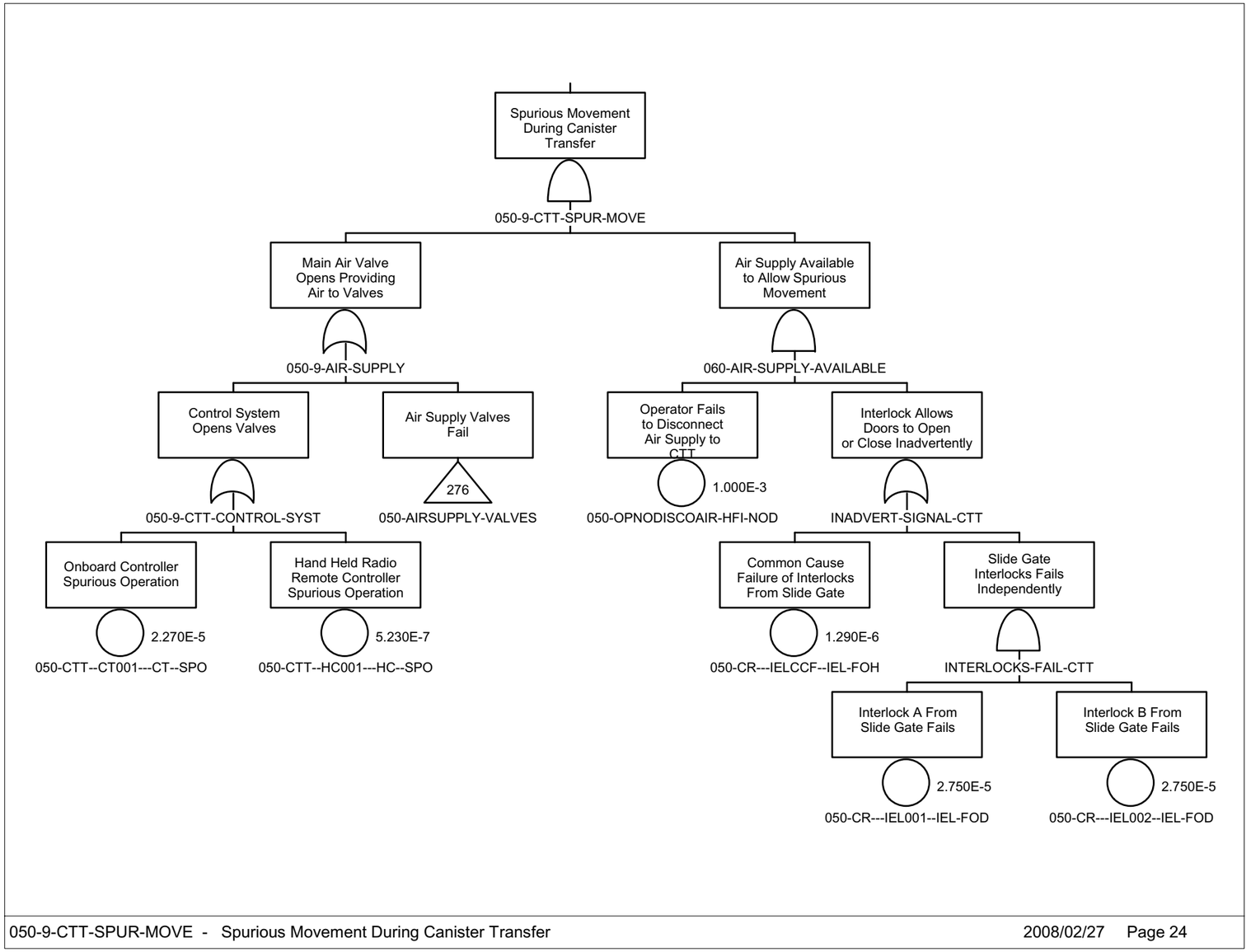
Fault Tree	% Cut Set	Prob./Freq.	Basic Event	Description	Probability
050-9-CTT-SPUR-MOVE	99.91	2.928E-014	050-CR---IELCCF--IEL-FOH	Common Cause Failure of Interlocks From Slide Gate	1.290E-006
			050-CTT--CT001---CT--SPO	Onboard Controller Spurious Operation	2.270E-005
			050-OPNODISCOAIR-HFI-NOD	Operator Fails to Disconnect Air Supply to CTT	1.000E-003
2.931E-014 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B2.4.4.8 Fault Trees

The fault tree for "Spurious Movement during Canister Transfer" is shown in Figures B2.4-14. Note that the transfer gate 276 in Figure B2.4-14 refers to the fault tree in Figure B2.4-4.



Source: Original

Figure B2.4-14. Fault Tree for Spurious Movement during Canister Transfer

B3 LOADING/UNLOADING ROOM SHIELD DOOR AND SLIDE GATE FAULT TREE ANALYSIS

B3.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designed categories described in Section 4.1, relative to suitability for intended use.

B3.1.1 BSC (Bechtel SAIC Company) 2007. *Nuclear Facilities Equipment Shield Door Process and Instrumentation Diagram*. 000-M60-H000-00101-000 REV 00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0024.

B3.1.2 BSC 2007. *Wet Handling Facility General Arrangement Ground Floor Plan*. 050-P10-WH00-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0032.

B3.1.3 BSC 2007. *Wet Handling Facility General Arrangement Second Floor Plan.* 050-P10-WH00-00104-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0034.

B3.1.4 BSC 2008. *Nuclear Facilities Slide Gate Process and Instrumentation Diagram*. 000-M60-H000-00201-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080123.0025.

B3.2 SLIDE GATE AND SHIELD DOOR SYSTEM DESCRIPTION

B3.2.1 Overview

The WHF Cask Unloading Room has a slide gate providing access to the Canister Transfer Room and a shield door providing access to the Cask Preparation Room. The Cask Loading Room also has a slide gate and shield door (Ref. B3.1.2 and Ref. B3.1.3). The shield doors and slide gates provide shielding during canister unloading and loading. The slide gates and shield doors are important to safety (ITS), protecting workers from the hazardous operations that go on inside the loading and unloading rooms.

B3.2.2 Operations Description

The Cask Unloading Room shield doors are opened to allow cask-carrying equipment, such as the cask transfer trolley (CTT), to enter the room. Once equipment is positioned properly in an

unloading room, shield doors are closed in preparation for removing canisters from the cask. Once the shield doors are shut, the slide gate is opened to allow the canister transfer machine (CTM) to perform cask unloading operations. Loading of the aging overpack is analogous to cask unloading operations. The slide gate is opened to allow aging overpack loading access if the shield doors are closed. Once loading is complete and the slide gate is closed, the shield doors are opened to allow aging overpack removal.

B3.2.3 Physical Description

The shield doors consist of pairs of large heavy doors that are operated by individual motors with over-torque sensors to prevent crushing of an object. Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The obstruction sensor is also alarmed to provide operators indication when an object is between the shield doors. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand lever that must be enabled by an enable/disable switch. An emergency open switch exists enabling the doors to be opened in case of an emergency situation.

Similar to the shield doors, the slide gates consist of two gates that close together between the loading/unloading rooms and the Canister Transfer Room. The gates are operated by individual motors that also have over-torque sensors. Each gate has limit switches to indicate open or closed gates. A CTM skirt-in-place switch is interlocked to the slide gate to prevent the gates from opening without the CTM in place. A CTM in-place bypass hand switch exists for maintenance activities. Slide gate operation is controlled by a hand switch coupled with an enable/disable switch and shield door interlocks prevent the slide gate from opening when the shield door is open. Open/closed and CTM in-place indicators exist to assist operators in their activities.

B3.2.4 Schematics

Schematics for the shield door and slide gate are available separately for review (Ref. B3.1.1 and Ref. B3.1.4).

Additional shield door details are available in *Nuclear Facilities Slide Gate Process and Instrumentation Diagram* (Ref. B3.1.4), including slide gate instrumentation.

B3.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B3.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B3.3-1. Dependencies and Interactions Analysis

Systems, Structures, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Door/gate motors	—	—	—	Inadvertent operation	—
Door/gate position limit switches	CTM	—	—	—	—
CTM	Gate position switches, obstruction sensors	—	—	—	—
Obstruction sensor	CTM	—	—	—	—

NOTE: CTM = canister transfer machine

Source: Original

B3.4 SLIDE GATE AND SHIELD DOOR FAILURE SCENARIOS

The slide gate and shield door system has three credible failure scenarios as follows:

1. Inadvertent opening of the shield door causing direct exposure.
2. Inadvertent opening of the slide gate causing direct exposure.
3. Shield door closes on conveyance.

B3.4.1 Inadvertent Opening of the Shield Door

B3.4.1.1 Description

Inadvertent opening of the shield door while a canister is being unloaded from a cask or loaded into an aging overpack can cause an exposure. For this situation to occur, the slide gate must be open for the CTM to be unloading/loading a canister. Interlocks between the slide gate and shield door prevent an operator from being able to open the shield door during canister unloading or aging overpack loading. However, this situation can occur if the interlocks fail and an operator attempts to open the door, or a spurious open signal is received.

B3.4.1.2 Success Criteria

The success criteria for this failure scenario require that the interlocks between the slide gate and shield door prevent the shield door from opening when the slide gate is open.

B3.4.1.3 Design Requirements and Features

Redundant hard-wired interlocks prevent the shield door from opening while the slide gate is open and vice versa. The shield door system does not have any test, maintenance, or other modes/settings that allow bypass of interlocks.

B3.4.1.4 Fault Tree Model

The top event in this fault tree is "Shield Door Inadvertently Opened While Unloading Cask." This is defined as an opening of the shield door during unloading operations while the cask is in a position that would result in a direct exposure to personnel outside of the unloading room. Faults considered in the evaluation of this top event include: failure of components in the control circuitry of the slide door and a human event that could contribute to the inadvertent door opening. The fault tree is shown in Figure B3.4-3.

B3.4.1.5 Basic Event Data

Six basic events, as shown in Table B3.4-1, are used to model this failure scenario, including one HFE, one common cause failure, and one situational event.

The basic event, "Canister is Exposed During Mid-Unloading" represents the probability that the canister is removed from of the cask, but has not reached the CTM skirt yet. The screening value of 1.0 is used for this event.

Table B3.4-1. Basic Event Probabilities for Inadvertent Opening of Shield Door

Basic Event	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-CR---IELCCF--IEL-CCF	Common-cause failure of interlocks from slide gate	1	1.290E-06	12900E-06	0.000E+00	0.000E+00
050-CR--- IEL001 — IEL-FOD	Interlock A from slide gate fails	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CR--- IEL002— IEL-FOD	Interlock B from slide gate fails	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CR---PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CR-CASK-UNLOADING	Canister is exposed during mid-unloading	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
050-OPDIREXPOSE1-HFI-NOD	Operator mistakenly opens door	1	1.000E-01	1.000E-01	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.1.5.1 Human Failure Events

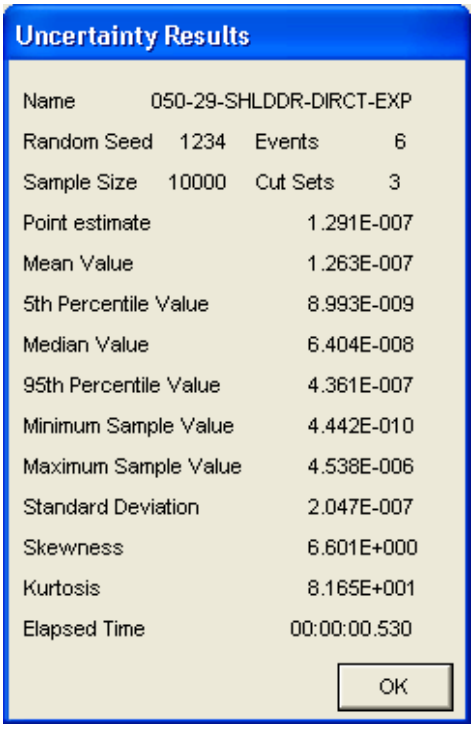
One human failure event (HFE) is modeled in the fault tree as an operator attempting to open the shield doors during a CTM loading or unloading operation. However, for the operator to open the shield door while the slide gate is open the interlock must fail. The screening value used for this HFE has a probability of 1.0E-01 (Table 6.4-1).

B3.4.1.5.2 Common Cause Failures

One common cause failure (CCF) scenario is modeled in the fault tree. The redundant interlocks that prevent the shield door from opening while the slide gate is open can both fail to a common cause. The common-cause alpha factor for two of two successes is 0.047 (Attachment C) which is multiplied with the probability of failure of the component to establish the failure probability of the common-cause event associated with the two common-cause elements.

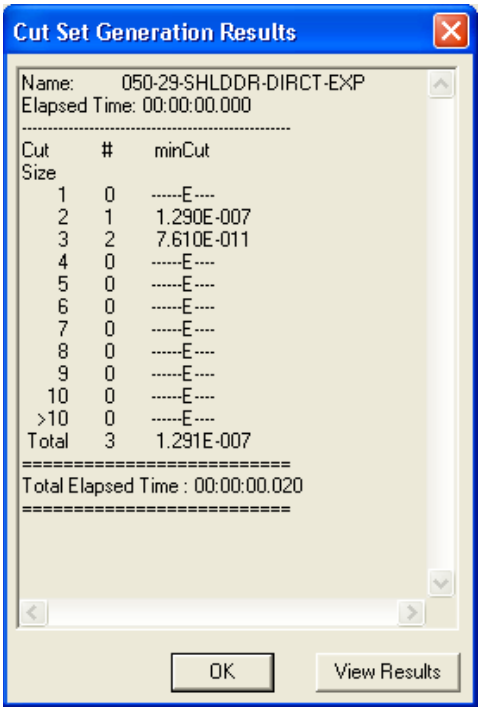
B3.4.1.6 Uncertainty and Cut Set Generation Results

Figure B3.4-1 contains the uncertainty results obtained from running the fault trees for "Shield Door Inadvertently Opened While Unloading Cask" using a cutoff probability of 1E-15. Figure B3.4-2 provides the cut set generation results for the "Shield Door Inadvertently Opened While Unloading Cask" fault tree.



Source: Original

Figure B3.4-1. Uncertainty Results for the Inadvertent Opening of Shield Door Fault Tree



Source: Original

Figure B3.4-2. Cut Set Generation Results for the Inadvertent Opening of Shield Door Fault Tree

B3.4.1.7 Cut Sets

Cut sets for "Inadvertent Opening of Shield Door" are displayed in Table B3.4-2.

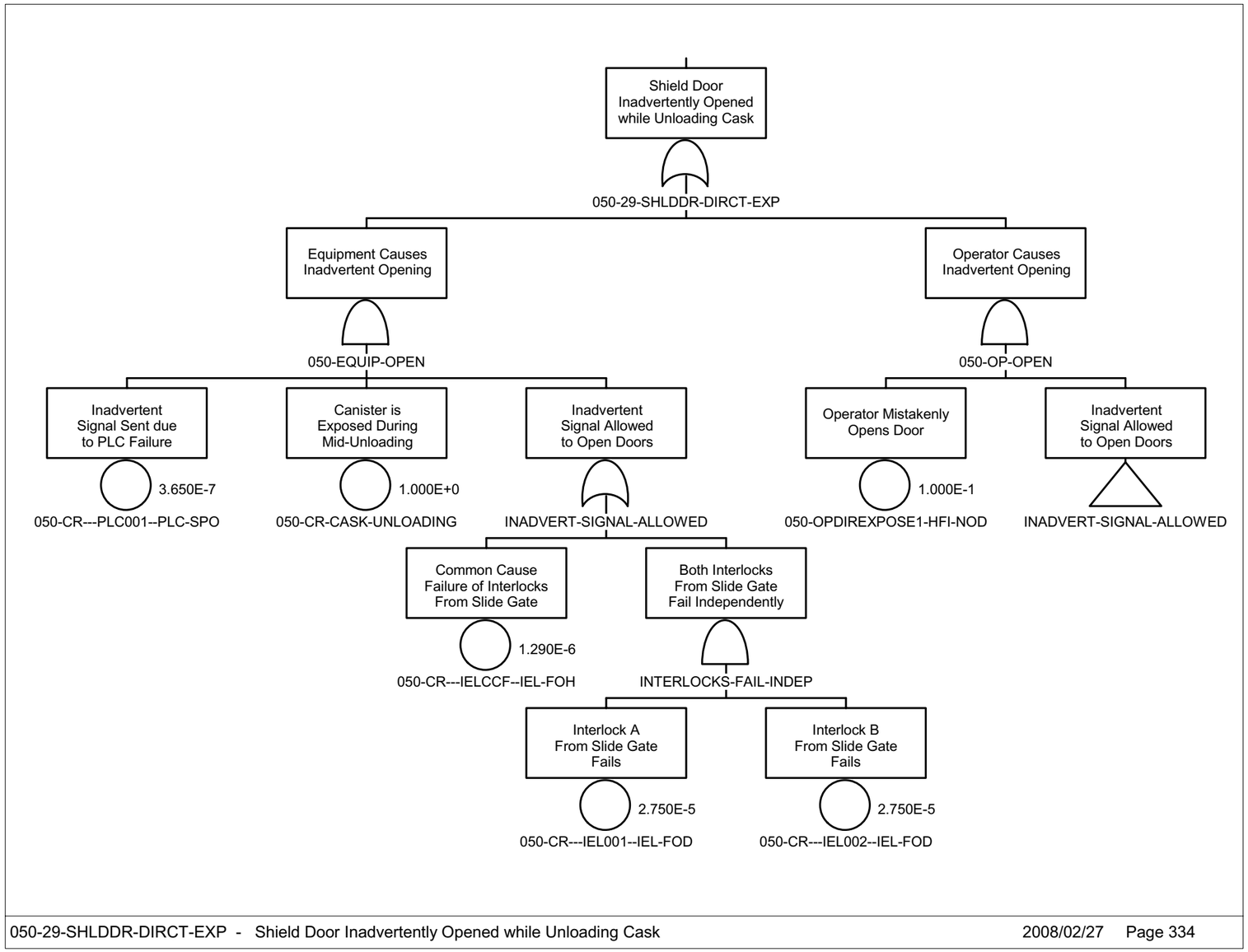
Table B3.4-2. Cut Sets for Inadvertent Opening of Shield Door

Fault Tree	% Cut Set	Prob./Freq.	Basic Event	Description	Probability
050-29-SHLDDR-DIRCT-EXP	99.94	1.290E-007	050-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.290E-006
			050-OPDIREXPOSE1-HFI-NOD	Operator Mistakenly Opens Door	1.000E-001
	0.06	7.562E-011	050-CR---IEL001--IEL-FOD	Interlock A From Slide Gate Fails	2.750E-005
			050-CR---IEL002--IEL-FOD	Interlock B From Slide Gate Fails	2.750E-005
			050-OPDIREXPOSE1-HFI-NOD	Operator Mistakenly Opens Door	1.000E-001
	0.00	4.708E-013	050-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.290E-006
			050-CR---PLC001--PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3.650E-007
			050-CR-CASK-UNLOADING	Canister is Exposed During Mid-Unloading	1.000E+000

NOTE: Freq. = frequency; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.1.8 Fault Trees



Source: Original

Figure B3.4-3. Fault Trees for Inadvertent Opening of the Shield Door

B3.4.2 Inadvertent Opening of Slide Gate

B3.4.2.1 Description

Inadvertent opening of a slide gate can result in exposure if personnel are present in the Canister Transfer Room and a radiation source is exposed in a loading or unloading room. There are two ways that a slide gate may be inadvertently opened: (1) an operator mistakenly opens the slide gate or, (2) the control electronics spuriously opens the slide gate. Additionally, an interlock that prevents the slide gate from opening unless CTM skirt is in place must also fail or be disabled. In this situation, the shield door may be closed; therefore the interlocks that prevent the slide gate from opening while the shield door is open do not prevent the slide gate from opening.

B3.4.2.2 Success Criteria

The success criteria for this failure scenario require that the shield bell slide gate not open during canister transfer operations unless the shield skirt is lowered.

B3.4.2.3 Design Requirements and Features

A single interlock prevents the slide gate from opening when the CTM skirt is not in place.

B3.4.2.4 Fault Tree Model

The top event in this fault tree is “Inadvertent Opening of Slide Gate Causing Direct Exposure.” This is defined as an opening of the slide gate during unloading operations while the cask is in a position that would result in a direct exposure to personnel in the Canister Transfer Room. Faults considered in the evaluation of this top event include: failure of components in the control circuitry of the slide gate and a human event that could contribute to the inadvertent gate opening. The fault tree is shown in Figure B3.4-6.

B3.4.2.5 Basic Event Data

Three basic events, as shown in Table B3.4-3, are used to model this failure scenario, including one human failure events and two hardware events.

Table B3.4-3. Basic Event Probabilities for Inadvertent Opening of Slide Gate causing Direct Exposure

Name	Description	Calc. Type[a]	Calc. Prob.	Failure Prob.	Lambda	Miss. Time[a]
050-CR---IEL001--IEL-FOD	Skirt Interlock Failed	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
050-CR---PLC001--PLC-SPO	Inadvertent Signal Sent Due to PLC Failure	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-OPFAILRSTINT-HFI-NOM	Operator Fails to Reset Interlock after Maint	1	1.000E-02	1.000E-02	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
PLC = programmable logic controller; Calc = calculation; Miss = mission; Prob = probability.

Source: Original

B3.4.2.5.1 Human Failure Events

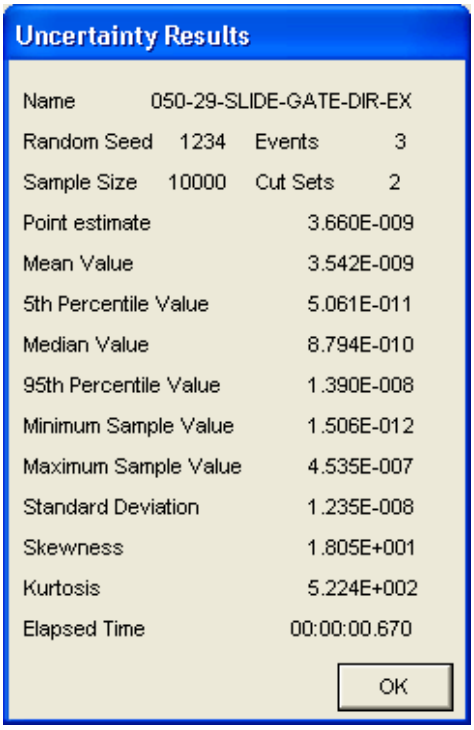
One HFE is modeled in the fault tree. This HFE is a combination of operator actions and interlock failures that can result in the slide gate being opened when the shield skirt is raised. The development of this event is presented in detail as part of the Human Reliability Analysis.

B3.4.2.5.2 Common-Cause Failures

No CCFs were identified for this fault tree.

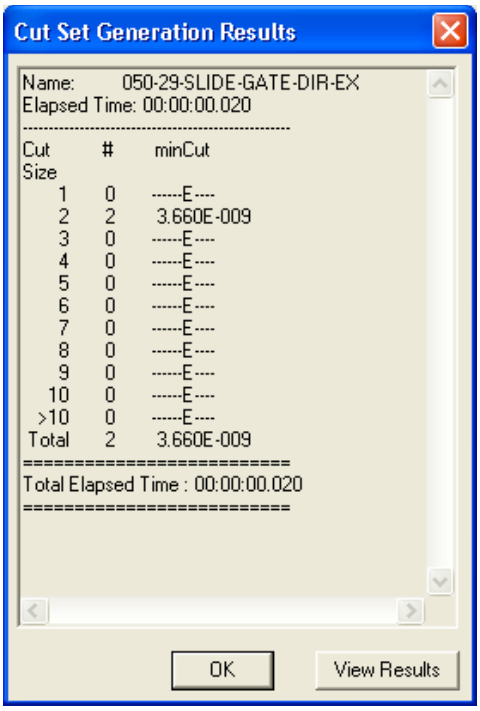
B3.4.2.6 Uncertainty and Cut Set Generation

Figure B3.4-4 contains the uncertainty results obtaining from running the fault tree for "Slide Gate Inadvertently Opens Causing a Direct Exposure" using a cutoff probability of 1E-15. Figure B3.4-5 provides the cut set generation results for "Slide Gate Inadvertently Opens Causing a Direct Exposure" fault tree.



Source: Original

Figure B3.4-4. Uncertainty Results for the Slide Gate Inadvertently Opens Causing Direct Exposure Fault Tree



Source: Original

Figure B3.4-5. Cut Set Generation Results for the Slide Gate Inadvertently Opens Causing a Direct Exposure Fault Tree

B3.4.2.7 Cut Sets

Table B3.4-4 contains the cut sets for "Inadvertent Opening of Slide Gate Causing Direct Exposure".

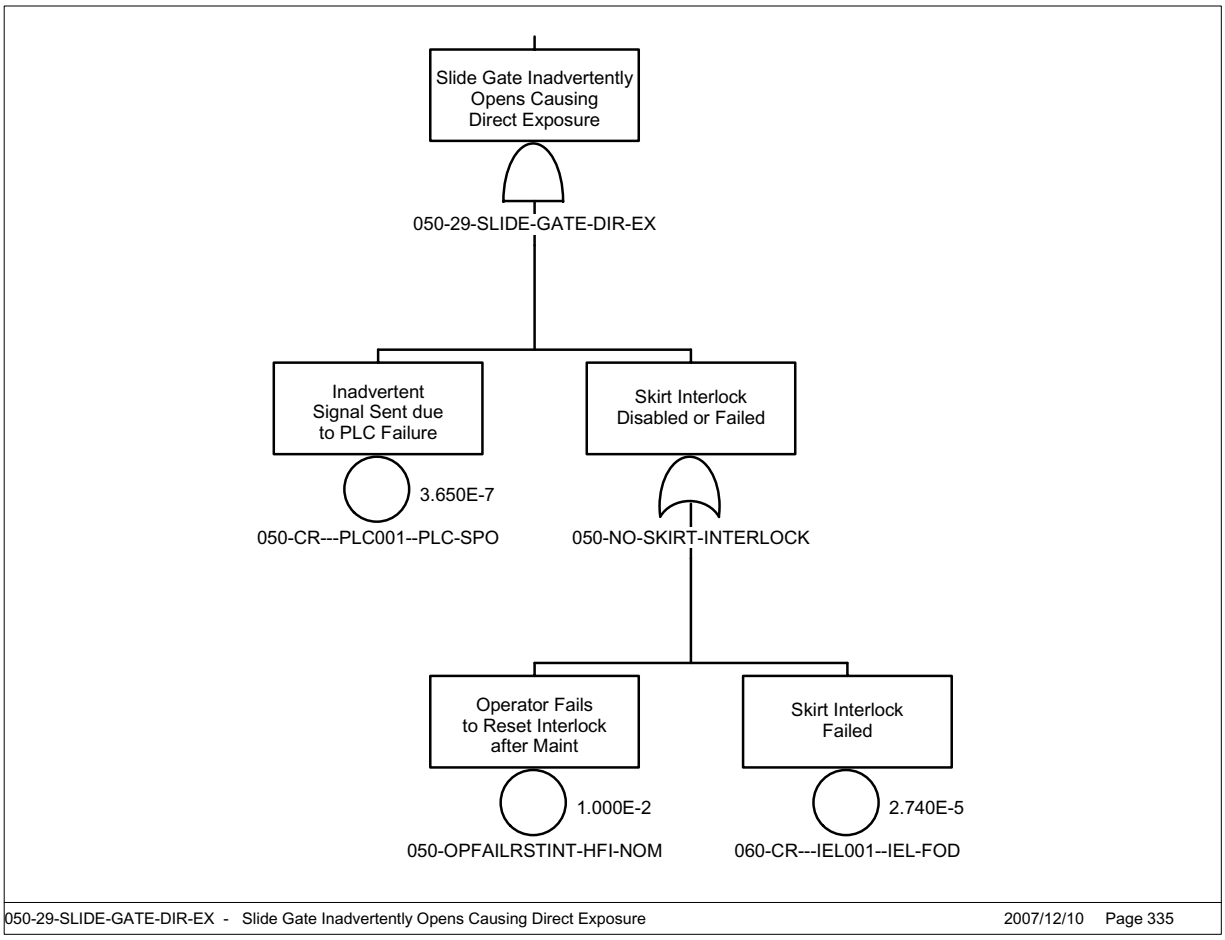
Table B3.4-4. Cut Sets for Inadvertent Opening of Slide Gate Causing Direct Exposure

Fault Tree	% Cut Set	Prob./Freq,	Basic Event	Description	Probability
050-29-SLIDE-GATE-DIR-EX	99.73	3.650E-009	050-CR---PLC001--PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3.650E-007
			050-OPFAILRSTINT-HFI-NOM	Operator Fails to Reset Interlock after Maintenance	1.000E-002
	0.27	1.004E-011	050-CR---IEL001--IEL-FOD	Interlock A From Slide Gate Fails	2.750E-005
			050-CR---PLC001--PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3.650E-007

NOTE: No. = number; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.2.8 Fault Trees



Source: Original

Figure B3.4-6. Fault Trees for Inadvertent Opening of the Slide Gate

B3.4.3. Shield Door Closes on Conveyance

B3.4.3.1 Description

If the shield doors to the loading/unloading rooms are closed as casks or aging overpacks are transferred to/from the unloading/loading rooms, a release may occur as a result. Measures are in place to ensure this situation does not occur, including the presence of an obstruction sensor and motor over-torque sensors.

B3.4.3.2 Success Criteria

A success criterion for this scenario is defined as the shield doors not causing a release due to closure on the conveyance. Specifically, success criteria are defined as follows:

- Obstruction sensor prohibits the initiation of shield door closure

- In the event that the obstruction sensor fails and the shield doors do close on a conveyance, the motor over-torque sensors prevent excessive closure force ensuring no release.

B3.4.3.3 Design Requirements and Features

Objects or obstructions are detected between the shield doors to prevent door closure initiation. Motor over-torque sensors prevent shield doors from causing damage to casks or aging overpacks in the event of closure on a conveyance.

B3.4.3.4 Fault Tree Model

The top event in this fault tree is "Collision of Shield Door into Conveyance." This is defined as an inadvertent closure of the shield doors due to either operator action of component failure while the conveyance is in position to be hit by the doors. Faults considered in the evaluation of this top event include: failure of components in the control circuitry of the shield doors and human events that could contribute to the inadvertent shield door closing. The fault tree is shown in Figure B3.4-9. The fault tree for closure of the shield door on the CTT (050-12-CTT-COLLIDE-SDR) is identical to the fault tree for closure of the shield door on the ST (050-12-ST-COLLIDE-SDR).

B3.4.3.5 Basic Event Data

Six basic events listed in Table B3.4-5 are used to model this failure scenario, including one human failure event and one common cause failure.

Table B3.4-5. Basic Event Probabilities for Shield Door Closes on Conveyance

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-OPSDCLOSE001-HFI-NOD	Operator initiates shield door closure on Conveyance	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
050-SD---PLC001--PLC-SPO	Spurious signal from PLC closes door	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-SD---SRU001--SRU-FOH	Ultrasonic obstruction sensor fails	7	2.161E-03**	0.000E+00	2.161E-03	1.000E+00
050-SD---TL000---TL--CCF	Common-cause failure of over-torque sensors	3	6.801E-04*	0.000E+00	3.780E-06	1.000E+00
050-SD---TL001---TL--FOH	Motor #1 over-torque sensor fails	3	1.435E-02*	0.000E+00	8.050E-05	1.000E+00
050-SD---TL002---TL--FOH	Motor #2 over-torque sensor fails	3	1.435E-02*	0.000E+00	8.050E-05	1.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
*Tau = 360 hours; **Tau = 45 hours.
PLC = programmable logic controller; Prob. = probability; ST = site transporter.

Source: Original

B3.4.3.5.1 Human Failure Events

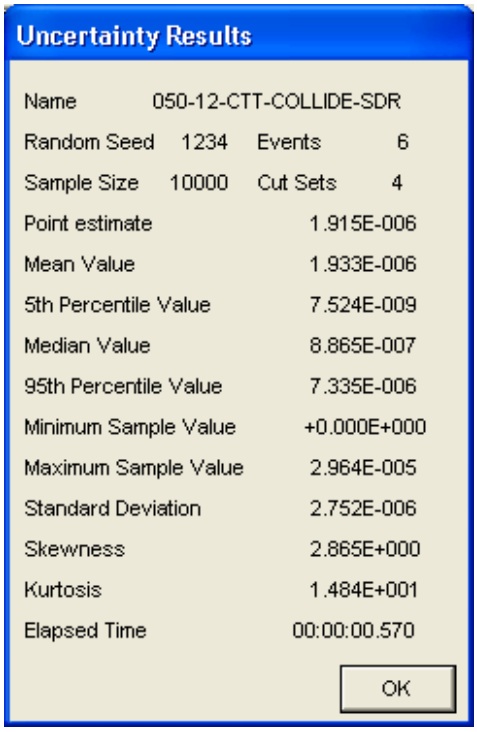
One human failure event (050-OPSDCLOSE001-HFI-NOD) is modeled in the fault tree as an operator attempting to close the shield doors while a conveyance is between the doors. The screening value used for this HFE has a probability of 1.0E+00 (Table 6.4-1).

B3.4.3.5.2 Common-Cause Failures

One common-cause failure, the common-cause failure of the shield door over torque sensors, is considered. This common-cause failure allows the shield doors to continue to attempt to close once an obstruction, in this case the conveyance, is encountered.

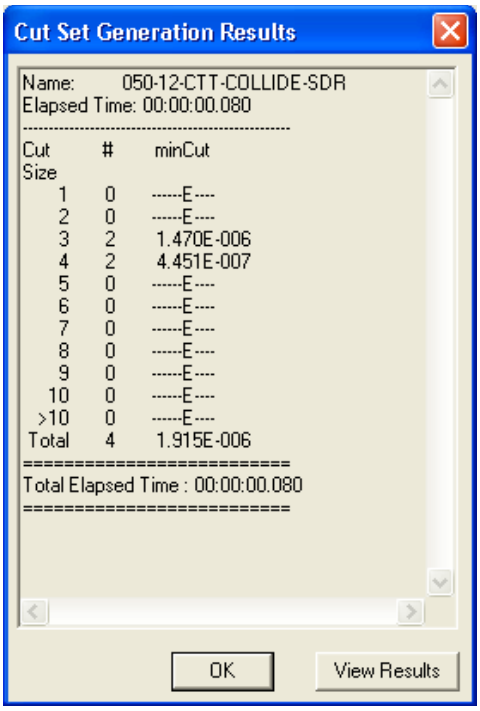
B3.4.3.6 Uncertainty and Cut Set Generation

Figure B3.4-7 contains the uncertainty results obtaining from running the fault tree "Collision of Shield Door into Conveyance" using a cutoff probability of 1E-15. Figure B3.4-8 provides the cut set generation results for the "Shield Door Closes on Conveyance" fault tree.



Source: Original

Figure B3.4-7. Uncertainty Results for the Shield Door Closes on Conveyance Fault Tree



Source: Original

Figure B3.4-8. Cut Set Generation Results for the Shield Door Closes on Conveyance Fault Tree

B3.4.3.7 Cut Sets

Table B3.4-6 contains the cut sets for “Shield Door Closes on Conveyance” fault tree.

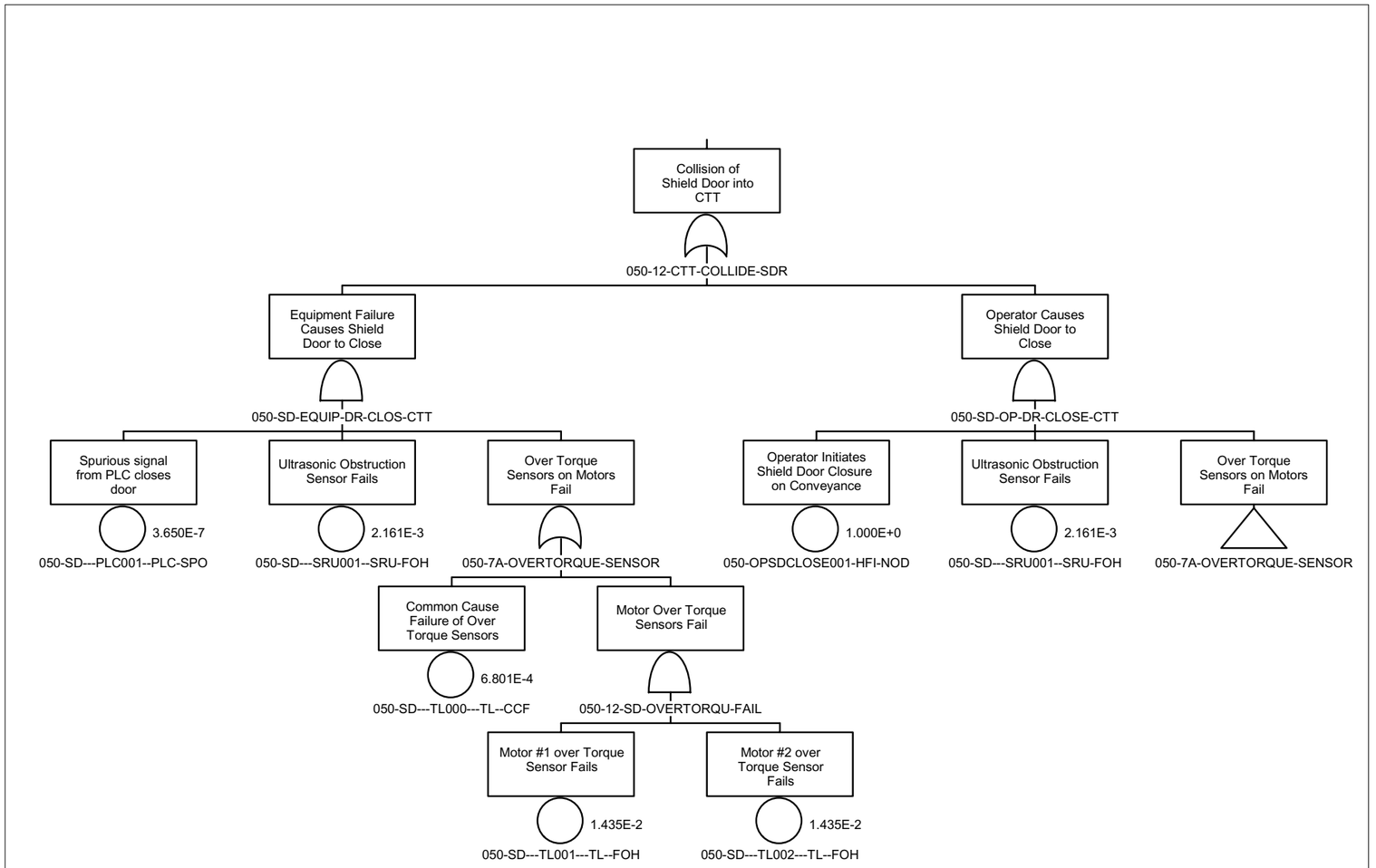
Table B3.4-6. Cut Sets for Shield Door Closes on Conveyance

Fault Tree	% Cut Set	Probability /Frequency	Basic Event	Description	Event Probability
050-12-CTT-COLLIDE-SDR	76.76	1.470E-006	050-OPSDCLOSE001-HFI-NOD	Operator Initiates Shield Door Closure on Conveyance	1.000E+000
			050-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.161E-003
			050-SD---TL000---TL--CCF	Common Cause Failure of Over Torque Sensors	6.801E-004
	23.24	4.451E-007	050-OPSDCLOSE001-HFI-NOD	Operator Initiates Shield Door Closure on Conveyance	1.000E+000
			050-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.161E-003
			050-SD---TL001---TL--FOH	Motor #1 over Torque Sensor Fails	1.435E-002
			050-SD---TL002---TL--FOH	Motor #2 over Torque Sensor Fails	1.435E-002
	0.00	5.365E-013	050-SD---PLC001--PLC-SPO	Spurious signal from PLC closes door	3.650E-007
			050-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.161E-003
			050-SD---TL000---TL--CCF	Common Cause Failure of Over Torque Sensors	6.801E-004
	0.00	1.625E-013	050-SD---PLC001--PLC-SPO	Spurious signal from PLC closes door	3.650E-007
			050-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.161E-003
			050-SD---TL001---TL--FOH	Motor #1 over Torque Sensor Fails	1.435E-002
			050-SD---TL002---TL--FOH	Motor #2 over Torque Sensor Fails	1.435E-002

NOTE: CTT = cask transfer trolley; Fail. = failure; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.3.8 Fault Trees



Source: Original

Figure B3.4-9. Fault Trees for Shield Door Closes on Conveyance

B4 WHF CANISTER TRANSFER MACHINE FAULT TREE ANALYSIS

B4.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designed categories described in Section 4.1, relative to suitability for intended use.

B4.1.1 ASME (American Society of Mechanical Engineers) NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2923-1.

B4.1.2 BSC (Bechtel SAIC Company) 2007. *CRCF, RF, WHF, and IHF Canister Transfer Machine Process and Instrumentation Diagram Sheet 1 of 4*. 000-M60-HTC0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071218.0028.

B4.1.3 BSC 2007. *CRCF, RF, WHF, and IHF Canister Transfer Machine Process and Instrumentation Diagram Sheet 2*. 000-M60-HTC0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071030.0022.

B4.1.4 BSC 2007. *CRCF, RF, WHF, and IHF CTM Canister Grapple Process and Instrumentation Diagram*. 000-M60-HTC0-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071011.0008.

B4.1.5 BSC 2007. *Nuclear Facilities Equipment Shield Door Process and Instrumentation Diagram*. 000-M60-H000-00101-000 REV 00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0024.

B4.1.6 BSC 2008. *CRCF, RF, WHF, and IHF Canister Transfer Machine Process and Instrumentation Diagram Sheet 3*. 000-M60-HTC0-00103-000 REV 00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080103.0011.

B4.1.7 BSC 2008. *Mechanical Handling Design Report – Canister Transfer Machine*. 000-30R-WHS0-01900-000 REV 002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0022.

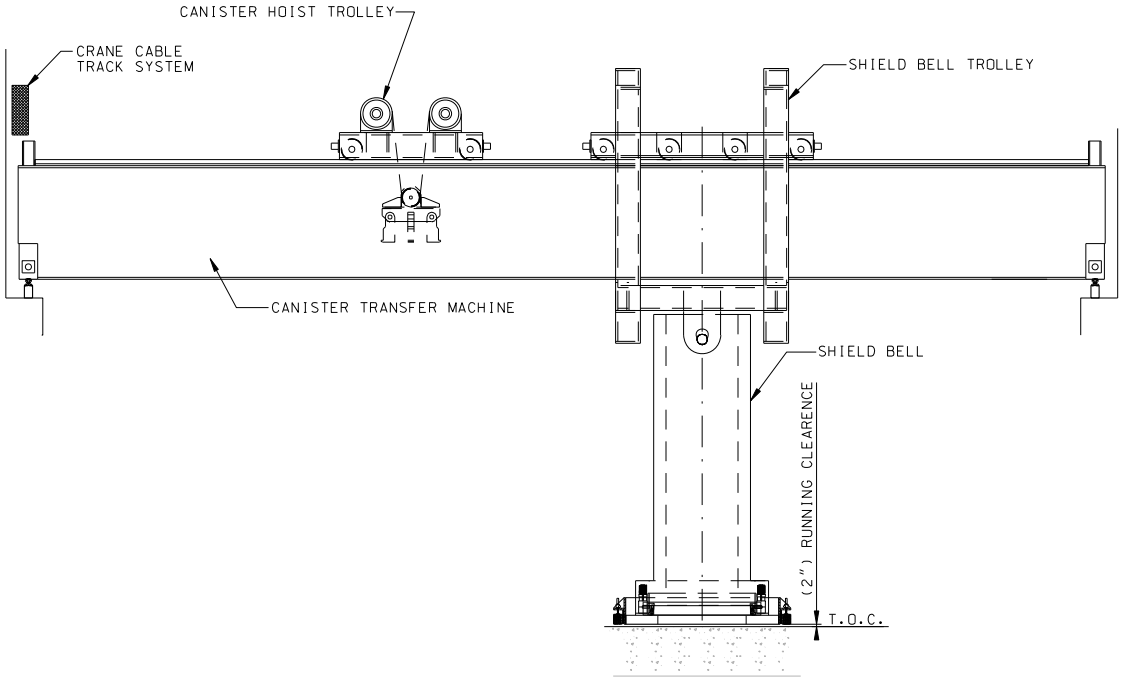
B4.1.8 BSC 2008. *Nuclear Facilities Slide Gate Process and Instrumentation Diagram*. 000-M60-H000-00201-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080123.0025.

B4.2 CANISTER TRANSFER MACHINE DESCRIPTION

B4.2.1 Overview

The CTM operates in the Canister Transfer Room of the WHF. Its function is to transfer waste canisters from a cask on a cask transfer trolley (CTT) or from an aging overpack on a site transporter to another cask or overpack. The ports in the floor of the transfer room provide access to the Cask Unloading Room and Cask Loading Room.

The CTM is an overhead bridge crane with two trolleys as shown in Figure B4.2-1. The first is a canister hoist trolley with a grapple attachment and hoisting capacity of 70 tons. The second is a shield bell trolley that supports the shield bell. The shield bell is approximately 25 feet tall with an inside diameter of about six feet. The bottom end of the shield bell is attached to a larger chamber to accommodate cask lids with a diameter of up to 84 inches. The CTM bottom plate assembly supports a 12-inch thick motorized slide gate. The slide gate, when closed, provides bottom shielding of the canister once the canister is inside the shield bell.



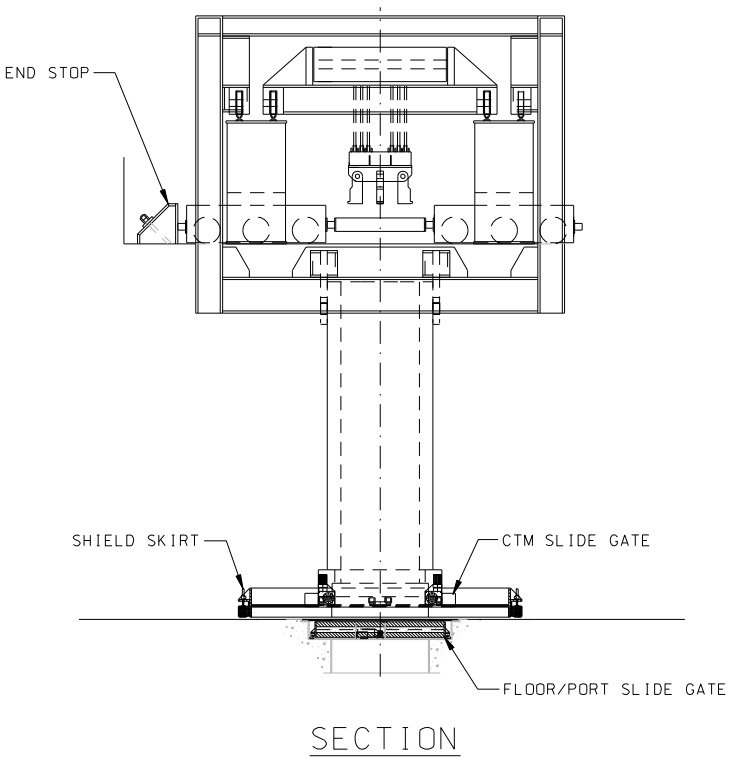
Source: Ref B4.1.7

Figure B4.2-1. Canister Transfer Machine Elevation

Around the perimeter of the bottom plate, a 9-inch thick shield skirt is provided which can be raised and lowered. The shield skirt is used to close any gap between the CTM bottom plate and floor surface to prevent lateral radiation shine during a canister transfer operation. The shield skirt, in its lowered position, is the only part of the CTM that touches the floor.

The CTM bridge is very similar to a typical crane bridge, with end trucks riding rails supported by wall corbels. Each bridge girder supports two sets of trolley rails; the two inner rails are for the canister hoist trolley and the two outer rails are for the shield bell trolley.

The CTM design allows for the two trolleys to move independently when required for maintenance but they are normally mechanically locked together and operate as a unit when performing a canister transfer operation. The hoist trolley with grapple is positioned over the shield bell and the grapple center is aligned with the shield bell center as depicted in Figure B4.2-2.



Source: Ref B4.1.7

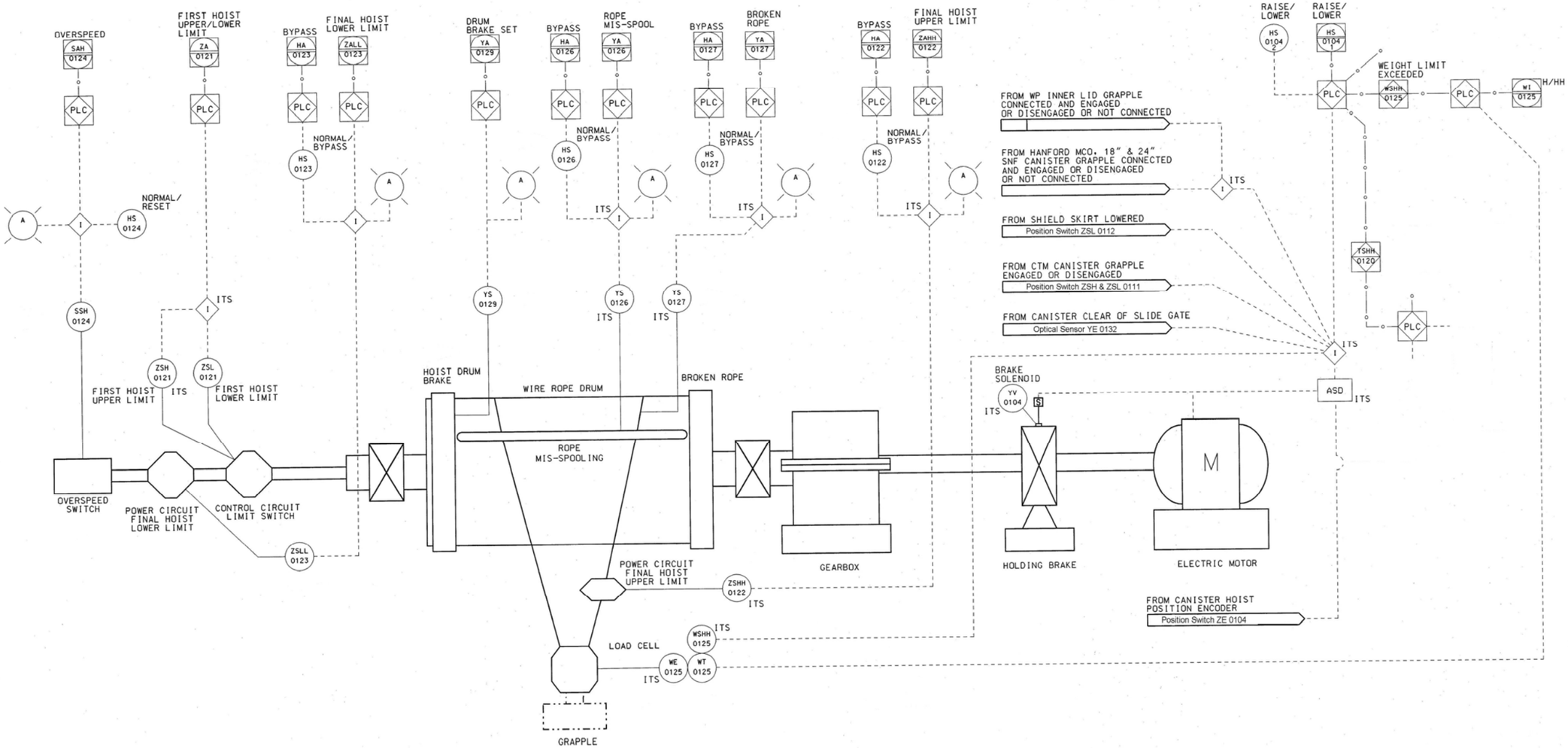
Figure B4.2-2. Canister Transfer Machine Cross Section

Figures B4.2-3 through B4.2-6 show the ITS related instrumentation and controls incorporated into the CTM (Ref. B4.1.2 Ref. B4.1.3, and Ref. B4.1.6) Additional interlocks between the CTM and other systems (e.g., shield doors) are shown and described in Ref. B4.1.4, Ref. B4.1.5, and Ref. B4.1.8. Hard-wired interlocks are provided to limit the possibility of operator error resulting in a CTM drop (of either a canister or any other object) or collision. While much of the operational control is provided by PLCs, the operation of these non-ITS devices is not credited in

the system analysis. However, spurious operation of the PLCs is considered when such operation may contribute to a drop or collision event. Hard-wired interlocks are provided to:

- Prevent bridge and trolley movement when the shield bell skirt is lowered
- Prevent raising the shield bell skirt when the slide gate is open
- Prevent hoist movement unless the grapple is fully engaged or disengage
- Stop the hoist and erase the lift command when a canister clears the shield bell slide gate
- Stop a lift before upper lift heights are reached (two interlocks are provided for this function)
- Prevent opening of the port slide gate unless the shield bell skirt is lowered and in position
- Prevent hoist movement unless the shield bell skirt is lowered
- Prevent lifting of a load beyond the operational load limit of the CTM (load cells).

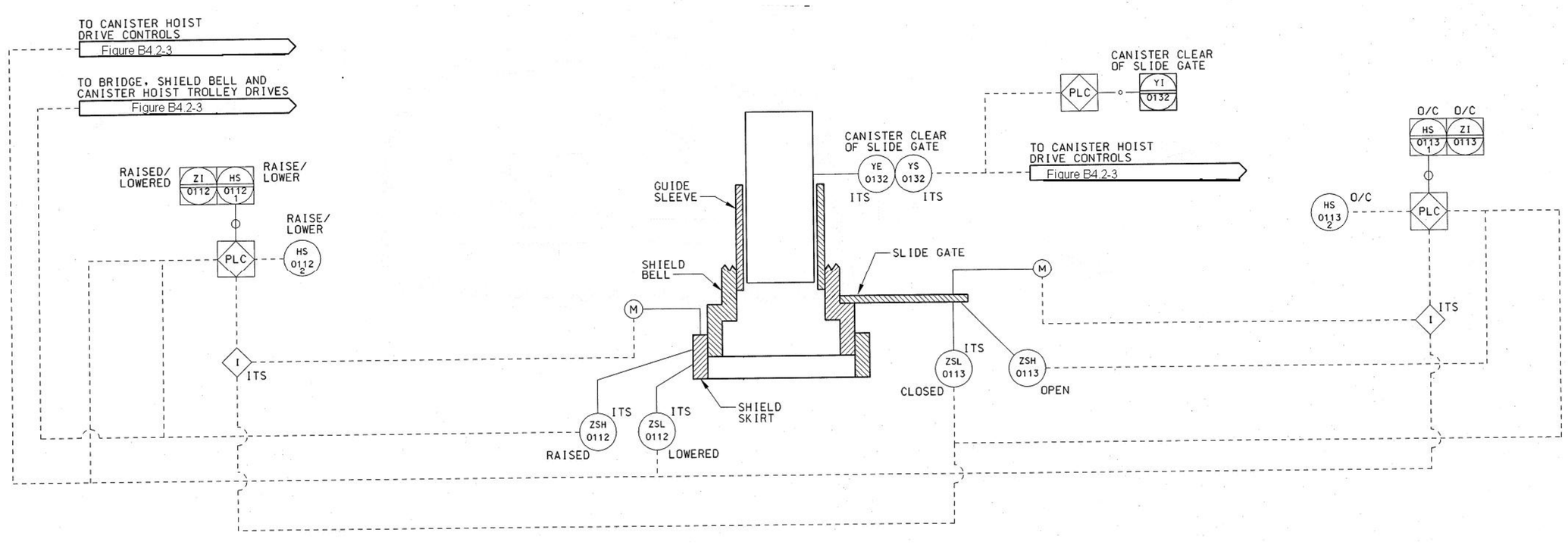
Some of these interlocks can be bypassed during maintenance. The most significant of these interlocks that can be bypassed is the interlock between the shield skirt position and the position of the slide gate (shield skirt cannot be raised unless the slide gate is closed or the bypass is engaged.) The design of the grapple interlock ensures that this interlock cannot be bypassed when the CTM is being used during operation.



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Ref. B4.1.6

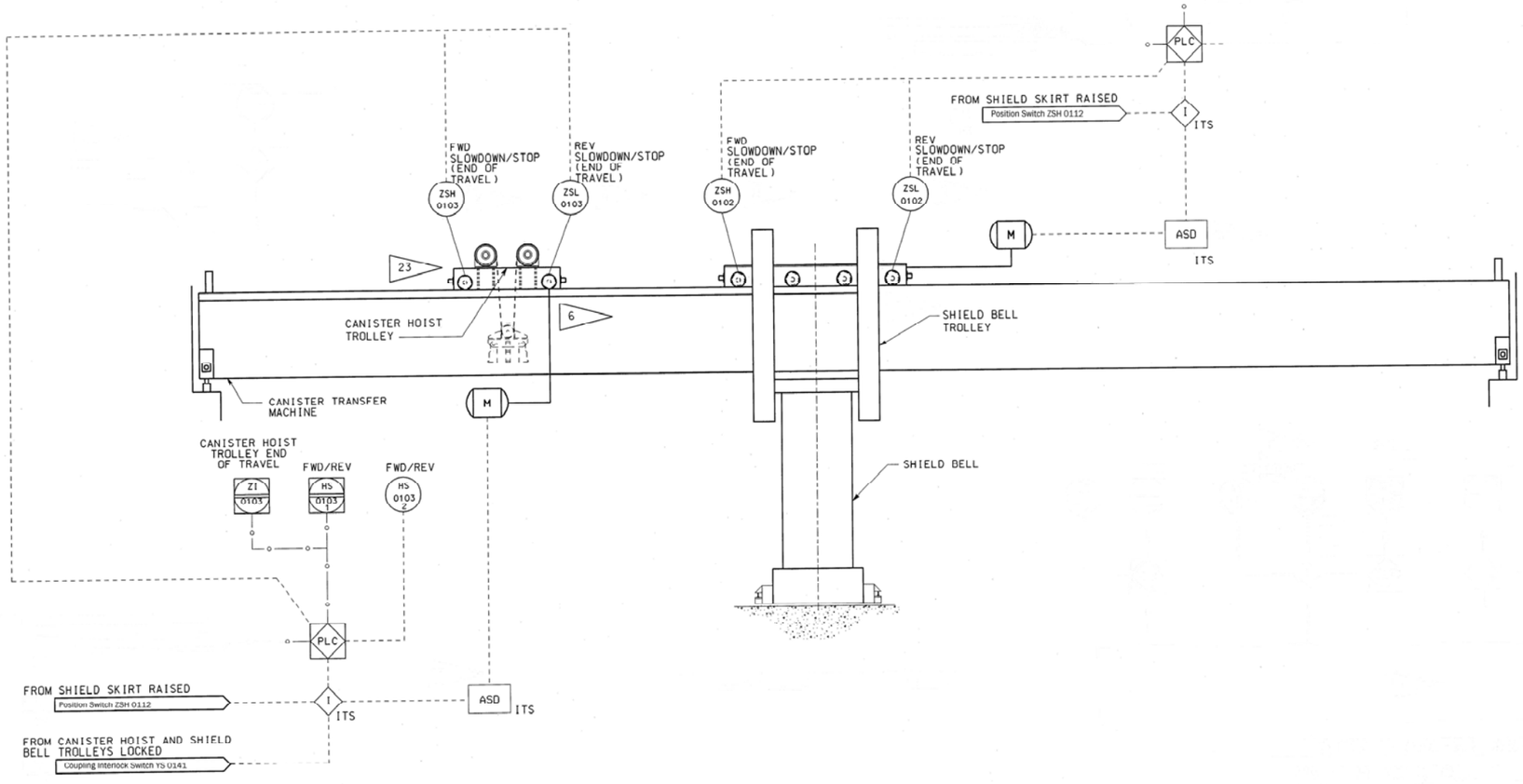
Figure B4.2-3. Canister Hoist Instrumentation



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Ref. B4.1.6

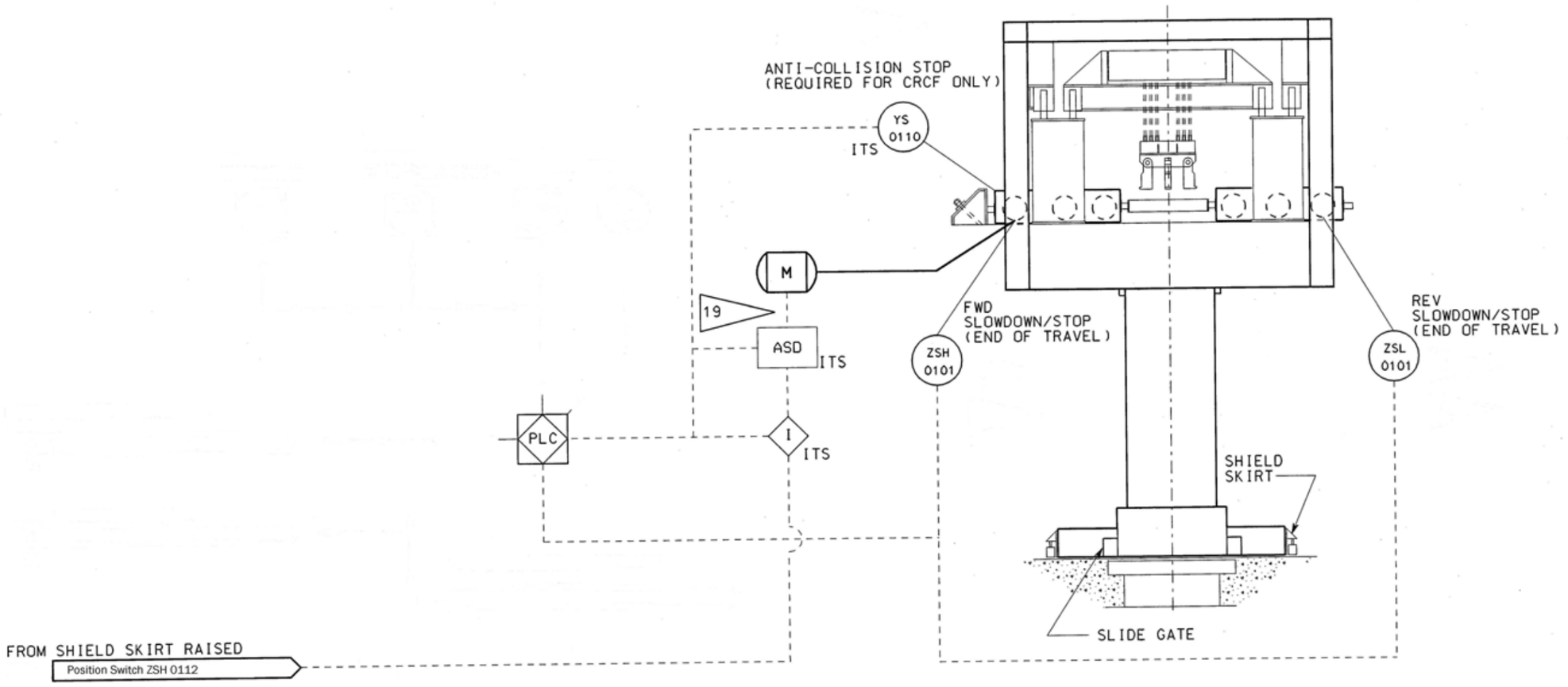
Figure B4.2-4. Shield Skirt and Slide Gate Instrumentation



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Ref. B4.1.3

Figure B4.2-5. Trolley Instrumentation



Source: Ref. B4.1.3

Figure B4.2-6. Bridge Instrumentation

B4.2.2 CTM Bridge

The bridge design meets the requirements of (Ref. B4.1.1) for a type I crane. The girder design resists the compression, bending, shear, torsion, and buckling loads induced by the fully-loaded trolley, crane dead weight, and impact loads due to seismic events. The end trucks are a box section and of high strength design, minimizing deflection, and constraining horizontal crane skewing. The flame hardened wheels are attached to the end truck using wheel bearing capsules. Four seismic restraints are provided to prevent excessive horizontal and vertical uplifts.

Hoist, trolley, and bridge drive gearing are enclosed in sealed gear boxes and lubricated with oil of a high flash point, which will not support a flame and fire.

The electric power to the bridge is provided by a crane cable track system along the runway length and supported by the facility wall as shown in Figure B4.2-1.

B4.2.3 Shield Bell Trolley

The shield bell trolley design meets the requirements of ASME NOG-1-2004, (Ref. B4.1.1) for a type I crane. During a seismic event, seismic restraints prevent the trolley from coming off the rails by limiting the amount of uplift. Electrical power to the trolley is provided through hard-wired connections using a cable track system.

B4.2.4 Canister Hoist Trolley

The hoist trolley design meets the requirements of ASME NOG-1-2004, (Ref. B4.1.1) for a type I crane and is also equipped with seismic restraints. The electrical power to the trolley is provided through hard-wired connections using a festoon system. The trolley incorporates a 70 ton hoist system that uses single-failure-proof technology. A canister grapple is supported by the lower block of the 70-ton hoist. The remotely operated grappling system utilizes limit switches to verify grapple engagement. The grapple utilizes a mechanism that includes a mechanical fail-safe drive that will not allow the grapple to disengage when a load is suspended from the canister grapple.

The hoist motor is designed to lift and lower the load at a nominal speed of 5 feet per minute. The hoist motor is controlled by an adjustable speed drive (ASD).

B4.2.5 ITS CTM Nominal Operations

The WHF canister transfer system handles dual-purpose canisters (DPCs) and transportation, aging, and disposal (TAD) canisters. A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to an aging overpack. For this operation a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. The cask lid is in place but unbolted. Similarly, an empty aging overpack is positioned under the adjacent transfer port.

The CTM is moved to a position over the center of the port above the loaded cask. The shield skirt is lowered to rest on the floor, and the port slide gate is opened. The CTM slide gate is opened and the canister grapple is lowered through the shield bell. The grapple engages a lift

fixture on the cask lid. The cask lid is raised into the larger chamber of the CTM. The port slide gate is closed and the shield skirt is raised. The CTM is moved to a cask lid staging area, which is a recess in the floor of the transfer room. The cask lid is lowered and placed in the staging area and the grapple is raised.

The CTM is moved over the port above the loaded cask, the CTM grapple is positioned and aligned for the canister pickup, and the shield skirt is lowered. The port slide gate is opened and the grapple is lowered to engage the canister lifting feature. The canister is raised into the shield bell and the hoist stops when a sensor detects that the bottom of the canister has cleared the CTM slide gate. The CTM slide gate and the port slide gate are closed, and the shield skirt is raised.

The CTM is moved to the port above the empty aging overpack and positioned for canister loading. The shield skirt is lowered and the port slide gate and CTM slide gate are opened. The canister is lowered and placed into the aging overpack and the grapple is disengaged from the canister.

The CTM canister grapple is used for handling large diameter canisters such as TAD canisters and DPCs. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the transfer room floor. The CTM hoist is lowered through the shield bell until the CTM grapple is accessible in the room below for canister grapple attachment.

The CTM is normally controlled from the facility operations room, but a local control station is also provided.

B4.2.6 ITS CTM Off Nominal Operations

Generally, under off normal conditions the CTM is not in operation. Following a loss of AC offsite power, all power to the CTM motors (hoist, bridge, trolley, and bell trolley) is lost. If a transfer is underway when power is lost, all of the CTM motors would stop and the hoist holding brake engages. Operations would be suspended until power is restored and the load can be safely moved. Under other off normal conditions, transfer operations would be suspended and the CTM would remain idle.

B4.2.7 ITS CTM Testing and Maintenance

The CTM is operated, if not on a continual basis, regularly (e.g., once a shift). Most component functionality will be verified during CTM operation. For those components that are not exercised during routine operations (e.g., bridge and trolley end-of-travel endstops, hoist upper limit position switches) routine verification of functionality will be required.

B4.2.8 Testing and Maintenance

Requirements

Testing of components not exercised during routine operation of the CTM is tested annually at a minimum.

Feature

Normal maintenance is performed in accordance with manufacture's recommendations; maintenance is performed only when the CTM is not in use.

B4.2.9 Fault Trees

Requirements

The fault tree model for the CTM only includes those components that have been declared as ITS. There is an exception: the spurious operation of PLCs is included in the fault tree model. Spurious operation can result in inadvertent CTM movements.

The mission time for the ITS CTM is set to 1 hour. Most lifts/transfers will require less than one hour. When a transfer consists of several separate activities (e.g., auxiliary equipment movements, lifts, transfers, etc.) each of these activities require less than an hour, but all have been assigned a one-hour mission time.

Features

Common-cause failures have been included for four events. Three are associated with position indication sensors: the two upper limit switches on the CTM hoist used to prevent raising a load too high (a two blocking event), the grapple engage/disengage position indication sensors, and the port gate position sensors (two gates, one sensor for each gate). Common-cause failure of the hoist cables is also considered.

Seven human error conditions are incorporated into the model. These are for drops initiated by operator actions, inadvertent crane movements resulting in impacts, and a failure to restore interlocks allowing movement of the crane when the shield skirt is raised and the slide gates are open.

B4.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B4.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B4.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
ASDs	Position sensors	—	—	—	—
	CTM hoist, bridge, and trolley motors control	—	—	—	—
CTM Bridge	—	—	CTM bridge	—	—
CTM Motors	ASDs, non-ITS power	—	—	Operational control	Off-site power
Port/Slide Gate Position Switches	ASDs	—	—	—	—
Grapple Position (Engaged /Disengaged)	ASDs	—	—	—	—
Shied Skirt Position	ASDs	—	—	—	—
Non ITS Power	CTM motors	—	—	—	—
Obstruction sensor	Hoist motor ASD	—	—	—	—

NOTE: ASD = adjustable speed drive; CTM = canister transfer machine; ITS = important to safety;

Source Original

B4.4 CTM RELATED FAILURE SCENARIOS

The CTM has five credible failure scenarios:

1. The CTM drops a canister from a height below the design basis height for canister damage (this includes canister drops within the shield bell once the bell slide gate has been closed and drops through the canister transfer room ports to the loading/unloading areas that can occur before the bell slide gate is closed).

2. The CTM drops a canister from a height above the design basis height for canister damage.

3. The CTM drops an object onto a canister.

4. Canister impact. A collision between the canister and the shield bell or Canister Transfer Area floor from any cause during the lift, lateral movement, and lower portions of the canister transfer

5. CTM movement subjects canister to shearing forces. The CTM, while carrying a canister, moves in such a manner (e.g., spurious movements, exceeding bridge or trolley end of travel limits) as to cause an impact of the canister with the shield bell.

B4.4.1 Canister Drops from Below the Canister Design-Limit Drop Height

B4.4.1.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of the canisters. These drops have been divided into two classes: drops from heights below the design basis drop height of the canister and drops from heights above the design basis drop height of the canister. The fault tree for canister drops addresses the first of these two scenarios.

B4.4.1.2 Success Criteria

Success criteria for the CTM is the prevention of a canister drop from any cause, during the lift, lateral movement, and lowering portions of the canister transfer.

B4.4.1.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.

- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.

- An interlock between the slide gate and shield skirt–the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed, to allow the CTM to move with the slide gate open during lid removal.

- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end-of-travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.1.4 Fault Tree Model

The top event in this fault tree is "CTM Drop All Heights." This is defined as a drop of a canister during transfer operations. Faults considered in the evaluation of this top event include: human events that contribute to a drop (considered in conjunction with the interlocks intended to prevent the erroneous human action) and mechanical (structural) failures of the CTM components. The interlocks and safety features (position controls, load cells, and drum and holding brakes) intended to either prevent CTM failure or given failure of the CTM to prevent a load drop are included in the model.

Structural failures of components including the hoist cables, sheaves, drum, and grapples can result in canister drops. Operator events are addressed for actions including improper grapple connections, misalignments of the hoist and the canister, improper hoist activities and improper lateral movement of the CTM. Protection from these actions are provided by hard-wired interlocks keyed to the position of the CTM (both hoist position and CTM lateral position), slide and port gate doors, and the shield bell skirt. Also considered in the analysis is a canister drop initiated by improper operation of the shield bell slide gates and the port slide gates. While the gate motors are sized to prevent damage to the canister in the event of an inadvertent closure of the gates, the possibility that the gates would close above the canister during a lift blocking the lift and causing a canister drop was considered.

Failures specifically considered are:

- Electro-mechanical failures that occur as a result of the random catastrophic failure of hoisting components, such as the grapple of the CTM, or the redundant wire ropes failing independently or by common-cause.

- Electro-mechanical failures that occur as a result of the conveyance, from which the canister is being extracted, moving spuriously during the transfer. In response, a misalignment can develop that may result in the canister getting caught on the edge of the shield bell; tension can develop in the wire ropes, conceivably leading to their failure. A load control safety system is capable of detecting such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister.

- Electro-mechanical failures that occur as a result of a slide gate spuriously closing during transfer of a canister. There are two types of slide gates: one that closes the port between the lower and the upper floor in the Canister Transfer Machine Room and another that closes the bottom part of the shield transfer bell. When the canister is lifted from its container, a spurious slide gate closure can result in the canister getting caught up against the gate; tension can develop in the wire ropes, conceivably leading to their failure. The load control safety system detects such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister.

- Electro-mechanical failures that occur as a result of a spurious movement of the CTM. The CTM has several trolleys that govern lateral movements; one controls the CTM bridge movement, one controls the movement of the shield bell, while another one controls the movement of the load being transferred inside the shield bell (these last two are physically interlocked during canister transfer operations). Spurious actuation of a trolley motor after the grapple has been attached to the canister but before the canister is raised above the Canister Transfer Area floor can result in tension developing in the wire ropes, conceivably leading to their failure. Because the load control safety system does not control lateral movements of the CTM, it is not capable of stopping operations in this case.

- Human related actions associated with the operator inappropriately closing a slide gate during vertical canister movement. As for the spurious electro-mechanical slide gate closure discussed previously, tension in the wire ropes can develop as a result of this event, conceivably leading to their failure. The load control safety system detects such abnormal tension and reacts by stopping the transfer operations and applying brakes to retain the canister in a safe position. Failure of this system is considered to cause the drop of the canister. The human error probability assigned to this HFE is a screening value of 0.001 (i.e., it is a conservative estimate based upon predetermined characteristics of the human failure event (HFE) (Table 6.4-1)).

- Human related actions associated with the operator causing a drop of a canister, from a low height, during its extraction from its container. The human error probability for this event required a detailed analysis, entailing an examination of human failure scenarios that account for interactions and error-forcing context resulting from the combination of equipment conditions and human factor. The result of this analysis was condensed into a single basic event whose probability embeds the combination of both human and equipment failures necessary to cause a drop, which explains its relatively low value (5×10^{-7}) (Table 6.4-1).

B4.4.1.5 Basic Event Data

Table B4.4-1 contains a list of basic events used in the CTM fault trees. Included are the HFEs and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The canister drop probability modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are put into operation. They are consequently evaluated over the interval of time between their actuation which is considered to be the duration of a shift (i.e., eight hours). In another example, brakes are analyzed over a mission time of twenty-four hours. This duration is deemed to encompass the time required to revert to normal transfer operations after a malfunction that would have caused a safety system of the CTM to cease transfer activities.

Table B4.4-1. Basic Event Probability for the CTM Canister Drop from Below Canister Drop Height Limit Fault Tree

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM--CBL0001-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0002-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	1	9.400E-08	9.400E-08	0.000E+00	0.000E+00
050-CTM--DRTRN-CT--FOD	Controller Failure	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	1	4.000E-08	4.000E-08	0.000E+00	1.000E+00
050-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	0.000E+00	1.000E+00
050-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure	3	2.011E-04	0.000E+00	8.380E-06	2.400E+01
050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	3	6.500E-06	0.000E+00	6.500E-06	1.000E+00
050-CTM--HOLDBRK-BRK-FOD	CTM Holding Brake Failure on Demand	1	1.460E-06	1.460E-06	0.000E+00	1.000E+00
050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3	3.520E-05	0.000E+00	4.400E-06	8.000E+00
050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	1	2.750E-05	2.750E-05	0.000E+00	1.000E+00
050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--OVERSP--ZS--FOD	CTM Hoist motor speed Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--PORTGT1-PLC-SPO	Port Gage 1 PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--PORTGT2-PLC-SPO	Port Gage 2 PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--SLIDGT2-IEL-FOD	CTM Slide Gate Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CTM--TROLLY-MOE-SPO	Motor (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	0.000E+00	1.000E+00
050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00

Table B4.4-1. Basic Event Probability for the CTM Canister Drop from Below Canister Drop Height Limit Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
050-CTM--YS01129-ZS--FOD	CTM Drum Brake Control Circuit Switch Fail	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	1.000E+00
050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-MISSPOOL--DM-MSP	CTM mis-spool event	3	6.860E-07	0.000E+00	6.860E-07	0.000E+00
050-CTM-PLC0101--PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM-PLC0102--PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM-PLC0103--PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	0.000E+00	1.000E+00
050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	1	5.000E-07	5.000E-07	0.000E+00	0.000E+00
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM--CBL0001-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0002-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	1	9.400E-08	9.400E-08	0.000E+00	0.000E+00
050-CTM--DRTRN-CT--FOD	Controller Failure	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

B4.4.1.5.1 Human Failure Events

Two basic events are associated with human error (Table B4.4-2). These are for drops initiated by operator actions and for operator action to close the shield or slide gate doors while a CTM lift is being performed.

Table B4.4-2. Human Failure Events

Name	Description
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close
050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit

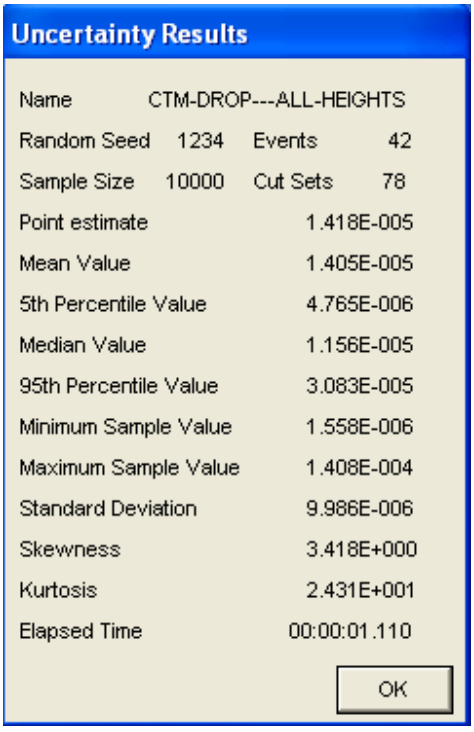
Source: Original

B4.4.1.5.2 Common-Cause Failures

One common-cause failure (CCF) event is considered in the evaluation of this top event. It is the common-cause failure of the hoist cables. An alpha factor of 0.047 was used to determine the CCF value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

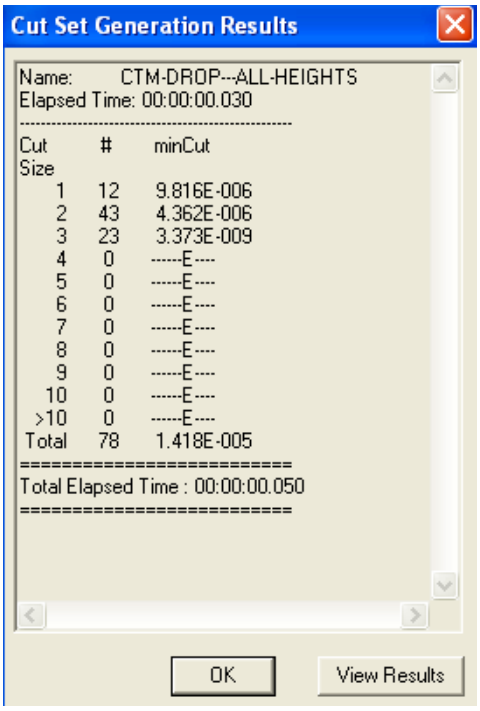
B4.4.1.6 Uncertainty and Cut Set Generation

Figure B4.4-1 contains the uncertainty results obtaining from running the fault trees for the CTM canister drop using a cutoff at 1E-15. Figure B4.4-2 provides the cut set generation results for the CTM canister drop fault tree.



Source: Original

Figure B4.4-1. Uncertainty Results of the CTM Canister Drop Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the CTM Canister Drop Fault Tree

B4.4.1.7 Cut Sets

Table B4.4-3 contains the top 20 cut sets for the CTM Canister Drop Fault Tree.

Table B4.4-3. Dominant Cut Sets for the CTM Canister Drop

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
28.13	28.13	3.990E-06	050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
37.16	9.03	1.280E-06	050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
46.19	9.03	1.280E-06	050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
54.30	8.11	1.150E-06	050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1.150E-06
62.41	8.11	1.150E-06	050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1.150E-06
70.52	8.11	1.150E-06	050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1.150E-06
78.63	8.11	1.150E-06	050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1.150E-06

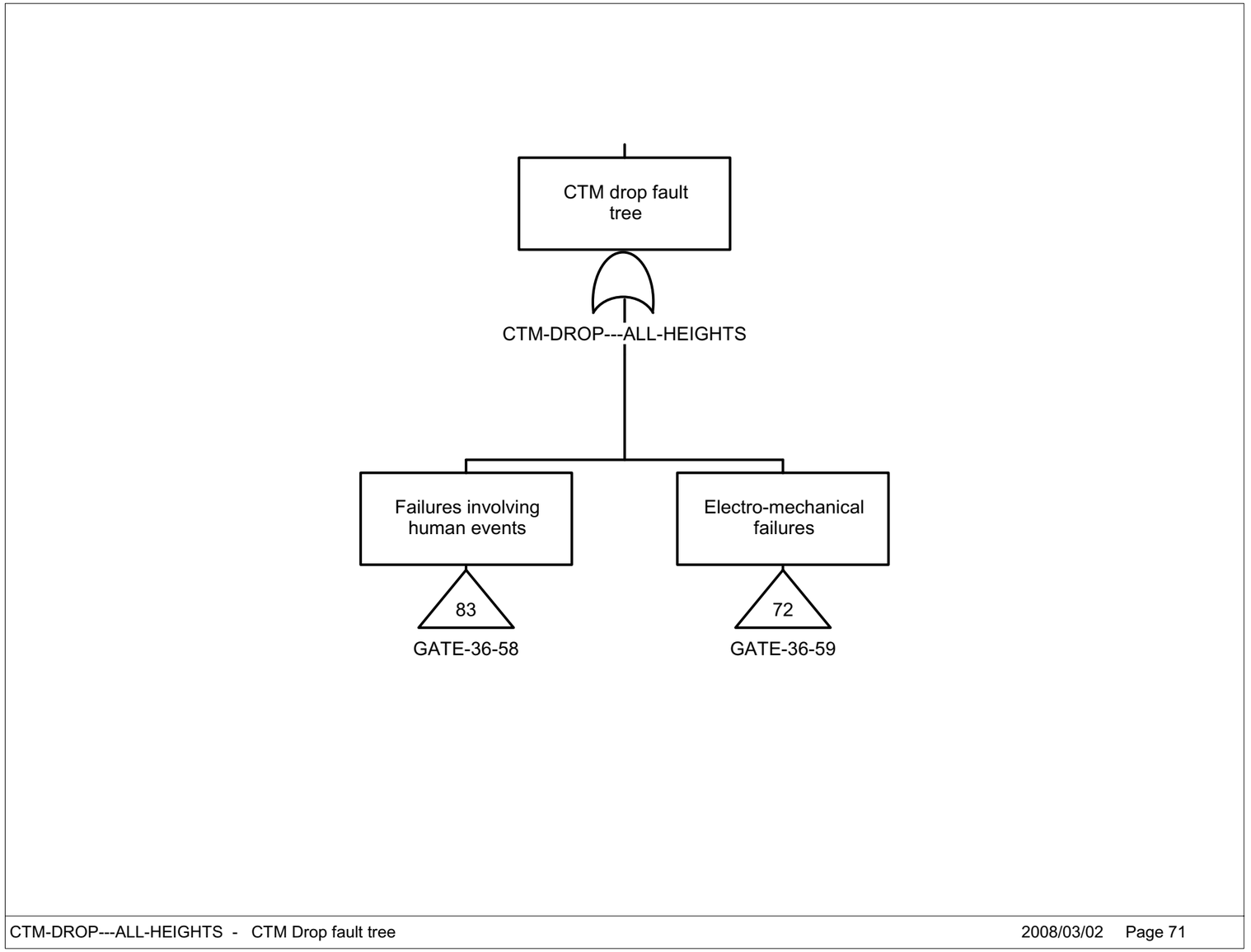
Table B4.4-3. Dominant Cut Sets for the CTM Canister Drop (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
83.38	4.75	6.740E-07	050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	6.740E-07
88.13	4.75	6.740E-07	050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	6.740E-07
92.88	4.75	6.740E-07	050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	6.740E-07
96.41	3.53	5.000E-07	050-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	5.000E-07
98.48	2.07	2.930E-07	050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	2.930E-04
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.14	0.66	9.400E-08	050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.400E-08
99.42	0.28	4.000E-08	050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	4.000E-08
99.67	0.25	3.520E-08	050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3.520E-05
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.86	0.19	2.750E-08	050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	2.750E-05
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03
99.88	0.02	2.689E-09	050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.90	0.02	2.689E-09	050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.92	0.02	2.689E-09	050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
99.94	0.02	2.689E-09	050-CTM--TROLLY-MOE-SPO	Motor (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
28.13	28.13	3.990E-06	050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
			050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1.000E-03

NOTE: ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine.

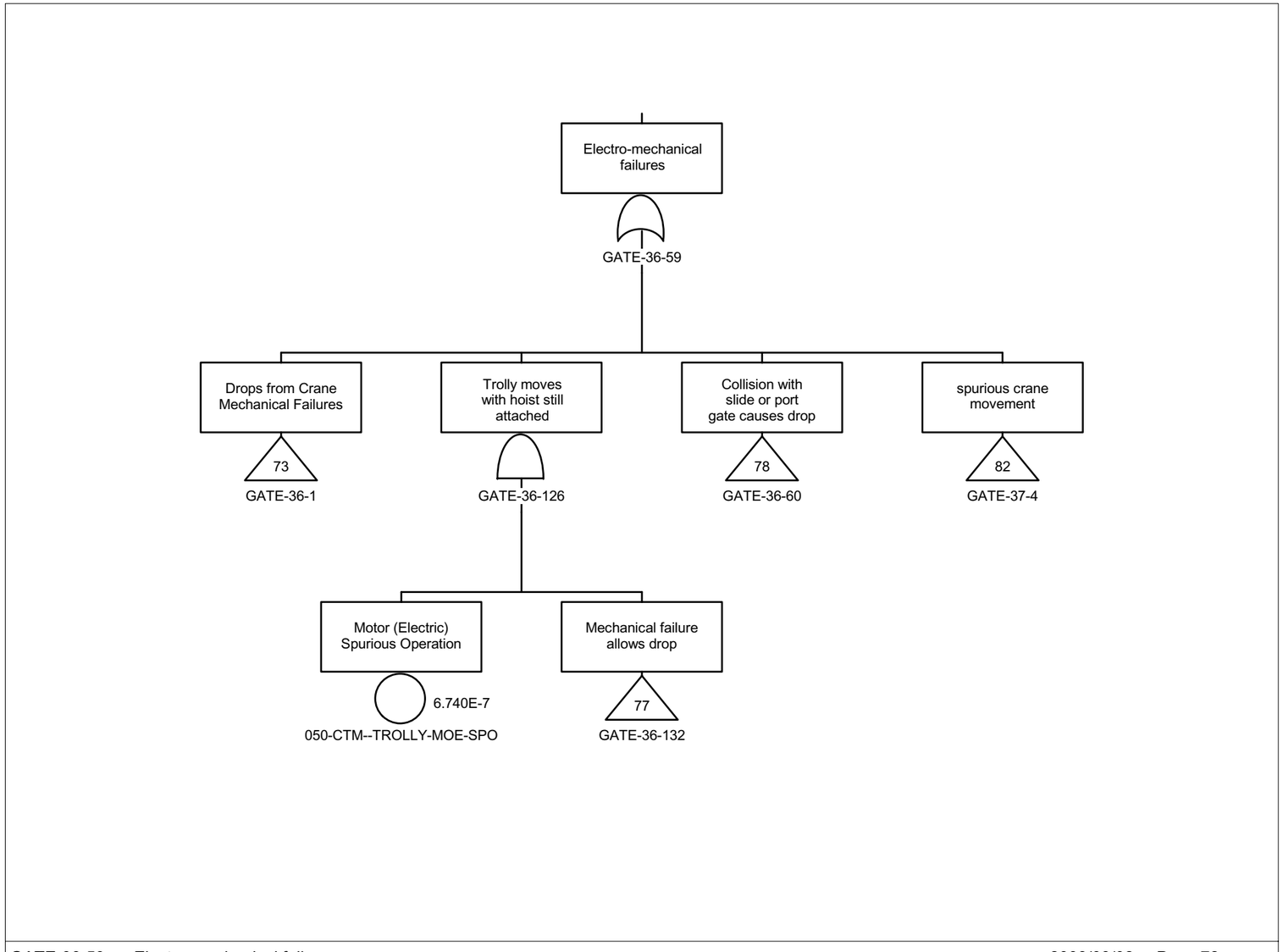
Source: Original

B4.4.1.8 Fault Trees



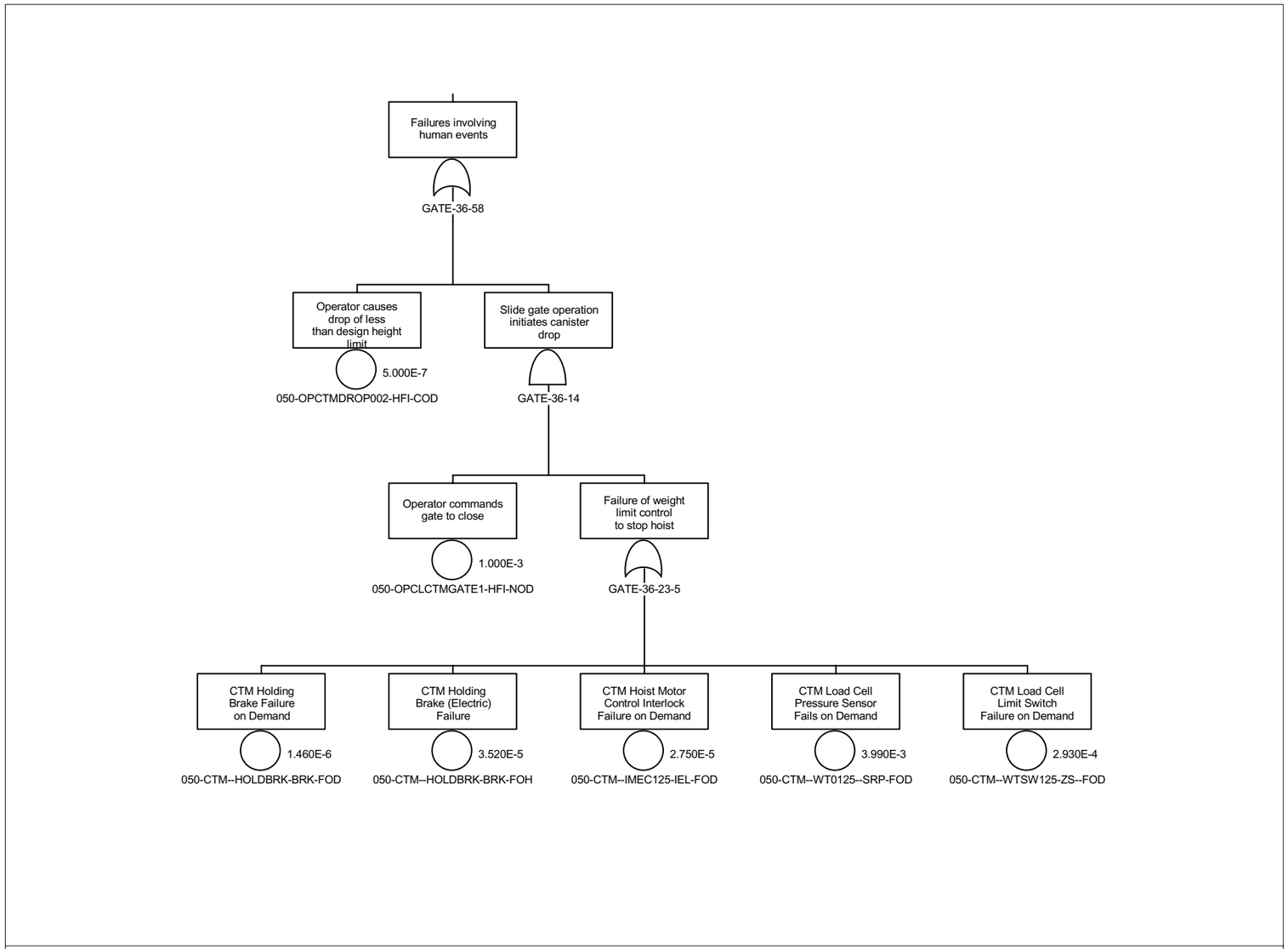
Source: Original

Figure B4.4-3. CTM Drop Fault Tree Sheet 1



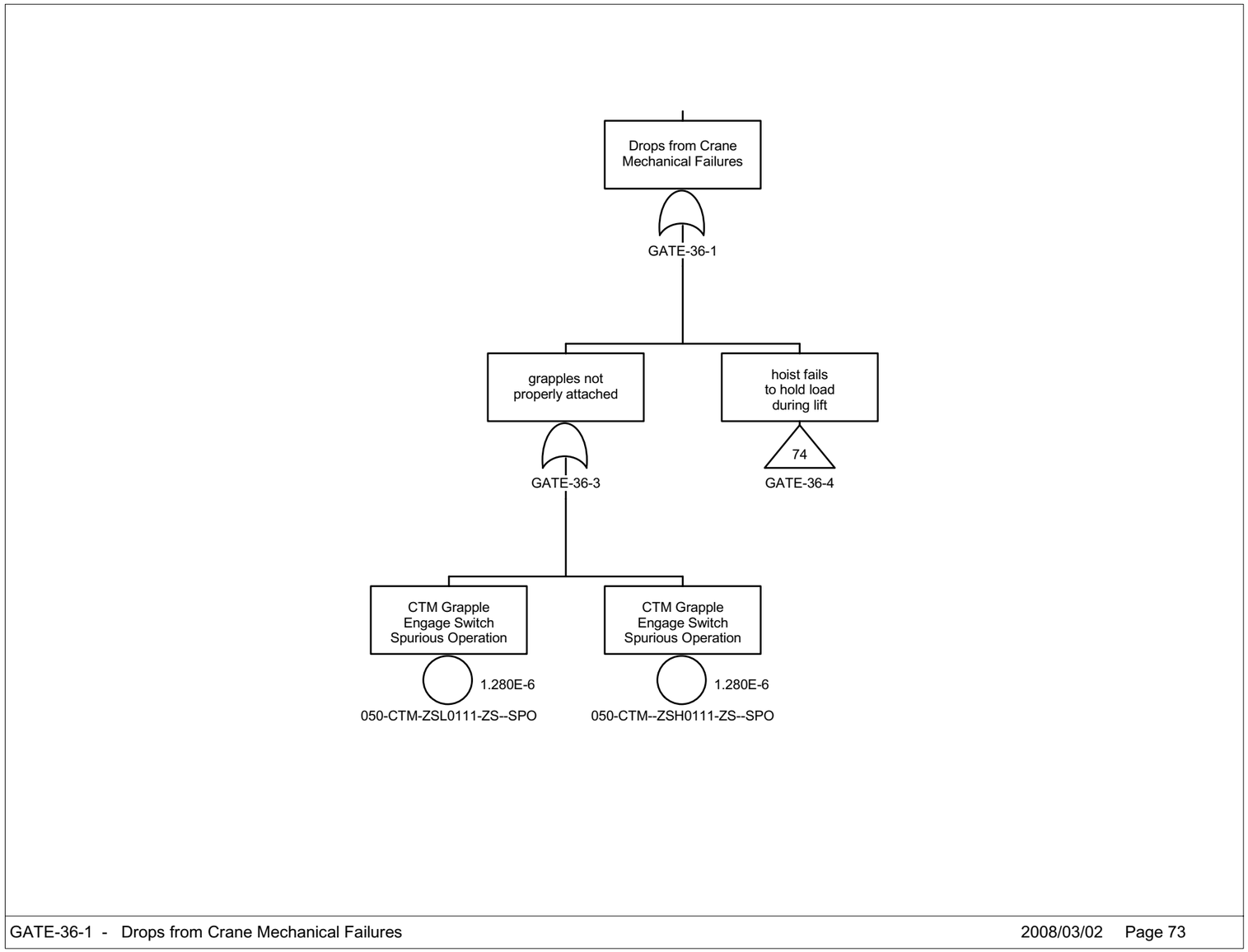
Source: Original

Figure B4.4-4. CTM Drop Fault Tree Sheet 2



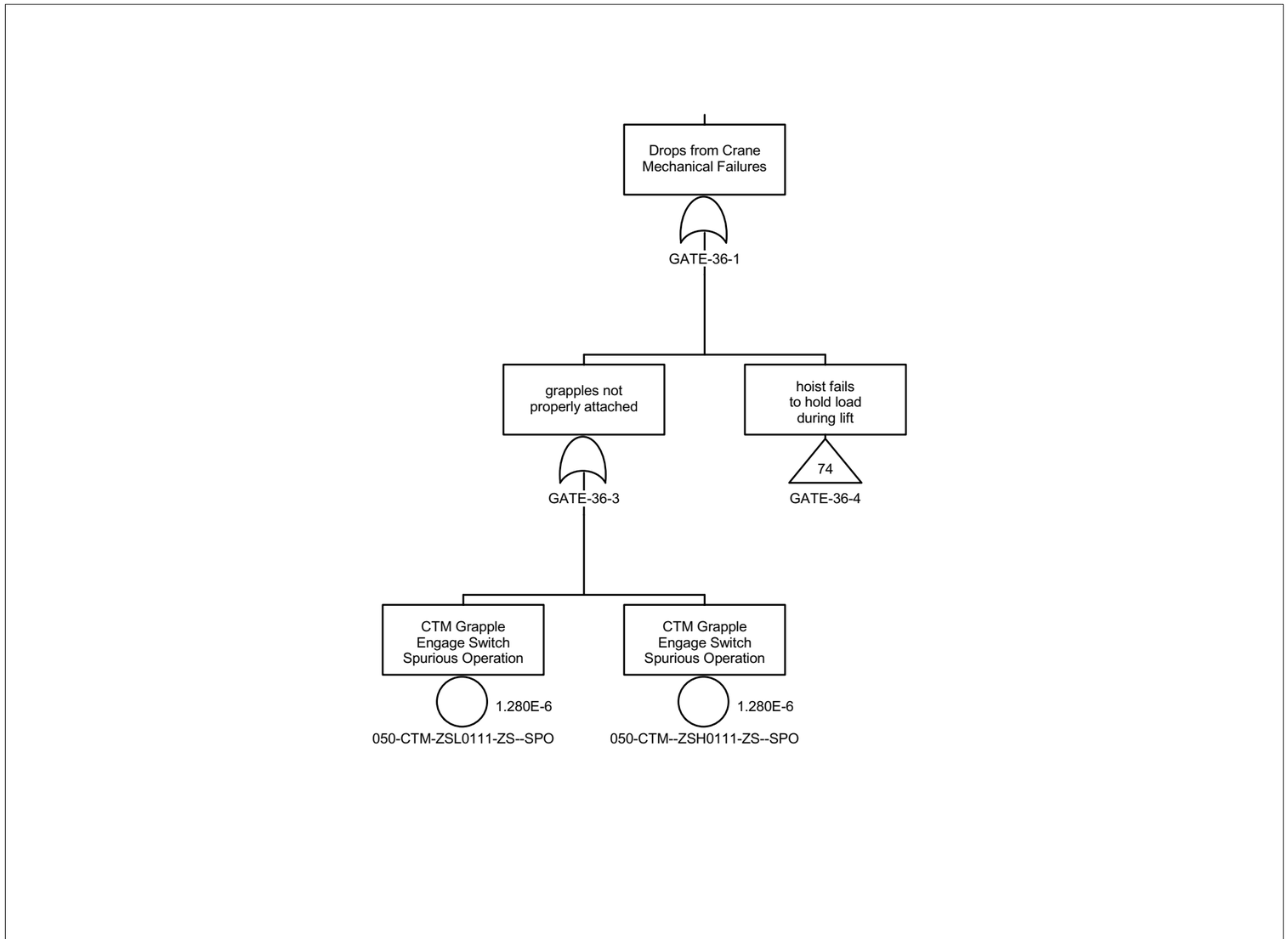
Source: Original

Figure B4.4-5. CTM Drop Fault Tree Sheet 3



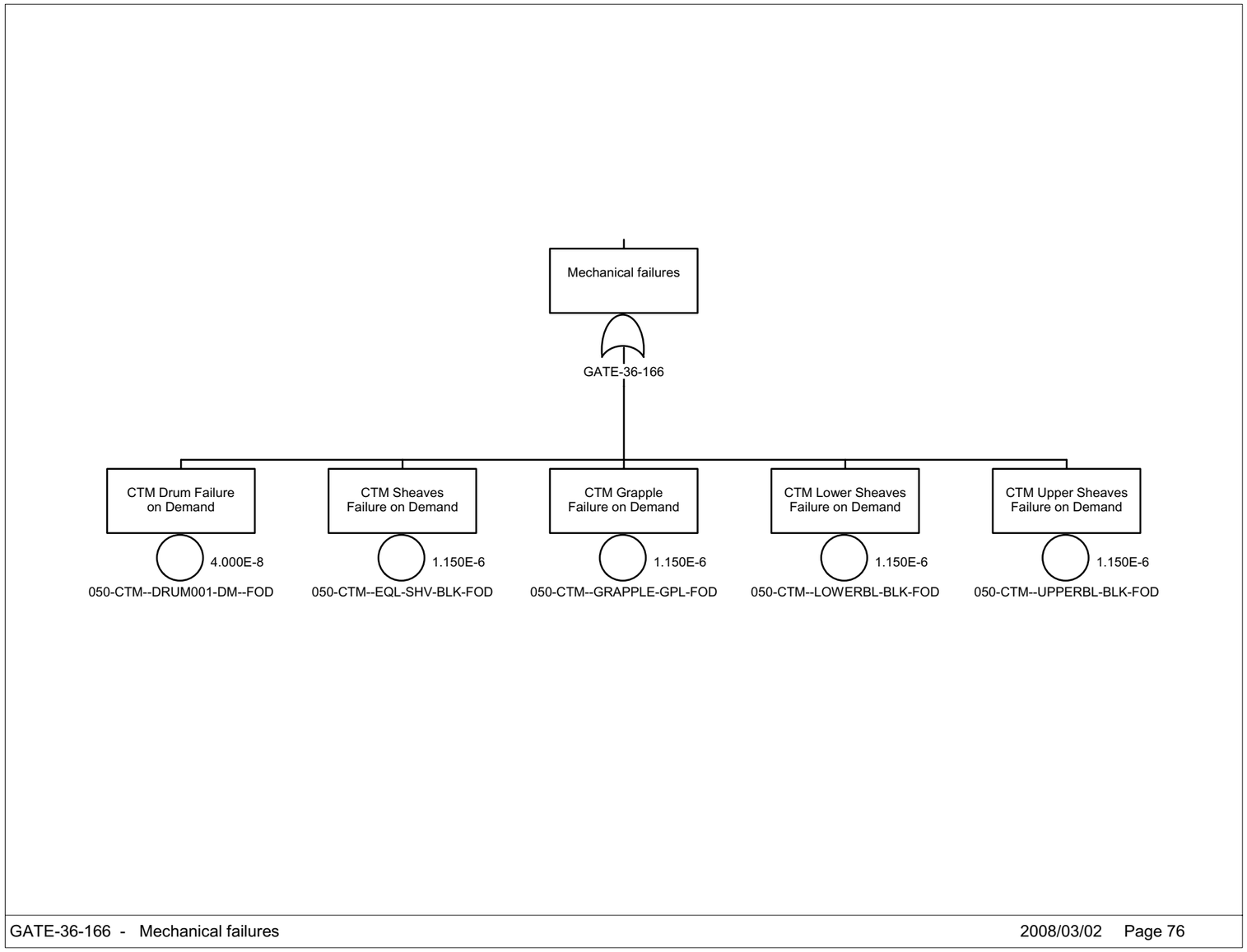
Source: Original

Figure B4.4-6. CTM Drop Fault Tree Sheet 4



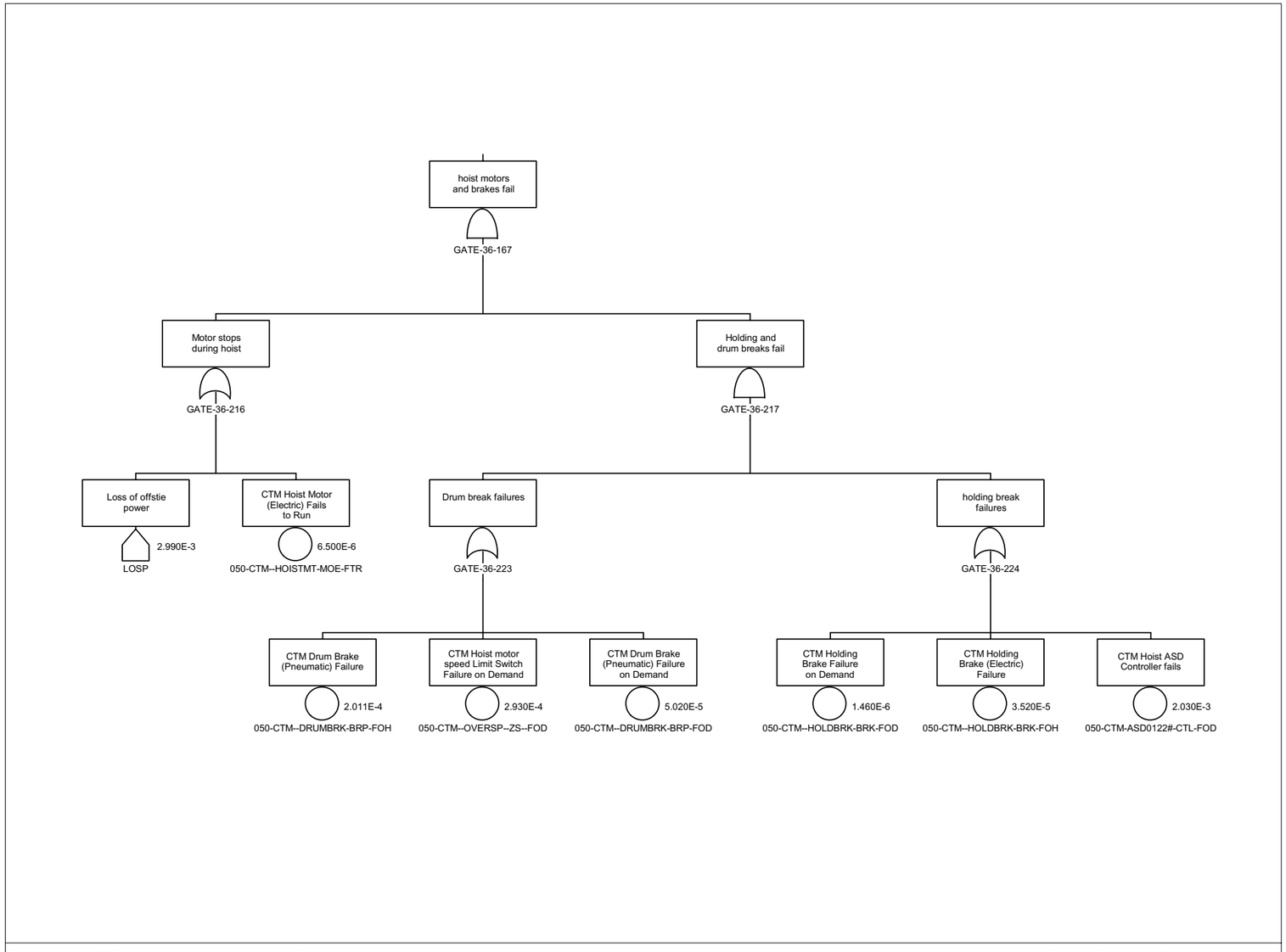
Source: Original

Figure B4.4-7. CTM Drop Fault Tree Sheet 5



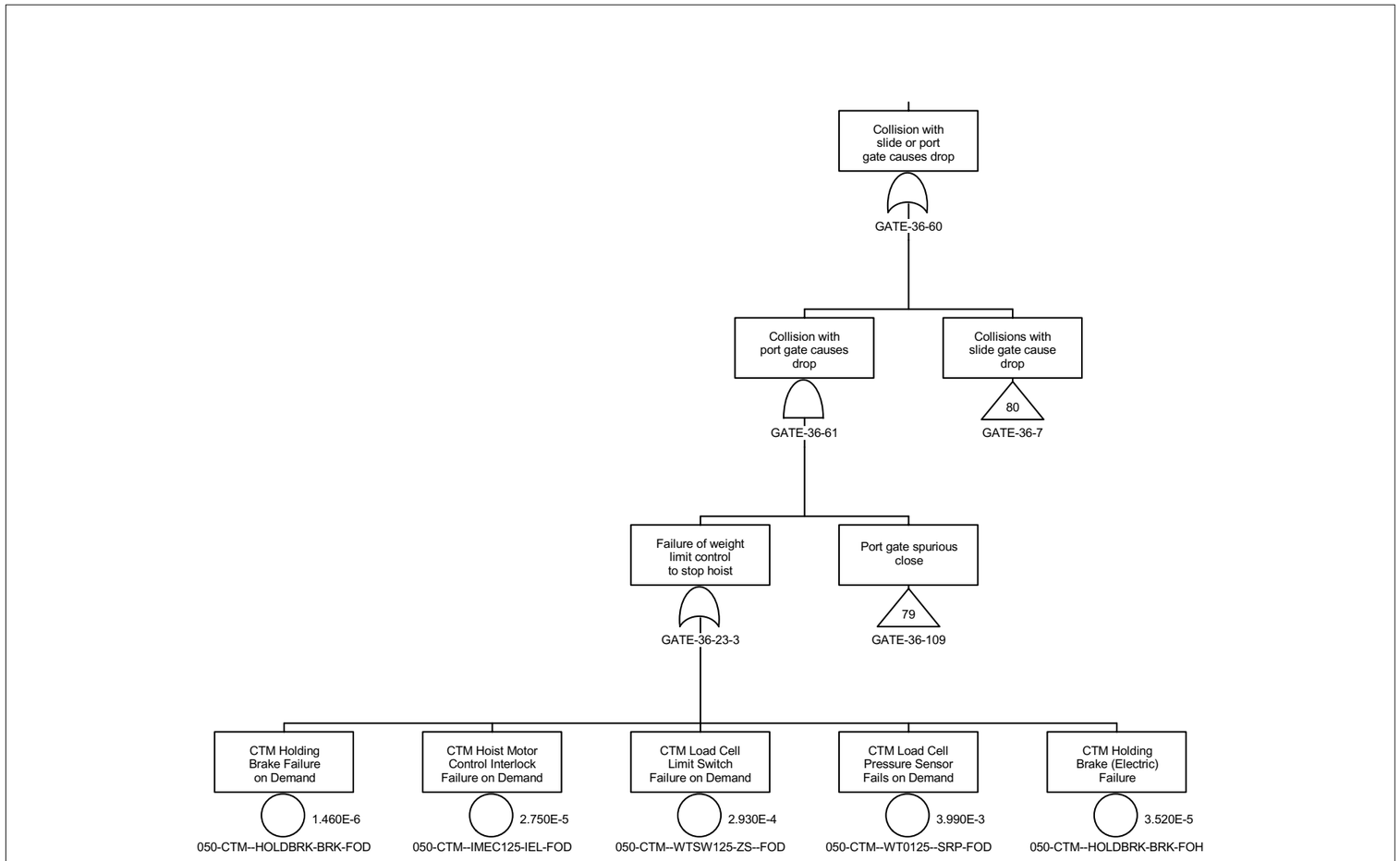
Source: Original

Figure B4.4-8. CTM Drop Fault Tree Sheet 6



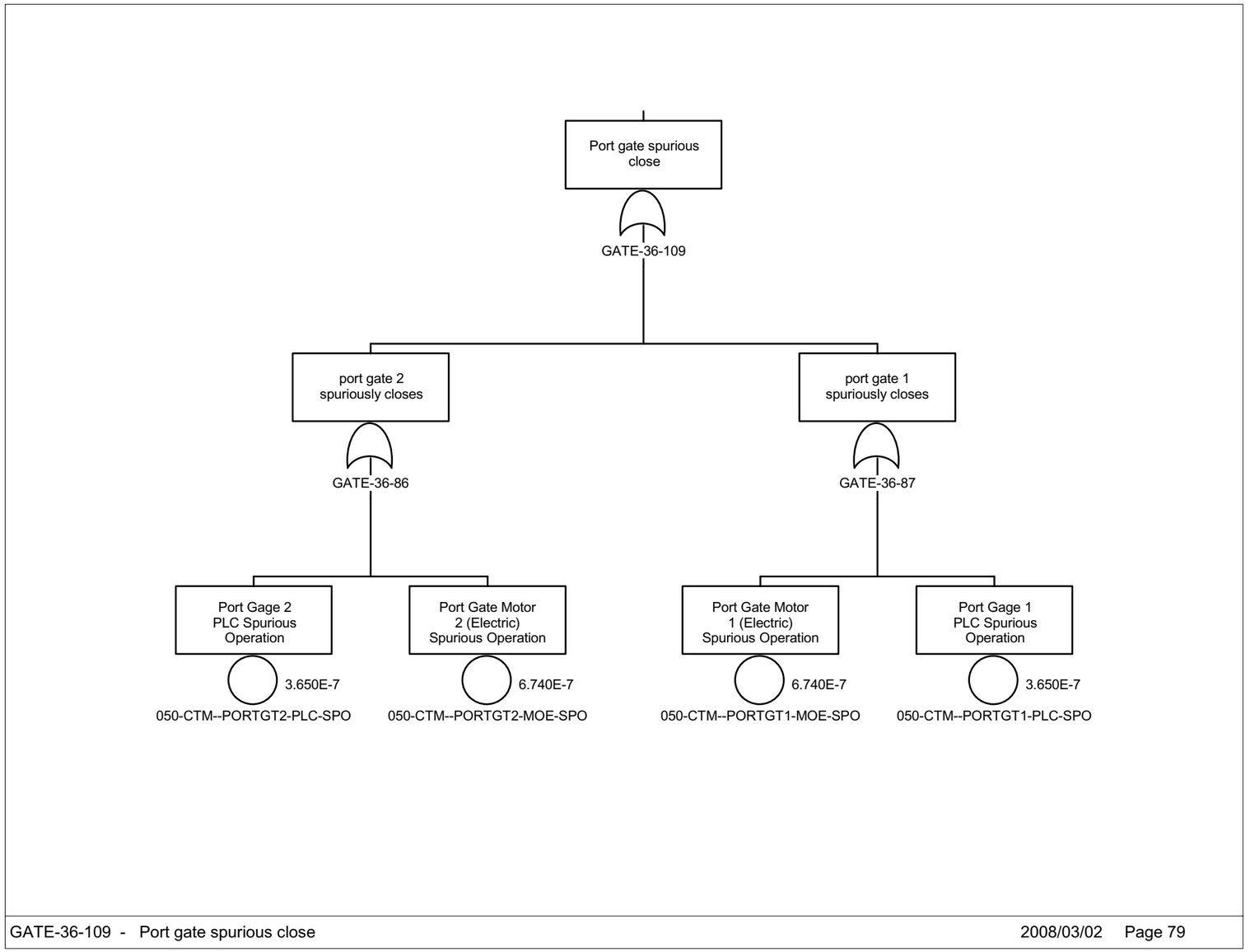
Source: Original

Figure B4.4-9. CTM Drop Fault Tree Sheet 7



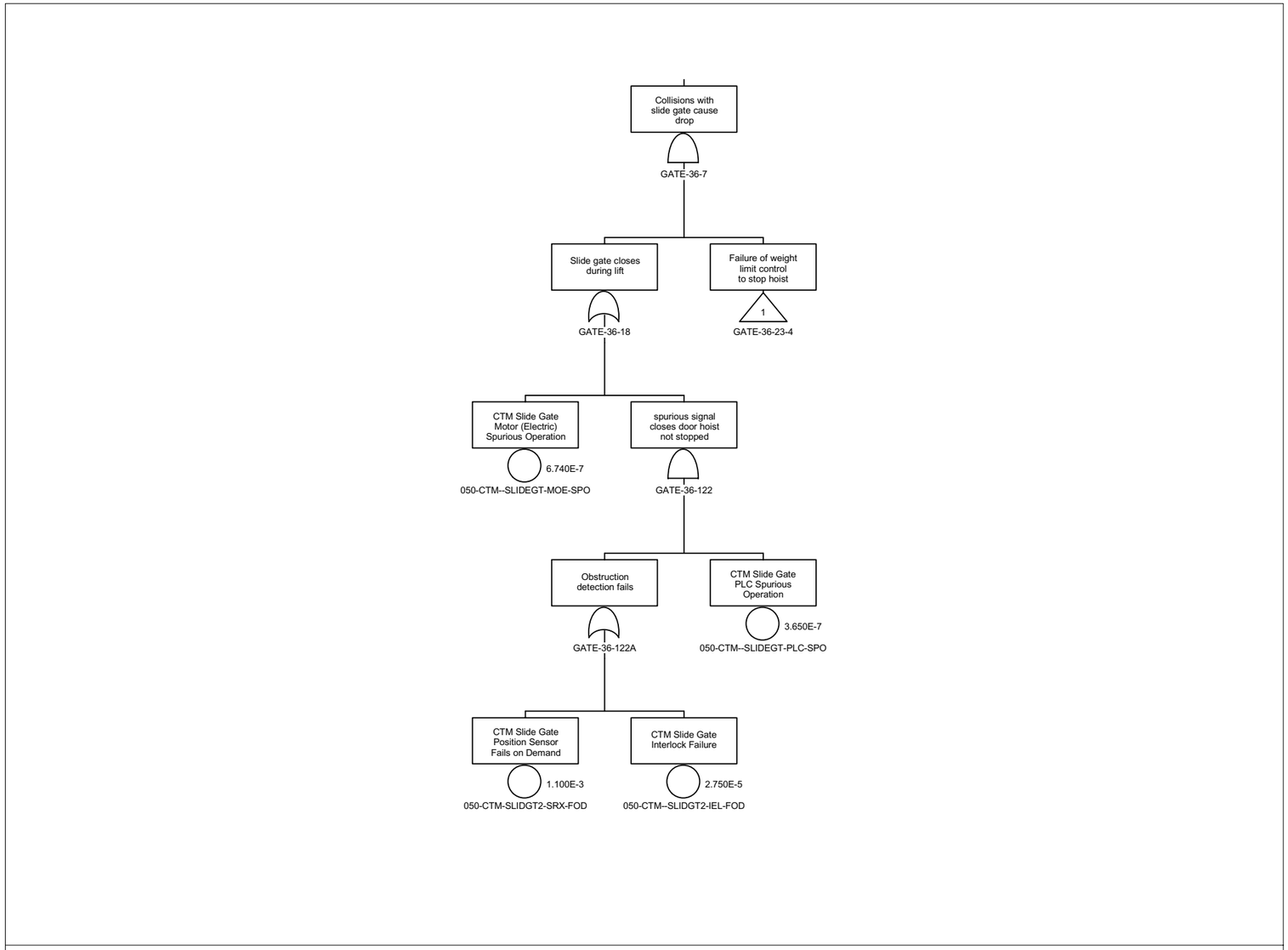
Source: Original

Figure B4.4-10. CTM Drop Fault Tree Sheet 8



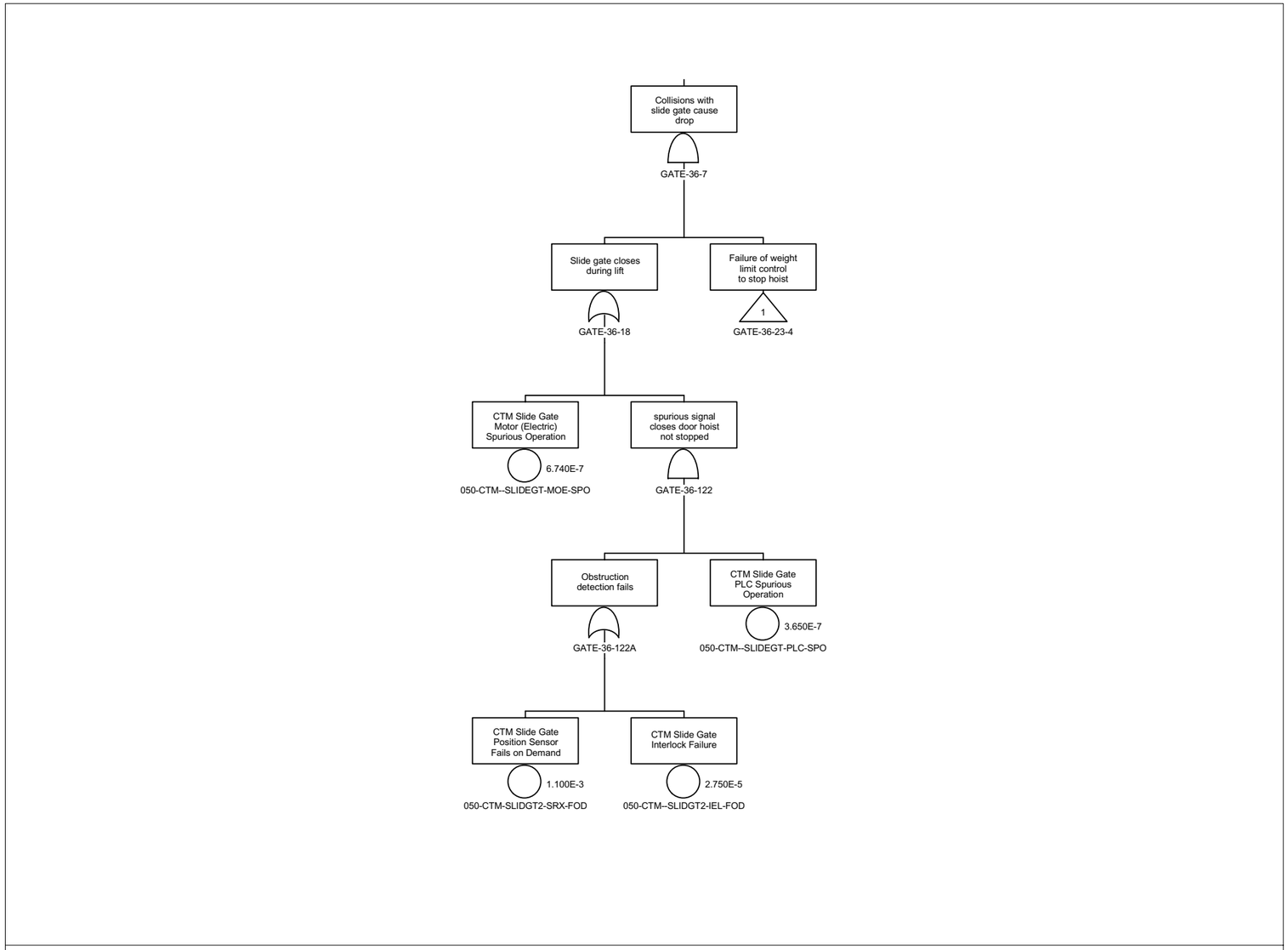
Source: Original

Figure B4.4-11. CTM Drop Fault Tree Sheet 9



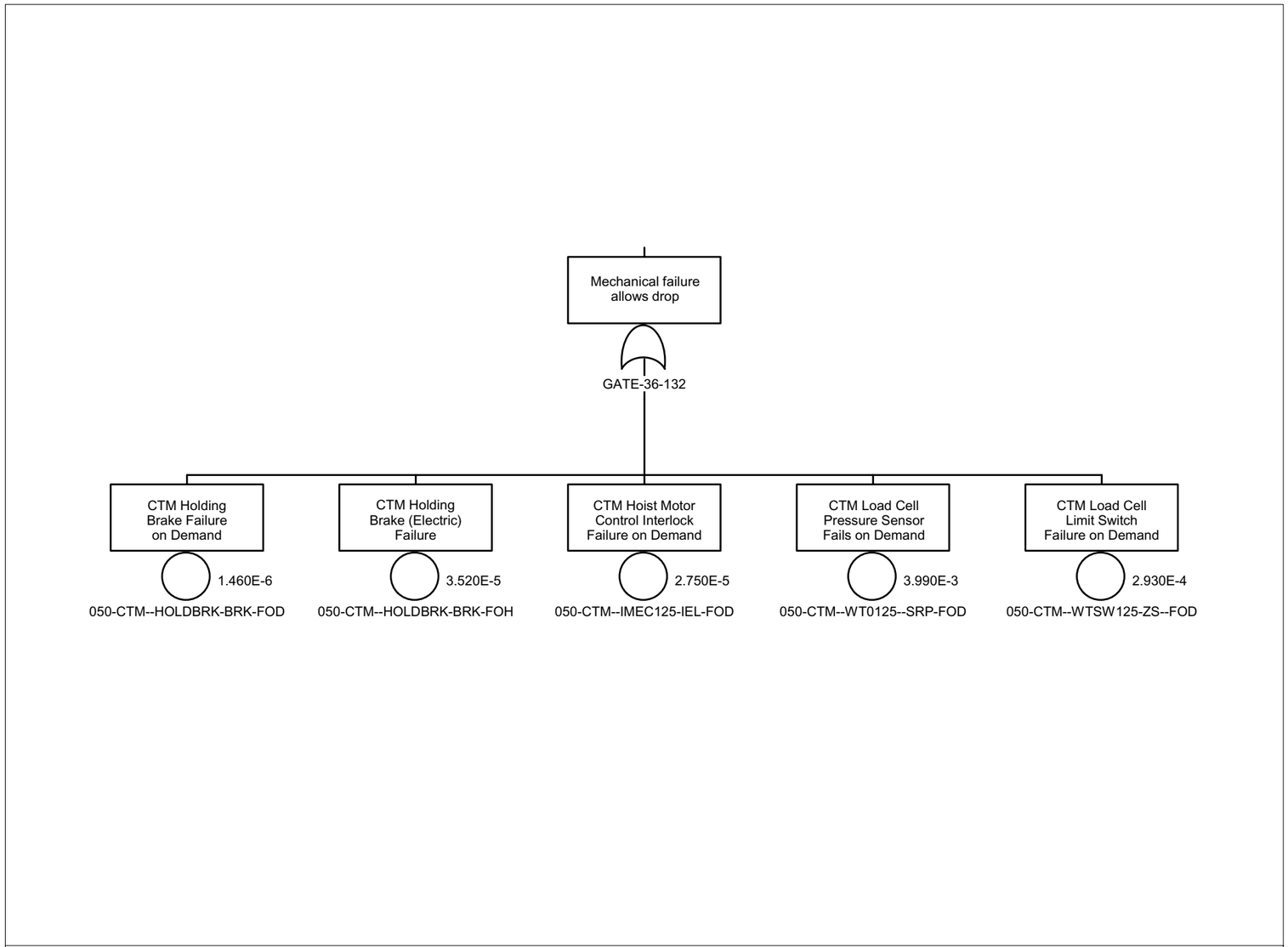
Source: Original

Figure B4.4-12. CTM Drop Fault Tree Sheet 10



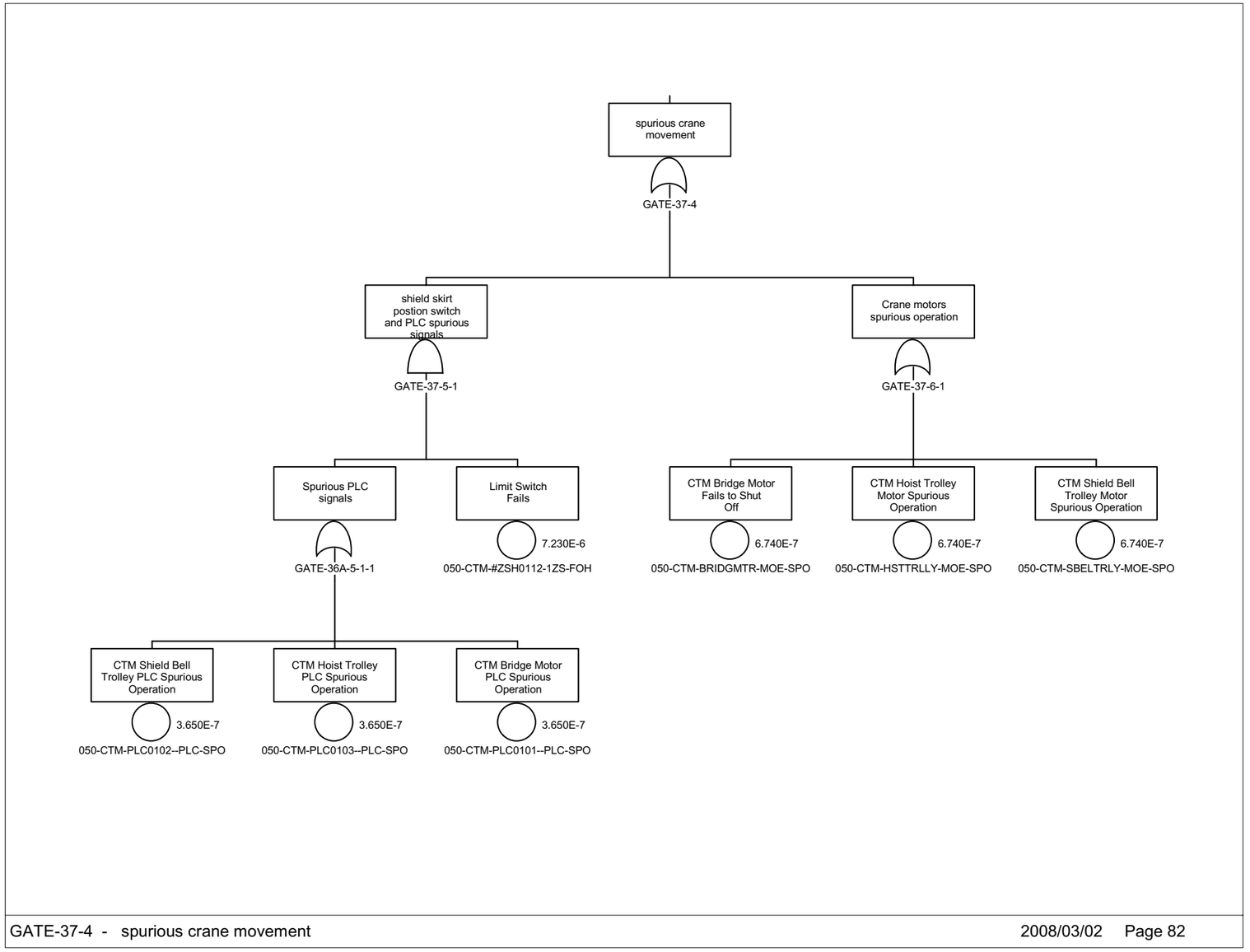
Source: Original

Figure B4.4-13. CTM Drop Fault Tree Sheet 11



Source: Original

Figure B4.4-14. CTM Drop Fault Tree Sheet 12



Source: Original

Figure B4.4-15. CTM Drop Fault Tree Sheet 13

B4.4.2 Canister Drops from Above the Canister Design Limit Drop Height

B4.4.2.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of the canisters. These drops have been divided into two classes: drops from heights below the design basis drop height of the canister and drops from heights above the design basis drop height of the canister. This fault tree for canister drops addresses the second of these two scenarios.

B4.4.2.2 Success Criteria

Success criteria for the CTM is simply the prevention of a canister drop from above the canister design limit drop height from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.2.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.

- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.

- An interlock between the slide gate and shield skirt–the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed, to allow the CTM to move with the slide gate open during lid removal.

- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, sufficient to ensure that, in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end-of-travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.2.4 Fault Tree Model

The top event in this fault tree is "CTM High Drops from Two Blocking Events." This is defined as a drop of a canister from a height above the design limit height for the canister during transfer operations. (The two block designation refers to the condition where the object being lifted is raised to the point where the upper and lower blocks of the crane come into contact. Attempts to continue to lift the load at this point places additional strains on the CTM components.) For this event to occur the canister must be lifted above the normal heights associated with a lift and the features designed to limit the drop height must fail. During normal operation, once the canister clears the optical sensor in the shield bell, the shield bell slide gate is closed. Provided the gate is closed at this time, the potential drop height for the canister never exceeds the canister design limit drop height. Faults considered in the evaluation of this top event include component and human events (considered in conjunction with the interlocks intended to prevent the erroneous human action) that contribute to raising the canister too high. The model does not credit CTM features that could mitigate the consequences of a two-block event. It was assumed that all two-block events result in a drop.

B4.4.2.5 Basic Event Data

Table B4.4-4 contains a list of basic events used in the CTM High Drops from Two Blocking Events fault tree. Included are the HFEs and the CCF events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The canister drop probability modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are put into operation. They are consequently evaluated over the interval of time between their actuation, considered to be the duration of a shift (i.e., eight hours).

Table B4.4-4. Basic Event Probability for the CTM High Drops from Two Blocking Events Fault Tree

Name	Description	Calc. Type[a]	Calculation Probability	Failure Prob.	Lambda	Mission Time[a]
050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1	1.100E-05	1.100E-05	0.000E+00	0.000E+00
050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	1.000E+00
050-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.080E-07	0.000E+00	1.350E-08	8.000E+00
050-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	0.000E+00	4.700E-06	0.000E+00
050-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; Cal = calculation; Prob = probability.

Source: Original

B4.4.2.5.1 Human Failure Events

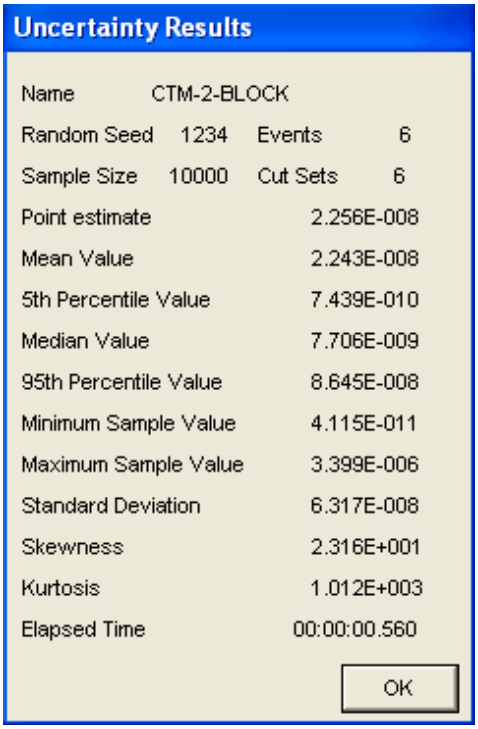
One basic event is associated with human error: 050-OPCTMDRINT01-HFI-COD (operator raises load too high–two block). This event models the combination of operator actions and interlock failures required to allow the operator to raise a load above design limits, and action that can lead to a two-blocking failure.

B4.4.2.5.2 Common-Cause Failures

One CCF event was considered in the evaluation of this fault tree. There are two upper limit switches intended to prevent raising a load too high. The CCF of these switches was considered. An alpha factor of 0.047 was used to determine the CCF value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

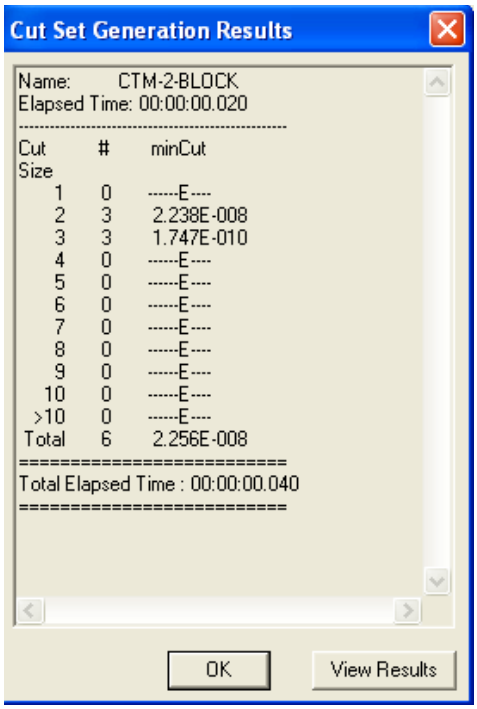
B4.4.2.6 Uncertainty and Cut Set Generation Results

Figure B4.4-17 contains the uncertainty results obtaining from running the fault tree for CTM two blocking using a cutoff at 1E-15. Figure B4.4-18 provides the cut set generation results for the CTM Two Blocking fault tree.



Source: Original

Figure B4.4-17. Uncertainty Results of the CTM Canister Drop Two Block Fault Tree



Source: Original

Figure B4.4-18. Cut Set Generation Results for the CTM Canister Drop Two Block Fault Tree

B4.4.2.7 Cut Sets

Table B4.4-5 contains the top six cut sets for the canister drop two blocking fault tree.

Table B4.4-5. Dominant Cut Sets for the CTM Canister Drop from Above the Canister Design Height Limit

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
98.99	98.99	2.233E-08	050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.100E-05
			050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
99.76	0.77	1.743E-10	050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	2.930E-04
			050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
99.99	0.23	5.170E-11	050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.100E-05
			050-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.700E-06
100.00	0.01	1.188E-12	050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.100E-05
			050-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.080E-07

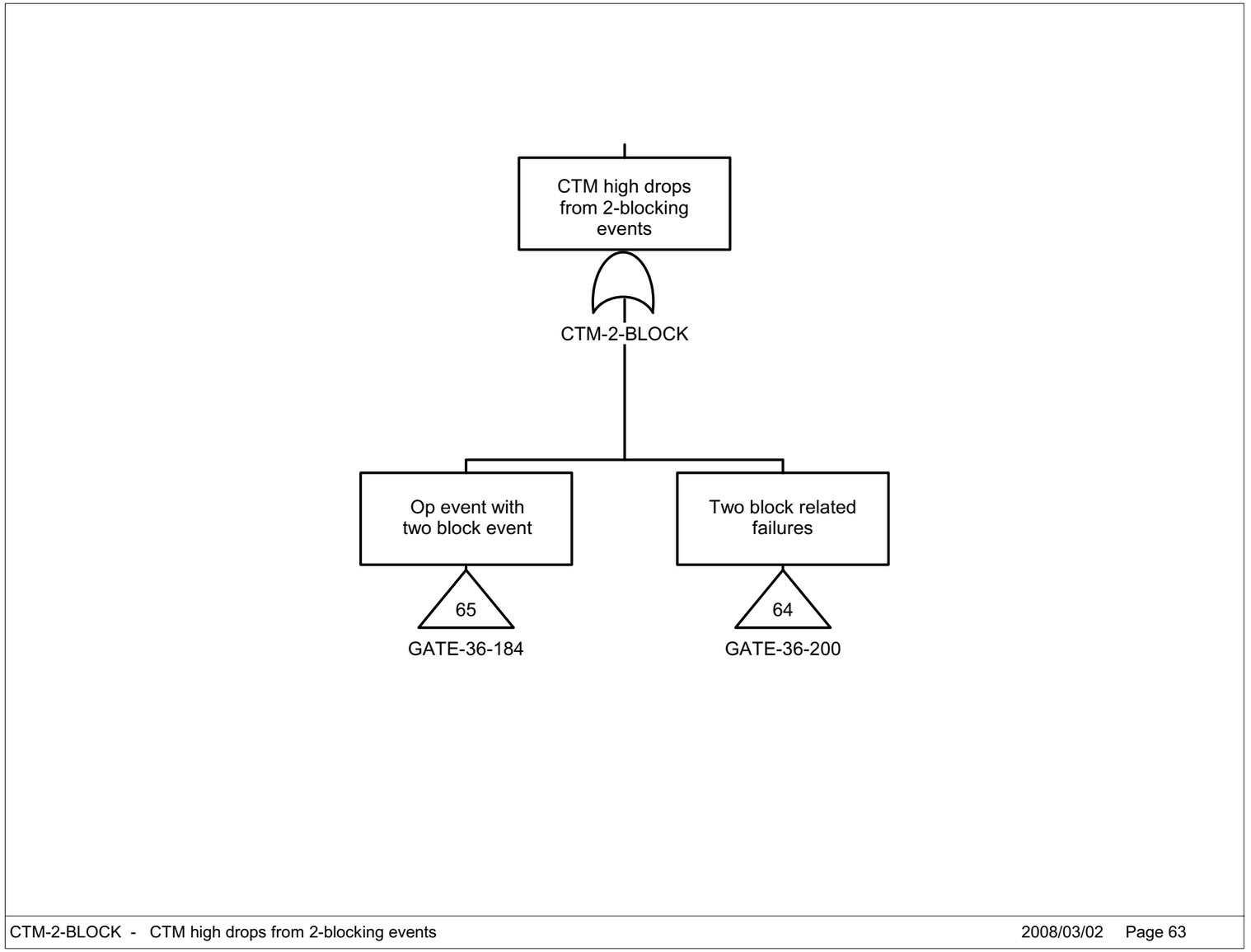
Table B4.4-5. Dominant Cut Sets for the CTM Canister Drop from Above the Canister Design Height Limit (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
100.00	0.00	4.035E-13	050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	2.930E-04
			050-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.700E-06
100.00	0.00	9.272E-15	050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	2.930E-04
			050-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.080E-07

NOTE: ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; Prob = probability.

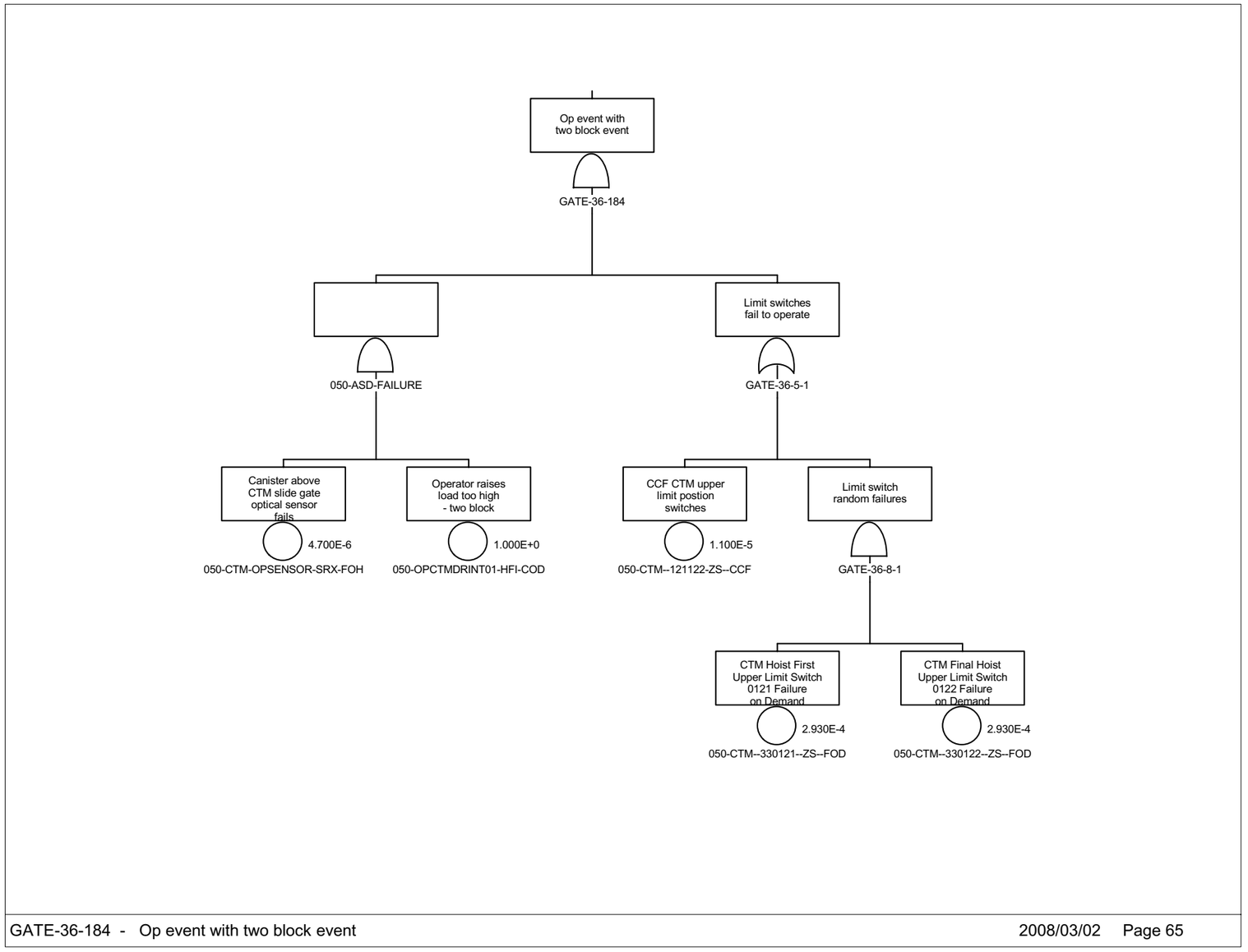
Source: Original

B4.4.2.8 Fault Trees



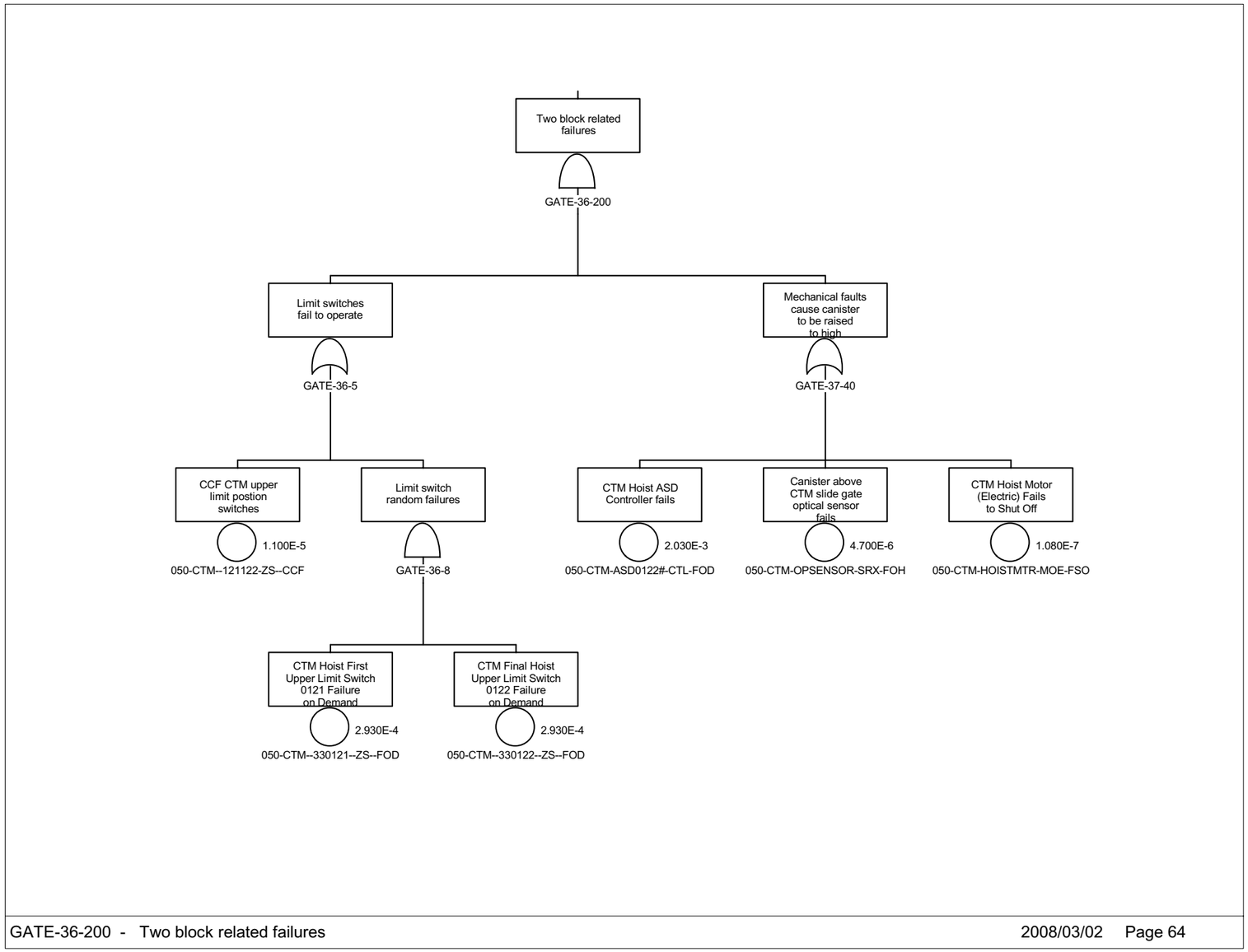
Source: Original

Figure B4.4-19. CTM High Drops from Two Blocking Event Sheet 1



Source: Original

Figure B4.4-20. CTM High Drops from Two Blocking Event Sheet 2



Source: Original

Figure B4.4-21. CTM High Drops from Two Blocking Event Sheet 3

B4.4.3 Drops of Objects onto Canister

B4.4.3.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of objects onto canisters. Cask lids, handling equipment, auxiliary grapples are handled during the canister transfer process. At times these objects are over the canister and could be dropped onto the canister.

B4.4.3.2 Success Criteria

The success criteria for the CTM is simply the prevention of a drop of any object onto the canister from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.3.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.

- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered

- An interlock between the slide gate and shield skirt–the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed, to allow the CTM to move with the slide gate open during lid removal.

- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end-of-travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.3.4 Fault Tree Model

The top event in this fault tree is "Drop of Object onto Canister." This is defined as a drop of an object onto a canister during transfer operations. Faults considered in the evaluation of this top event include: human events that contribute to a drop (considered in conjunction with the interlocks intended to prevent the erroneous human action) and mechanical (structural) failures of the CTM components. The interlocks and safety features (position controls, load cells, and drum and holding brakes) intended to either prevent CTM failure or given failure of the CTM, to prevent a load drop, are included in the model.

Structural failures of components including the hoist cables, sheaves, drum, and grapples can result in canister drops. Operator events are addressed for actions including improper grapple connections, misalignments of the hoist and the canister, improper hoist activities and improper lateral movement of the CTM. Protection from these actions are provided by hard-wired interlocks keyed to the position of the CTM (both hoist position and CTM lateral position), slide and port gate doors, and the shield bell skirt. Also considered in the analysis is a canister drop initiated by improper operation of the shield bell slide gates and the port slide gates. While the gate motors are sized to prevent damage to the canister in the event of an inadvertent closure of the gates, the possibility that the gates would close above the canister during a lift blocking the lift and causing a canister drop was considered.

B4.4.3.5 Basic Event Data

Table B4.4-6 contains a list of basic events used in the "CTM Drop of Object onto Canister" fault tree. Included are the HFEs and the CCF events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The object drop probability modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are put into operation. They are consequently evaluated over the interval of time between their actuation, considered to be the duration of a shift, (i.e., eight hours). In another example, brakes are also analyzed over a mission time of twenty-four hours. This duration is deemed sufficient to encompass the time required to revert to normal transfer operations, after a malfunction that would have caused a safety system of the CTM to cease transfer activities.

Table B4.4-6. Basic Event Probability for the CTM Drop of Objects onto Canister Fault Tree

Name	Description	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1	1.100E-05	1.100E-05	0.000E+00	0.000E+00
050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--CBL0001-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0002-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00
050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	1	9.400E-08	9.400E-08	0.000E+00	0.000E+00
050-CTM--DRTRN-CT--FOD	Controller Failure	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	1	4.000E-08	4.000E-08	0.000E+00	1.000E+00
050-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	0.000E+00	1.000E+00
050-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure	3	2.011E-04	0.000E+00	8.380E-06	2.400E+01
050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	3	6.500E-06	0.000E+00	6.500E-06	1.000E+00
050-CTM--HOLDBRK-BRK-FOD	CTM Holding Brake Failure on Demand	1	1.460E-06	1.460E-06	0.000E+00	1.000E+00
050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3	3.520E-05	0.000E+00	4.400E-06	8.000E+00
050-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Failure on Demand	1	2.750E-05	2.750E-05	0.000E+00	1.000E+00
050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--OVERSP--ZS--FOD	CTM Hoist motor speed Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00

Table B4.4-6. Basic Event Probability for the CTM Drop of Objects onto Canister Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM--PORTGT1-MOE-SPO	Port Gate Motor 1 (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--PORTGT1-PLC-SPO	Port Gage 1 PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--PORTGT2-PLC-SPO	Port Gage 2 PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
050-CTM--SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM--SLIDGT2-IEL-FOD	CTM Slide Gate Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	1.000E+00
050-CTM--WT0125--SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	0.000E+00	1.000E+00
050-CTM--WTSW125-ZS--FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--YS01129-ZS--FOD	CTM Drum Brake Control Circuit Switch Fail	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	1.000E+00
050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.080E-07	0.000E+00	1.350E-08	8.000E+00
050-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-MISSPOOL--DM-MSP	CTM mis-spool event	3	6.860E-07	0.000E+00	6.860E-07	0.000E+00
050-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	0.000E+00	4.700E-06	0.000E+00
050-CTM-PLC0101--PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00

Table B4.4-6. Basic Event Probability for the CTM Drop of Objects onto Canister Fault Tree (Continued)

Name	Description	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-PLC0102--PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM-PLC0103--PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
050-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	0.000E+00	1.000E+00
050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
050-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
050-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	1	4.000E-07	4.000E-07	0.000E+00	0.000E+00
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	0.000E+00	0.000E+00
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1	1.100E-05	1.100E-05	0.000E+00	0.000E+00
050-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	1.000E+00
050-CTM--CBL0001-WNE-BRK	CTM hoist wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	1.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller; Calc = calculation; Prob = probability.

Source: Original

B4.4.3.5.1 Human Failure Events

Four basic events are associated with human error (Table B4.4-7). These are for drops initiated by operator actions, drops caused by the operator initiating a two-block event, a failure to restore interlocks allowing movement of the crane when the shield skirt is raised and the slide gates are open and the operator closing the slide or port gates during a lift. The quantification of the event 050-OPCTMIMPACT1-HFI-COD includes operator actions and the failures of interlocks intended to prevent such operator action. The other three events were quantified using screening values.

Table B4.4-7. Human Failure Events

Name	Description
050-OPCLCTMGATE1-HFI-NOD	Operator commands gate to close
050-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block
050-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor

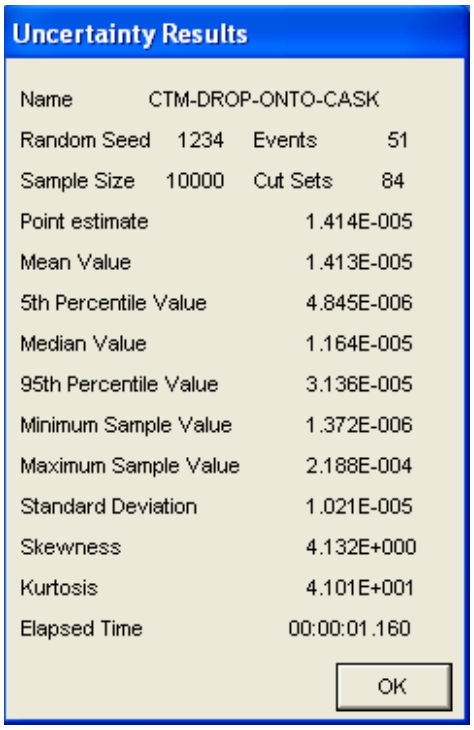
Source: Original

B4.4.3.5.2 Common-Cause Failures

Two CCF events were considered in the evaluation of this fault tree. The two upper limit sensors on the hoist are used to prevent a two-block event. The second CCF event considered is the CCF of the hoist cables. An alpha factor of 0.047 was used to determine the CCF value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

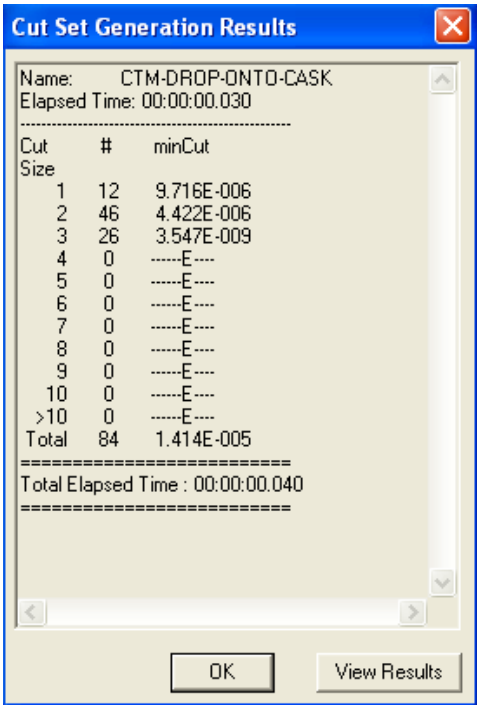
B4.4.3.6 Uncertainty and Cut Set Generation

Figure B4.4-22 contains the uncertainty results obtained from running the fault trees for the "CTM Drop onto Canister" using a cutoff at 1E-15. Figure B4.4-23 provides the cut set generation results for the "CTM Drop onto Canister" fault tree.



Source: Original

Figure B4.4-22 Uncertainty Results of the CTM Drop onto Canister Fault Tree



Source: Original

Figure B4.4-23. Cut Set Generation Results for the CTM Drop onto Canister Fault Tree

B4.4.3.7 Cut Sets

Table B4.4-8 contains the top 20 cut sets for the CTM Drop onto Canister fault tree.

Table B4.4-8. Dominant Cut Sets for the CTM Drop onto Canister Fault Tree

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
28.22	28.22	3.990E-06	050-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
			050-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
37.27	9.05	1.280E-06	050-CTM--ZSH0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
46.32	9.05	1.280E-06	050-CTM-ZSL0111-ZS--SPO	CTM Grapple Engage Switch Spurious Operation	1.280E-06
54.45	8.13	1.150E-06	050-CTM--EQL-SHV-BLK-FOD	CTM Sheaves Failure on Demand	1.150E-06
62.58	8.13	1.150E-06	050-CTM--GRAPPLE-GPL-FOD	CTM Grapple Failure on Demand	1.150E-06
70.71	8.13	1.150E-06	050-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Failure on Demand	1.150E-06
78.84	8.13	1.150E-06	050-CTM--UPPERBL-BLK-FOD	CTM Upper Sheaves Failure on Demand	1.150E-06
83.61	4.77	6.740E-07	050-CTM-BRIDGMTR-MOE-SPO	CTM Bridge Motor Fails to Shut Off	6.740E-07
88.38	4.77	6.740E-07	050-CTM-HSTTRLLY-MOE-SPO	CTM Hoist Trolley Motor Spurious Operation	6.740E-07
93.15	4.77	6.740E-07	050-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor Spurious Operation	6.740E-07
95.98	2.83	4.000E-07	050-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	4.000E-07
98.05	2.07	2.930E-07	050-CTM--WTSW125-ZS--FOD	Limit Switch Failure on Demand	2.930E-04
			050-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
98.71	0.66	9.400E-08	050-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.400E-08
98.99	0.28	4.000E-08	050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-08
			HRA-INTERLOCK	Interlock Human Error Relationship Addressed in HRA	1.000E+00
99.27	0.28	4.000E-08	050-CTM--DRUM001-DM--FOD	CTM Drum Failure on Demand	4.000E-08
99.52	0.25	3.520E-08	050-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Failure	3.520E-05
			050-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.71	0.19	2.750E-08	050-CTM--IMEC125-IEL-FOD	Interlock Failure on Demand	2.750E-05

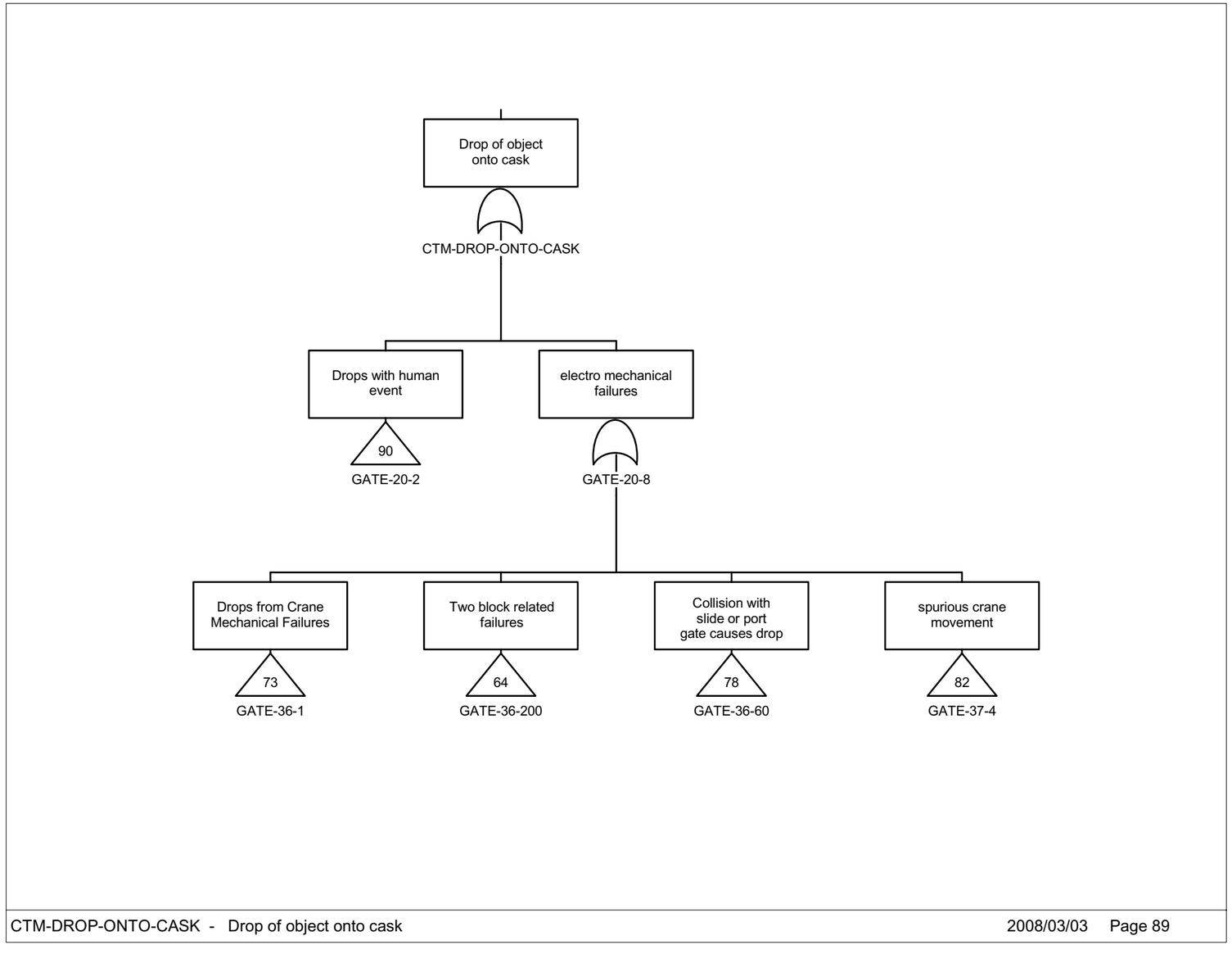
Table B4.4-8. Dominant Cut Sets for the CTM Drop onto Canister Fault Tree (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
			050-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.87	0.16	2.233E-08	050-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.100E-05
			050-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
99.89	0.02	2.689E-09	050-CTM--SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
99.91	0.02	2.689E-09	050-CTM--PORTGT2-MOE-SPO	Port Gate Motor 2 (Electric) Spurious Operation	6.740E-07
			050-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
28.22	28.22	3.990E-06	050-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03

NOTE: ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine; Prob = probability.

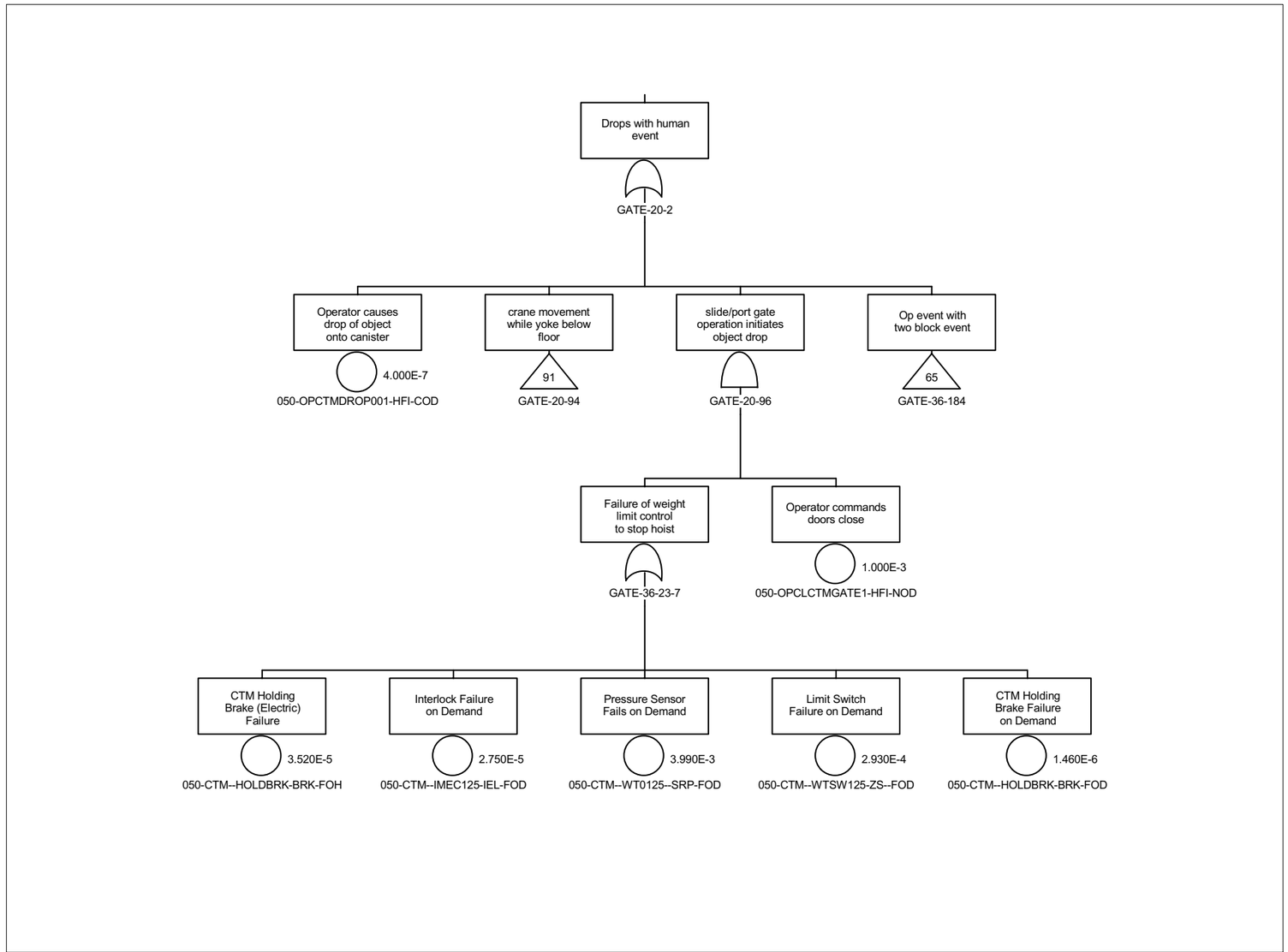
Source: Original

B4.4.3.8 Fault Trees



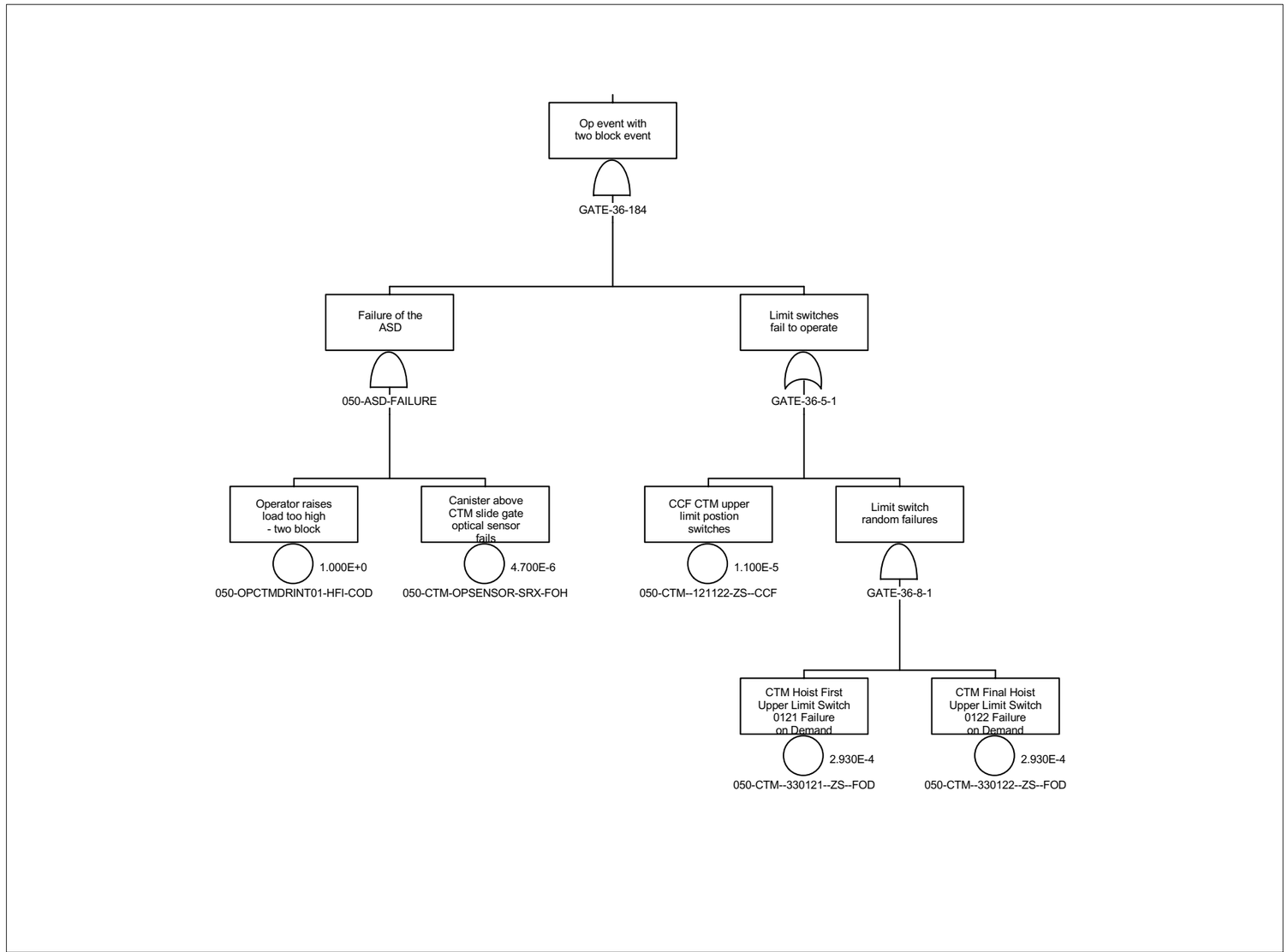
Source: Original

Figure B4.4-24. Drop of Object onto Cask
Sheet 1



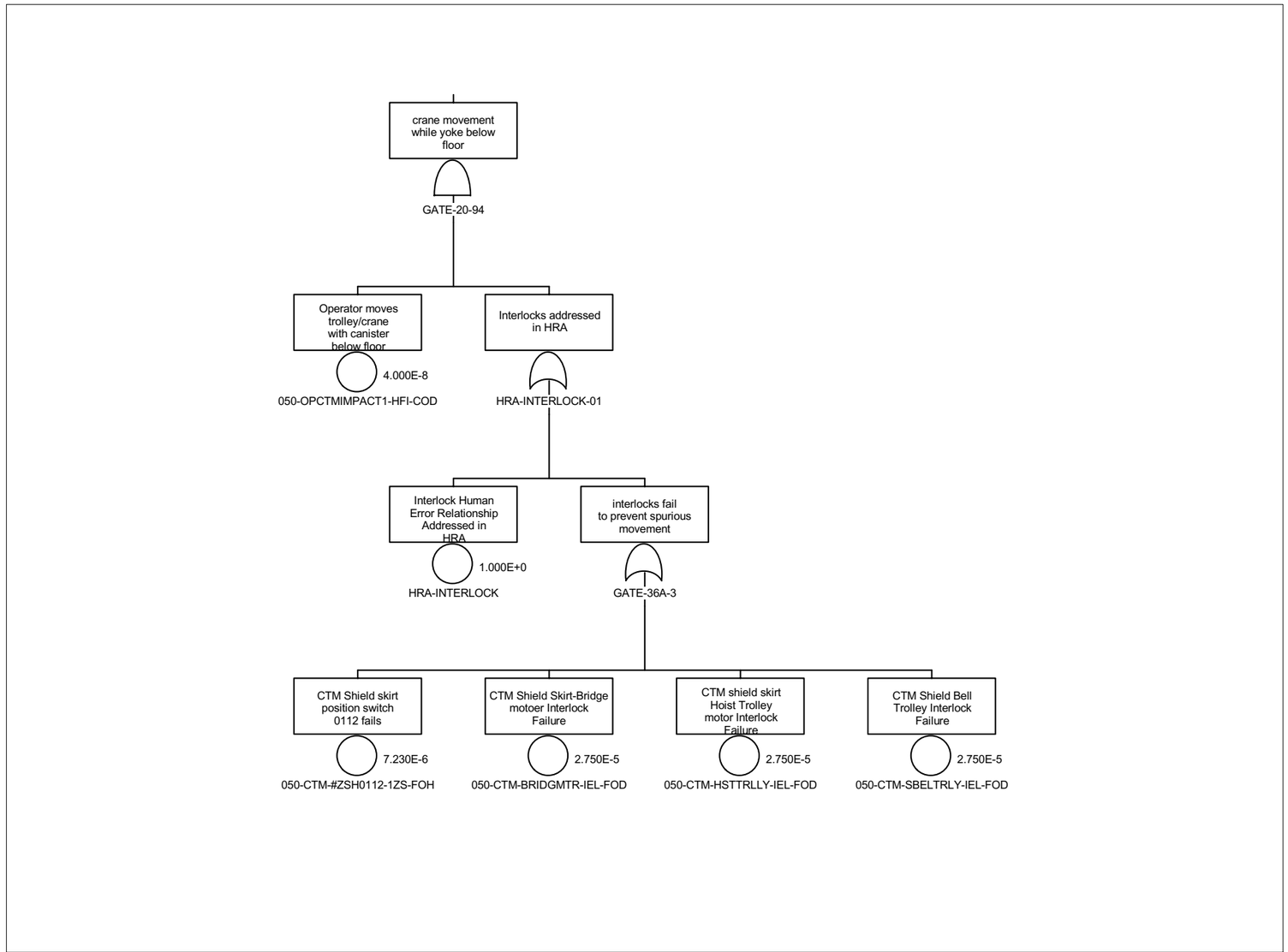
Source: Original

Figure B4.4-25. Drop of Object onto Cask
Sheet 2



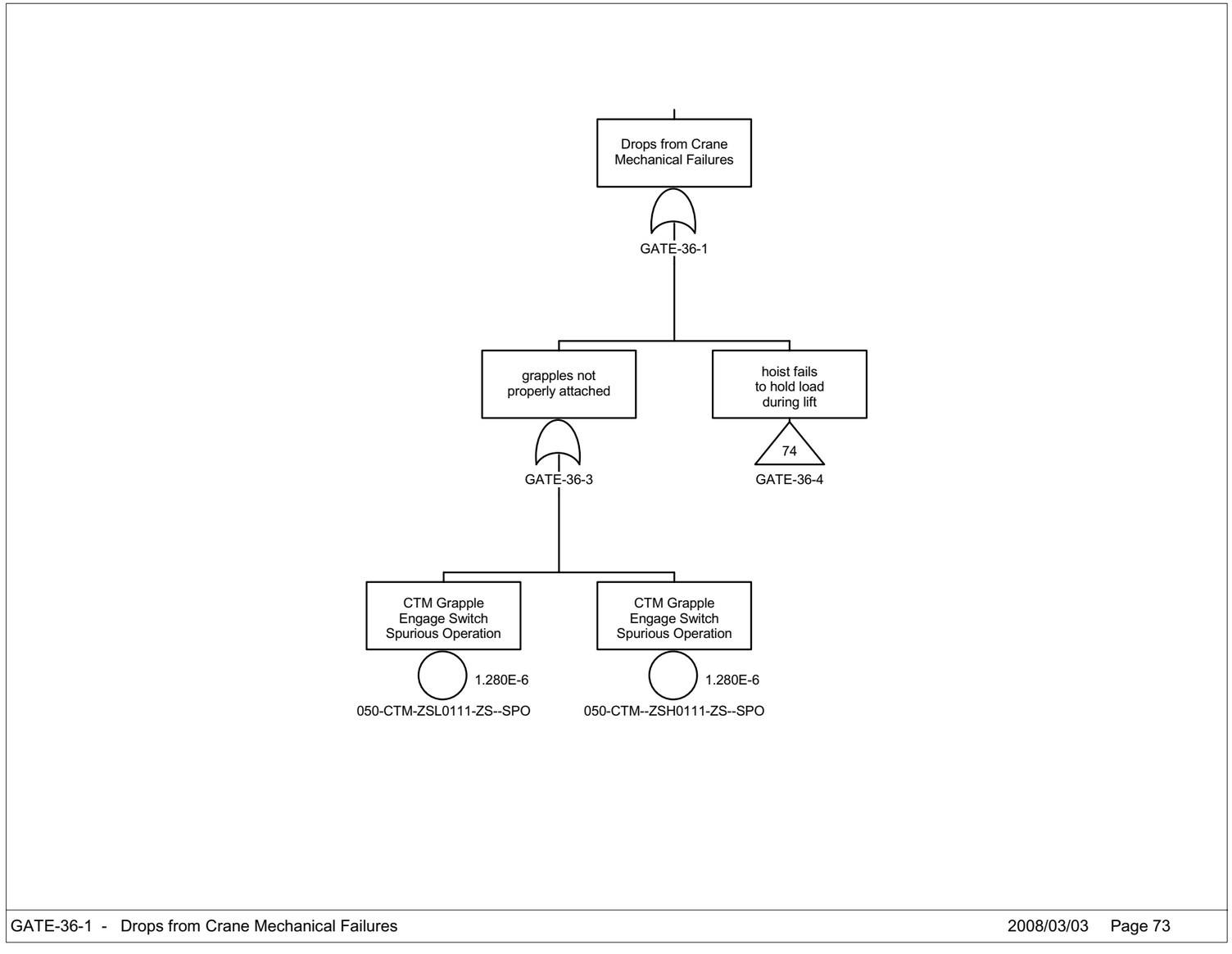
Source: Original

Figure B4.4-26. Drop of Object onto Cask
Sheet 3



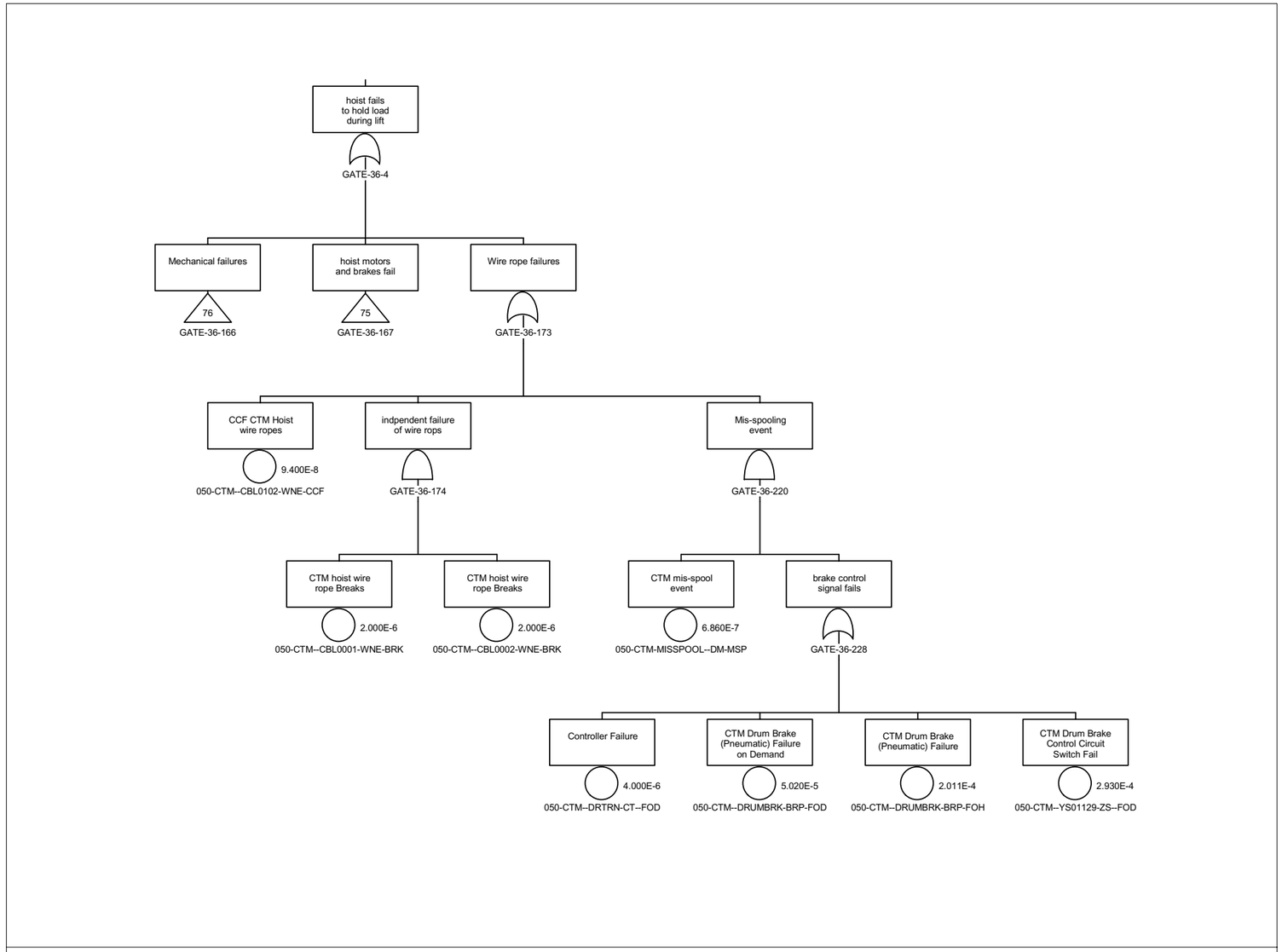
Source: Original

Figure B4.4-27. Drop of Object onto Cask
Sheet 4



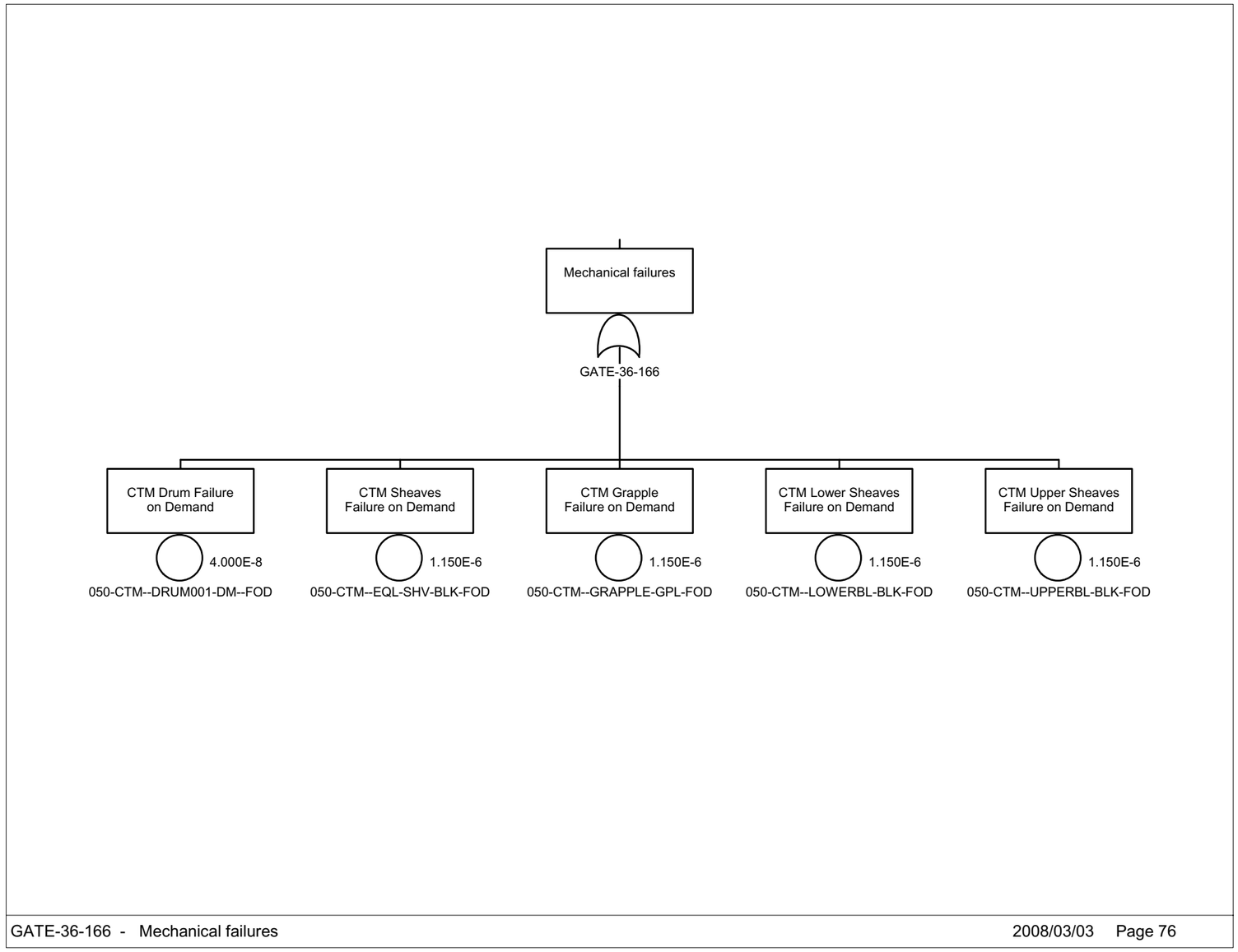
Source: Original

Figure B4.4-28. Drop of Object onto Cask
Sheet 5



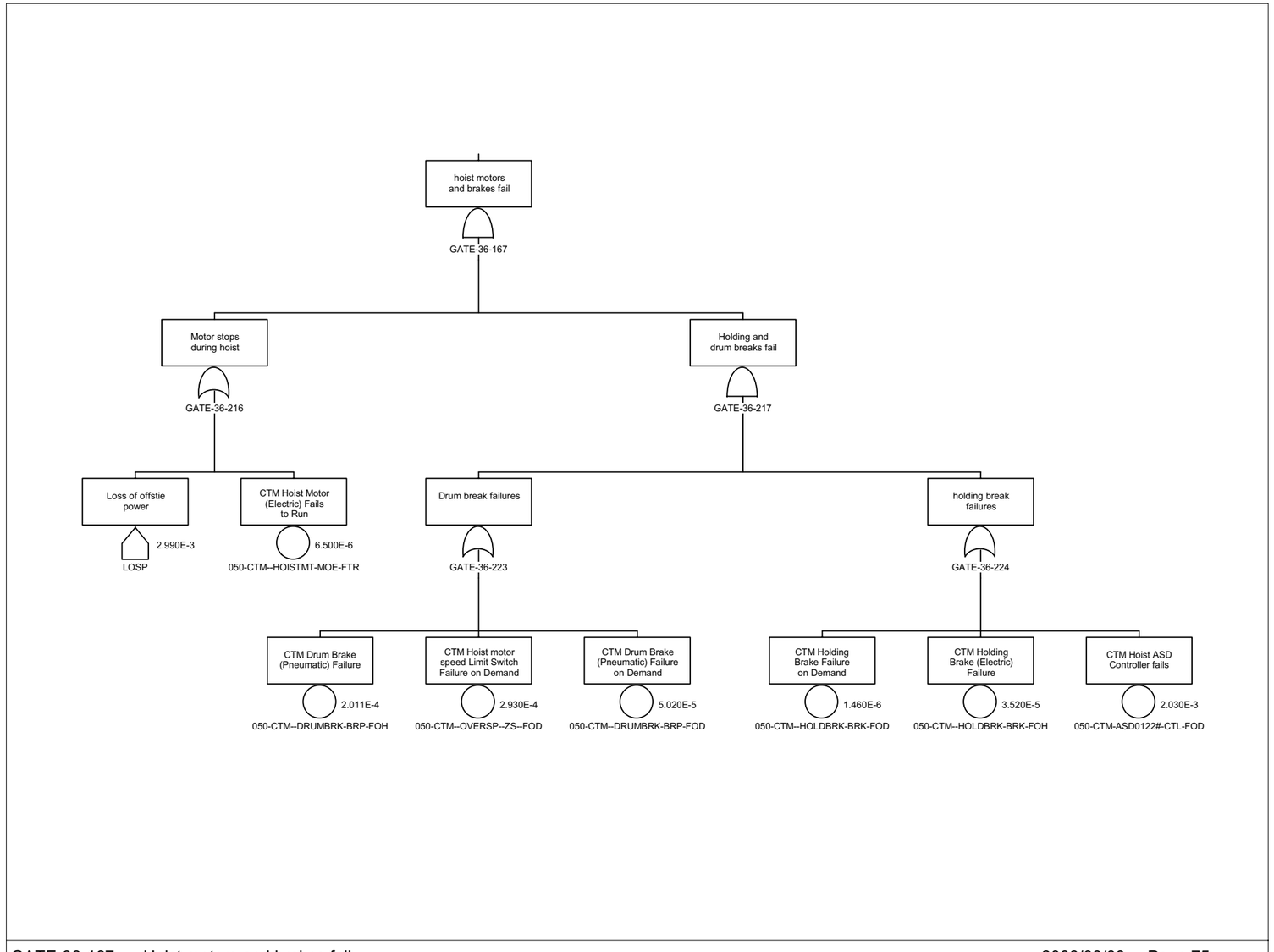
Source: Original

Figure B4.4-29. Drop of Object onto Cask
Sheet 6



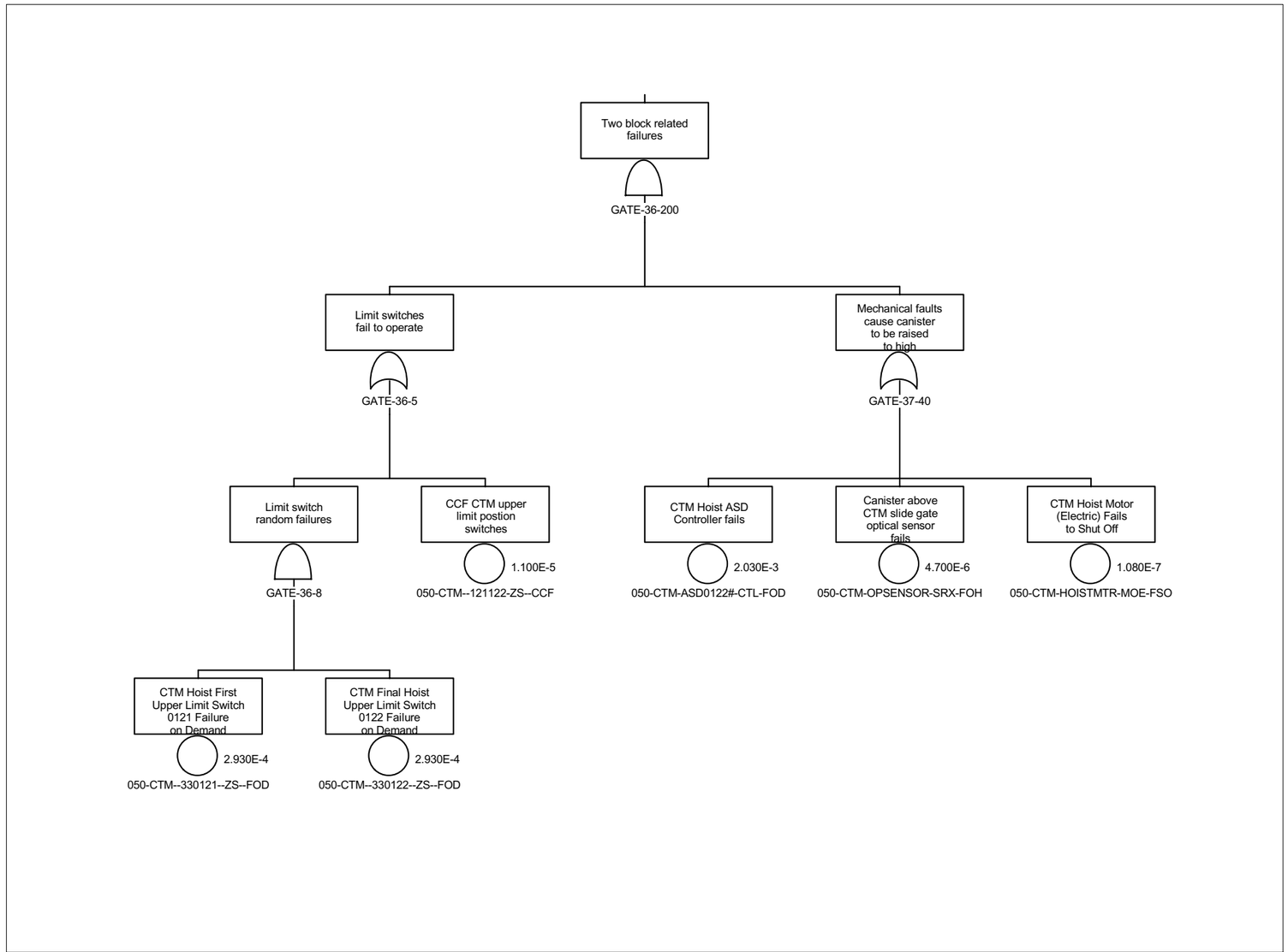
Source: Original

Figure B4.4-30. Drop of Object onto Cask
Sheet 7



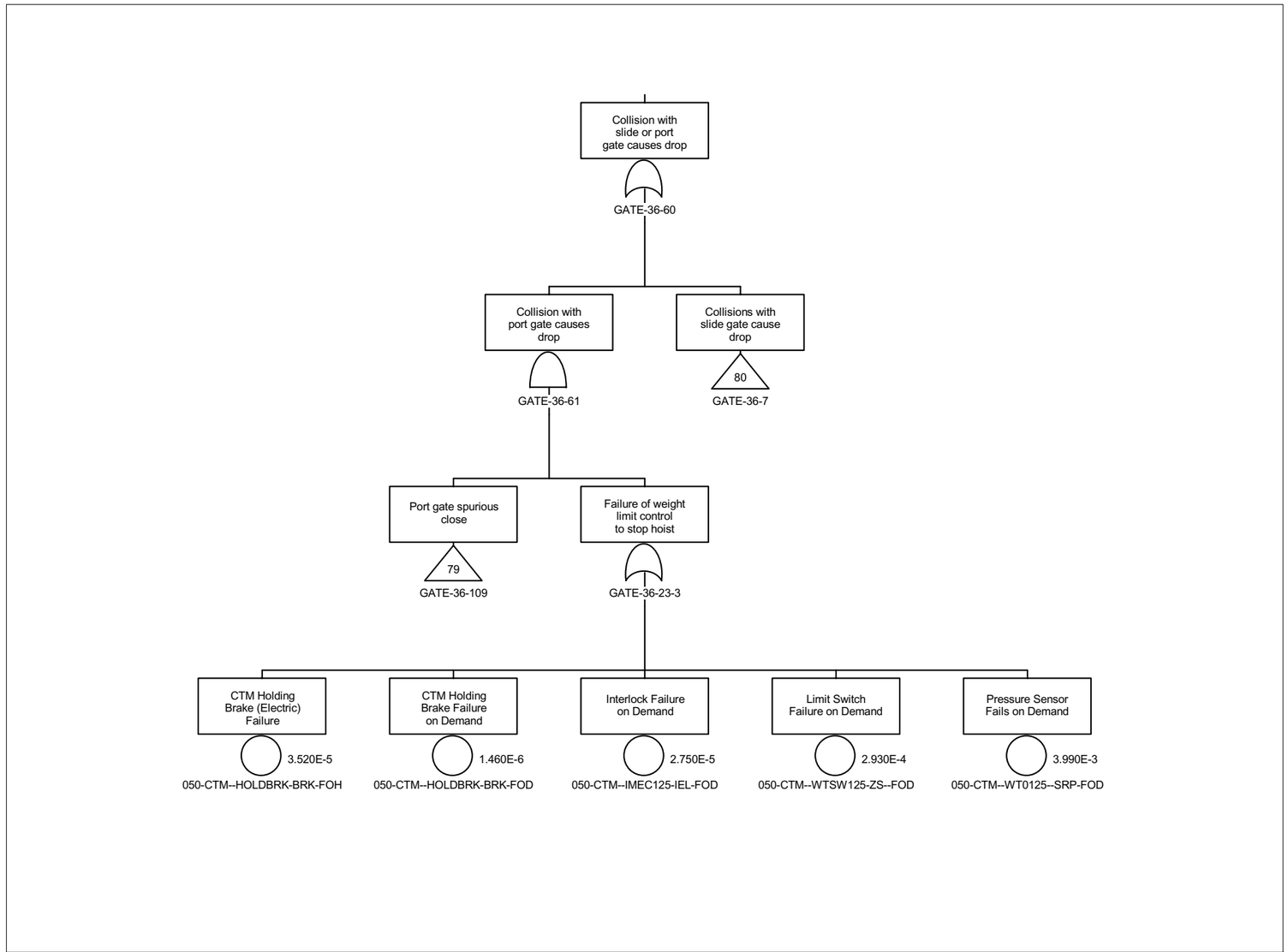
Source: Original

Figure B4.4-31. Drop of Object onto Cask
Sheet 8



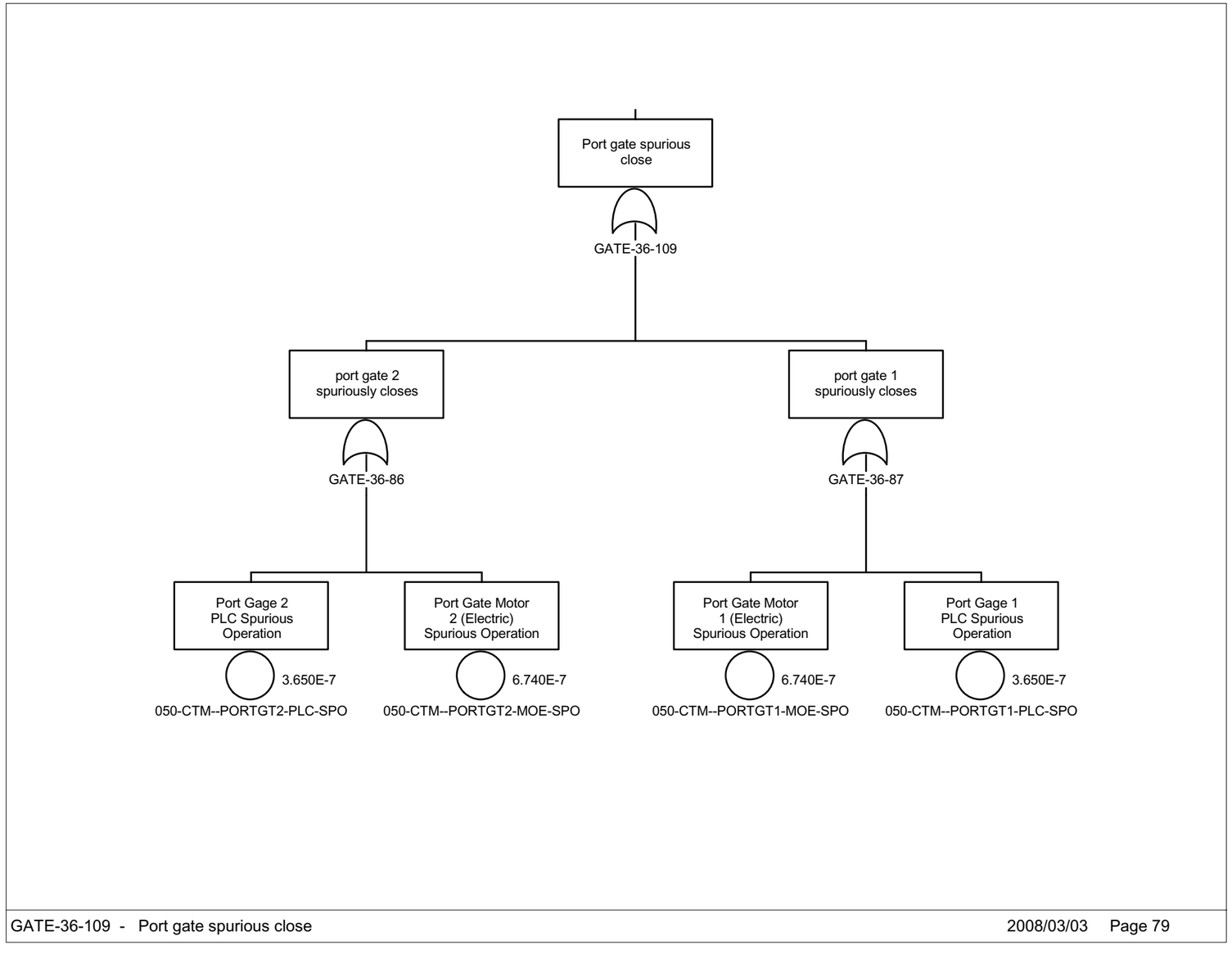
Source: Original

Figure B4.4-32. Drop of Object onto Cask
Sheet 9



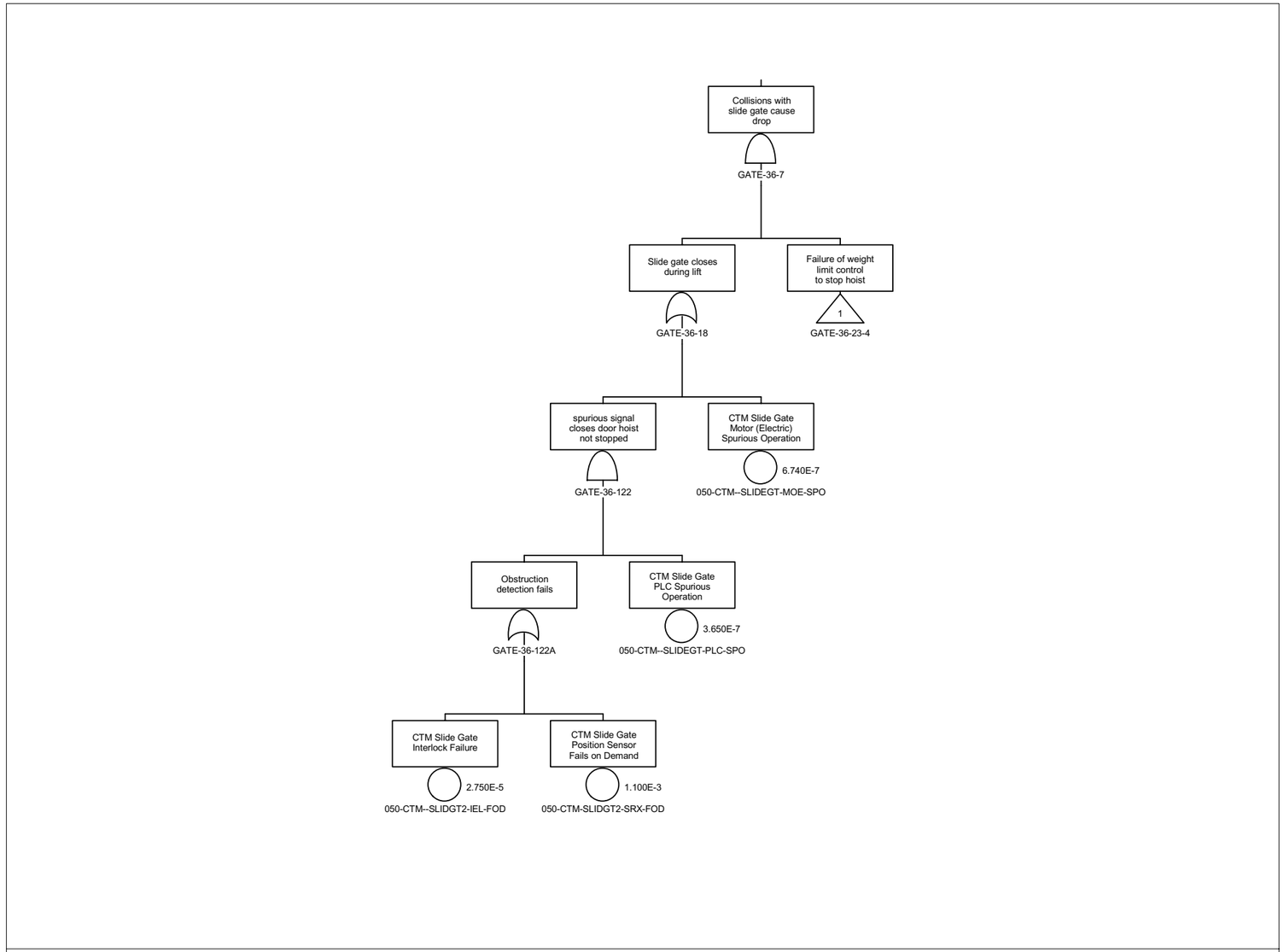
Source: Original

Figure B4.4-33. Drop of Object onto Cask
Sheet 10



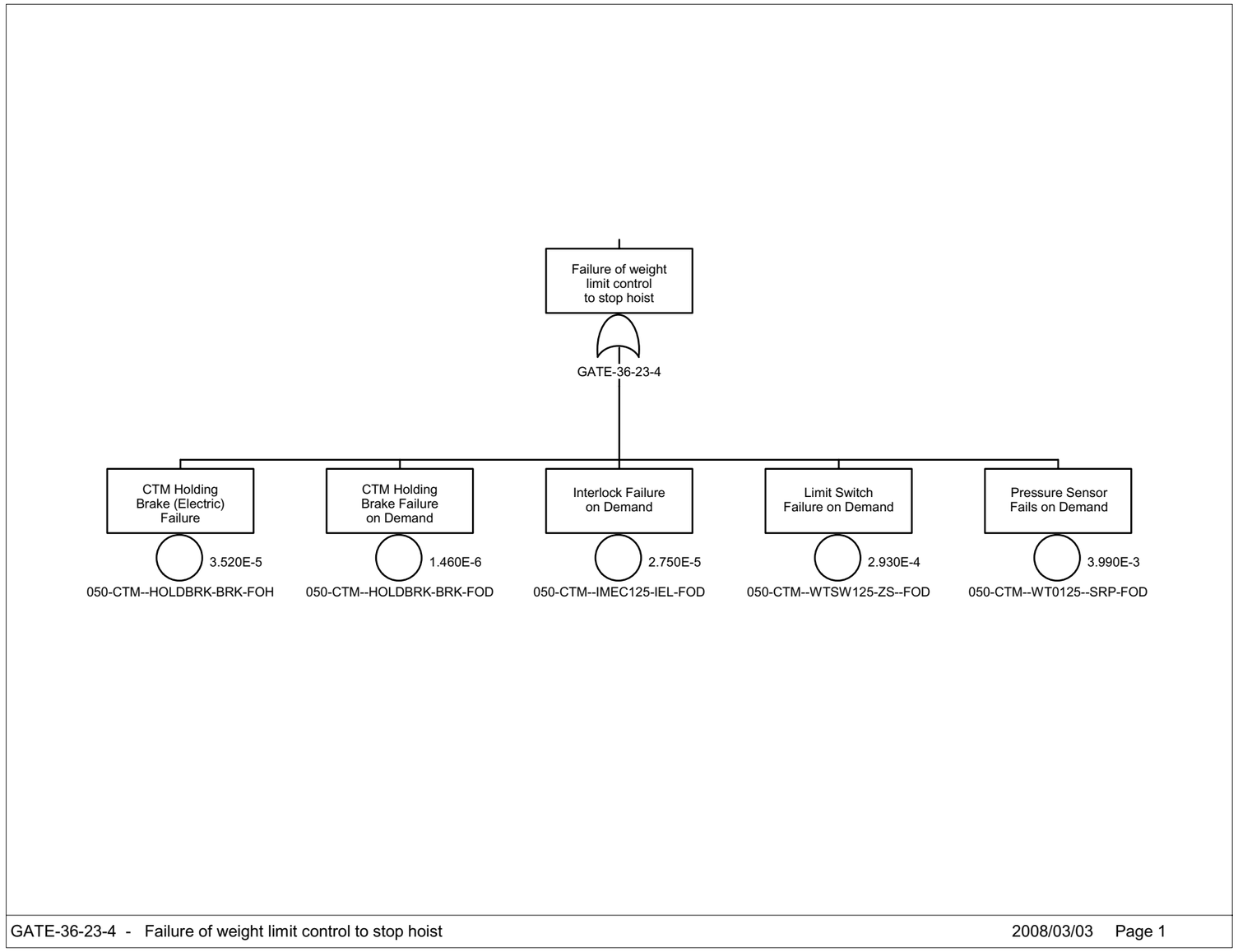
Source: Original

Figure B4.4-34. Drop of Object onto Cask
Sheet 11



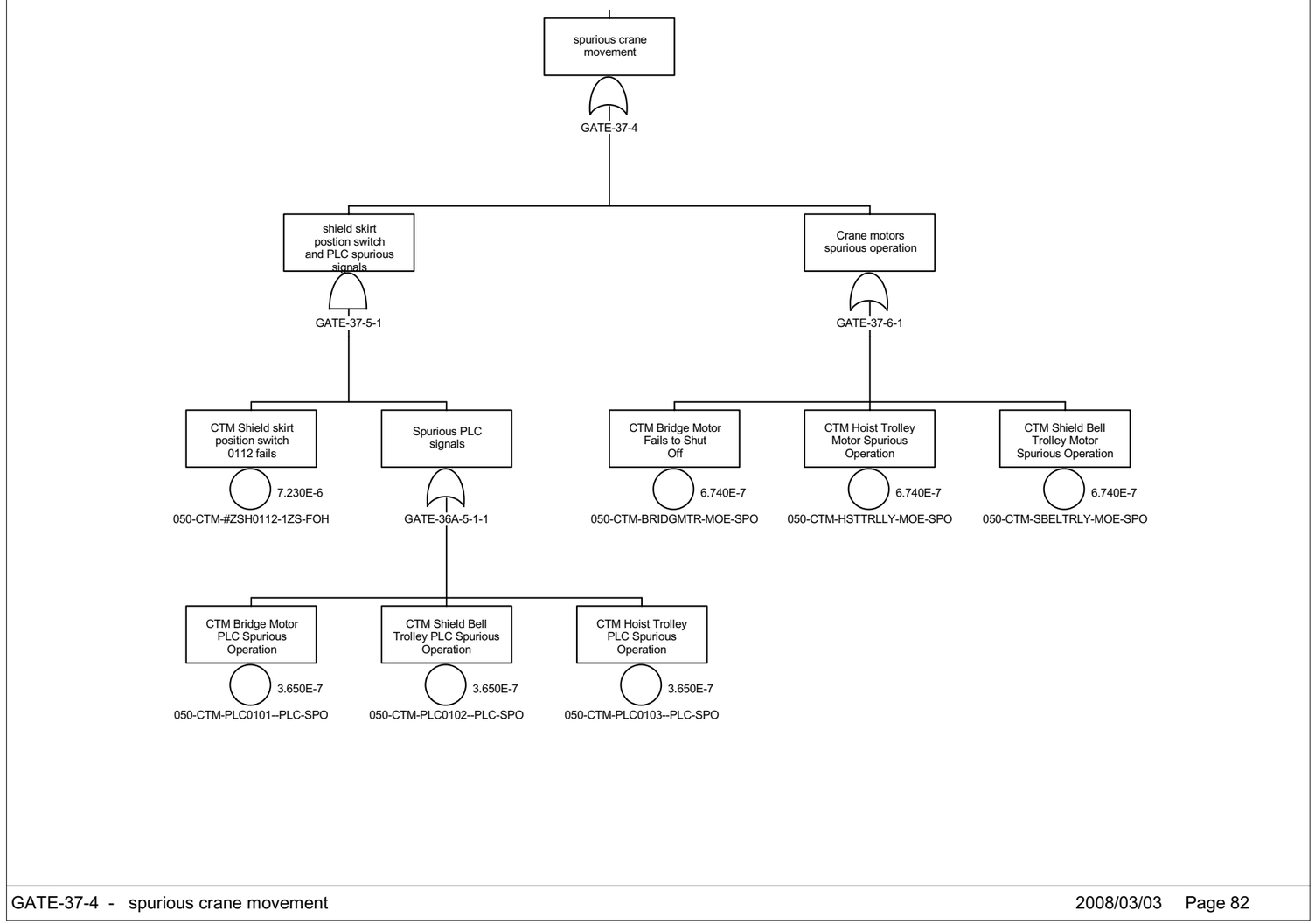
Source: Original

Figure B4.4-35. Drop of Object onto Cask
Sheet 12



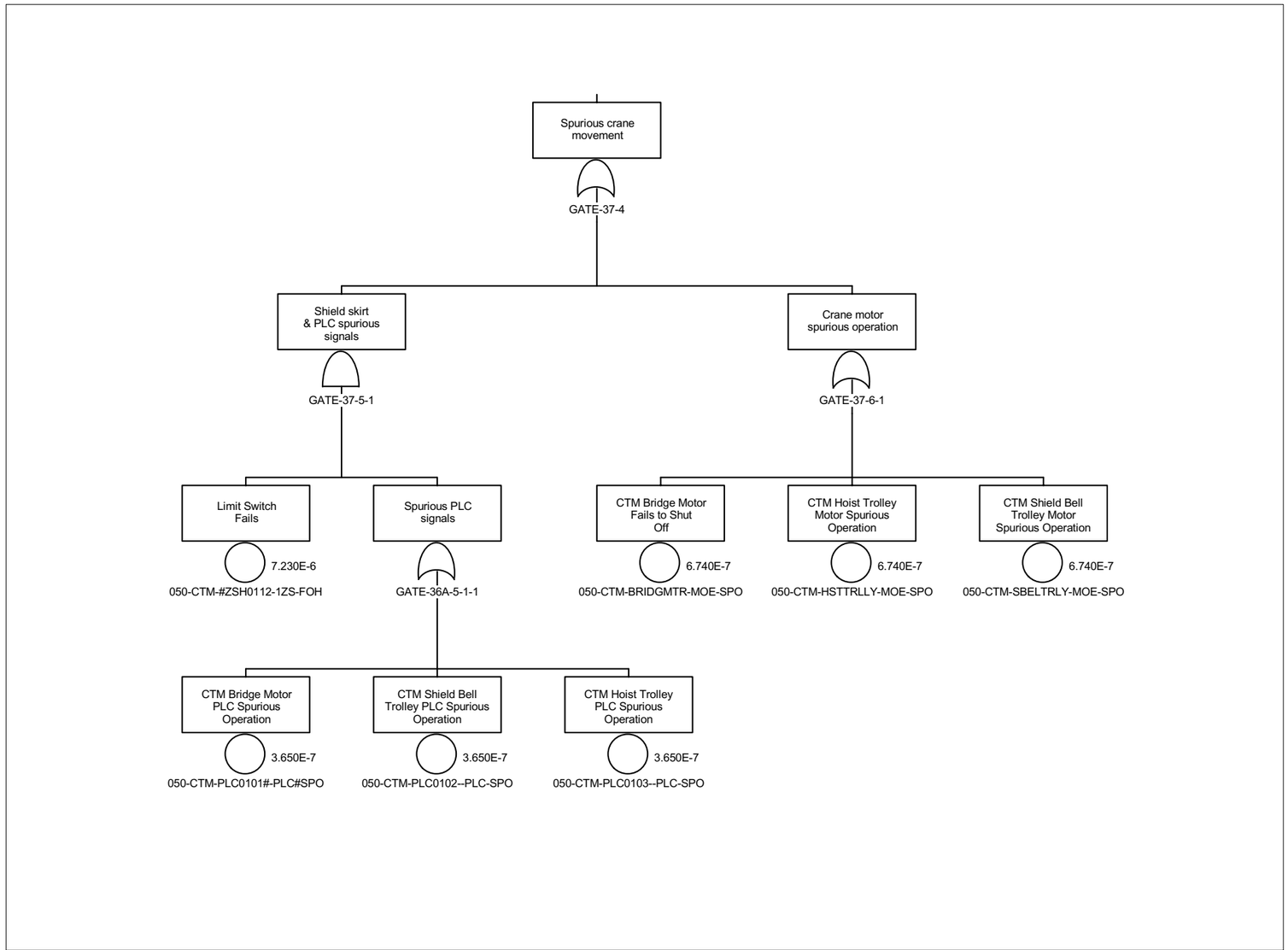
Source: Original

Figure B4.4-36. Drop of Object onto Cask
Sheet 13



Source: Original

Figure B4.4-37. Drop of Object onto Cask
Sheet 14



Source: Original

Figure B4.4-38. Spurious Crane Movement

B4.4.4 Canister Impacts

B4.4.4.1 Description

CTM movements that could result in a collision were modeled. Collisions between the CTM and a permanent structure were considered.

B4.4.4.2 Success Criteria

Success criteria for the CTM is simply the prevention of a collision between the canister and the shield bell or Canister Transfer Room floor from any cause during the lift, lateral movement, and lower portions of the canister transfer.

B4.4.4.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.

- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.

- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.

- An interlock between the slide gate and shield skirt–the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed, to allow the CTM to move with the slide gate open during lid removal.

- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard wired interlocks are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end-of-travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.4.4 Fault Tree Model

The top event in this fault tree is "CTM collision." The CTM collision fault tree addresses potential end of run over travel events and collisions between the two CTMs. Faults considered in the evaluation of this top event include: human events that contribute to a collision and mechanical (structural) failures of the CTM components. The interlocks intended to prevent improper CTM movement are included in the model.

B4.4.4.5 Basic Event Data

Table B4.4-9 contains a list of basic events used in the CTM fault tree. Included are the HFEs and the CCF events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

Table B4.4-9. Basic Event Probability for the CTM Collision Fault Tree

Name	Description	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	3	1.949E-006	0.000E+000	4.450E-010	4.380E+003
050-CTM-BRIDGETR-MOE-FSO	CTM Shield Skirt-Bridge motor Interlock Failure	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
050-CTM-BRIDGMTR-#CT-FOD	CTM bridge motor controller fails	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
050-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	1	3.990E-003	3.990E-003	0.000E+000	0.000E+000
050-CTM-TROLLEYT-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	3	1.949E-006	0.000E+000	4.450E-010	4.380E+003
050-CTM-TROLYCNT-#HC-FOD	Hand Held Remote Controller Failure to Stop (on Demand)	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-008	4.000E-008	0.000E+000	0.000E+000
050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into end stop	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
CTM = canister transfer machine; Calc = calculation.

Source: Original

The impact modeled by the fault tree is evaluated over a mission time of one hour. This mission time encompasses vertical lifting, lateral movement, and vertical lowering of the canister by the CTM. A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are tested. They are consequently evaluated over the interval of time between their test (i.e., mission time set to the average fault exposure time, one-half the test interval).

B4.4.4.5.1 Human Failure Events

Two basic events are associated with human error (Table B4.4-10). One addresses the movement of the CTM during a lift and the second addresses the potential overrun of the CTM (either the bridge trolley or the hoist/shield skirt trolley). The 050-OPCTIMPACT!-HFI-COD event was quantified considering human actions and the interlocks intended to prevent erroneous operator actions. The other event was quantified using screening HRA value.

Table B4.4-10. Human Failure Events

Name	Description
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor
050-OPCTMIMPACT5-HFI-COD	Operator overruns travel - collides into endstop

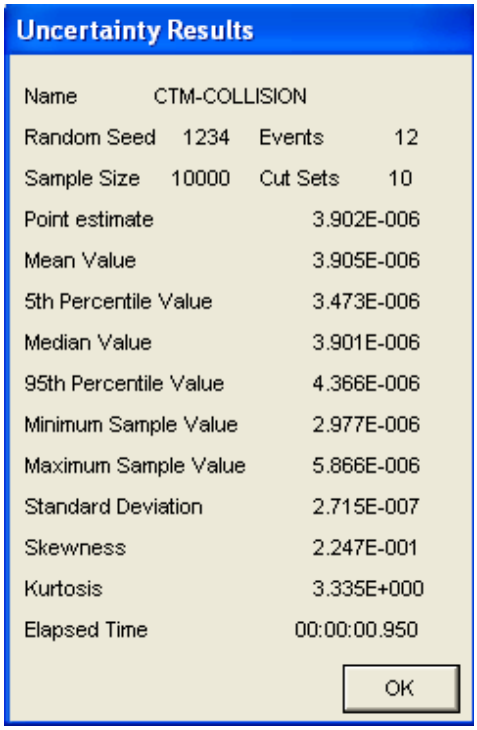
Source: Original

B4.4.4.5.2 Common-Cause Failures

There are no CCFs modeled in the CTM collision fault tree.

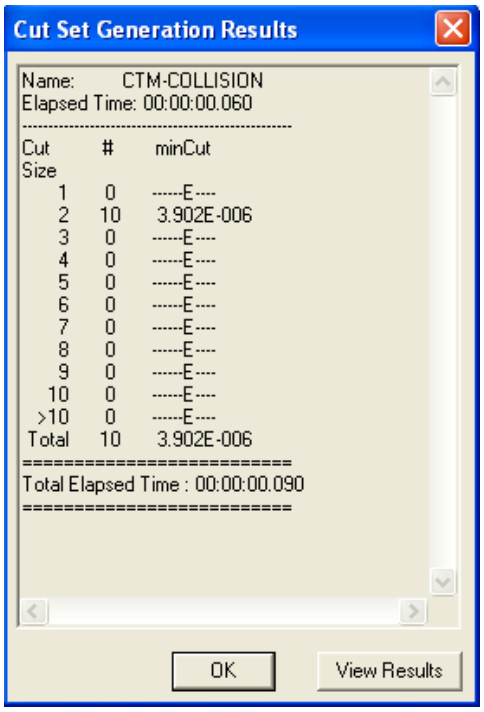
B4.4.4.6 Uncertainty and Cut Set Generation

Figure B4.4-39 contains the uncertainty results obtained from running the fault trees for the CTM collision using a cutoff at 1E-15. Figure B4.4-40 provides the cut set generation results for the CTM collision fault tree.



Source: Original

Figure B4.4-39. Uncertainty Results of the CTM Collision Fault Tree



Source: Original

Figure B4.4-40. Cut Set Generation Results for the CTM Collision Fault Tree

B4.4.4.7 Cut Sets

Table B4.4-11 contains the cut sets for the CTM collision fault tree.

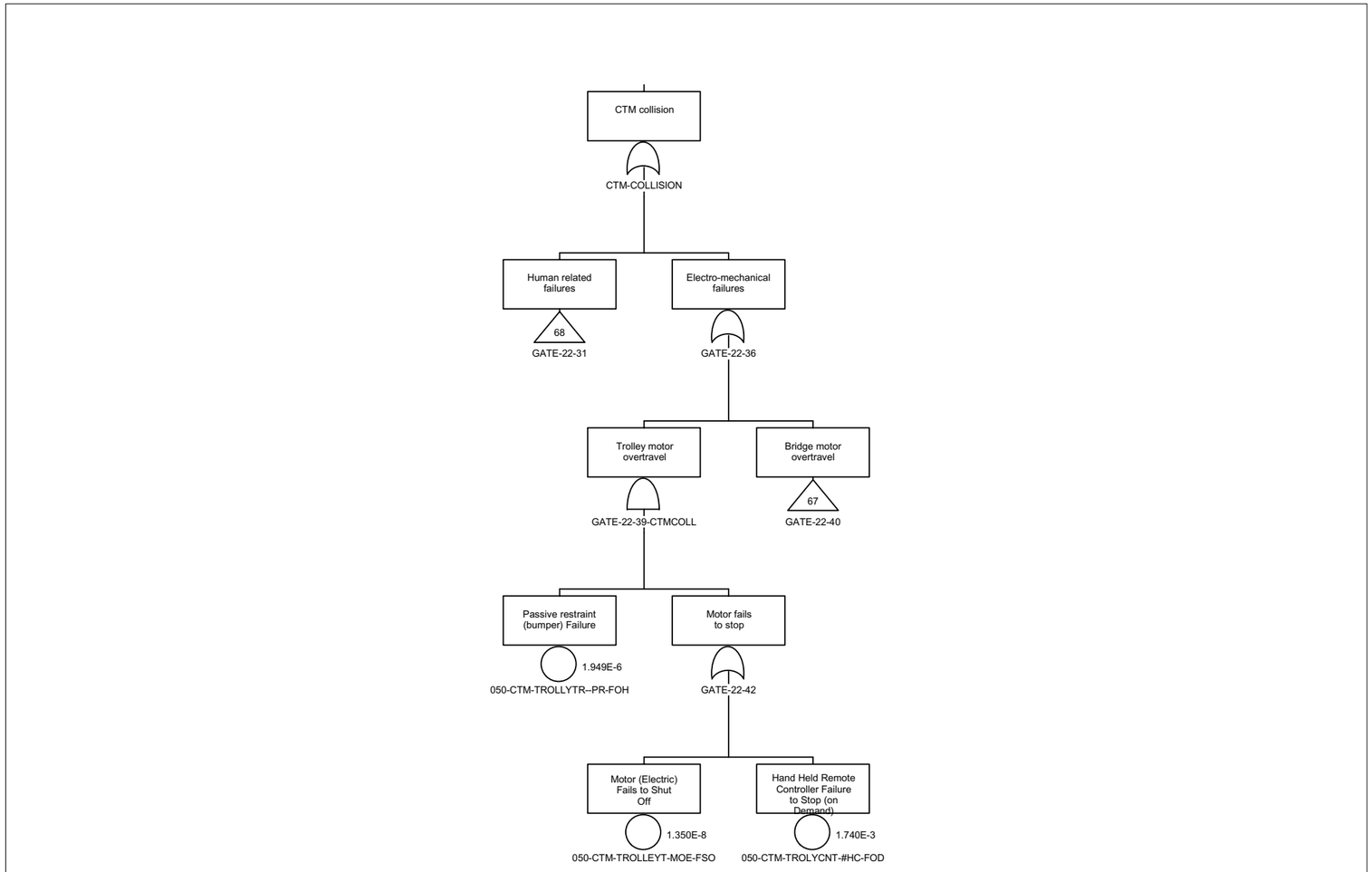
Table B4.4-11. Dominant Cut Sets for the CTM Collision Fault Tree

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
49.95	49.95	1.949E-006	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into endstop	1.000E+000
99.90	49.95	1.949E-006	050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into endstop	1.000E+000
99.99	0.09	3.391E-009	050-CTM-TROLLYTR--PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-TROLYCNT-#HC-FOD	Hand Held Remote Controller Failure to Stop (on Demand)	1.740E-003
99.99	0.00	1.596E-010	050-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	3.990E-003
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	7.796E-012	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-BRIDGMTR-#CT-FOD	CTM bridge motor controller fails	4.000E-006
99.99	0.00	1.100E-012	050-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	1.100E-012	050-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	1.100E-012	050-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.750E-005
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-008
99.99	0.00	2.631E-014	050-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-006
			050-CTM-BRIDGETR-MOE-FSO	CTM Shield Skirt-Bridge motor Interlock Failure	1.350E-008

NOTE: CTM = canister transfer machine.

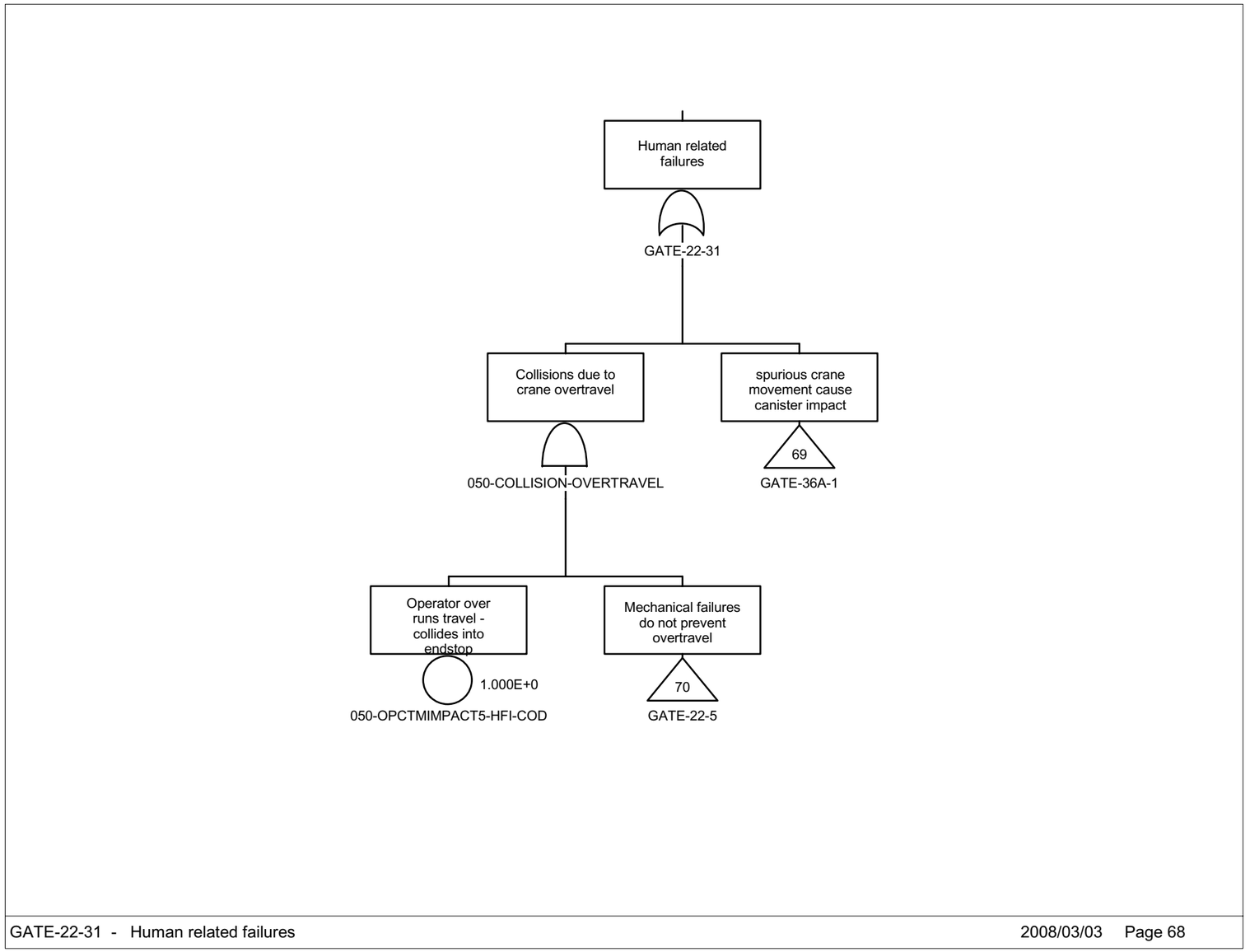
Source: Original

B4.4.4.8 Fault Trees



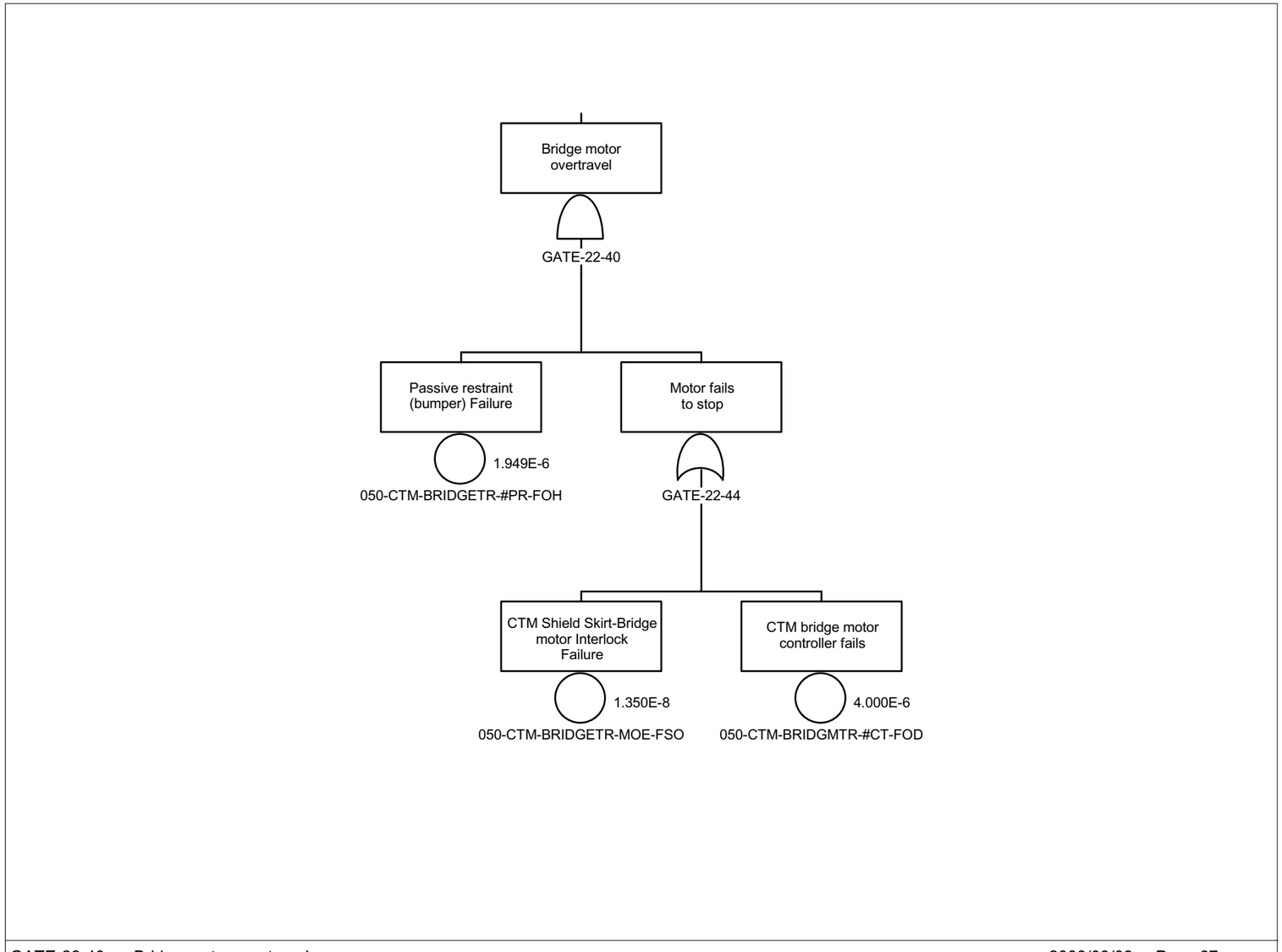
Source: Original

Figure B4.4-42. CTM Collision Sheet 1



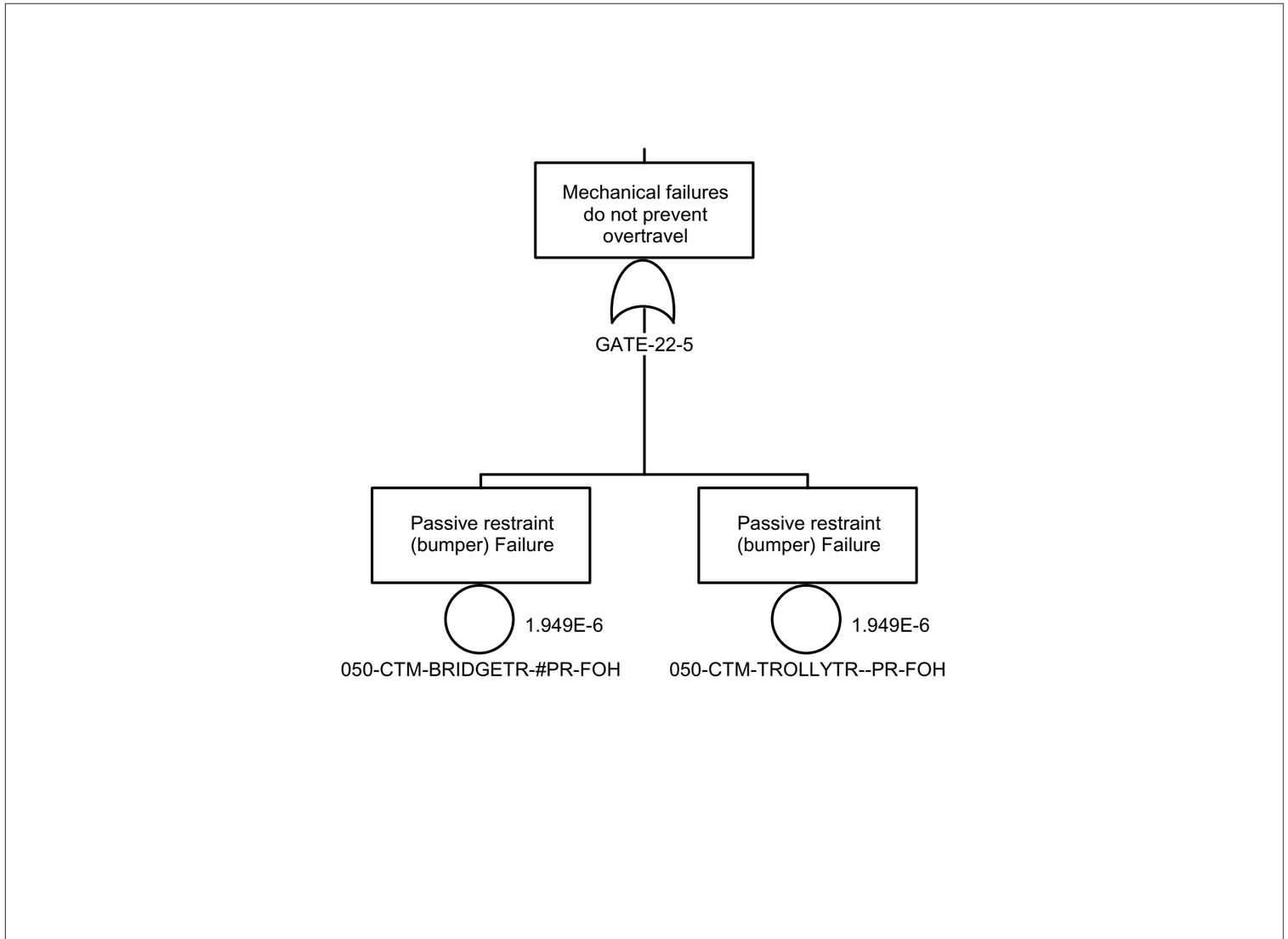
Source: Original

Figure B4.4-43. CTM Collision Sheet 2



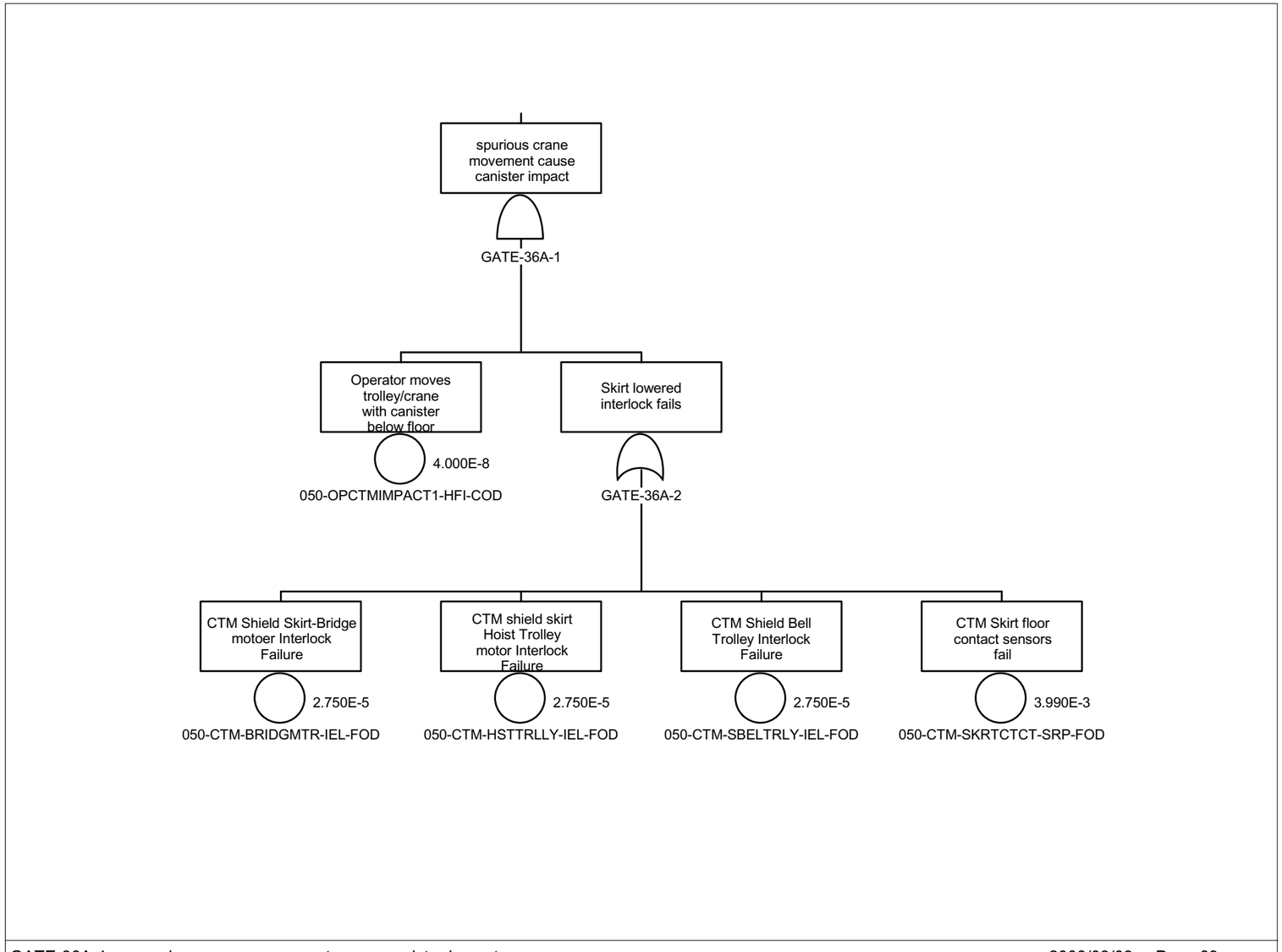
Source: Original

Figure B4.4-44. CTM Collision Sheet 3



Source: Original

Figure B4.4-45. CTM Collision Sheet 4



Source: Original

Figure B4.4-46. CTM Collision Sheet 5

B4.4.5 CTM Movement Subjects Canister to Shearing Forces

B4.4.5.1 Description

A fault tree was developed to address the potential for movement of the CTM when the canister being transferred is being lifted and is between the WHF floors. Movement initiated by the bridge or trolley motors could result in shear forces being applied to the canister should it be lifted when the CTM moves away from the floor port opening.

B4.4.5.2 Success Criteria

Success criteria for the CTM is the prevention of CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the WHF during the lift portions of the canister transfer.

B4.4.5.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, will stop the hoist and erase the lift command (can only lower hoist). This interlock is used only when lifting a canister.
- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.
- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock.
- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.
- An interlock between the slide gate and shield skirt–the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed to allow the CTM to move with the slide gate open during lid removal.
- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.
- The load cells cut off power to the hoist when the crane capacity is exceeded.

- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 feet per minute, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister.

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard wired interlocks are used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end-of-travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.5.4 Fault Tree Model

The top event in this fault tree is "CTM Movement Causes Canister Shear." The fault tree includes events (mechanical control failures and human actions, considered in conjunction with the interlocks intended to prevent the erroneous human action) that can initiate a spurious movement of the CTM trolley or bridge while the canister is between the first and second floors of the WHF.

B4.4.5.5 Basic Event Data

Table B4.4-13 contains a list of basic events used in the "CTM Shear" fault tree. Included are the HFEs and the CCF events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTMs will not be in service while they are undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability.

The shear impact probability modeled by the fault tree is evaluated over a mission time of one-tenth of an hour (limited to the time the canister is being lifted and is between the first and second floors). A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are tested. They are consequently evaluated over the interval of time between their tests, and the mission time is assigned a value of the average fault exposure time, half the test interval.

Table B4.4-13. Basic Event Probability for the CTM Fault Trees

Name	Description	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01
050-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01
050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
050-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3	3.650E-08	0.000E+00	3.650E-07	1.000E-01
050-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation - shear	3	3.650E-08	0.000E+00	3.650E-07	1.000E-01
050-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -shear	3	3.650E-08	0.000E+00	3.650E-07	1.000E-01
050-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01
050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	0.000E+00	0.000E+00
050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	3	7.230E-06	0.000E+00	7.230E-06	0.000E+00
050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
CTM = canister transfer machine; PLC = programmable logic controller; Calc = calculation.

Source: Original

B4.4.5.5.1 Human Failure Events

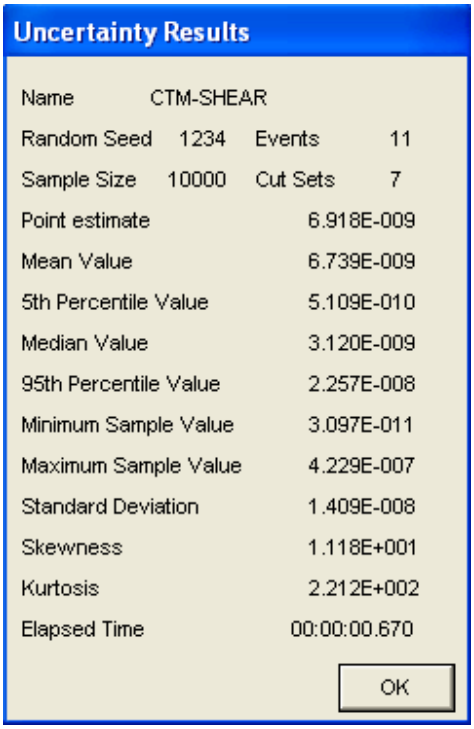
One basic event is associated with human error: 050-OPCTMIMPACT1-HFI-COD (operator moves trolley/crane with canister below floor). This event addresses the possible operator initiated movement of the bridge or trolleys while a canister is being lifted and is between WHF floors. This event was quantified using a detailed HRA that includes the human actions and the operation of interlocks intended to prevent erroneous actions.

B4.4.5.5.2 Common-Cause Failures

No CCFs apply to this fault tree.

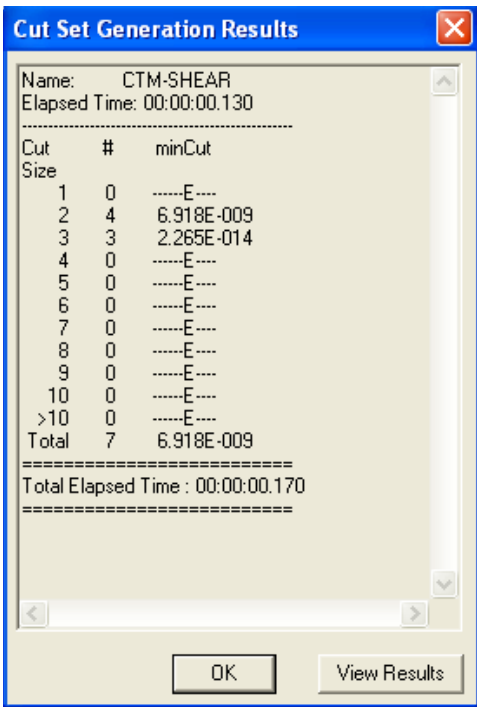
B4.4.5.6 Uncertainty and Cut Set Generation

Figure B4.4-49 contains the uncertainty results obtained from running the fault trees for the CTM-SHEAR using a cutoff at 1E-15. Figure B4.4-50 provides the cut set generation results for the CTM-SHEAR fault tree.



Source: Original

Figure B4.4-49. Uncertainty Results of the CTM Shear Fault Tree



Source: Original

Figure B4.4-50. Cut Set Generation Results for the CTM Shear Fault Tree

B4.4.4.7 Cut Sets

Table B4.4-14 contains the cut sets for the CTM shear fault tree.

Table B4.4-14. Dominant Cut Sets for the CTM Collision Fault Tree

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
27.83	27.83	1.925E-09	050-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	6.740E-08
			050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.856E-02
55.66	27.83	1.925E-09	050-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	6.740E-08
			050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.856E-02
83.49	27.83	1.925E-09	050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			050-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	6.740E-08
100.00	16.52	1.143E-09	050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.856E-02
			050-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.000E-08

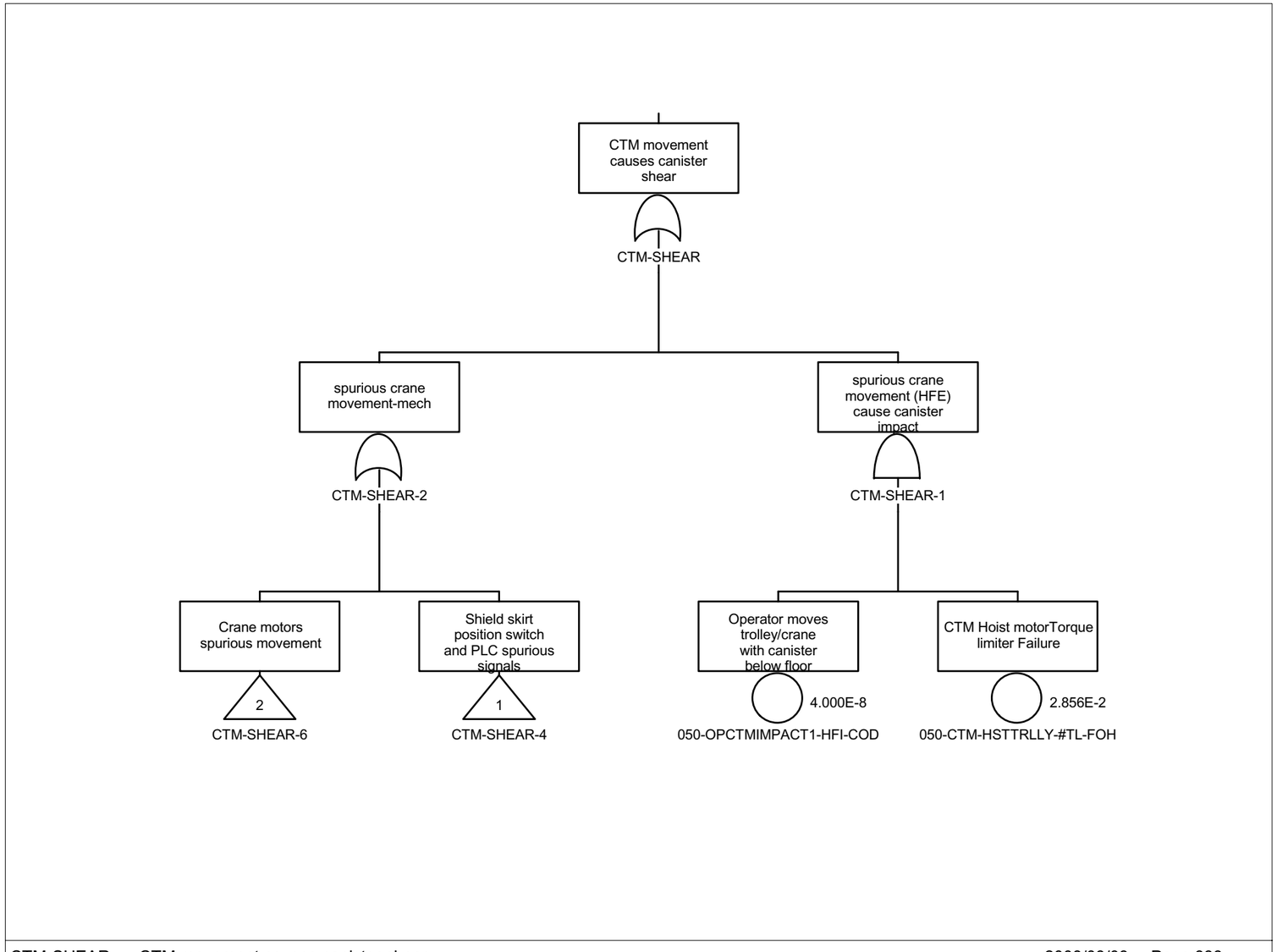
Table B4.4-14. Dominant Cut Sets for the CTM Collision Fault Tree (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
100.00	0.00	7.538E-15	050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	7.230E-06
			050-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			050-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3.650E-08
100.00	0.00	7.538E-15	050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	7.230E-06
			050-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.856E-02
			050-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -shear	3.650E-08
100.00	0.00	7.538E-15	050-CTM-#ZSH0112-1ZS-FOH	Limit Switch Fails	7.230E-06
			050-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3.650E-08
			050-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.856E-02

NOTE: CTM = canister transfer machine; PLC = programmable logic controller.

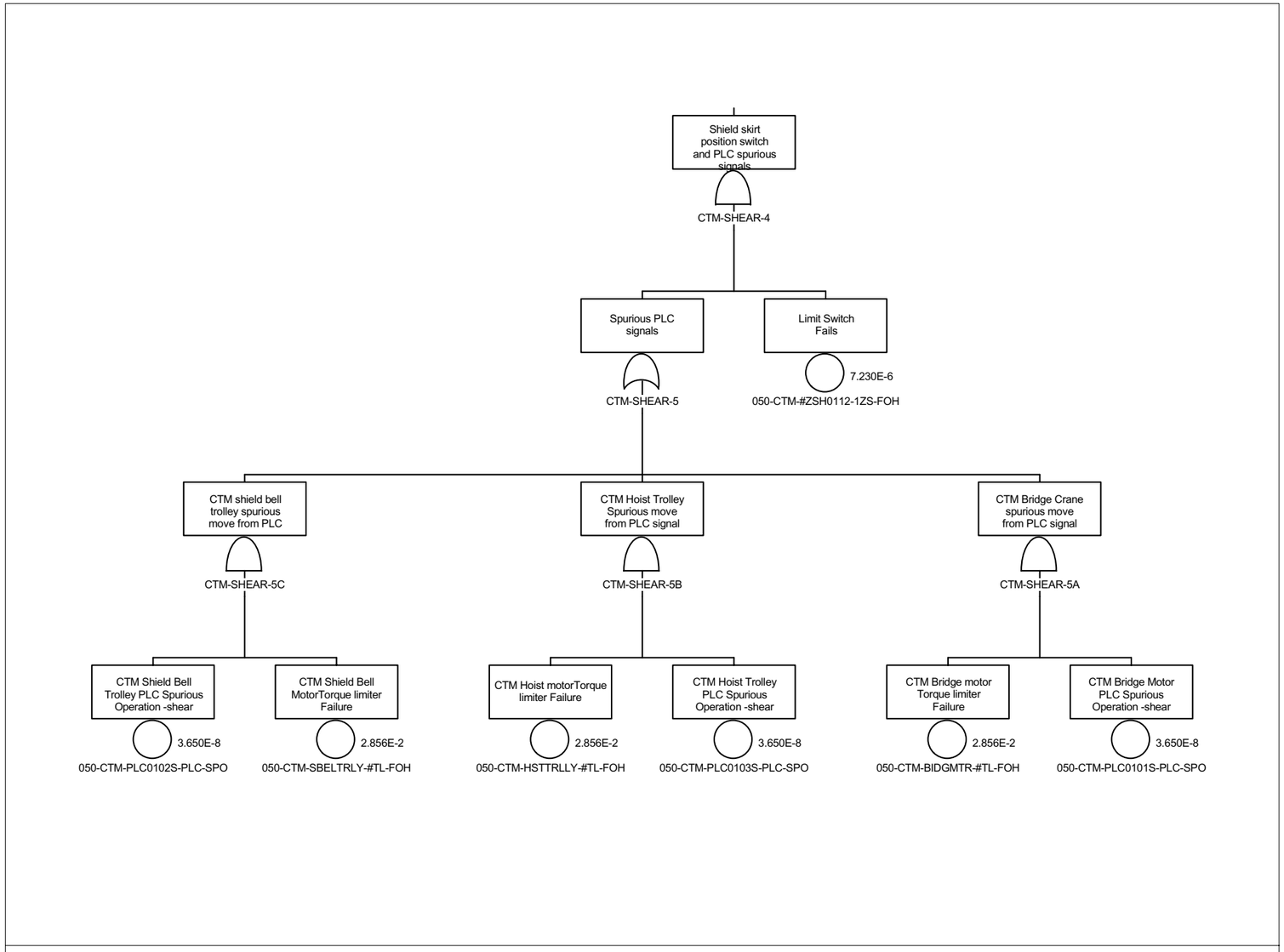
Source: Original

B4.4.5.8 Fault Tree



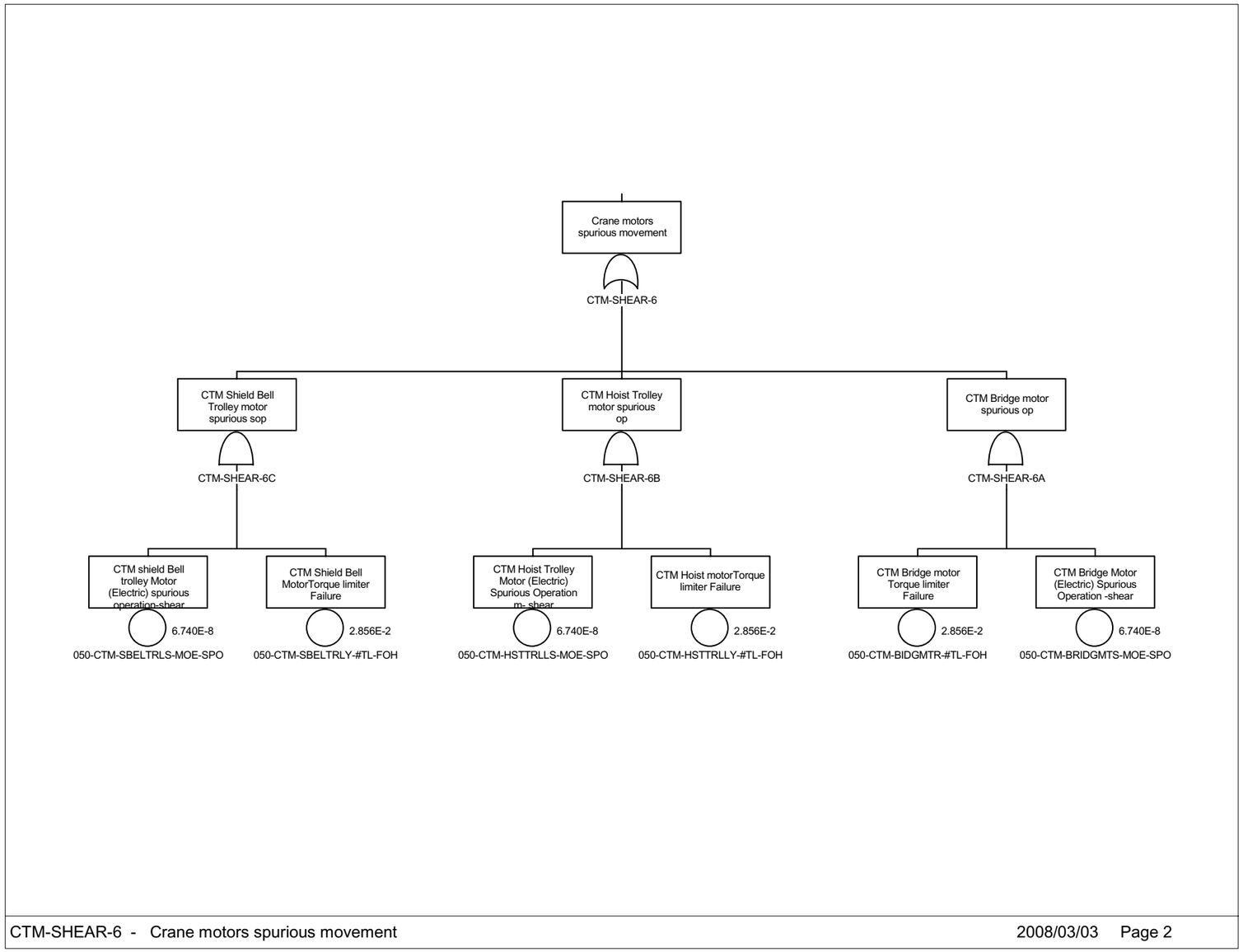
Source: Original

Figure B4.4-51. CTM Shear Sheet 1



Source: Original

Figure B4.4-52. CTM Shear Sheet 2



Source: Original

Figure B4.4-53. CTM Shear Sheet 3

B5 CASK COOLING SYSTEM– FAULT TREE ANALYSIS

B5.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B5.1.1 *BSC (Bechtel SAIC Company) 2007. *Cask and Canister Cooling System Calculation.* 050-M0C-MRC0-00100-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071030.0009.

B5.1.2 *BSC 2007. *Wet Handling Facility Preparation Station #1 Cask Cooling System Piping & Instrument. Diagram.* 050-M60-MRC0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071218.0015.

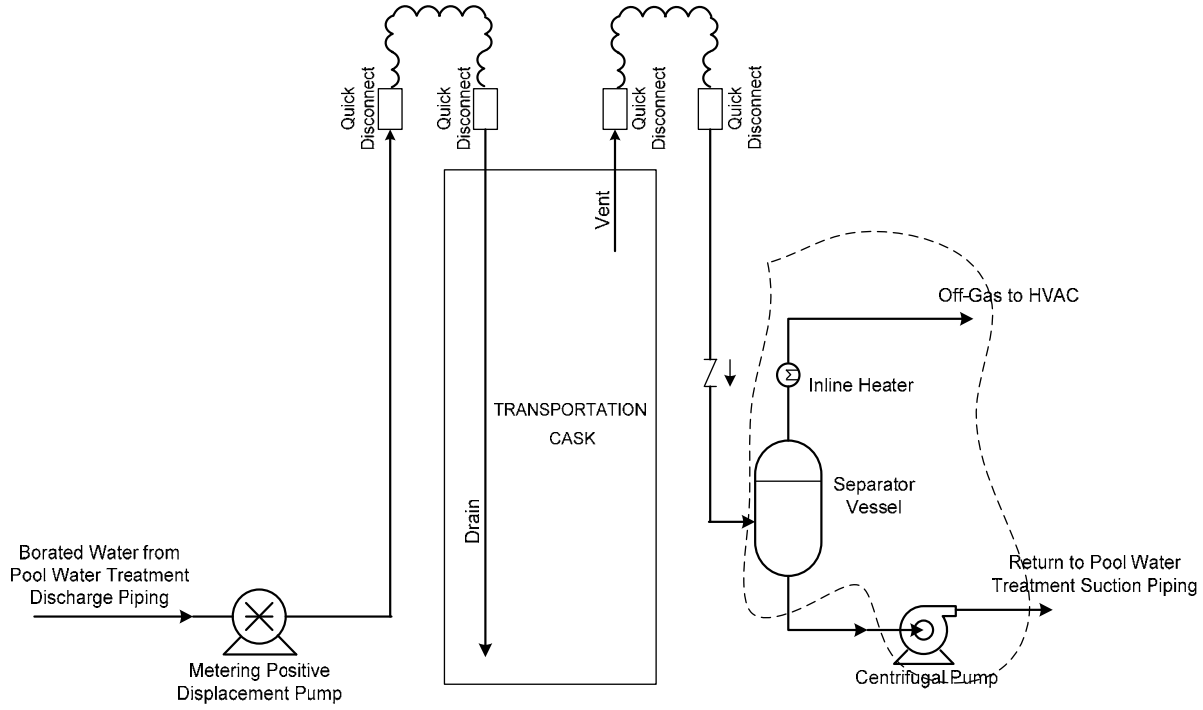
B5.2 CASK COOLING DESCRIPTION

B5.2.1 System Description

The cask cooling system, Figure B5.2-1, is a pump driven system that will be used to cool casks by introducing borated water into the cask. The system consists of two motor-driven pumps, a pressure relief valve, two interlocks, water piping, four quick disconnects, two sections of flexible tubing, and a separator vessel (Ref. B5.1.1).

The pumps serve to direct water from the pool, into the cask, and back to the pool. The positive displacement pump drives water out of the pool and into the cask, while the centrifugal pump directs water out of the cask and back into the pool for reuse. Borated water is injected via the drain pipe which is below the bottom of the spent fuel assemblies. Steam leaves the cask through the vent piping.

The water delivery and removal systems consist of a series of pipes, tubing, and quick disconnects. The flexible tubing connects the supply and return piping to the cask, with connections provided by quick disconnects. System piping runs from the pool to the flexible tubing which supplies the cask, and from the cask return to the separator vessel.



Source: Modified from Ref. B5.1.2.

Figure B5.2-1. Cask Cooling System (Components within dashed line added for completeness)

Two lines of piping follow out of the separator vessel: one provides water for treatment and the other routing air to off-gas treatment. The separator vessel serves the purpose of separating air and water delivered from the cask.

B5.2.2 Operations

The cask handling crane places the cask into the preparation station. At the preparation station, the gas sampling port is opened and the drain valve and drain port cover plates are removed. The borated water line is connected to the drain port, and the vent line is connected to the gas sampling port. Borated water is then introduced into the cask as the steam is vented. Once the cask is satisfactorily cooled, the lines are disconnected, and the cover plates are reinstalled.

B5.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B5.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B5.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies & Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Interlocks	Senses HI-HI water level and shuts down pump (Non-ITS)	—	—	Error point set too high	—
Positive Displacement Pump	Pumps water into the cask	—	—	Pump rate set too high	—
Flex lines and quick disconnects	Directs and contains water flowing into and out of the cask	—	—	—	Rupture or break of the line
Piping lines	Directs and contains water flowing into and out of the cask	—	—	—	Rupture or break of the line

Source: Original

B5.4 CASK RELATED FAILURE SCENARIOS

There are two fault trees associated with the cask cooling system:

1. Break of non-pressurized sample line.
2. Cask over-pressurization

Table B5.4-1 provides a cross reference between the ESD and the fault trees that support them.

Table B5.4-1. ESD Cross Reference with Cask Cooling Fault Trees

WHF ESD Number	Fault Tree	Non-pressurized leak	Overpressurization
WHF-ESD16-CSNF	ESD16-PREP-OVERPRESSURE		X
WHF-ESD16-CSNF	ESD16-PREP-SAMPLE	X	
WHF-ESD17-DPC	ESD17-PREP-OVERPRESSURE		X
WHF-ESD17-DPC	ESD17-PREP-SAMPLE	X	X

Source: Original

B5.4.1 Break of Non-pressurized Sample Line

B5.4.1.1 Description

The cask cooling fault tree describes the break of a non-pressurized sample line during cask cooling to satisfy WHF-ESD16-CSNF and WHF-ESD17-DPC, initiating event “Sampling line break.” The top event is “Release During DPC Sampling” which is defined as the break of a sample line while the cask is being cooled. This fault tree is shown in Figures B5.4-3 through B5.4-5. The top event is “Release During CSNF Sampling” is described by identical fault trees which are not replicated here.

Breaks that can impact the release of contaminated water/steam are between the gas sampling port and separator vessel. This includes the two quick disconnects, flex line, and piping. The quick disconnect at the gas sampling port cannot fail independently of a clapper closure failure.

B5.4.1.2 Success Criteria

Success criteria for cooling a cask using borated water requires the contaminated water to remain contained.

Before filling the cask, the positive displacement pump is set to pump at a pre-determined rate based on the cask type. Should this pump allow a higher flow rate than determined, there exists a potential for contaminated water to breach the system due to cask over pressurization. Similarly, failure of the centrifugal pump also has the potential to lead to the release of contaminated water.

During the cask cooling process, a breach of any of the piping or tubing (including quick disconnects) venting the cask would result in a release of contaminated steam. Blockages of the same piping or tubing can result in a release due to over-pressurization of the cask.

The pump failures and blockages which can cause cask over pressurization are controlled by a pressure relief valve. In the advent of an overpressure condition, the pressure relief valve relieves the pressure

B5.4.1.3 Design Features and Requirements

A pressure relief valve shall remedy a cask overfilling or over-pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition.

B5.4.1.4 Fault Tree Model

The fault tree in Figures B5.4-3 and B5.4-4 show two types of non-pressurized breaches or ruptures that can cause release from the cask cooling system:

1. Ruptures or leaks in discharge piping downstream of the cask.
2. Ruptures or leaks in the quick disconnect valves or flex piping.

The most likely failure of the flex piping is a disconnection from the quick disconnect valve. Ruptures or leaks are single point failures with the exception of a rupture of flex piping downstream of quick disconnect valve 01 that is attached directly to the vent line. In this case, the quick disconnect valve would close (check) and isolate the leak. This checking action must also fail to cause a leak.

B5.4.1.5 Basic Events Data

Table B5.4-2 contains a list of basic events used in the fault tree for a sample line break (non-pressurized).

Table B5.4-2. Basic Event Probabilities for a Sample Line Break Non-Pressurized

Name	Calc Type	Calculation Probability	Failure Probability	Lambda	Mission time
050-CCS-CSKVLV1-CKV-FOD	1	6.62E-04	6.62E-04	0.00E+00	0.00E+00
050-CCS-DRNHOSE-HOS-RUP	3	1.48E-06	0.00E+00	1.48E-06	8.00E+00
050-CCS-DRNQD01-QDV-FOH	3	4.26E-06	0.00E+00	4.26E-06	1.00E+00
050-CCS-DRNQD02-QDV-FOH	3	4.26E-06	0.00E+00	4.26E-06	1.00E+00
050-CCS-PIPBW03-PPL-RUP	3	3.54E-06	0.00E+00	4.42E-07	8.00E+00
050-CCS-PIPBW04-PPL-RUP	3	3.54E-06	0.00E+00	4.42E-07	8.00E+00
050-CCS-PIPBW05-PPL-RUP	3	3.54E-06	0.00E+00	4.42E-07	8.00E+00
050-OPSAMPLEREL2-HFI-NOD	1	5.000E-003	5.000E-003	0.00E+00	0.00E+00

Source: Original

B5.4.1.5.1 Human Failure Events

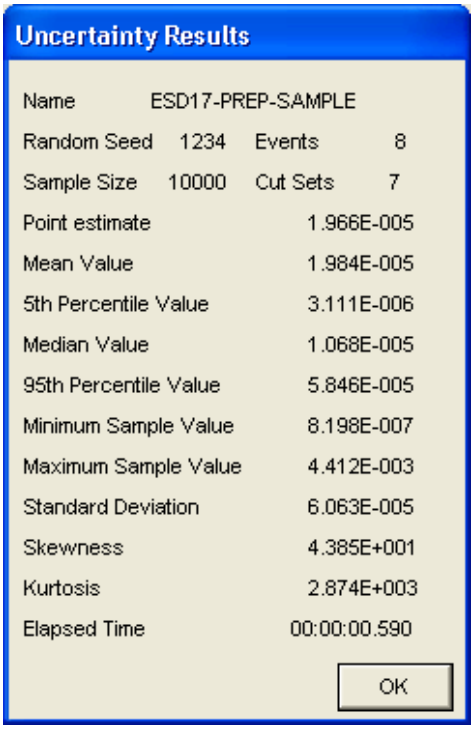
There is one human failure event involving operator release of material from the sample line.

B5.4.1.5.2 Common-Cause Failures

There is no common-cause failure event associated with this fault tree.

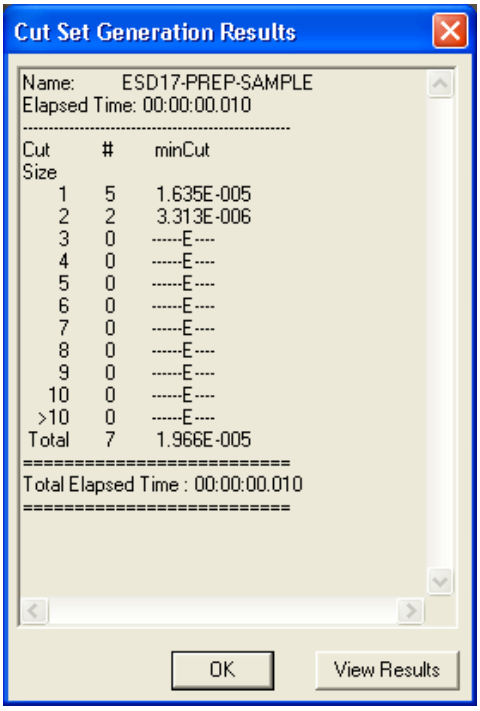
B5.4.1.6 Uncertainty and Cut Set Generation Results

Figure B5.4-1 contains the uncertainty results obtained from running the fault trees for a sample line break. Figure B5.4-2 provides the cut set generation results for a sample line break.



Source: Original

Figure B5.4-1. Uncertainty Results of the Sample Line Break Non-Pressurized



Source: Original

Figure B5.4-2. Cut Set Generation Results for a Sample Line Break Non-Pressurized

B5.4.1.7 Cut Sets

Table B5.4-3 contains the cut sets for a non-pressurized sample line during cask cooling. The total probability per cask is 1.75E-04.

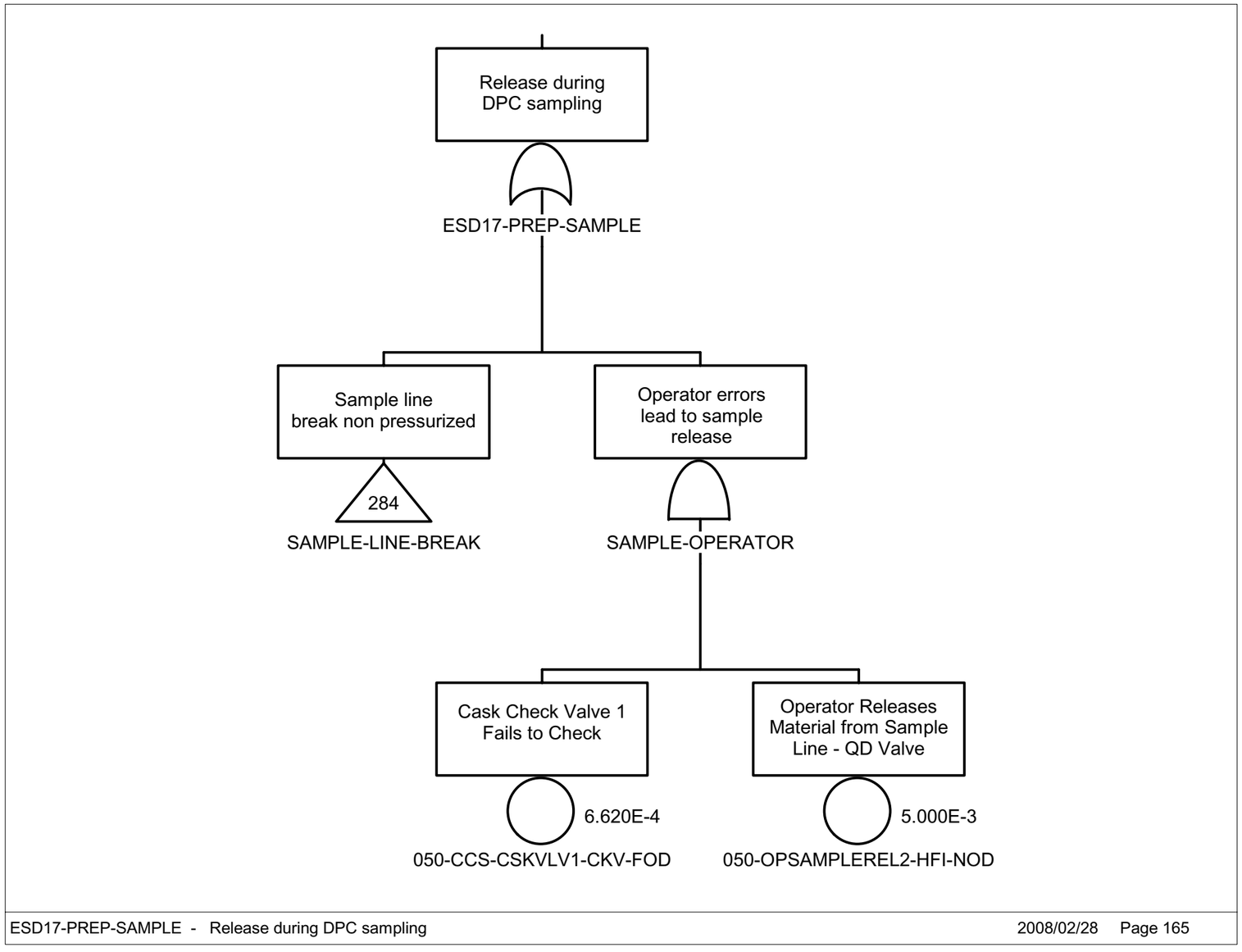
Table B5.4-3. Cut Sets for a Non-Pressurized Sample Line Break

Fault Tree	% Cut Set	Prob./Freq.	Basic Event	Description	Probability
ESD17-PREP-SAMPLE	21.67	4.260E-006	050-CCS-DRNQD01-QDV-FOH	Cask cooling QD Valve Fails	4.260E-006
	17.99	3.536E-006	050-CCS-PIPBW03-PPL-RUP	Drain Piping Catastrophic - Line BW-0003	3.536E-006
	17.99	3.536E-006	050-CCS-PIPBW04-PPL-RUP	Drain Piping Catastrophic - Line BW-0004	3.536E-006
	17.99	3.536E-006	050-CCS-PIPBW05-PPL-RUP	Drain Piping Catastrophic - Line BW-0005	3.536E-006
	16.84	3.310E-006	050-CCS-CSKVLV1-CKV-FOD	Cask Check Valve 1 Fails to Check	6.620E-004
			050-OPSAMPLEREL2-HFI-NOD	Operator Releases Material from Sample Line - QD Valve	5.000E-003
	7.53	1.480E-006	050-CCS-DRNHOSE-HOS-RUP	Cask Cooling Drain Hose Ruptures	1.480E-006
	0.01	2.820E-009	050-CCS-CSKVLV1-CKV-FOD	Cask Check Valve 1 Fails to Check	6.620E-004
			050-CCS-DRNQD02-QDV-FOH	Cask cooling QD 02 Valve Fails	4.260E-006

Source: Original

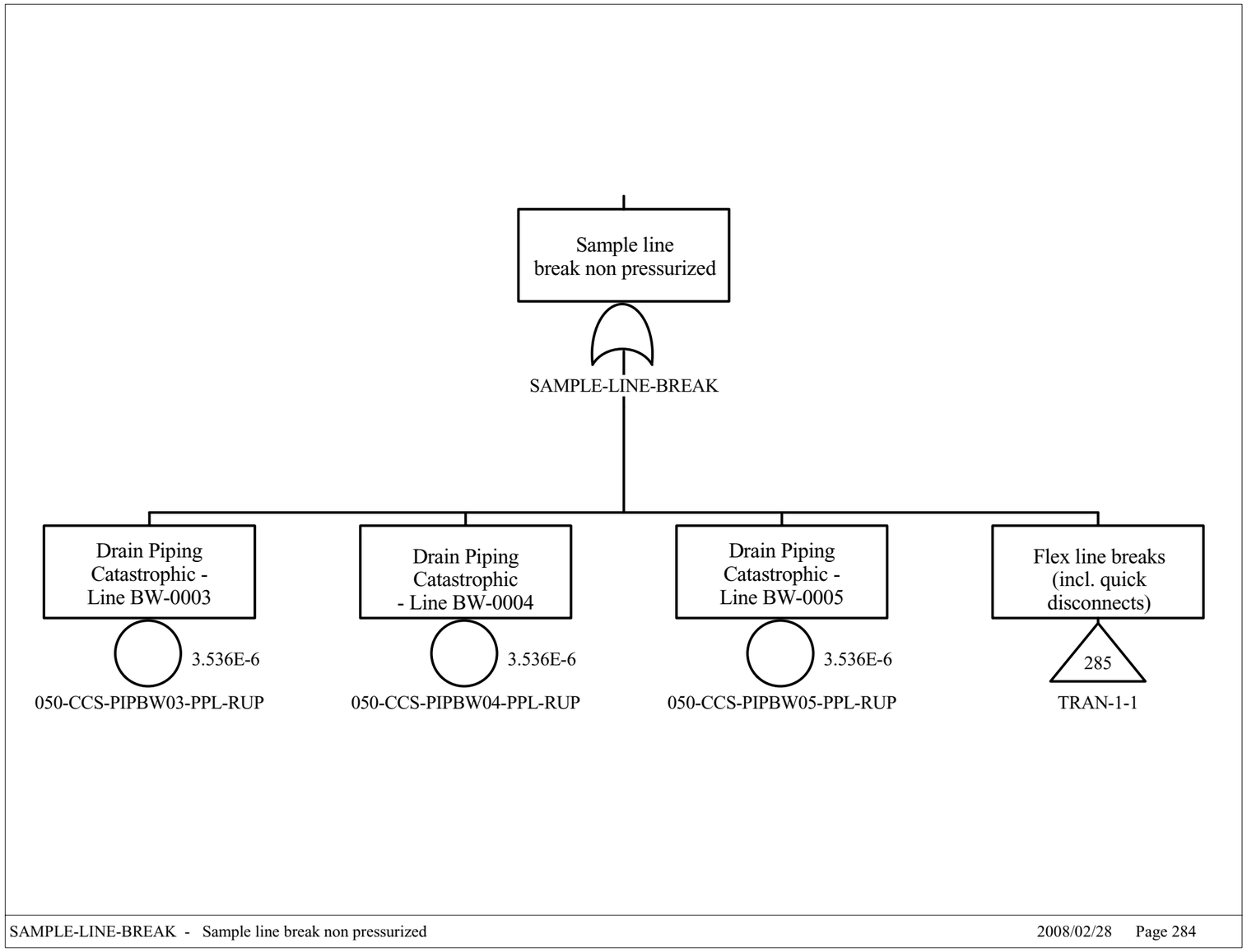
B5.4.1.8 Fault Tree

Figures B5.4-3 through B5.4-5 display the Fault Trees for a Non-Pressurized Sample Line Break.



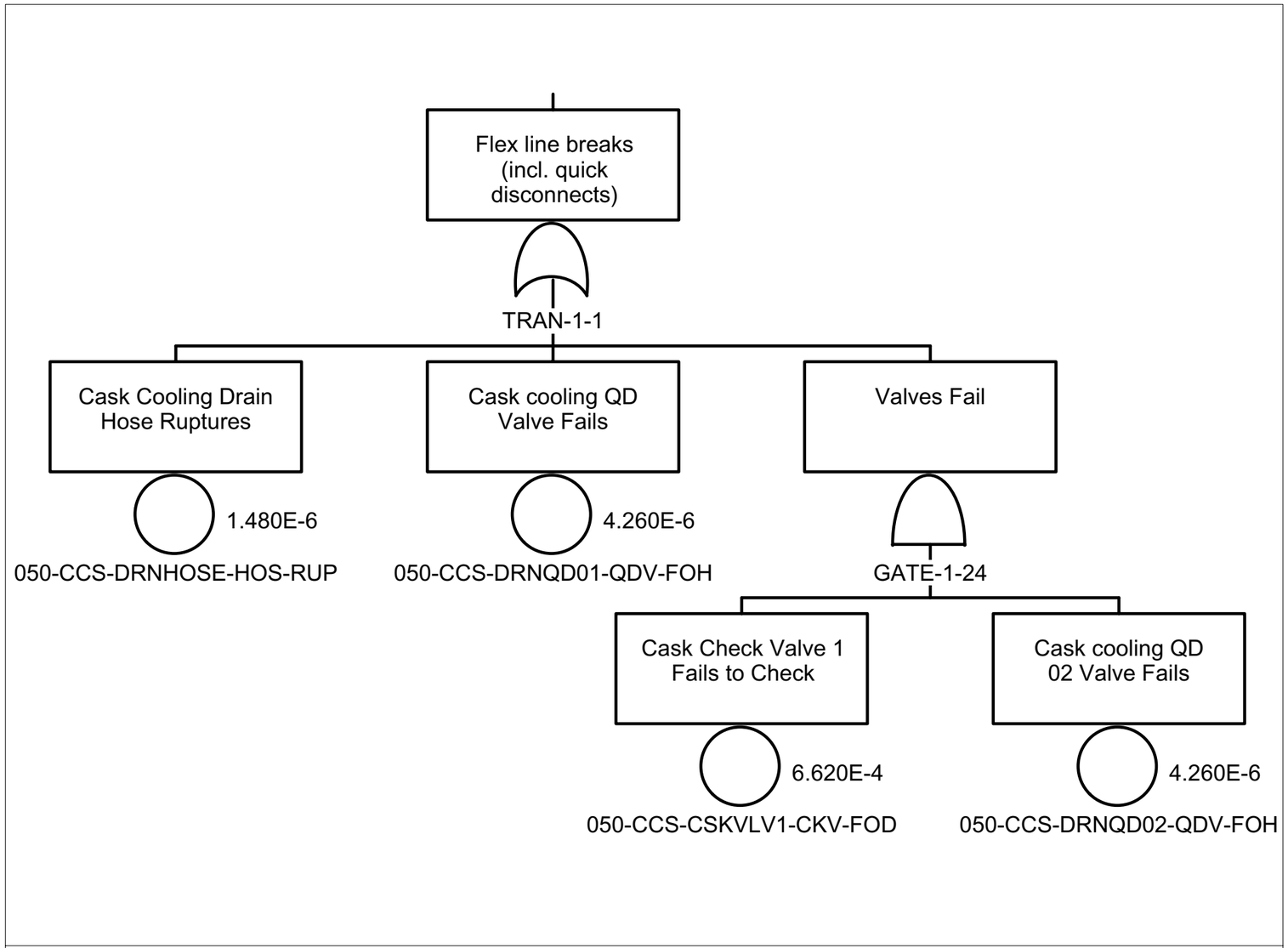
Source: Original

Figure B5.4-3. Fault Tree for a Non-Pressurized Sample Line Break



Source: Original

Figure B5.4-4. Sample Line Break



Source: Original

Figure B5.4-5. Fault Tree for a Non-Pressurized Sample Line Break (Transfer 1-1)

B5.4.2 Cask Over Pressurization

B5.4.2.1 Description

This fault tree describes the over pressurization of the cask to satisfy WHF-ESD16-CSNF and WHF-ESD17-DPC, initiating event "Over pressurization of canister." The top event is "cask/sample line over pressurized" which is defined as the abundance of pressure in the cask or sample line resulting in an unplanned escape of water into the facility during cask cooling. This fault tree is shown in Figures B5.4 -8 and B5.4-9.

The existence of an excess of pressure is caused by an excess of water introduced into the cask and a failure to reduce this excess. The existence of excess water can be caused by the metering pump running too fast, a blockage in piping, or the failure of the venting pump to run.

B5.4.2.2 Success Criteria

A pressure relief valve shall be part of the system as a final resource to remedy a cask overfilling or over pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition[1].

B5.4.2.3 Design Features and Requirements

A pressure relief valve shall remedy a cask overfilling or over-pressurization failure. This valve is physically activated by the presence of excess pressure, causing the valve to open and relieve the over-pressure condition. Mission time is set to eight (8) hours which equates to nominal DPC cooling time.

B5.4.2.4 Fault Tree Model

The fault trees in Figures B5.4-8 through B5.4-9 show two types of pressurized breaches or ruptures can cause release from the cask cooling system:

1. Operator error initiated over pressurization.
2. Mechanical failure initiated over pressurization.

For both of these events, failure of the pressure relief valve is considered as a preventative measure in relieving overpressure.

[1] There are two interlocks in this system to control the positive displacement pump, should an excess of water be detected. One interlock detects a high level of water entering the cask and the other interlock detects a high level of water leaving the cask. In either case, the interlock is designed to shut down the pump which delivers water to the cask. However, these interlocks depend upon PLCs and are not credited in the fault tree analysis. The pressure relief valve is the only credited safety feature.

B5.4.2.5 Basic Events Data

Table B5.4-4 contains a list of basic events used in the fault tree for cask/sample line over pressurization.

Table B5.4-4. Basic Event Probabilities for Over pressurization

Name	Calc Type	Calculation Probability	Failure Probability	Lambda	Mission time
050-CCS-PIPBLK3-PPM-PLG	3	5.81E-06	0.00E+00	7.26E-07	8.00E+00
050-CCS-PLCSPUR-PLC-SPO	3	2.92E-06	0.00E+00	3.65E-07	8.00E+00
050-CCS-PMTRFST-MSC-FOH	3	1.02E-03	0.00E+00	1.28E-04	8.00E+00
050-CCS-PUMPSTP-PMD-FTR	3	2.76E-04	0.00E+00	3.45E-05	8.00E+00
050-CCS-RLFVLVF-PRV-FOD	1	6.54E-03	6.54E-03	0.00E+00	0.00E+00
050-CCS-THVLVFL-NZL-FOH	3	2.28E-05	0.00E+00	2.85E-06	8.00E+00
050-OPDPC-OVP01-HFI-NOW	1	7.00E-08	7.00E-08	0.00E+00	0.00E+00

Source: Original

B5.4.2.5.1 Human Failure Events

There is one human failure event associated with this fault tree—050-OPDPC-OVPR01-HFI-NOD.

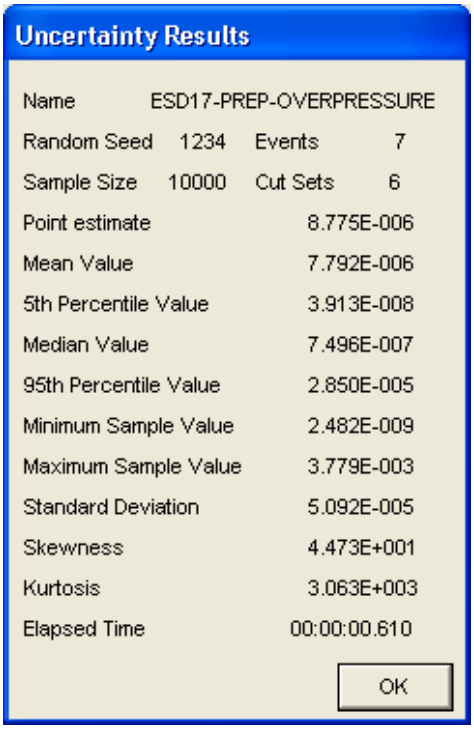
As described in detail in Attachment E, this HFE addresses potential failures during operator preparation activities when the DPC is filled and flushed with water to prevent a crud burst when put into the pool.

B5.4.2.5.2 Common Cause Failures

There is no common cause failure event associated with this fault tree.

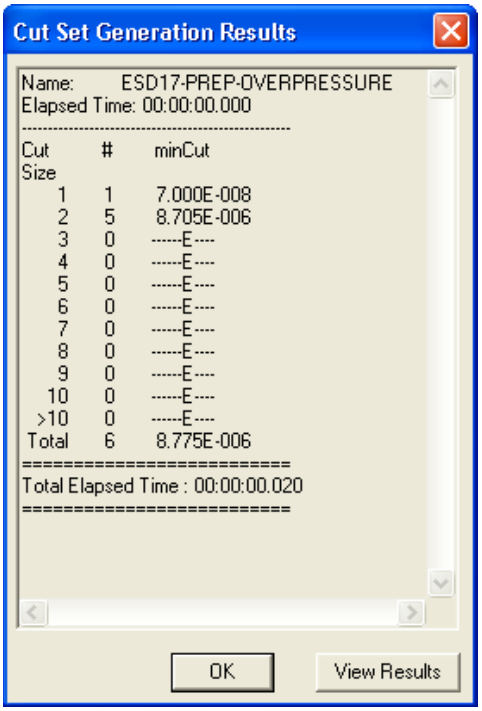
B5.4.2.6 Uncertainty and Cut set Generation Results

Figure B5.4-6 contains the uncertainty results obtained from running the fault trees for cask/sample line over pressurization. Figure B5.4-7 provides the cut set generation results for a sample line break.



Source:

Figure B5.4-6. Uncertainty Results of the Sample Line Break Overpressurized



Source:

Figure B5.4-7. Cut Set Generation Results for a Sample Line Break Overpressurized

B5.4.2.7 Cut Sets

Table B5.4-5 contains the cut sets for cask/sample line over pressurization. The total probability per cask is 8.08E-6.

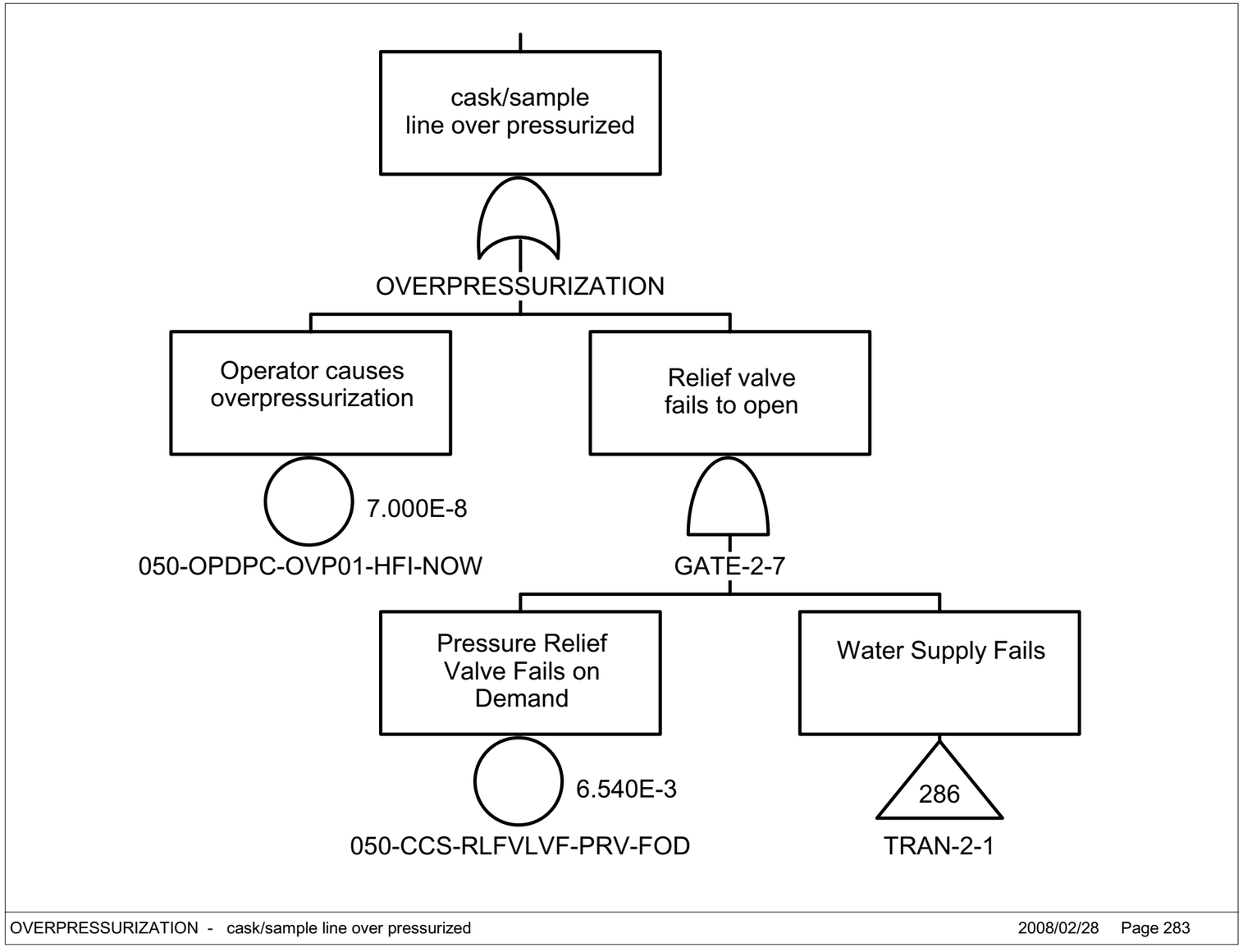
Table B5.4-5. Cut Sets for Over Pressurization

Fault Tree	% Cut Set	Prob./Freq.	Basic Event	Description	Probability
OVERPRESSURIZATION	76.28	6.694E-006	050-CCS-PMTRFST-MSC-FOH	Pump motor runs too fast	1.023E-003
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
	20.57	1.805E-006	050-CCS-PUMPSTP-PMD-FTR	Pump P-00002 fails to run	2.760E-004
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
	1.70	1.491E-007	050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
			050-CCS-THVLVFL-NZL-FOH	Throttle valve to pump fails open	2.280E-005
	0.80	7.000E-008	050-OPDPC-OVP01-HFI-NOW	Operator causes overpressurization	7.000E-008
	0.43	3.798E-008	050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003
			050-CCS-VNTPIPE-PPM-PLG	Pipe BW-0003 plugs	5.808E-006
	0.22	1.910E-008	050-CCS-PLCSPUR-PLC-SPO	PLC spurious operation causes pump motor to run too fast	2.920E-006
			050-CCS-RLFVLVF-PRV-FOD	Pressure Relief Valve Fails on Demand	6.540E-003

Source: Original

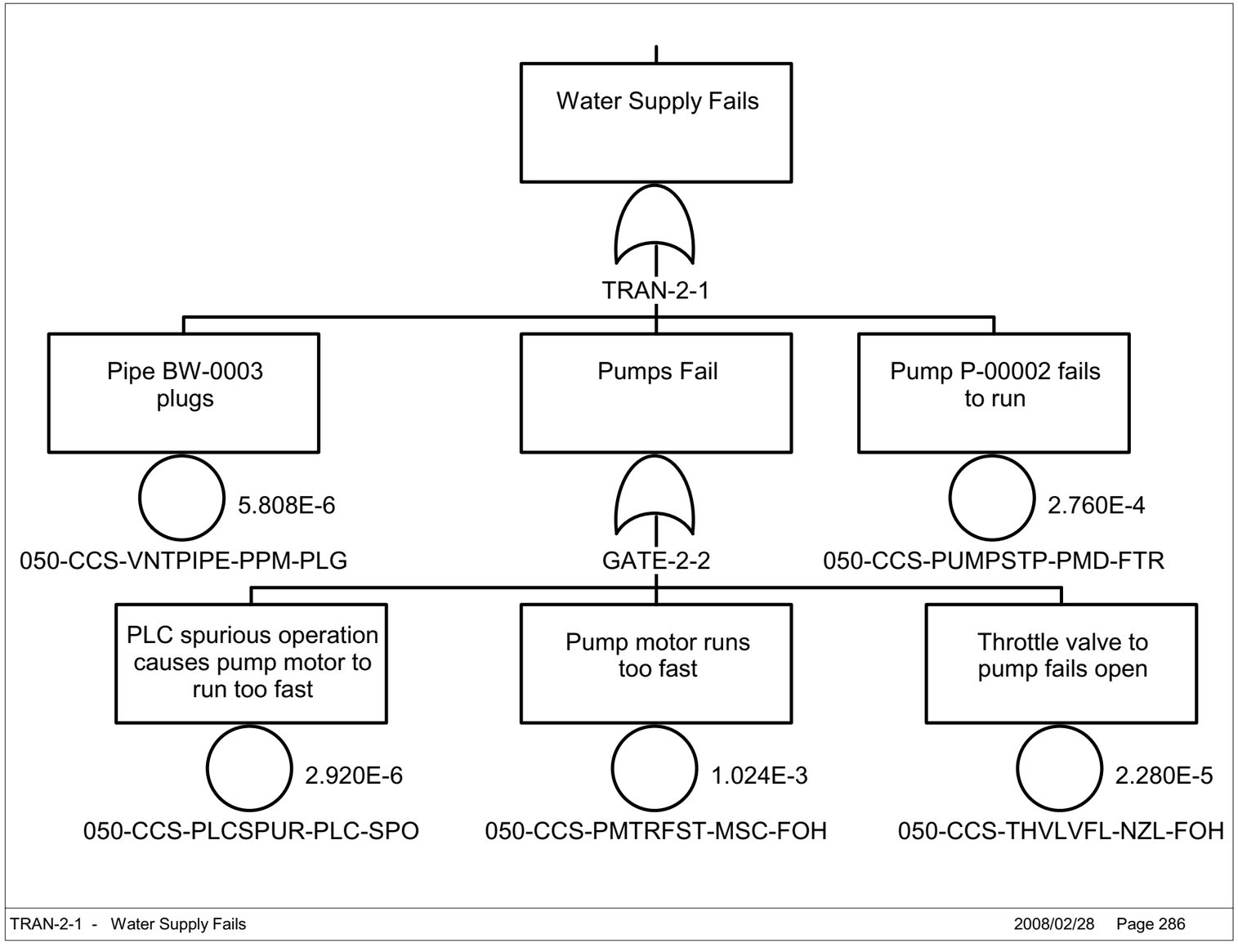
B5.4.2.8 Fault Tree

Figures B5.4-8 and B5.4-9 display the fault trees for “Cask/Sample Line Over Pressurization”.



Source: Original

Figure B5.4-8. Fault Tree for an Over Pressurization



Source: Original

Figure B5.4-9. Fault Tree for a Cask/Sample Line Over-pressurized Rupture (Transfer 2-1)

B6 SITE TRANSPORTER FAULT TREE ANALYSIS

B6.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designed categories described in Section 4.1, relative to suitability for intended use.

B6.1.1 BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report – Site Transporter.* 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015. (DIRS 184489)

B6.1.2 BSE 2007. *Exhibit D, Statement of Work for Mechanical Handling Equipment Design.* 000-3SW-MGR0-00100-000 Rev. 003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070904.0031.

B6.1.3 Morris Material Handling 2007. *P&ID Site Transporter.* V0-CY05-QHC4-00459-00049-001 Rev. 004. Oak Creek, Wisconsin: Morris Material Handling. ACC: ENG.20071022.0012.

B6.2 SITE TRANSPORTER DESCRIPTION

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a cylindrical concrete and steel ventilated aging overpack. The transport occurs both Intra-Site and within the Canister Receipt and Closure Facility (CRCF), the Wet Handling Facility (WHF), and the Receipt Facility (RF)[2]. In the WHF, the site transporter is used to deliver aging overpacks with a DPC, for loading an aging overpack with a DPC or TAD canister, and for removing the loaded aging overpacks from the facility.

Movement of the site transporter within the WHF is limited to the Loading Room and the Site Transporter Vestibule.

B6.2.1 Overview

The interface between the site transporter and the aging overpack is via two parallel rectangular lift slots that pass through the containers near their lower ends. Orientation of the aging overpack is such that the axis of the aging overpack is vertical with lid, at the top. Access to the top of the aging overpack is unobstructed.

[2] Variations in the use of the site transporter for Intra-Site, RF and CRCF are addressed in their respective volumes.

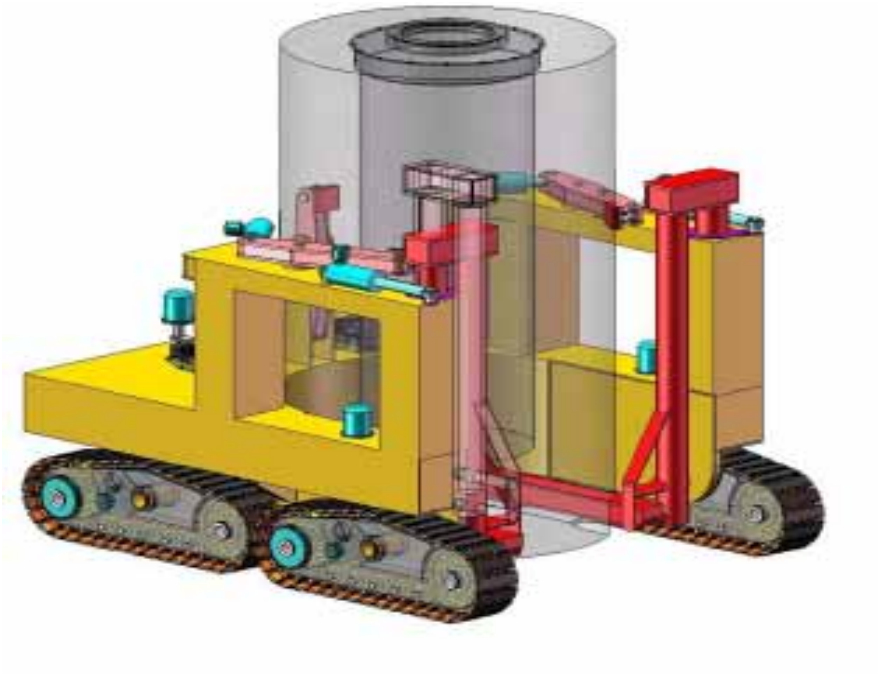
An integrated diesel powered electric generator and diesel fuel provides the electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable (or remote control) from the facility main electrical supply (Ref, B6.1.1, Section 2.1).

The site transporter is a track driven vehicle with four synchronized tracks (two on each side of the site transporter). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not important to safety (ITS).

A rear fork assembly consists of a pair of arms that extend to the front of the site transporter. These forks move up and down for the purpose of raising, lowering, and supporting the aging overpack during movement. A pair of support arms is located at the front of the site transporter which is moved into position around the forks to provide support and assistance during the lifting and lowering of the aging overpack.

A passive restraint system provides stabilization during aging overpack movement. There are two mechanisms that control aging overpack movement on the pitch and roll axis. These restraints are not engaged until the aging overpack has been raised to the desire height. Once engaged, three pins are inserted, one in each restraint arm that keep the restraints in place should there be a failure of the electromechanical assembly used to position and secure the restraint device. Properly installed, they also serve as an interlock that prevent movement of a loaded site transporter.

Control of the site transporter is provided by a wireless remote control or a wired pendant. Although these devices only provide a subset of the controls and indicators that are available on the control console located on the site transporter, they do contain all the necessary controls and indicators to perform and monitor the operation state of the site transporter during normal operations. The site transporter is shown in Figure B6.2-1.



Source: Ref. B6.1.1

Figure B6.2-1 Site Transporter

The site transporter system is composed of six subsystems (Ref. B6.1.1):

1. Crawler Tracks Subsystem—Four crawlers, two on each side of the site transporter, are used to move the vehicle. These crawlers use tracks with chamfered flat steel plates mounted to double grouser shoes on a continuous chain.

2. Power Plant Subsystem—a diesel engine, generator, and diesel fuel tank are enclosed in the back of the site transporter. During Intra-Site Operations, the diesel engine drives the generator, which provides the required 480 V, 3-phase, 60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480V AC/3-phase/60 Hz power is supplied to operate the vehicle.

3. Rear Lift Fork Subsystem—site transporter contains a pair of arms that extend forward from the site transporter through slots in the aging overpack. The lift/lower drive system utilizes an ACME type nut that changes the elevation of the fork as the screw lift mechanism turns through the ACME nut. A lift synchronizer controls the lift/lower operation.

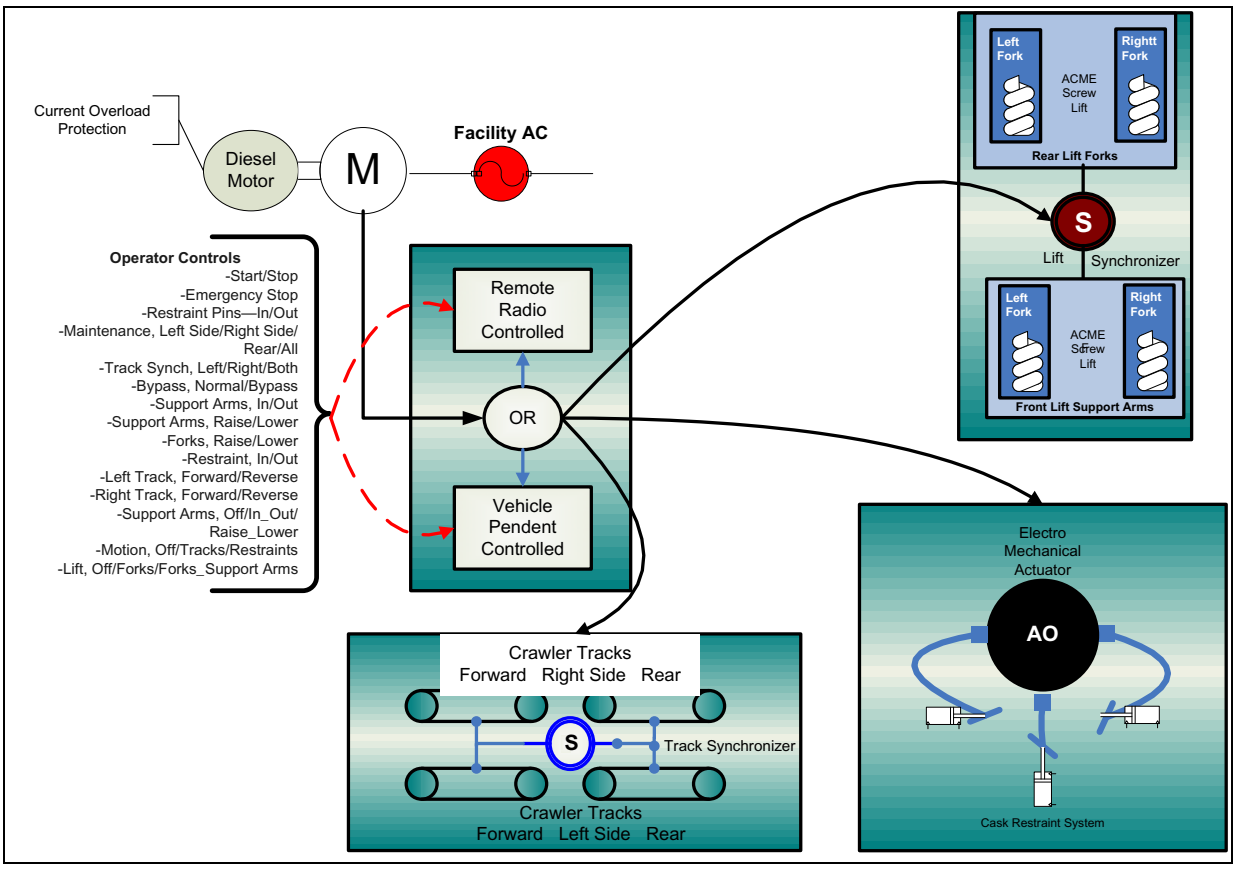
4. Lift Support Arms Subsystem—two support arms with electromechanical actuators are located on the front of the site transporter. These support arms are rotated 90 degrees to provide support and stabilization for the lift forks during lifting/lowering/moving operations. ACME nuts are used on these arms and synchronized with the lift forks during lifting/lowering/moving.

5. Restraint Subsystem—a two axis restraint system is incorporated to stabilize the aging overpack during site transporter movement. The restraints are emplaced/retracted with electromechanical actuators. These restraints when positioned against the aging overpacks will be secured with a locking pin. The three locking pins serve as an interlock and must be properly installed before the site transporter can be moved.

6. Vehicle Controls Subsystem—there are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter.

Note: In addition to the six subsystems identified above, (Ref. B6.1.1) also includes a description of the site transporter "car body." Events associated with car body failure are screened from this analysis based on the results of the stress analysis contained in this reference.

A simplified block diagram of the functional subsystems on the site transporter is shown in Figure B6.2-2.



NOTE: AO = aging overpack; M = motor; S = synchronizer;

Source: Original

Figure B6.2-2. Simplified Block Diagram of the Site Transporter Subsystems

B6.2.1.1 Site Transporter Crawler Tracks Subsystem Description

The site transporter moves by four tracks mounted on the crawler frames with two on each side of the vehicle to increase stability when traversing terrain that includes sudden changes in elevation such as a drainage trough or curb. The site transporter is designed to negotiate roadways with a 5% grade and up to a 2% cross-slope (Ref. B6.1.2, Section 7.2.2-11). Special pads are included on the tracks to reduce the wear and tear on concrete or roadways.

Each track is driven by its own electric motor (50 HP @ 900 rpm) through its own gear reduction and final chain drive reduction. During forward operations, motors on both sides of the machine drive are synchronized. During turns, the outside tracks are driven faster and for very sharp turns the tracks are counter-rotated to turn the site transporter about its own vertical centerline (Ref. B6.1.1, Section 2.1.2).

B6.2.1.2 Power Plant Subsystem Description

The power plant subsystem supplies the site transporter with 480 volts AC, 3-phase power at 60 Hz. Because of the risk of contamination from their various fluids, there are no storage batteries or capacitors in the system. The generator is sized approximately 110% more than the highest power requirement for the vehicle.

The 150 kW generator is sized for seven hours of continuous operation with a fuel tank containing 99-gallons of diesel fuel (Ref. B6.1.1, Section 2.2.3). The fuel tank capacity is sized to minimize the amount of fuel taken inside the facilities but sufficient to transport a loaded aging overpack three miles and return to the site transporter's point of origin without refueling (Ref. B6.1.2, Section 7.2.2.2).

When entering a building the generator is shut down and a power source from the building is plugged into the site transporter integral receptacle to allow the site transporter to operate inside the building without a source of combustion.

The motor drive and current over load protection system prevents the site transporter from exceeding 2.5 mph (Ref. B6.1.1, Section 3.2.1).

B6.2.1.3 Rear Lift Forks Subsystem Description

The rear forks are only capable of moving up or down. Each fork is driven by its own gear reduction and 16 HP, 900 rpm electric motor. The output of the drive is a rotating ACME type screw which, as it turns inside the rear fork lift tube, drives an ACME nut that raises or lowers the fork. The height of the rear lift fork is controlled by limit switches as well as being mechanically unable to lift an aging overpack height more than 12 inches above the floor/ground (Ref. B6.1.1, Sections 2.1.4 and 2).

B6.2.1.4 Lift Support Arms Subsystem Description

The front support arms have constrained movement which consists of a clockwise/counterclockwise rotation and up and down movement. The right and left assemblies

are mirror images of one another and move as a synchronous pair although they are each driven by its own gear reduction and 20 HP, 900 rpm electric motor (Ref. B6.1.1, Section 2.1.5).

The operator positions the lift support arms around the lifting forks. After the site transporter has been positioned properly around the aging overpack or STC, the rear forks are raised to contact the bottom of the aging overpack's lifting slots. Limit and position switches ensure the lift support arms are in the correct position. Additional limit switches prevent the support arms from exceeding the 12-inch lift.

B6.2.1.5 Restraints Subsystem Description

When the load on the site transporter is ready to be lifted, the three arms of the restraint system are activated and moved to a location "near" the aging overpack. This location is determined by a combination of operator observation and integral limit switches.

After the aging overpack has been raised to the specified transportation height, the restraint arms are engaged to hold the aging overpack in place during movement. The arms are moved by linear electromechanical actuators. In addition, a locking pin is utilized to take extreme loads as well as serve as an interlock device. The three restraint arms must be properly pinned before the interlock will allow the site transporter to be moved (Ref. B6.1.3, Sheet 1 of 3).

B6.2.1.6 Vehicle Controls Subsystem Description

The site transporter can be operated in two modes: a remote (wireless) control and an operator controlled pendant (Ref. B6.1.1, Section 2.1.7). Both of these devices have the same capability. Table B6.2-1 contains a list of controls that are available on the controller and the corresponding activation device (Ref. B6.1.3, Sheet 3 of 3).

Table B6.2-1. Site Transporter Remote or Pendant Controls

Site Transporter Operation	Activation Device on Controller
Start/Stop	Pushbutton
Emergency stop	Palm button
Restraint pin—Engage(In)/Disengage (Out)	Selector switch
Maintenance--left side/right side/rear/all	Keyed selector switch
Track synch—left/right/both	Selector switch
Bypass—Normal/bypass	Keyed selector switch
Support arms—in/out	Induction pushbutton
Support arms—raise/lower	Induction pushbutton
Forks—raise/lower	Induction pushbutton
Restraint—in/out	Induction pushbutton
Left Track—forward/reverse	Induction pushbutton
Right Track—forward/reverse	Induction pushbutton
Support Arms—off/in_out/raise_lower	Selector switch
Motion—off/tracks/restraints	Selector switch
Lift—off/forks/forks_support arms	Selector switch

Source: Original

All safety interlocks and controls of the site transporter are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No programmable logic controller (PLC) or computer is used to control the machine.

B6.2.2 Normal Operations

Once the lift has been completed, the operator performs the final positioning of the upper restraint arms and inserts a pin in each arm. When the pins are properly installed, the site transporter can move.

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. Once the site transporter arrives at the facility, the operator stops the vehicle outside the Site Transporter Vestibule and turns off the diesel generator. An electrical umbilical cord is manually retrieved from inside the building and attached to the site transporter. The site transporter is never operated inside the WHF on diesel power.

Once inside the building, the operator positions the site transporter in the Loading Room. When work is being performed on the aging overpack, the site transporter operator will remove the pins from the restraint arms and disengage them from the aging overpack. The movement interlock is engaged when the pins are removed. The operator lowers the aging overpack to the floor. The procedure is reversed when it is necessary to move the site transporter again inside the facility: the pins will be inserted, the restraints will be engaged, the aging overpack is raised from the floor and the umbilical cord attached.

The operations used to move an unloaded aging overpack are identical but not considered in this analysis.

B6.2.3 Site Transporter Off-Normal Operations

There are four off nominal conditions that could occur during the movement of an aging overpack in the WHF. When any of these occur, the operator response encompasses only those actions to return the aging overpack to a safe state. These are:

1. Lowering the forks without electrical power.
2. Rotating the lift support arms without electrical power.
3. On-board generator fails to operate.
4. Track belt fails.

In the event of a loss of power, the site transporter is designed to stop, retain its load and enter a "lock mode" safe state. Upon the restoration of power the site transporter shall stay in the "lock mode" safe state until operator action is taken (Ref. B6.1.2, Section 7.2.3-5).

B6.2.4 Site Transporter Testing and Maintenance

Testing and maintenance of the site transporter is done on a periodic basis and does not affect the normal operations of the site transporter. Testing and/or maintenance are not performed on a site transporter loaded with an aging overpack or an STC. A site transporter that has malfunctioned or has a warning light lit on the site transporter will be deemed unserviceable and turned in for maintenance. Unserviceable vehicles will not be used.

If an unserviceable state is identified during a lift/lower or movement activity, the site transporter shall immediately be placed in a safe state (as quickly as possible) and recovery actions for the site transporter will be invoked.

B6.2.5 Site Transporter System/Pivotal Event Success Criteria

A site transporter failure is the initiating event in three event sequences in the WHF as shown in Table B6.2-2.

Table B6.2-2. Site Transporter Initiating Events by ESD

Site Transporter Initiating Event	Affected ESD
• Site transporter collision	ESD03: Receipt of AO within WHF ESD11: Movement of the ST in the WHF or Export of AO from WHF
• Site transporter rollover	ESD03: Receipt of AO within WHF ESD11: Movement of the ST in the WHF or Export of AO from WHF
• Site transporter spurious movement	ESD13: Lifting and lowering a canister during transfer with CTM

NOTE: AO = aging overpack; WHF = Wet Handling Facility; CTM = canister transfer machine; ESD = event sequence diagram.

Source: Original

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals can not be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

Requirements

Two means of stopping the site transporter are incorporated in the controllers. One is the normal stop button and the other shall consist of an emergency stop that is the equivalent of a dead man switch.

On the loss of AC power derived from the facility, the site transporter shall immediately enter the “lock mode” safe state. The “lock mode” safe state shall not be reversible without specific operator action.

There is no testing or maintenance permitted on a site transporter loaded with an aging overpack.

Since the dominant contributor to site transporter collision in the facility is human error, no priority shall be given to either the remote or the pendant controllers.

Design Features

Stopping the site transporter is accomplished by pushing the “stop” button on the remote or pendant controller. The site transporter, upon receiving a stop command from either control source immediately responds by removing power from the propulsion system.

The site transporter is only able to perform one function at any time. It can lift a aging overpack or it can move it, but it can not perform both functions at the same time. This feature is accomplished by interlock and by power limitations inherent in the sizing of the power plant that ensures a limited amount of power for each of the electromechanical devices and drive system.

B6.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with system, structures, and components. The five areas considered are addressed in Table B6.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B6.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Lift booms	Material failure ACME screw/nut	—	—	—	—
Lift support arms	Material failure ACME screw/nut	—	—	—	—
Restraint arms	Material failure	—	—	—	—
Power plant	Current overload protection fails Safe state on	—	—	Failure: - to stop Failure to remove power cable	—
Remote control	Spurious commands	—	—	Improper command	Collide with crane rigging
Tracks	—	—	—	Failure to stop	—

Source: Original

B6.4 RELATED FAILURE SCENARIOS

There are three basic site transporter fault trees developed for the WHF. The top events for these fault trees are:

1. Site transporter collides with WHF structures.
2. Site transporter rollover.
3. Site transporter spurious movement during canister transfer.

A fourth scenario, site transporter load drop, was screened from further consideration in the WHF, see T able 6.02.

B6.4.1 Site Transporter Collides with WHF Structures (ESD-03, -11)

B6.4.1.1 Description

The fault trees for the collision events are identical. Collisions can occur as a result of human error or mechanical failures (human error events are uniquely identified but all have the same screening value of 3E-3 with a lognormal error factor of 5). Mechanical failures leading to a collision consist of: the site transporter fails to stop when commanded, the site transporter exceeding a safe speed, or the site transporter moves in the wrong direction.

B6.4.1.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the site transporter for mechanical failures. The site transporter operator continuously maintains situational awareness and proper control of the movement of the site transporter. To avoid collisions, the site transporter must stop when commanded, be prevented from entering a runaway situation or respond correctly to a site transporter movement command.

The site transporter is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the site transporter by either commanding a stop from the start/stop button or by releasing the palm switch which initiates an emergency stop. At anytime there is a loss of power detected, the site transporter will immediately stop all movement and enters into a “lock mode” safe state. The site transporter will remain in this “lock mode” safe state until power is returned and the operator restarts the site transporter.

Runaway situations on the site transporter are prevented by mechanical constraints. The maximum speed of the site transporter is limited by motor current overload protection (Ref. B6.1.1, Section 3.2.1). The site transporter motor speed and gearing prevents the site transporter from exceeding 2.5 miles per hour.

The prevention of site transporter movements in the wrong direction is prevented by the limitation of the power plant that prevents simultaneous operations.

B6.4.1.3 Design Requirements and Features

Requirements

The site transporter has two off-equipment control devices that have complete control over the site transporter

Features

Drive system consists of an electric motor and a transmission constraint which limits the maximum speed of the site transporter to 2.5 mph.

B6.4.1.4 Fault Tree Model

The fault tree model for "Site Transporter Collides with WHF Structures in the WHF," accounts for the both human error and/or site transporter mechanical problems that could result in collision. There are three distinct movements within the WHF which are reversed if an aging overpack is picked up in the WHF and taken to the aging pads. Movement within the facility is restricted and even at low speeds a collision can occur.

The fault tree considers mechanical failures that fail to stop the site transporter, events that could cause the site transporter to exceed a safe speed, and events that could cause the site transporter to move in the wrong direction.

B6.4.1.5 Basic Event Data

Table B6.4-1 lists the basic events used in the Site Transporter Collides with WHF Structures fault tree.

Table B6.4-1. Basic Event Probability for Site Transporter Collides with WHF Structures

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN ST Collision in Facility		**Case : Current Units: Per Hour**			
Name	**Calc. Type[a]**	**Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time[a]**
050-OPSTCOLLIDE1-HFI-NOD	1	3.00E-03	3.00E-03	0.00E+00	0.00E+00
050-ST---BRK001--BRK-FOD	1	1.46E-06	1.46E-06	0.00E+00	1.00E+00
050-ST---CBP004-CBP--OPC	3	9.13E-08	0.00E+00	9.13E-08	1.00E+00
050-ST---CBP004-CBP--SHC	3	1.88E-08	0.00E+00	1.88E-08	1.00E+00
050-ST---CT000---CT--FOD	1	4.00E-06	4.00E-06	0.00E+00	1.00E+00
050-ST---CT002---CT--FOH	3	6.88E-05	0.00E+00	6.88E-05	1.00E+00
050-ST---HC001--HC--FOD	1	1.74E-03	1.74E-03	0.00E+00	1.00E+00
050-ST---HC002---HC--SPO	3	5.23E-07	0.00E+00	5.23E-07	1.00E+00
050-ST---MOE000--MOE-FSO	3	1.35E-08	0.00E+00	1.35E-08	1.00E+00
050-ST---MOE021--MOE-FSO	3	1.35E-08	0.00E+00	1.35E-08	1.00E+00
050-ST---SC021---SC--FOH	3	1.28E-04	0.00E+00	1.28E-04	1.00E+00
050-ST---SC021---SC--SPO	3	3.20E-05	0.00E+00	3.20E-05	1.00E+00
050-ST---SEL021--SEL-FOH	3	4.16E-06	0.00E+00	4.16E-06	1.00E+00
LOSP-4	1	4.1E-06	4.1E-06	0.00E+00	0.00E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc = calculation; ST = site transporter.

Source: Original

B6.4.1.5.1 Human Failure Events

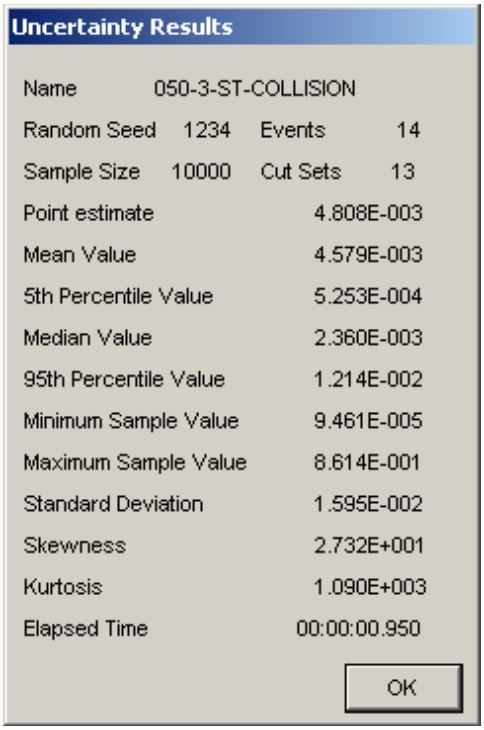
There is one human event in the collision trees for the site transporter and accounts for the site transporter operator causing the collision. This human error is set at the screening value of 3E-03 for all three ESD events.

B6.4.1.5.2 Common-Cause Failures

There are no CCF events identified for this fault tree.

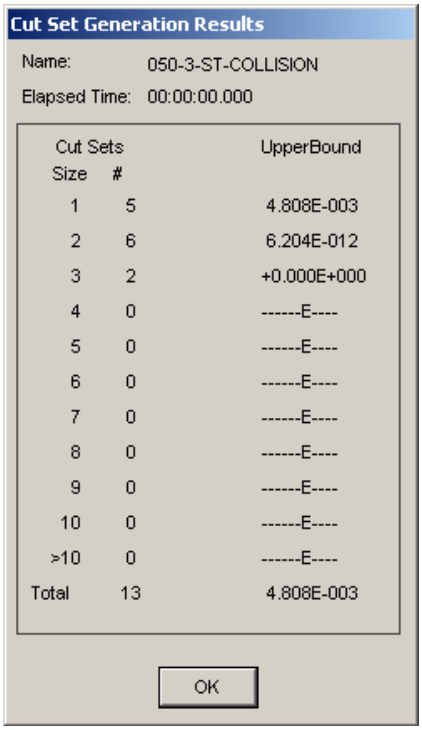
B6.4.1.6 Uncertainty and Cut Set Generation

Figures B6.4-1 and B6.4-2 contain the uncertainty and the cut set generation results for site transporter collision in facility using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-1. Uncertainty Results for the Site Transporter Collides with WHF Structures



Source: Original

Figure B6.4-2. Cut Set Generation Results for the Site Transporter Collides with WHF Structures

B6.4.1.7 Cut Sets

Table B6.4-2 contains the cut sets for "Site Transporter Collides with Facility Structures" fault tree.

Table B6.4-2. Cut Sets for the Site Transporter Collides with Facility Structures

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
050-3-ST-COLLISION	62.40	3.000E-003	050-OPSTCOLLIDE2-HFI-NOD	Operator Error Causes Collision	3.0E-003
	36.19	1.740E-003	050-ST---HC001--HC--FOD	Remote Control Transmits Wrong Signal	1.7E-003
	1.43	6.880E-005	050-ST---CT002---CT--FOH	Direction Controller Fails	6.9E-005
	0.08	4.000E-006	050-ST---CT000---CT--FOD	ST Primary Stop Switch Fails	4.0E-006
	0.01	5.230E-007	050-ST---HC002---HC--SPO	Spurious Command to Lift/Lower AO or STC	5.2E-007
	0.00	5.986E-012	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006
			LOSP-4	Failure of Off Site Power	4.1E-006
	0.00	1.333E-013	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006

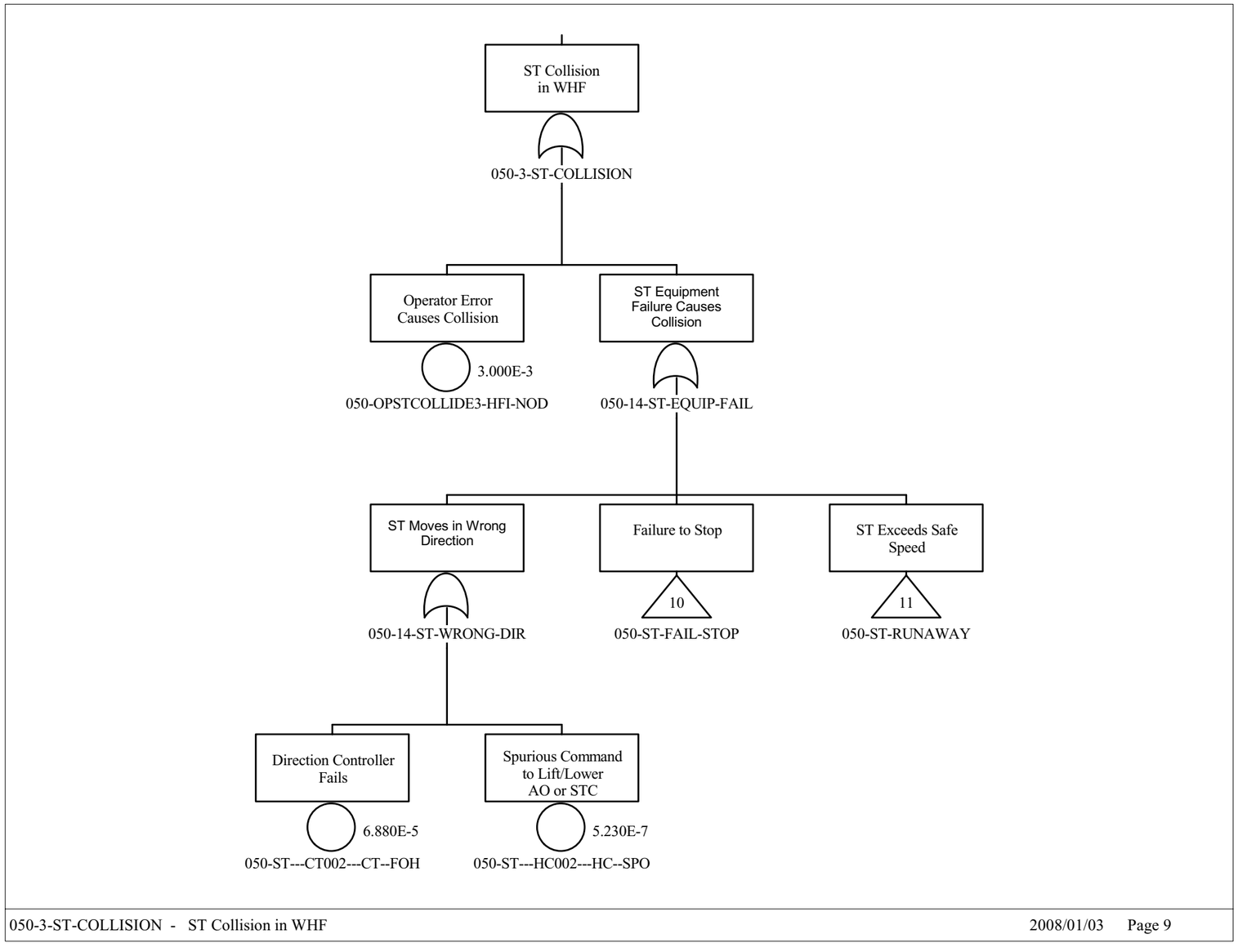
Table B6.4-2. Cut Sets for the Site Transporter Collision in Facility (Continued)

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
			050-ST---CBP004-CBP--OPC	ST Power Cable - Open Circuit	9.1E-008
	0.00	5.535E-014	050-ST---MOE000--MOE-FSO	Motor (Electric) Fails to Shut Off	1.4E-008
			LOSP-4	Failure of Off Site Power	4.1E-006
	0.00	2.745E-014	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006
			050-ST---CBP004-CBP--SHC	ST Power Cable Short Circuit	1.9E-008
	0.00	1.233E-015	050-ST---CBP004-CBP--OPC	ST Power Cable - Open Circuit	9.1E-008
			050-ST---MOE000--MOE-FSO	Motor (Electric) Fails to Shut Off	1.4E-008
		4.808E-003		= Total	

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask.

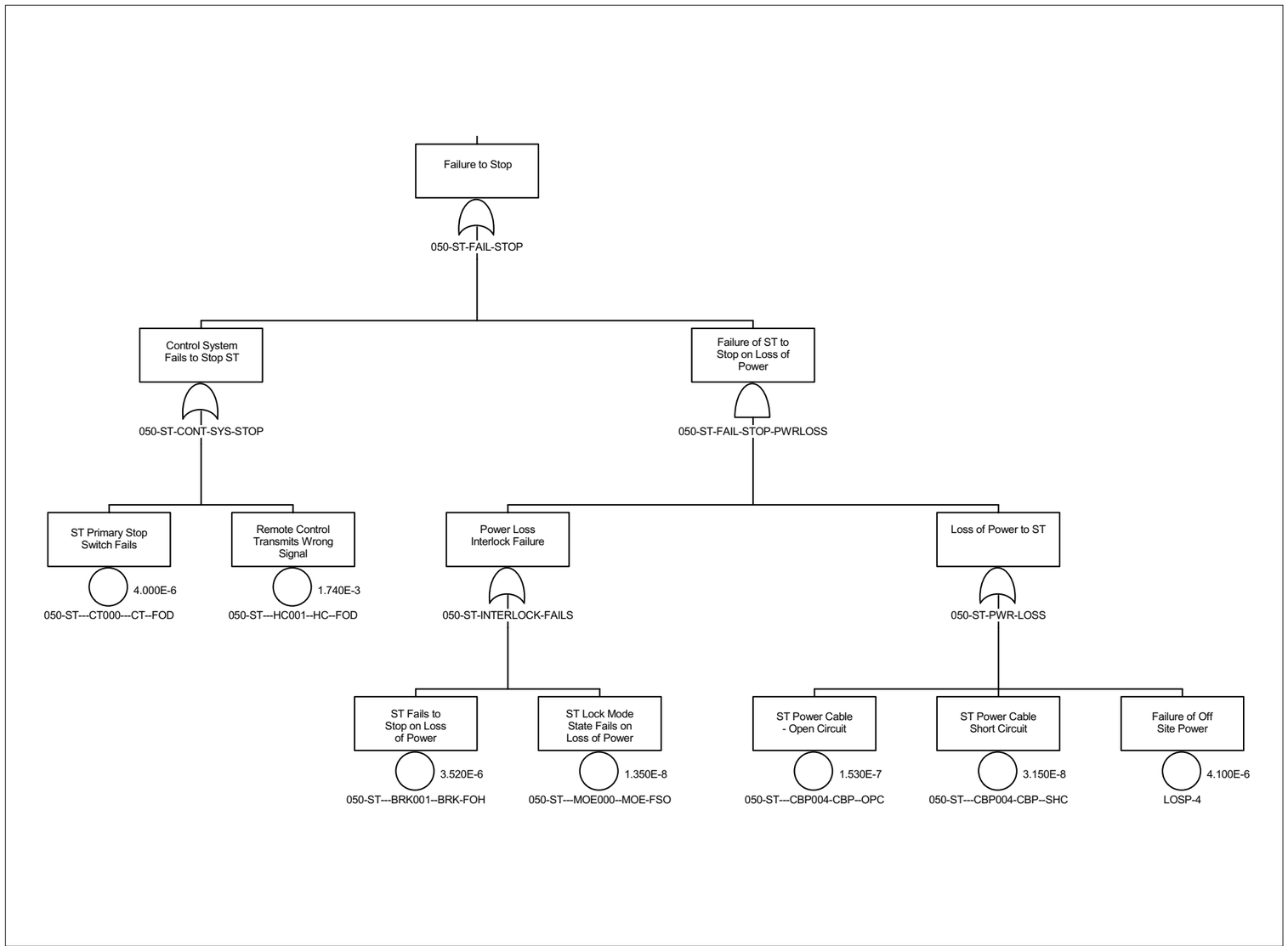
Source: Original

B6.4.1.8 Fault Tree



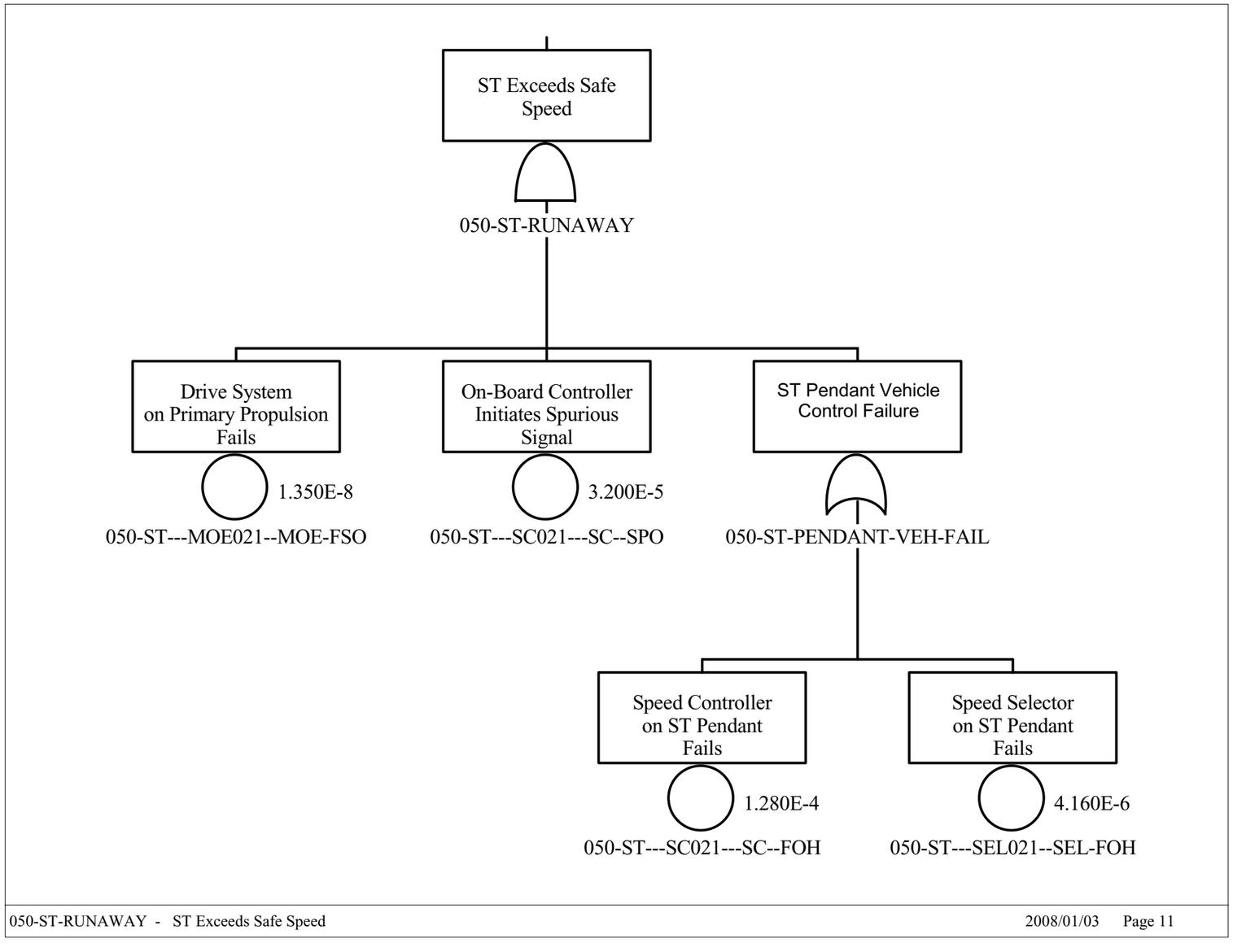
Source: Original

Figure B6.4-3. Site Transporter Collision in the WHF



Source: Original

Figure B6.4-4. Failure to Stop



Source: Original

Figure B6.4-5. Site Transporter Exceeds Safe Speed

B6.4.2 Site Transporter Rollover (Tip-over) (ESD-03, -11)

B6.4.2.1 Description

Although the site transporter has been designed to have a low center of gravity and a wide footprint, there is a possibility of a rollover caused by a track failure with a subsequent operator failure to stop the site transporter upon loss of a track. The track would have to fail in a manner such that it binds (i.e., rolls up), the site transporter drives over the failed track, and the site transporter tilts to an angle that results in a tipover condition.

B6.4.2.2 Success Criteria

The design of the site transporter prevents the majority of scenarios that could potentially cause a site transporter rollover. The site transporter is designed to negotiate a 5% grade and a 2% cross-slope. In addition, the aging overpack is physically prevented from being lifted more than 12 inches. The combination of the low lift of the aging overpack or STC, the low center of gravity, and wide footprint of the site transporter results in stable platform during movements.

During movement, a site transporter track failure could result in a potential tip-over situation. There is no design constraint for this failure mode, preventing this situation relies on an operator awareness and response time to this situation to initiate an emergency stop command. The operator has several seconds to respond to the track failure; however, since this is a recovery action, no credit is taken for the operator response.

B6.4.2.3 Design Requirements and Features

Requirements

Operator shall have the capability of stopping the site transporter in sufficient time to keep the site transporter from running off the end of a broken track.

Features

The center of gravity of a loaded site transporter with aging overpack ensures stability.

The site transporter operator has the capability to stop the operation of the site transporter during abnormal conditions.

B6.4.2.4 Fault Tree Model

Human error is conservatively postulated to result in a rollover/tip-over if the operator does not stop the site transporter in sufficient time to prevent the site transporter from running off the broken track.

B6.4.2.5 Basic Event Data

Table B6.4-3 lists the basic events used in the site transporter drop load during lift/movement fault tree.

Table B6.4-3. Basic Event Probability for the Site Transporter Rollover

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN ST Rollover Name	Calculation Type[a]	Case : Current Units: Per Hour Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-CRWT-TRD0001-TRD-FOH	3	1.414E-005	1.000E+000	5.890E-007	1.000E+000
050-CRWT-TRD0002-TRD-FOH	3	1.414E-005	1.000E+000	5.890E-007	1.000E+000
050-CRWT-TRD0003-TRD-FOH	3	1.414E-005	1.000E+000	5.890E-007	1.000E+000
050-CRWT-TRD0004-TRD-FOH	3	1.414E-005	1.000E+000	5.890E-007	1.000E+000
050-CRWT-TRK0001-TRD-FOH	3	1.414E-005	1.000E+000	5.890E-007	1.000E+000
050-OP-FAILSTOP-HFI-FOD	1	1.000E+000	1.000E+000	0.000E+000	1.000E+000

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
ST = site transporter.
Source Original

B6.4.2.5.1 Human Failure Events

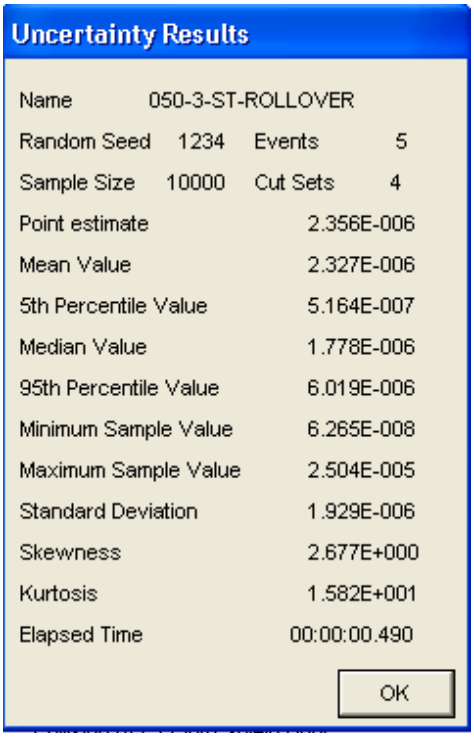
There is one human error failure event included in this model. It is conservatively set to a value of 1E+0 because unsafe actions that require an equipment failure to cause an initiating event are generically assigned a screening HEP of 1.0 (see Attachment E, Table E6.4-1).

B6.4.2.5.2 Common Cause Failures

There are no CCFs identified for this fault tree.

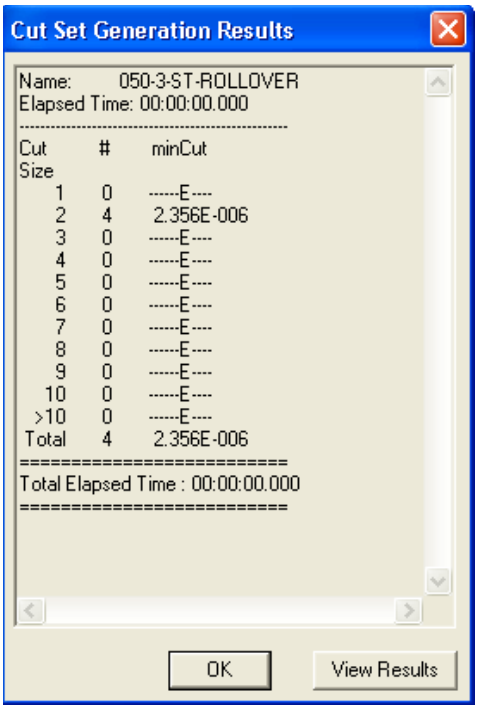
B6.4.2.6 Uncertainty and Cut Set Generation

Figures B6.4-6 and B6.4-7 contain the uncertainty and the cut set generation results for ”Site Transporter Rollover (tip-over)” fault tree using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-6. Uncertainty Results Site Transporter Rollover



Source: Original

Figure B6.4-7. Cut Set Generation Results for Site Transporter Rollover

B6.4.2.7 Cut Sets

Table B6.4-4 contains the cut sets for “Site Transporter Rollover”.

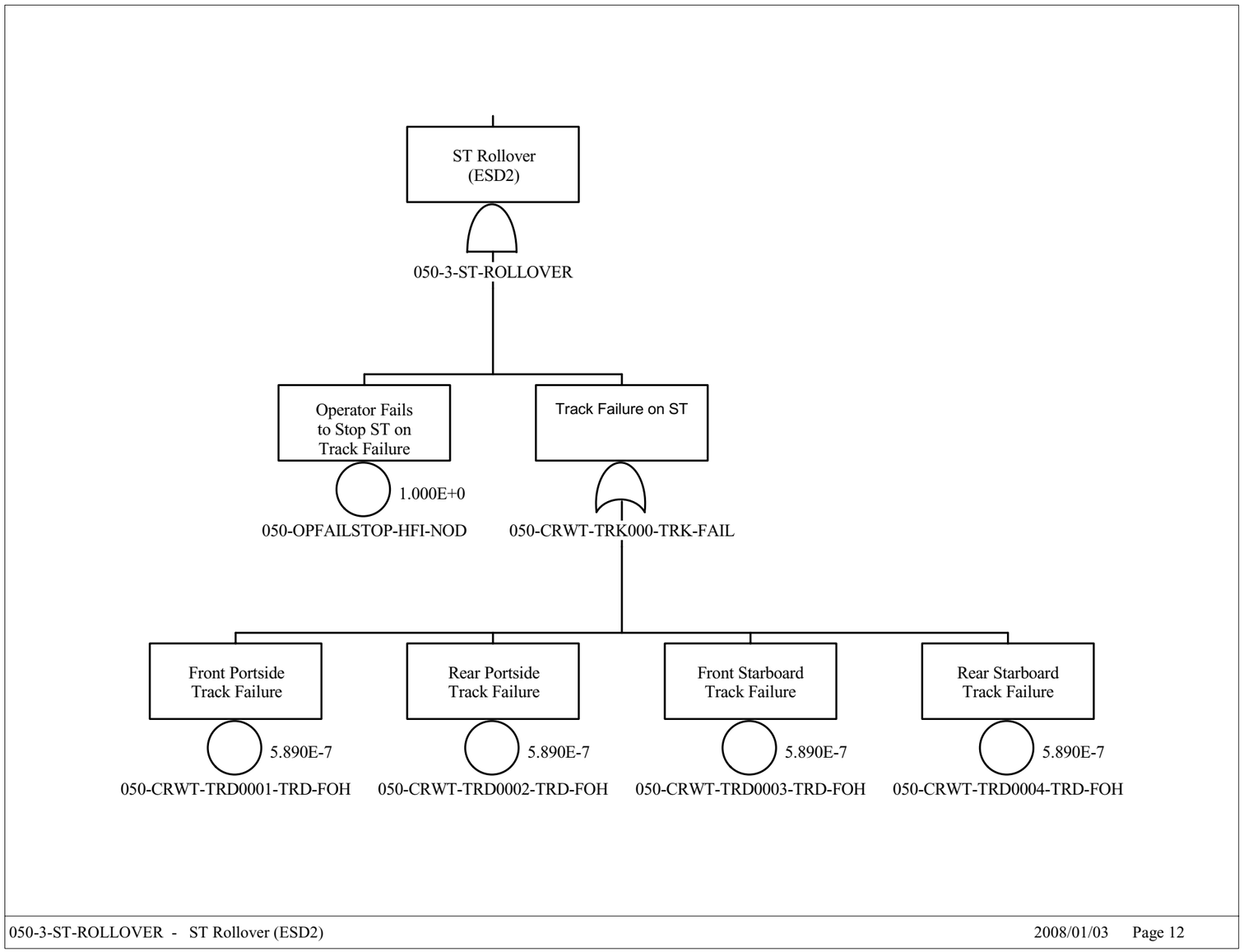
Table B6.4-4. Cut Sets for the Site Transporter Rollover (Tip-over)

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-3-ST-ROLLOVER	25.00	5.890E-007	050-CRWT-TRD0001-TRD-FOH	Front Portside Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0002-TRD-FOH	Rear Portside Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0003-TRD-FOH	Front Starboard Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0004-TRD-FOH	Rear Starboard Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
2.356E-006 = Total					

NOTE: ST = site transporter.

Source Original

B6.4.2.8 Fault Tree



Source: Original

Figure B6.4-8. Site Transporter Rollover Fault Tree

B6.4.3 Site Transporter Spurious Movement (ESD-13)

B6.4.3.1 Description

The fault tree for "Site Transporter Spurious Movement" in this event sequence addresses activities associated with transfers of canisters from or to aging overpacks in the Loading Room.

B6.4.3.2 Success Criteria

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals cannot be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

B6.4.3.3 Design Requirements and Features

Requirements

Site transporter power and the remote control pendant shall be removed from the site transporter when it has been positioned within the Loading Room.

Facility power and the control pendant are removed from the site transporter when it has been properly position within the Loading Room.

On removal of AC power derived from the facility, the site transporter immediately enters the "lock mode" safe state. The "lock mode" safe state is not be reversible without specific operator action.

Features

There are no electrical storage devices in the design of the site transporter. When the facility AC power cable is removed, the site transporter is incapable of movement.

A shield door interlock shall be designed to ensure facility power has been removed from the site transporter.

B6.4.3.4 Fault Tree Model

The fault tree model for "Site Transporter Spurious Movement" in the Loading Room accounts for failure to remove facility power and the possibility of the site transporter receiving a spurious movement command for the remote control device.

B6.4.3.5 Basic Event Data

Table B6.4-5 lists the basic events used in the "Site Transporter Spurious Movement" fault tree.

Table B6.4-5. Basic Event Probability for Site Transporter Spurious Movement

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN ST Spurious Movement Name	**Case: Current Calculation Type[a]**	**Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time[a]**
050-CR---IEL00A--IEL-FOD	1	2.75E-05	2.75E-05	0.00E+00	0.00E+00
050-CR---IEL00B--IEL-FOD	1	2.75E-05	2.75E-05	0.00E+00	0.00E+00
050-CR---IELCCF--IEL-CCF	1	1.30E-06	1.30E-06	0.00E+00	0.00E+00
050-OPNOUNPLUGST-HFI-NOD	1	1.00E-03	1.00E-03	0.00E+00	0.00E+00
050-ST---HC000--HC--SPO	3	5.23E-07	0.00E+00	5.23E-07	1.00E+00
050-ST---SC002--SC--FOH	3	1.28E-04	0.00E+00	1.28E-04	1.00E+00
050-ST---SC021---SC--SPO	3	3.20E-05	0.00E+00	3.20E-05	1.00E+00
050-CR---IEL00A--IEL-FOD	1	2.75E-05	2.75E-05	0.00E+00	0.00E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
ST = site transporter.

Source: Original

B6.4.3.5.1 Human Failure Events

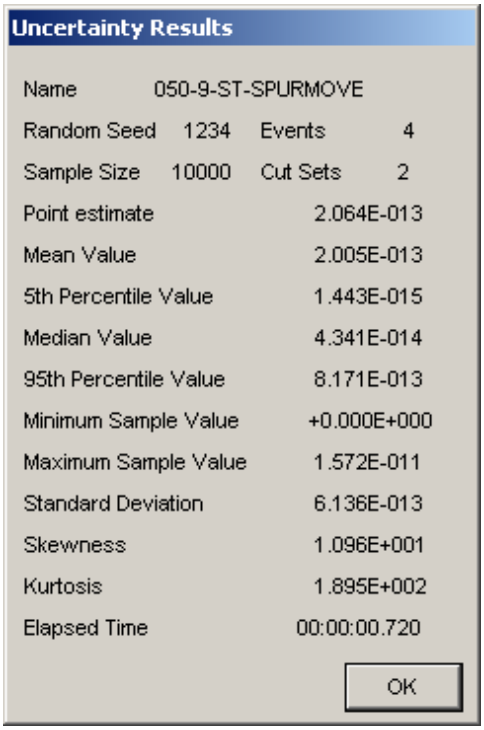
There is one human error associated with this fault tree that addresses an operator failure to unplug the site transporter power cable after it has been parked in the Loading Room.

B6.4.3.5.2 Common Cause Failures

There is one common-cause failure associated with two interlock failures on the slide gates. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

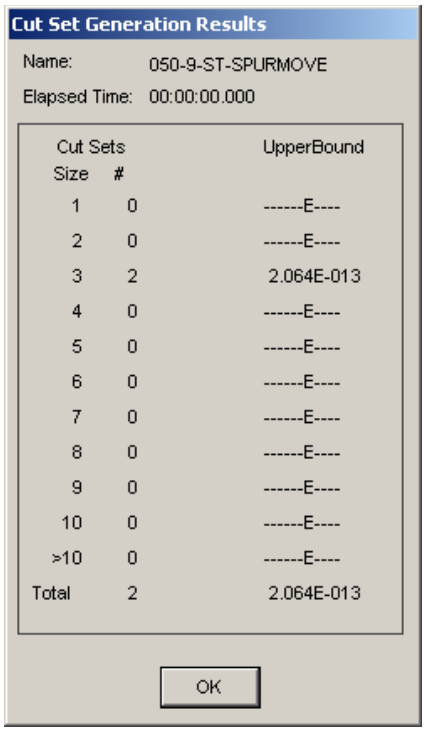
B6.4.3.6 Uncertainty and Cut Set Generation

Figures B6.4-9 and B6.4-10 contain the uncertainty and the cut set generation results for "Site Transporter Spurious Movement" using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-9. Uncertainty Results for the Site Transporter Spurious Movement Fault Tree



Source: Original

Figure B6.4-10. Cut Set Generation Results for the Site Transporter Spurious Movement Fault Tree

B6.4.3.7 Cut Sets

Table B6.4-6 contains the cut sets for the "Site Transporter Spurious Movement" fault tree.

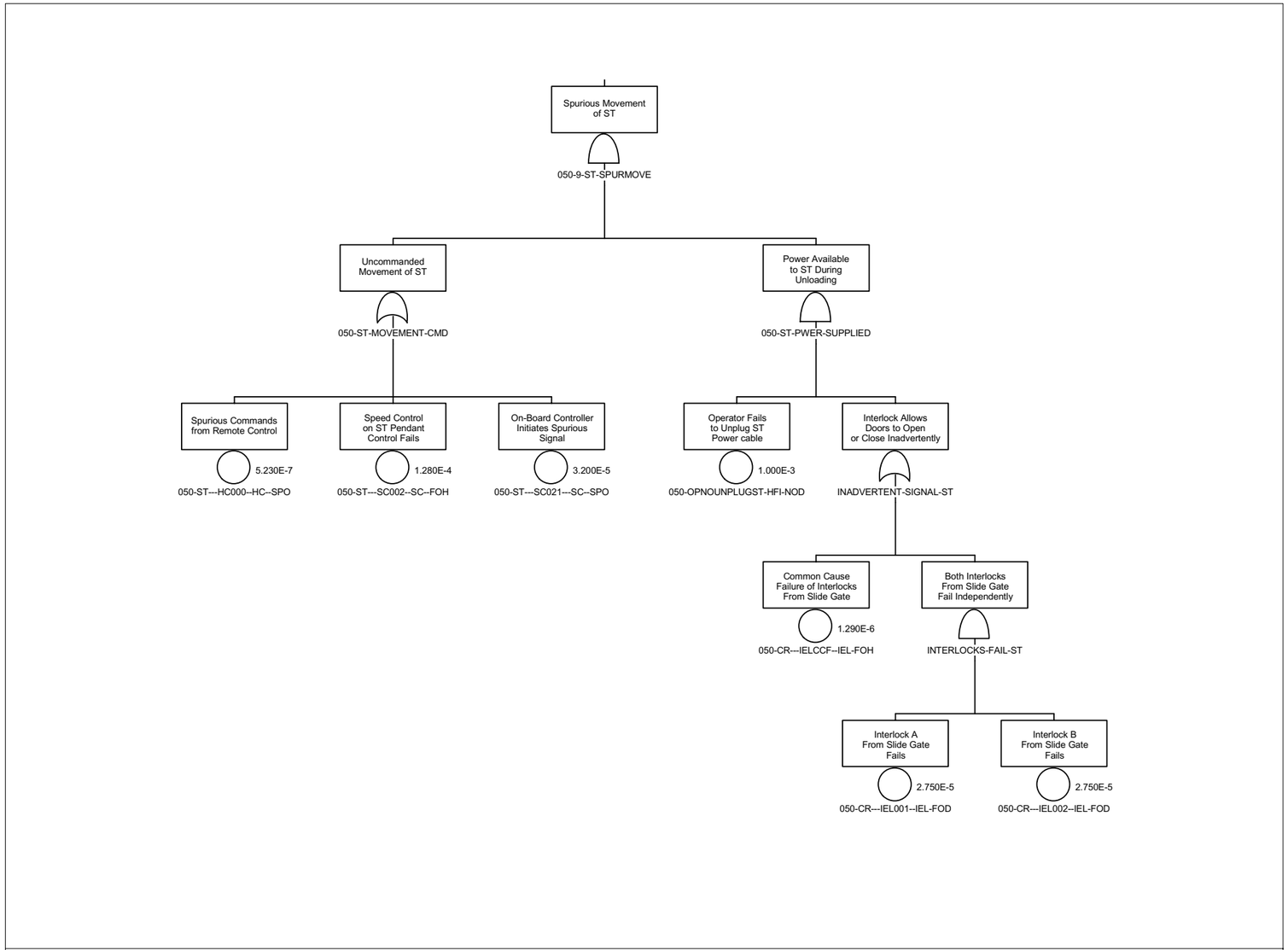
Table B6.4-6. Cut Sets for the Site Transporter Spurious Movement

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-9-ST-SPURMOVE	80.00	1.651E-013	060-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			060-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			060-ST---SC002--SC--FOH	Speed Control on ST Pendant Control Fails	1.3E-004
	20.00	4.128E-014	060-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			060-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			060-ST---SC021---SC--SPO	On-Board Controller Initiates Spurious Signal	3.2E-005
				2.064E-013	

NOTE: ST = site transporter.

Source Original

B1.4.3.8 Fault Tree



Source: Original

Figure B6.4-11. Site Transporter Spurious Movement

B7 HEATING VENTILATION AND AIR CONDITIONING FAULT TREE ANALYSIS

B7.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B7.1.1 BSC 2007. *WHF Equipment sizing and Selection Calculation (ITS)*. 050-M8C-VC00-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071031.0001.

B7.1.2 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System—Train A Ventilation & Instrumentation Diagram*. 050-M80-VC00-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0014.

B7.1.3 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System—Train B Ventilation & Instrumentation Diagram*. 050-M80-VC00-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0015.

B7.1.4 *BSC 2007. *Wet Handling Facility Composite Vent Flow Diagram Tertiary Confinement Non-ITS HVAC Supply & Exhaust System.* 050-M50-VCT0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0002.

B7.1.5 BSC 2007. *Project Design Criteria*. 000-3DR-MGR0-00100-000-007. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071016.0005.

B7.1.6 BSC 2007. *WHF Air Pressure drop Calculation (ITS),* 050-M8C-VC00-00600-000-00A, Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070503.0009.

B7.1.7 BSC 2007. *Leak Path Factors For Radionuclide Releases From Breached Confinement Barriers And Confinement Areas.* 000-00C-MGR0-01500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0002.

B7.1.8 Not used.

Design Constraints

B7.1.9 NRC (Nuclear Regulatory Commission) 2007. *Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program.* HLWRS-ISG-03. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20070918.0096.

B7.2 IMPORTANT TO SAFETY HVAC DESCRIPTION

The important to safety (ITS) heating, ventilation, and air-conditioning (HVAC) is a two train system of identical components. One train is always operational and one train is in standby mode. This system is not configured to run both trains at the same time without bypassing control circuitry. This off-normal situation is not addressed in this analysis.

Figure B7.2-1 shows the locations of the various pieces of ITS HVAC equipment described in the following sections. Sizing of the ITS HVAC in the Wet Handling Facility (WHF) (Ref. B7.1.1) was performed to ensure desired air distribution, ventilation rates, and transport velocities were attainable to maintain the required delta pressure within the C2 confinement zones in this facility.

In the WHF, each HVAC train exhausts air through separate discharge ducts to the atmosphere. Although these trains are interconnected through interior duct work, the trains are independent. A backdraft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

This HVAC system is composed of four subsystems:

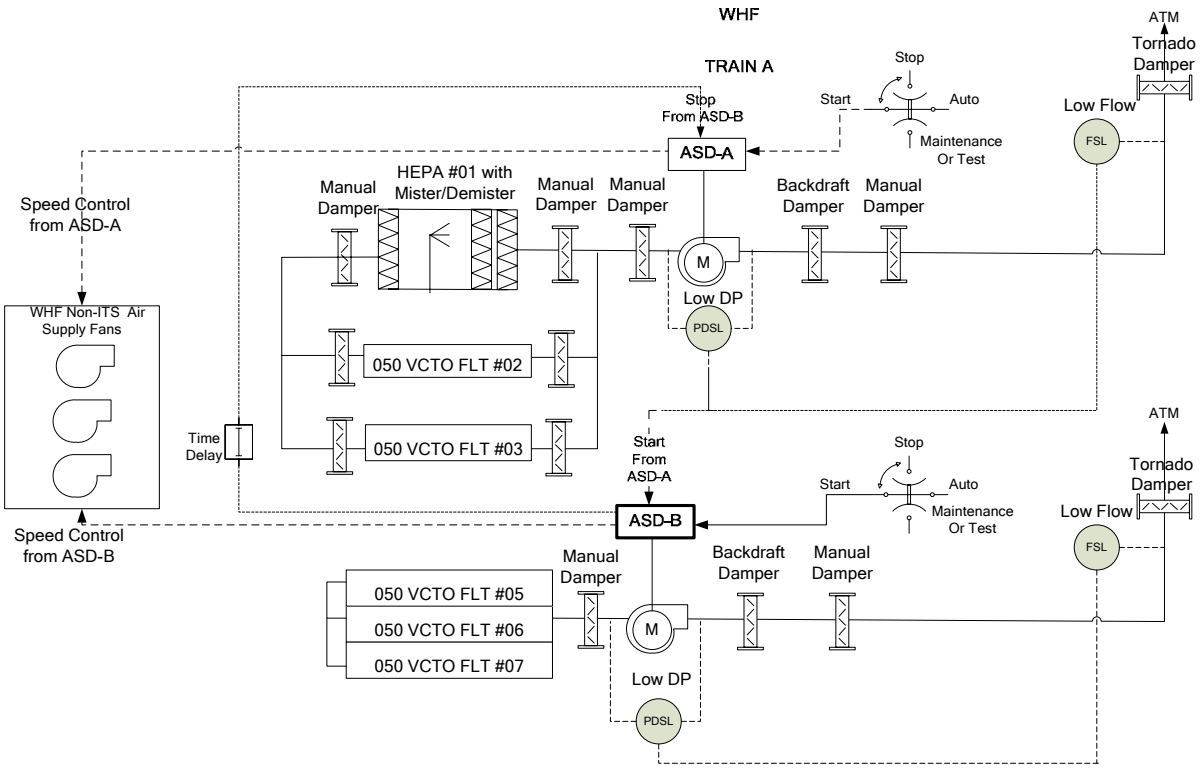
1. A series of dampers are used to control pressure, flow, and flow direction.

2. Three high-efficiency particulate air (HEPA) filters, each consisting of one medium efficiency roughing filter (60 to 90% efficiency), two high efficiency filters for particulate removal (99.97% efficiency) (Ref. B7.1.7, Section 6.1) and a mister/demister for maintaining proper humidity levels[3].

3. One exhaust fan with a rated capacity of 40,500 cubic feet per minute (cfm) and an exhaust fan motor rated at 200 horsepower (Ref. B7.1.1, Section 6.1.2).

4. Control circuitry with logic contained in an erasable programmable read-only memory located in the adjustable speed drive (ASD) controller used for controlling the speed of the operating fan and on fault detection (Ref. B7.1.1, Section 3.2.3) for off-nominal conditions, shutting down the operating train and transmitting signals to the standby system to start[4].

[3] There is a water deluge system in each HEPA filter which is used in fire scenarios. Refer to the facility fire analysis for information regarding these pieces of equipment.
[4] The ASD also controls non-ITS supply fans that are adjusted to maintain airflow in the facility.



NOTE: The diagram has been simplified with respect to the HEPA filter equipment shown for Train A and B. The equipment configuration for HEPA filters identified as 050 VCTO FLT 02, 03, 05, 06 and 07are identical to the HEPA FLT 01. In addition, Train B has the same input/output dampers shown for Train A. Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Original

Figure B7.2-1. Block Diagram of the WHF ITS HVAC System

B7.2.1 Damper Subsystem Description

The ITS HVAC system utilizes manual, backdraft, and tornado dampers to control the delta pressure inside the containment area or to isolate the standby system from the outside atmosphere.

Manual dampers are located on the input and output sides of the HEPA filter. These filters are used to isolate the HEPA filter, if required, during maintenance. There is a manual damper on the input side of the exhaust fan that is used to isolate the entire HEPA filter subsystem for maintenance on the HEPA filters or the exhaust fan. One additional manual damper is located between the backdraft and the tornado damper which can be used to isolate the entire train.

A backdraft damper is located on the exhaust side of the fan. This damper is normally open for the operating train and closed on the standby train. This damper prevents a reverse airflow through the standby system as a result of the negative-delta pressure in the containment Class C2 areas.

A tornado damper is used to control airflow automatically to prevent the transmission of tornado pressure surges from outside the facility.

B7.2.2 HEPA Filters

The three HEPA filter units are identical consisting of a 3 by 3 array of medium (nine filters) and two banks of high-efficiency HEPAs (18 filters). A bag-in/bag-out procedure is used to replace the HEPA filters. Each filter is sized for a flow of 1,500 cfm, which is in the range specified in the *Project Design Criteria Document* (Ref. B7.1.5, Section 4.9.2.2.7). The failure analysis includes the HEPA filter bank for plugs and leaks, mister/demister for humidity control, and the medium roughing filter.

The HEPA subsystem also contains the following components that are not modeled in the analysis: inlet test section, combination test section, the outlet test section, and the deluge system during fire scenarios.

B7.2.3 Direct Drive Exhaust Fan and Motor

The exhaust fan and motor are sized to provide a maximum airflow rate of 40,500 cfm. To meet delta pressure requirements for the WHF, the exhaust system must provide an airflow rate of 38,910 cfm (Ref. B7.1.1, Appendix A, Table A-1). At this airflow rate, the exhaust system will provide for a total of 14.6 inches of water column required to maintain delta pressure in the facility (Ref. B7.1.6, Section 7).

The exhaust fan motor is rated at 1800 revolutions per minute (rpm), but the actual speed is controlled by an ASD. The ASD will adjust the speed to maintain delta pressure when facility doors are opened, HEPA filters loose efficiency, or high outside wind speeds.

B7.2.4 Control Circuitry

The ITS HVAC system is controlled by erasable programmable read-only memory[5]. This control logic is contained in the ASD which is used to monitor the delta pressure across the exhaust fan and airflow rate exhausting to the atmosphere. Changes in air pressure will cause the ASD to change the rpm of the exhaust fan motor. The ASD will also control the rpm of the non-ITS supply fans (Ref. B7.1.2, Ref. B7.1.3, and Ref. B7.1.4)[6].

At any time the ASD can not return the delta pressure to normal operating conditions, the ADS will shut down the operating train and send a signal to the standby train to start up. When the standby ASD receives this signal, it will start the standby system and send a signal to the operational train to shutdown. There is an interlock to preclude the operation of both trains at the same time. Time delays are built-in to the ASD processing system to preclude spurious signals received from the sensors triggering a false transfer.

[5] Although there are programmable logic controls in various locations throughout the WHF, none of these are ITS

[6] The supply fans are used to stabilize the airflow within the WHF. These fans are non-ITS so they are not accounted for in this analysis except in a degraded mode of operation.

B7.2.5 ITS HVAC Normal Operations

In normal operations, Train A is operational and Train B is in standby. Electronics (EPROM) within the ASD monitor the pressure differential across the exhaust fan and the flow rate of the exhaust to the atmosphere. There are no programmable logic controllers used in the ITS HVAC control system and all interlocks are hardwired for ITS operation. The delta pressure sensor and low flow sensor are ITS equipment with defined set points for WHF ASD-A response to the various deviations from these set points are shown in Table B7.2-1.

Table B7.2-1. ASD Response to Variations in Delta Pressure

DP Pressure Sensor	Low Flow Sensor	ASD Response
High DP (Plugged HEPA)	Low Flow	Switch Trains
High DP	High Flow	Decrease RPM of Exhaust Fan
High DP	Nominal Flow	Increase RPM of Supply Fans
Low DP (HEPA Leak)	High Flow	Switch Trains
Low DP	Nominal Flow	Decrease RPM of Supply Fans
Low DP	Low Flow	Increase RPM of Exhaust Fan

NOTE: ASD = adjustable speed drive; DP = delta pressure; HEPA = high-efficiency particulate air (filter); RPM = revolutions per minute.

Source: Original

If the responses can not return the delta pressure and flow rates to nominal states, the ASD will issue the command to the ASD-B to startup train B. ASD-B will command the startup of Train B exhaust fan and send a signal back to ASD-A to shut down. An interlock prevents both trains from operating at the same time.

Under normal operations with non-ITS supply fans working, all three HEPA filter assemblies in the train must be working to achieve the exhaust flow rate of 38,910 cfm (Ref. B7.1.1, Section 6.1.1). Each HEPA filter array can filter 13,500 cfm at maximum efficiency (Ref. B7.1.1, Section 6.1.1). The design has some reserve capacity but not enough to maintain the required delta pressure if one of the HEPA filters fail. Under normal operations, the only redundancy in the design is the second train.

Misters/demisters are included as part of the HEPA filters to control the temperature and relative humidity of the air passing through the filters. The water deluge system is not considered to be normal operations and is handled in the fire suppression analyses.

During receipt of a transportation cask or aging over pack or during the export of an aging overpack, delta pressure is lost for a period of time not to exceed seven minutes per event.[7] This occurs as a direct consequence of opening vestibule doors to allow entry or exit of the site transporter, the site prime mover, or the horizontal cask tractor trailer.

[7] This is a conservative estimate of the time it will take for the HVAC system to return the vestibule to a negative pressure.

B7.2.6 ITS HVAC Off-Nominal Operations

The ITS HVAC system maintains proper delta pressure throughout Class C2 designated containment areas. Exhausted air from the WHF is made-up from opening/closing doors to the outside, leaks in the structure and from three supply fans which are controlled by the ASD on the operating train. These fans in conjunction with other air makeup sources can provide sufficient airflow through the C2 containment areas for the HVAC to maintain delta pressure. These supply fans are not ITS and therefore, are not connected to the ITS power system for the WHF. Should there be a loss of non-ITS site power or for a mechanical reason these fans shut down, the HVAC system can be operated in a degraded mode. Since there is less air to exhaust, Train A no longer has to exhaust 38,910 cfm. It then becomes possible to maintain delta pressure with two of three HEPA filters. This special case has been added to the fault trees for the failure to maintain delta pressure in the WHF. In this case, there is redundancy within the train and a common-cause failure mode has been added to the fault tree.

B7.2.7 ITS HVAC Testing and Maintenance

Under normal operations Train A will continue to operate until a failure is detected or the train is shut down for maintenance. Normal maintenance will render train B unavailable 40 hours per year[8]. During maintenance, the train B start/stop/auto/maintenance switch is placed in the maintenance position. When maintenance is completed, the standby system (train B) will be started and operational system (train A) will be shut down and is now considered to be the standby train (train B). Maintenance may be scheduled consecutively for this train or at some future date. Under normal operations, maintenance will not result in the loss of/or the inability of the operating train to perform its intended function.

Testing is considered part of routine maintenance. When the maintenance has been completed, maintenance personnel will turn the standby train on and check for normal operations including delta pressure, flow rate, and that all failure indicators are reset/off. Maintenance personnel will also observe the forced shutdown of the operating system as the standby train is turned on.

Flow rates are monitored as part of testing to ensure that the manual dampers for the active train are in the proper position to achieve a balanced airflow across the three HEPA filters. Once the dampers have been adjusted, they will not require further adjustment unless a damper or combination of dampers must be closed to isolate a component in the train or the entire train.

B7.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B7.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.

[8] The majority of operational-level maintenance can be performed on the operational train and therefore does not affect the overall availability of the standby train.

4. Human dependence.
5. Failures based on external events.

Table B7.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
ASD	Flow and pressure sensors	—	—	—	—
	Speed control for fan/motor	—	—	—	—
DP Exhaust Fans	—	Wind speed	—	—	—
Stop/Start/Auto Switch Position	—	—	—	Wrong position	—
Dampers	—	—	—	Wrong position	—
ITS Power	HVAC shuts down	—	—	—	—
Non-ITS Power	—	—	—	—	Supply fans stop
HEPA	—	—	—	Failure to notice leak	—
HVAC Maintenance	—	—	—	Trains can not switch	—
Vestibule Doors	Open only one door at a time	—	—	—	—

NOTE: ASD = adjustable speed drive; DP = delta pressure; HEPA = high-efficiency particulate air (filter); HVAC = heating, ventilation and air-conditioning; ITS = important to safety.

Source: Original

B7.4 HVAC RELATED FAILURE SCENARIO

B7.4.1 Failure to Maintain Delta Pressure

B7.4.1.1 Description

There is a single failure scenario used in this analysis. The components of the HVAC system used inside buildings to maintain C2 in areas that are normally clean and where airborne contamination is not expected during normal facility operations. The ITS HVAC equipment maintains a positive airflow from outer confinement areas through the HEPA filters to the atmosphere (Ref. B7.1.4).

Within the WHF the areas designated as C2 are the following: Cask Preparation Area, Cask Unloading Room, Loading Room, and the Canister Transfer Room on the second floor.

B7.4.1.2 Success Criteria

Success criteria for maintaining delta pressure in the WHF requires that one of two HVAC trains is operational. The sizing of the exhaust motor and fan assembly will maintain the delta pressure in sustained winds of 40 mph with less than three second gusts up to 90 mph. In addition, delta pressure will be lost for a period of time not to exceed seven minutes in the WHF if and only if one of the vestibule doors is open. These doors are interlocked to ensure only one door is open at a time during normal operations.

Switching between the active and standby trains is controlled by ASD-A (active train) which continually monitors the pressure across the exhaust fan and the air flow rate exhausting from the WHF. These sensors are in a one of two configuration which means that the ASD will initiate the transfer of operations from the active train to the standby train when either one of these sensors can not be returned to a normal operating range by the ASD by controlling, in some combination, the speed of the supply and exhaust fans.

ASD-A must be able to recognize an uncorrectable airflow rate in train A and transmit a signal to ASD-B to start. Having received the start command, ASD-B must send a signal back to ASD-A commanding a stop.

Maintaining delta pressure during/after the switchover requires the "Start/Stop/Maintenance" or "Test/Auto" switch be in the auto position, the train B exhaust fan and motor start, and the airflow across the HEPA filters adjusted by ASD-B to maintain delta pressure.

With the exception of the tornado and backdraft dampers, all control dampers in the ITS HVAC system are manual dampers. These dampers are typically set once for air balancing. These dampers may be adjusted or closed when maintenance is required on the standby train. Should the damper setting be changed, it would require the maintenance personnel to return the damper to its proper position to ensure balanced airflow.

B7.4.1.3 Design Features and Inputs

System configuration and operating conditions requirements:

- There is only one HVAC train in operation at anytime. The second train shall always be in standby (exception—when train B is off-line for maintenance).

- Alarms are on a panel in the continuously manned central control station and responded to by operators. Alarm conditions are: ASD trouble, fan failure, motor running/stop, and flow rate problem. Operators are not required to respond to the alarm (ITS-HVAC trains are switched automatically); however, operators are expected to notify maintenance that a switch has occurred and maintenance will be required to determine the cause of the failure and correct it.

Design Feature:

ITS HVAC system is in normal operations with three HEPA filter units. Each HEPA filter unit consists of one 3 × 3 medium filter array and two 3 × 3 HEPA high-efficiency filter arrays.

The only difference between the ITS HVAC in the WHF, CRCF, and RF facilities are the number of non-ITS fans operating in the facility.

Testing and Maintenance

Requirements:

- HVAC maintainers shall be notified when an alarm condition exists. Repair shall be performed as soon as possible to return train to standby status.
- While HVAC train is in maintenance, the other train is not available for service..
- Testing performed on the HVAC system must be done on the active system since both trains can not be operational at the same time.

Design Feature:

Normal maintenance is performed in accordance with manufacture's recommendations; however, the majority of preventative maintenance will not require shutting down the active system.

B7.4.1.4 Fault Tree Model

The top event in this fault tree is "Delta Pressure not Maintained in WHF Facility." This is defined as the inability of the ITS HVAC system to maintain proper delta pressure within the facility. The ITS HVAC system is a two train system. The configuration of the ITS HVAC systems in these facilities is essentially identical. The only variations are the number of non-ITS supply fans used to stabilize the airflow within these buildings.

- The fault tree model for the loss of delta pressure in the facility includes those components that have been designated as ITS. There is only one exception and that is the inclusion of two non-ITS supply fans. The fans were added to stabilize air pressure differentials in the facility during normal operations and provide a capability for operating in a degraded mode.
- There are two interlocks in the ITS HVAC system. The first addresses the potential for opening two or more of the entrance/exit vestibule doors. (Note: There is no physical connection between this door interlock and the HVAC system.) The second interlock prevents two HVAC trains from operating at the same time.
- The mission time for the ITS HVAC system is currently set to 720 hours (Ref. B7.1.9). To take into account the differences in failure rates for active and standby systems, all basic events in the standby train are set to half that of the active system. For ease of implementation in SAPHIRE, the rate data is maintained constant and the mission time is set to 1/2 the mission time or 360 hours.

B7.4.1.5 Basic Event Data

Table B7.4-1 contains a list of basic events used in the loss of delta pressure in the WHF. Five basic events have been highlighted:

- Three associated with human error
- One to account for the unavailability of the standby train due to scheduled maintenance
- Common-cause failure to account for the possibility that, in the degraded mode, a failure of one of the three HEPA filters may result in a common-cause failure of the second or third filter. This is applicable to both trains. The alpha method was used to determine the common-cause value using two-of-three as the success criteria.
- Common-cause failure to account for the possibility that the three supply fans fail due to a common-cause failure. The alpha method was used to determine the common-cause value using three-of-three as the success criteria.

Table B7.4-1. Basic Event Probability for the HVAC Loss of Delta Pressure in the WHF

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN Loss of Delta P in WHF Name	**Calculation Type**	**Case : Current Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time**
050-EXCESSIVE-WIND-SPEED	1	4.700E-003	4.700E-003	0.000E+000	0.000E+000
050-VC5O-HFIA000-HFI-NOM	1	1.000E-003	1.000E-003	0.000E+000	0.000E+000
050-VCOO-NITS-PWR-FAILS	3	3.536E-002	1.000E+000	5.000E-005	0.000E+000
050-VCOO-SFAN001-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	0.000E+000
050-VCOO-SFAN002-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	0.000E+000
050-VCOO-SFAN003-FAN-FTR	3	2.562E-002	0.000E+000	7.210E-005	3.600E+002
050-VCSO-B000000-FAN-FTS	1	2.020E-003	2.020E-003	0.000E+000	0.000E+000
050-VCSO-DMP000A-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP000B-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP000B-DMP00B	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-DMP001A-DMP-FOH	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP001A-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP001A-DMP00A	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-DMP001B-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP001B-DMP00B	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-DMP001I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP001O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP002I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP002O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
050-VCSO-DMP003I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	7.200E+002

Table B7.4-1. Basic Event Probability for the HVAC Loss of Delta Pressure in the WHF (Continued)

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN Loss of Delta P in WHF Name	**Calculation Type**	**Case : Current Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time**
050-VCSO-DMP003O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	7.200E+002
050-VCSO-DMP005I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP005O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP006I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP006O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP007I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DMP007O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
050-VCSO-DR00001-HFI-NOD	1	1.000E-002	1.000E-002	0.000E+000	0.000E+000
050-VCSO-DRS0000-DRS-OPN	1	1.600E-004	1.600E-004	0.000E+000	0.000E+000
050-VCSO-DTC0A-DTC-RUP	3	2.675E-003	0.000E+000	3.720E-006	7.200E+002
050-VCSO-DTC0B-DTC-RUP	3	1.338E-003	0.000E+000	3.720E-006	3.600E+002
050-VCSO-ELEC-CIRCUITBRK	I	0.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-FAN00A-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	7.200E+002
050-VCSO-FAN00B-FAN-FTR	3	2.562E-002	0.000E+000	7.210E-005	3.600E+002
050-VCSO-FAN00B-FAN-FTS	1	2.020E-003	2.020E-003	0.000E+000	0.000E+000
050-VCSO-FANA-PRM-FOH	3	1.820E-003	0.000E+000	2.530E-006	7.200E+002
050-VCSO-FANB-PRM-FOH	3	9.104E-004	0.000E+000	2.530E-006	3.600E+002
050-VCSO-FANB-SC-FOH	3	3.873E-004	0.000E+000	5.380E-007	7.200E+002
050-VCSO-FSLAB0-SRF-FOH	3	7.701E-004	0.000E+000	1.070E-006	7.200E+002
050-VCSO-HEPAB-CCF	3	3.852E-005	0.000E+000	1.070E-007	7.200E+002
050-VCSO-HEPA01-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	7.200E+002
050-VCSO-HEPA02-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	7.200E+002
050-VCSO-HEPA03-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	7.200E+002
050-VCSO-HEPA05-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
050-VCSO-HEPA06-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
050-VCSO-HEPA07-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
050-VCSO-HEPAA01-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	7.200E+002
050-VCSO-HEPAA01-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	7.200E+002
050-VCSO-HEPAA02-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	7.200E+002
050-VCSO-HEPAA02-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	7.200E+002
050-VCSO-HEPAA03-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	7.200E+002
050-VCSO-HEPAA03-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	7.200E+002
050-VCSO-HEPAB05-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002
050-VCSO-HEPAB05-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
050-VCSO-HEPAB06-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002
050-VCSO-HEPAB06-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
050-VCSO-HEPAB07-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002

Table B7.4-1. Basic Event Probability for the HVAC Loss of Delta Pressure in the WHF (Continued)

BASIC EVENTS PROBABILITY REPORT					
Project: YUCCA-MOUNTAIN Loss of Delta P in WHF Name	**Calculation Type**	**Case : Current Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time**
050-VCSO-HEPAB07-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
050-VCSO-HEPALK-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-HFIA000-HFI-NOM	1	1.000E-001	1.000E-001	0.000E+000	0.000E+000
050-VCSO-HVAC-DEGRADED	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-IEL0001-IEL-FOD	3	2.439E-002	0.000E+000	3.430E-005	7.200E+002
050-VCSO-PDSLA0B-SRP-FOD	1	3.990E-003	3.990E-003	0.000E+000	0.000E+000
050-VCSO-SUPFAN-CCF	3	3.213E-003	0.000E+000	4.470E-006	7.200E+002
050-VCSO-TDMP00A-DTM-FOD	3	1.614E-002	0.000E+000	2.260E-005	7.200E+002
050-VCSO-TDMP00A-DTM-FOH	3	1.614E-002	0.000E+000	2.260E-005	7.200E+002
050-VCSO-TDMP00B-DTM-FOD	1	8.710E-004	8.710E-004	0.000E+000	0.000E+000
050-VCSO-TDMP00B-DTM-FOH	3	8.103E-003	0.000E+000	2.260E-005	3.600E+002
050-VCSO-TRAIN-A-RC-FAIL	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-TRAIN-B-FAILS	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-TRAIN-B-REDOPS	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
050-VCSO-TRAINB-MAINT	1	4.570E-003	4.570E-003	0.000E+000	0.000E+000
050-VCSO-UDMP000-UDM-FOH	3	8.103E-003	0.000E+000	2.260E-005	3.600E+002
050-VSCO-HEPA-CCF	3	7.704E-005	0.000E+000	1.070E-07	7.200E+002

NOTE: WHF = Wet Handling Facility; P = pressure.

Source: Original

B7.4.1.5.1 Human Failure Events

There are three basic failure events (HFE) associated with human error listed in Table B7.4-2. They are for inadvertently opening two or more vestibule doors at the same time, failure to notice that there is a HEPA leak and leaving the start/stop/auto/maintenance switch on the standby train in the wrong position.

Table B7.4-2. Human Failure Events

Basic Event Name	Basic Event Description
050-VCSO-DR00001-HFI-NOD	Operators open two of more vestibule doors in WHF
050-VCSO-HEPALK-HFI-NOD	Operator fails to notice HEPA filter leak in Train A (or Train B)
050-VCSO-HFIA000-HFI-NOM	Human error exhaust fan switch wrong position

NOTE: HEPA = high-efficiency particulate air (filter); WHF = Wet Handling Facility.

Source: Original

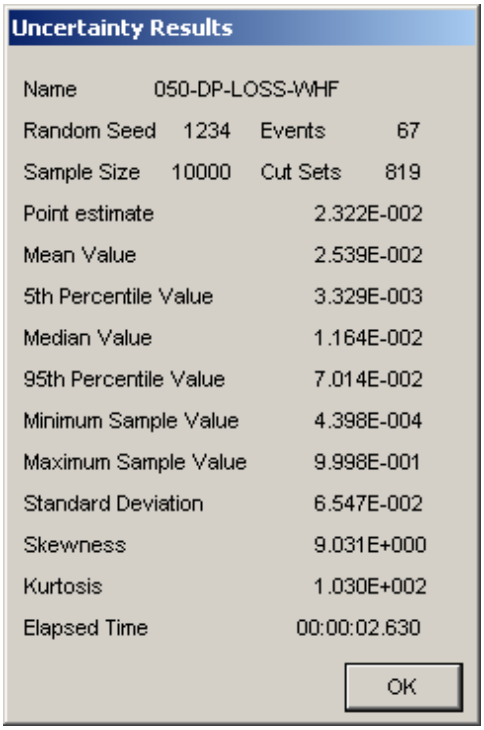
B7.4.1.5.2 Common-Cause Failures

There are two common-cause failures identified in the HVAC model associated with the potential of a HEPA filter failure in the degraded mode where there is a two of three success situation.

There is one common cause failure associated with the three Non-ITS supply fans where a 3 of 3 successes is required to maintain delta pressure.

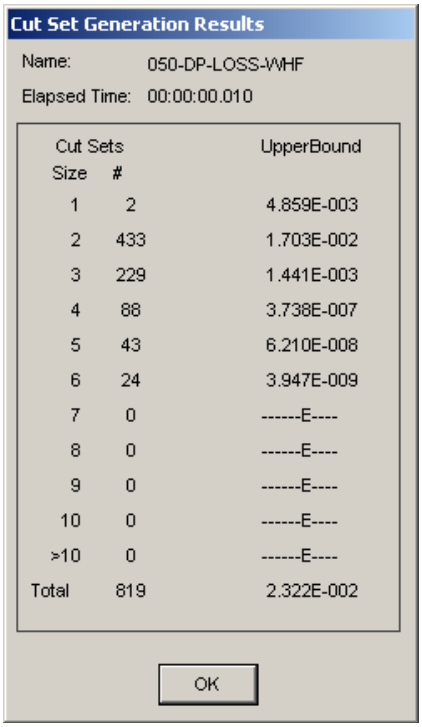
B7.4.1.6 Uncertainty and Cut Set Generation

Figure B7.4-1 contains the uncertainty results obtained from running the fault trees for the loss of delta pressure in the WHF. Figure B7.4-2 provides the cut set generation results for the loss of delta pressure in the WHF.



Source: Original

Figure B7.4-1. Uncertainty Results of the RF Loss of Delta Pressure Fault Tree



Source: Original

Figure B7.4-2. Cut Set Generation Results of the RF Loss of Delta Pressure Fault Tree

B7.4.1.7 Cut Sets

Table B7.4-3 contains the top 25 cut sets for the "Loss of Delta Pressure" in the WHF.

Table B7.4-3. Dominant Cut Sets for the Loss of Delta Pressure in the WHF

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-DP-LOSS-WHF	21.79	5.059E-003	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	20.24	4.700E-003	050-EXCESSIVE-WIND-SPEED	Sustained Wind Exceeds 40 MPH & Gust to 90 MPH	4.7E-003
	6.95	1.614E-003	050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
			050-VCSO-TDMP00A-DTM-FOD	Tornado Damper Train A Fails	1.6E-002
	5.58	1.296E-003	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002

Table B7.4-3. Dominant Cut Sets for the Loss of Delta Pressure in the WHF (Continued)

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
	2.82	6.545E-004	050-VCSO-HEPA01-DMS-FOH	Moisture Separator/Demister HEPA 01 Fails	6.5E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	2.82	6.545E-004	050-VCSO-HEPA02-DMS-FOH	Moisture Separator/Demister HEPA 02 Fails	6.5E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	2.82	6.545E-004	050-VCSO-HEPA03-DMS-FOH	Moisture Separator/Demister HEPA 03 Fails	6.5E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.78	4.136E-004	050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			050-VCSO-TDMP00A-DTM-FOD	Tornado Damper Train A Fails	1.6E-002
	1.77	4.099E-004	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-TDMP00B-DTM-FOH	Tornado damper Train B Fails	8.1E-003
	1.77	4.099E-004	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-UDMP000-UDM-FOH	Backdraft Damper for Train B exhaust Fails	8.1E-003
	1.32	3.070E-004	050-VCSO-HEPAA01-HEP-PLG	HEPA #A01 Train A Plugged	3.1E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001

Table B7.4-3. Dominant Cut Sets for the Loss of Delta Pressure in the WHF (Continued)

Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-DP-LOSS-WHF (continued)	1.32	3.070E-004	050-VCSO-HEPAA02-HEP-PLG	HEPA #A02 Train A Plugged	3.1E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.32	3.070E-004	050-VCSO-HEPAA03-HEP-PLG	HEPA #A03 Train A Plugged	3.1E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.15	2.675E-004	050-VCSO-DTC0A-DTC-RUP	Duct Fails between HEPA and Exhaust Fan (10 feet)	2.7E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.05	2.439E-004	050-VCSO-DR00001-HFI-NOD	Operators Open 2 of Mores Vestibule Doors in WHF	1.0E-002
			050-VCSO-IEL0001-IEL-FOD	WHF Door Interlock Failure	2.4E-002
	1.00	2.312E-004	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-TRAINB-MAINT	Train B HVAC is Off-Line for Maintenance	4.6E-003
	0.93	2.158E-004	050-VCSO-HEPA0A1-HEP-LEK	HEPA #01 Train A Leaks	2.2E-003
			050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.93	2.158E-004	050-VCSO-HEPAA02-HEP-LEK	HEPA #02 Train A Leaks	2.2E-003
			050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.93	2.158E-004	050-VCSO-HEPAA03-HEP-LEK	HEPA #03 Train A Leaks	2.2E-003
			050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001

Table B7.4-3. Dominant Cut Sets for the Loss of Delta Pressure in the WHF (Continued)

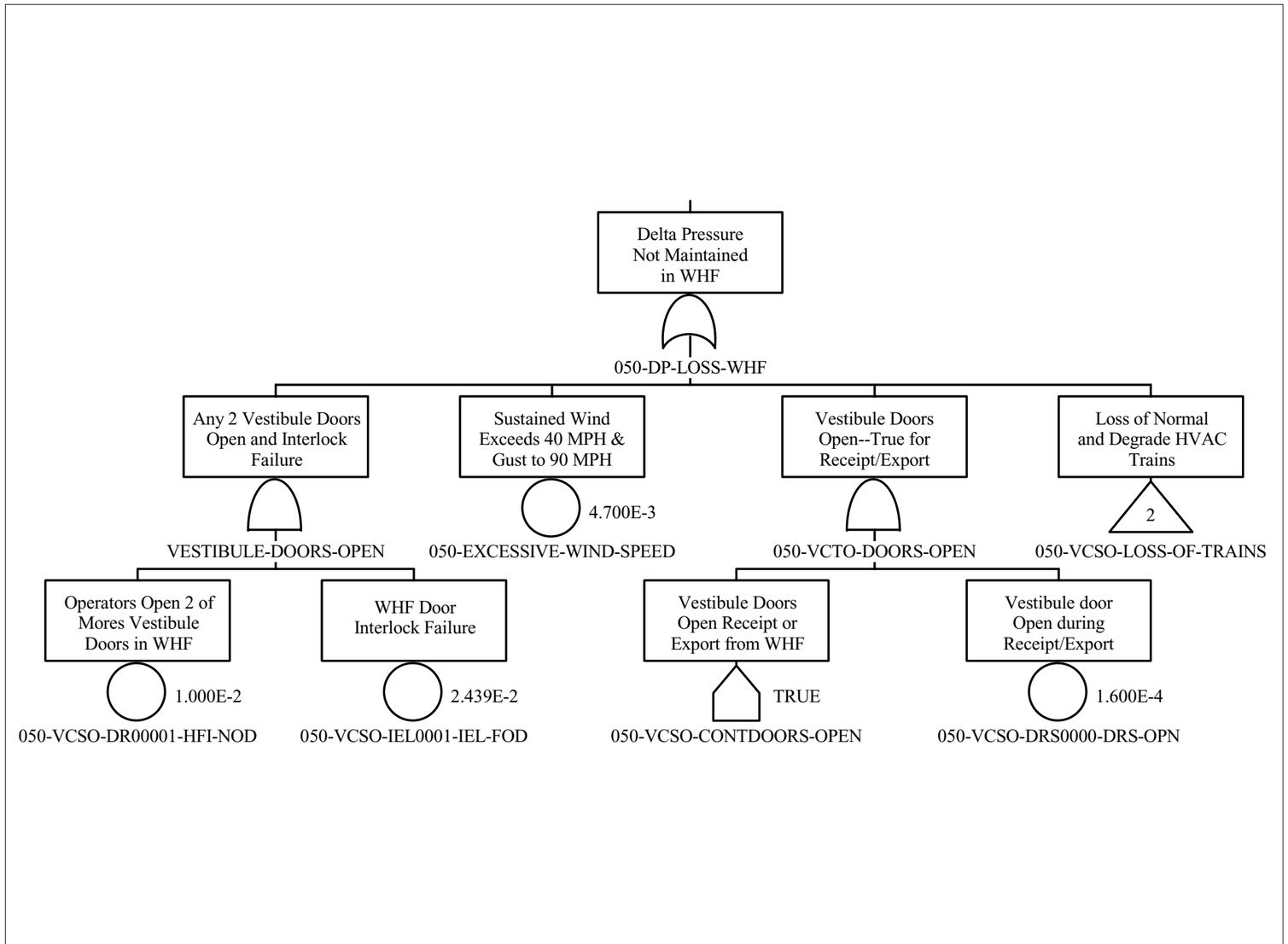
Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
	0.78	1.820E-004	050-VCSO-FANA-PRM-FOH	Speed Control Exhaust fan train A Fails to maintain Delta P	1.8E-003
			050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.72	1.677E-004	050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			050-VCSO-HEPA01-DMS-FOH	Moisture Separator/Demister HEPA 01 Fails	6.5E-003
	0.72	1.677E-004	050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
050-DP-LOSS-WHF (continued)			050-VCSO-HEPA02-DMS-FOH	Moisture Separator/Demister HEPA 02 Fails	6.5E-003
	0.72	1.677E-004	050-VCSO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			050-VCSO-HEPA03-DMS-FOH	Moisture Separator/Demister HEPA 03 Fails	6.5E-003
	0.71	1.658E-004	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-HEPA05-DMS-FOH	Moisture Separator/Demister HEPA 05 Fails	3.3E-003
	0.71	1.658E-004	050-VCSO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			050-VCSO-HEPA06-DMS-FOH	Moisture Separator/Demister HEPA 06 Fails	3.3E-003
	2.322E-002			= Total	

NOTE: HEPA = high efficiency particulate air; MPH = miles per hour.

Source: Original

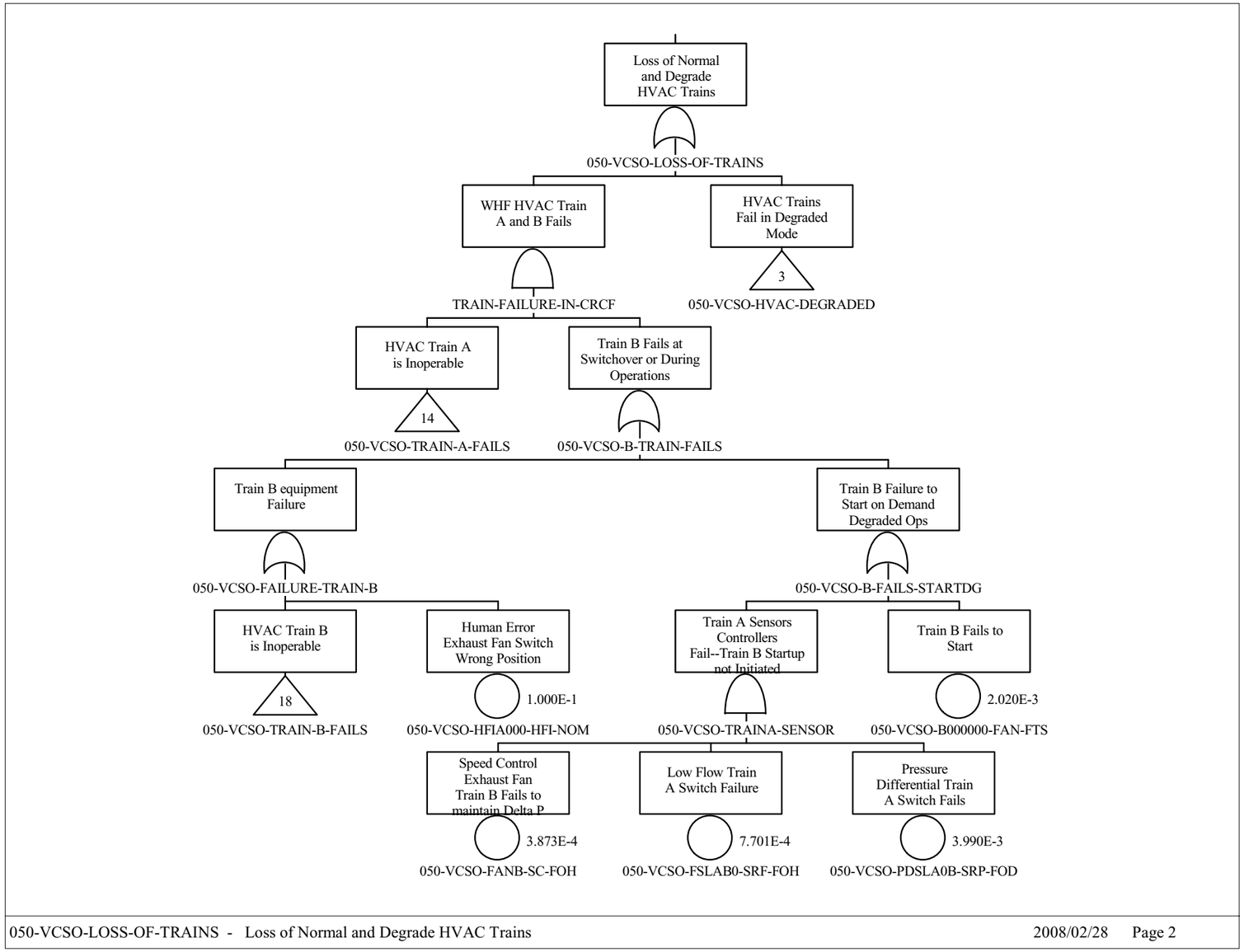
B7.4.1.8 HVAC Fault Trees

For purposes of this report, the transfers to the ITS electrical system for the HVAC equipment is ignored. For specifics on the electrical system, refer to the AC Power System Fault Tree Analysis.



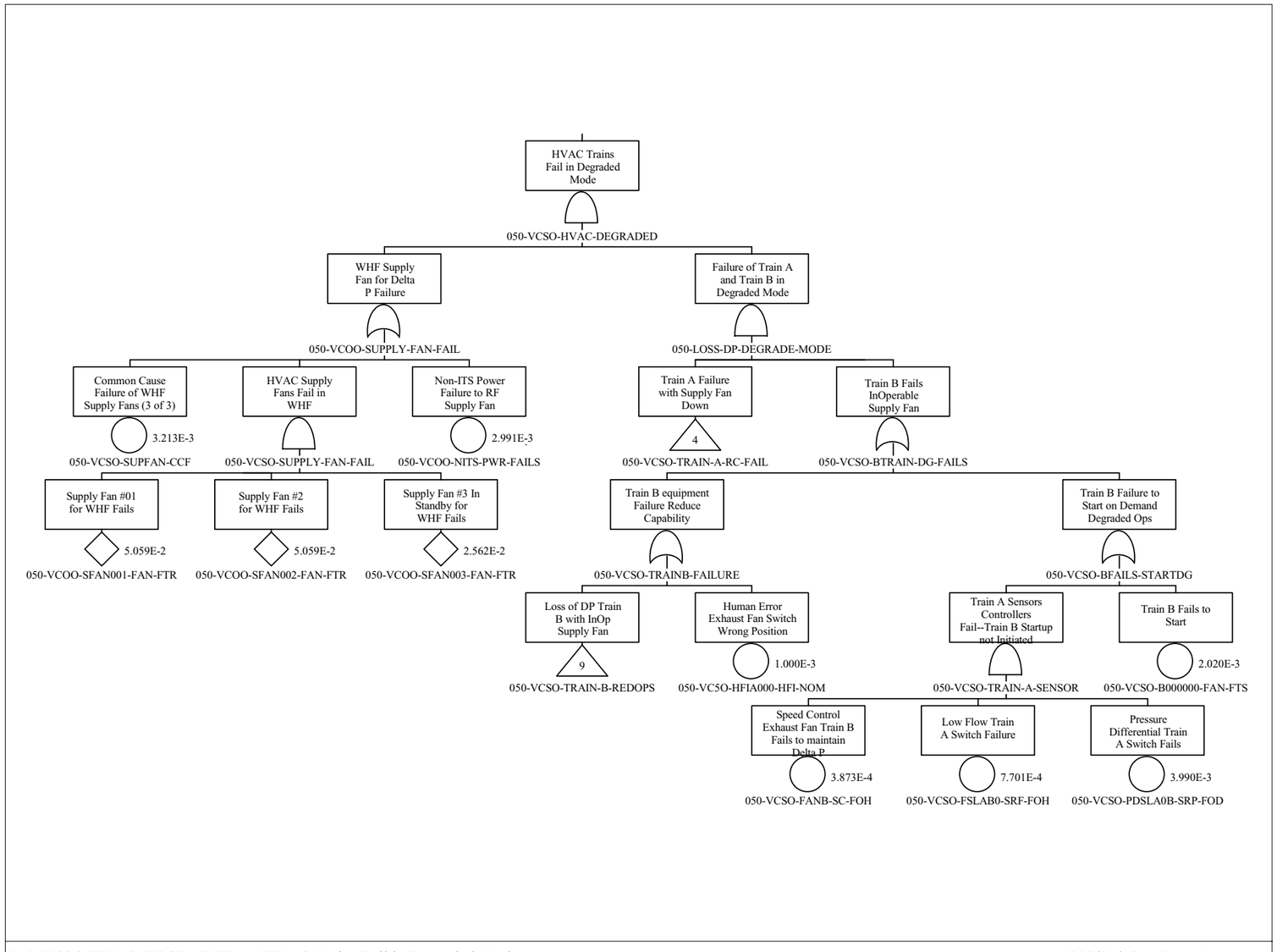
Source: Original

Figure B7.4-3. Delta Pressure not Maintained in WHF



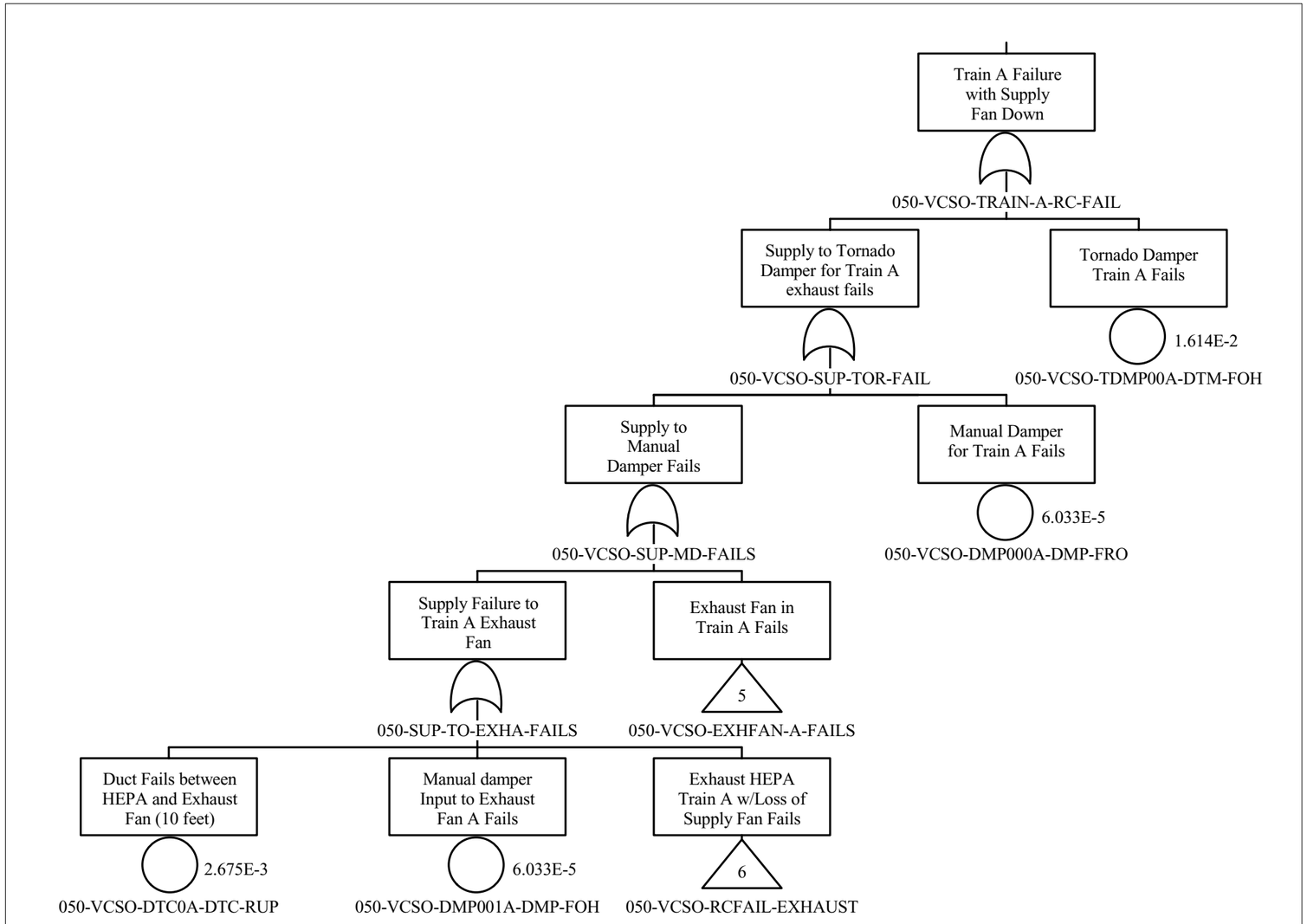
Source: Original

Figure B7.4-4. Loss of Normal and Degrade HVAC Trains



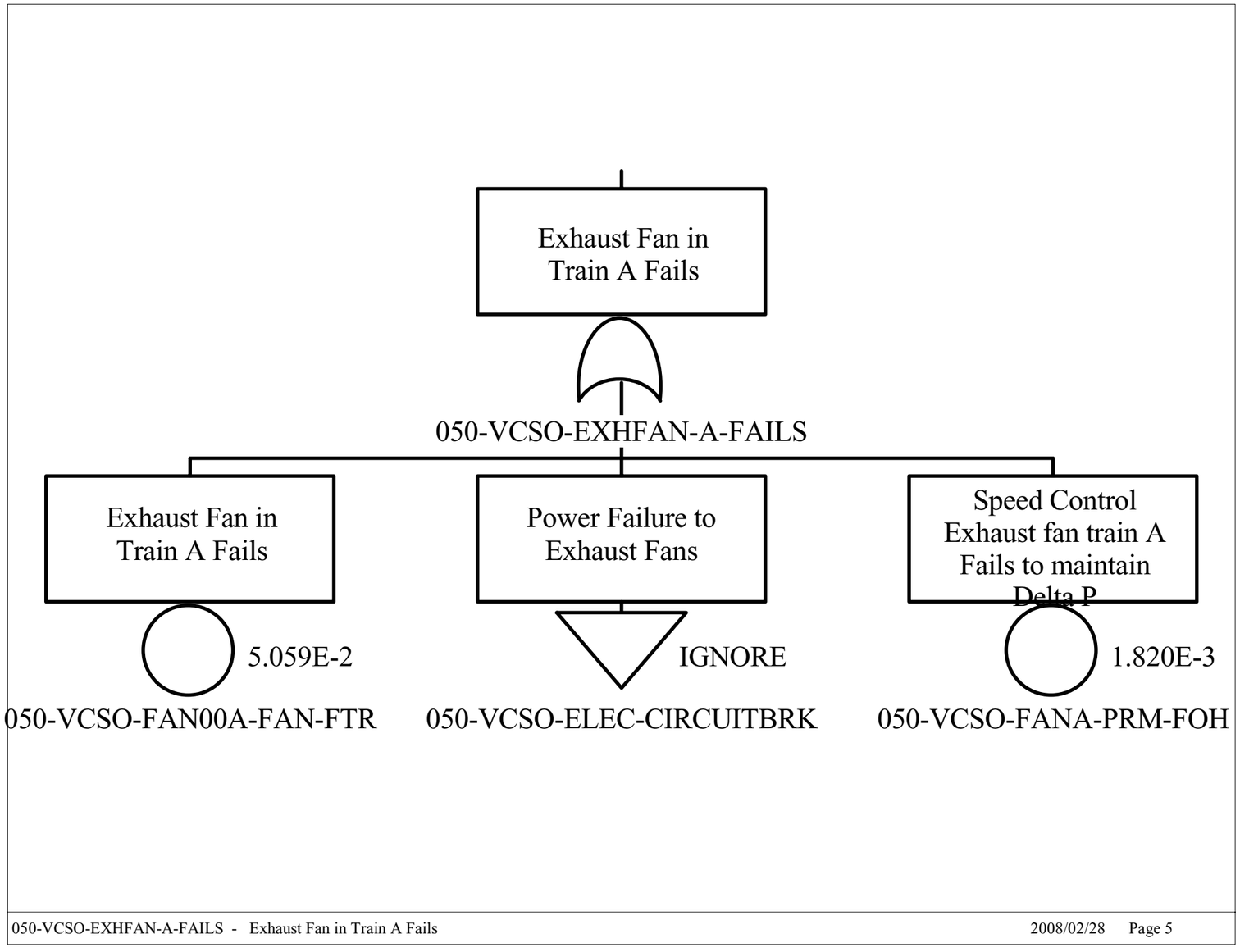
Source: Original

Figure B7.4-5. HVAC Trains Fail in Degraded Mode



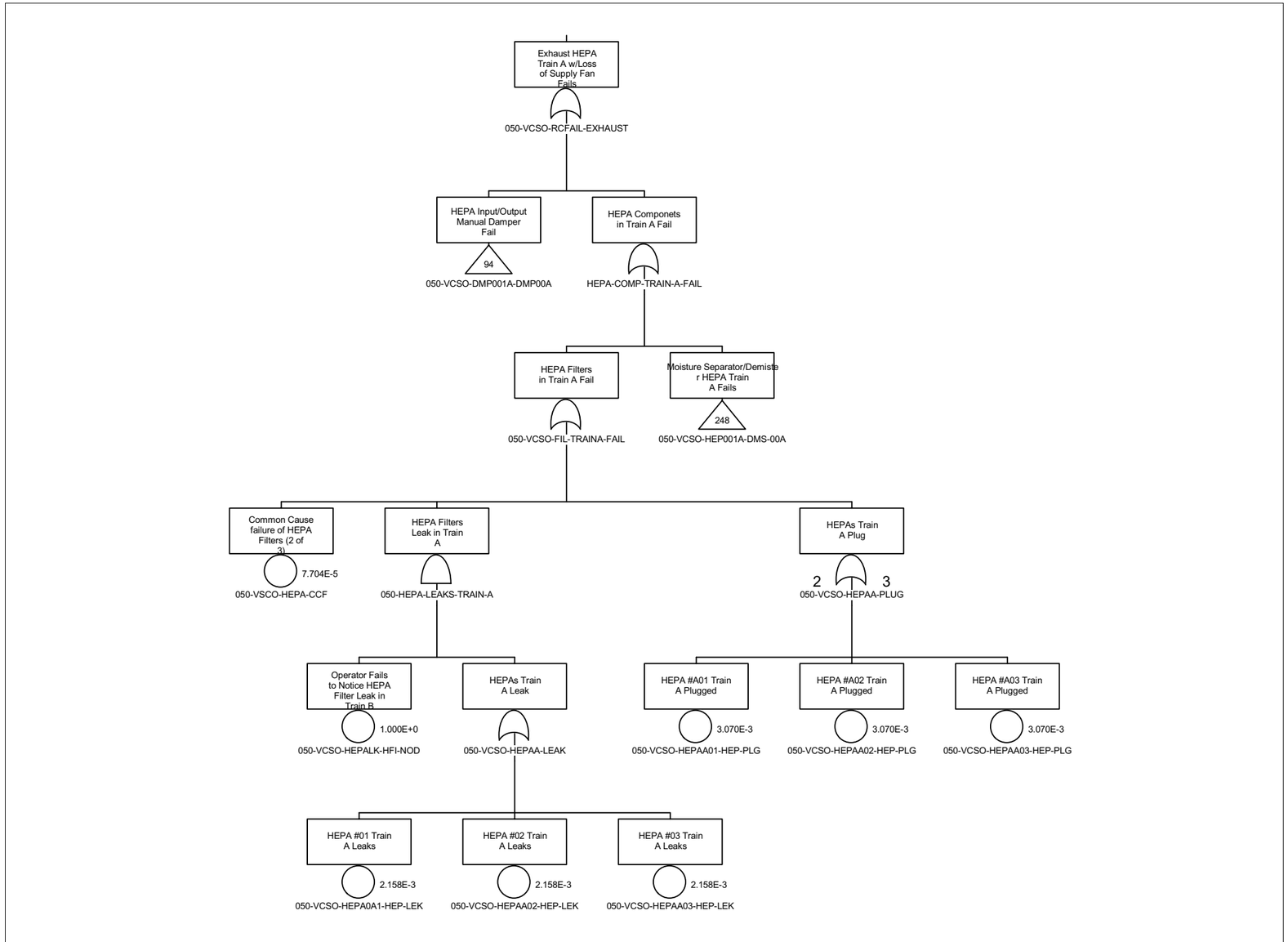
Source: Original

Figure B7.4-6. Train A Failure with Supply Fan Down



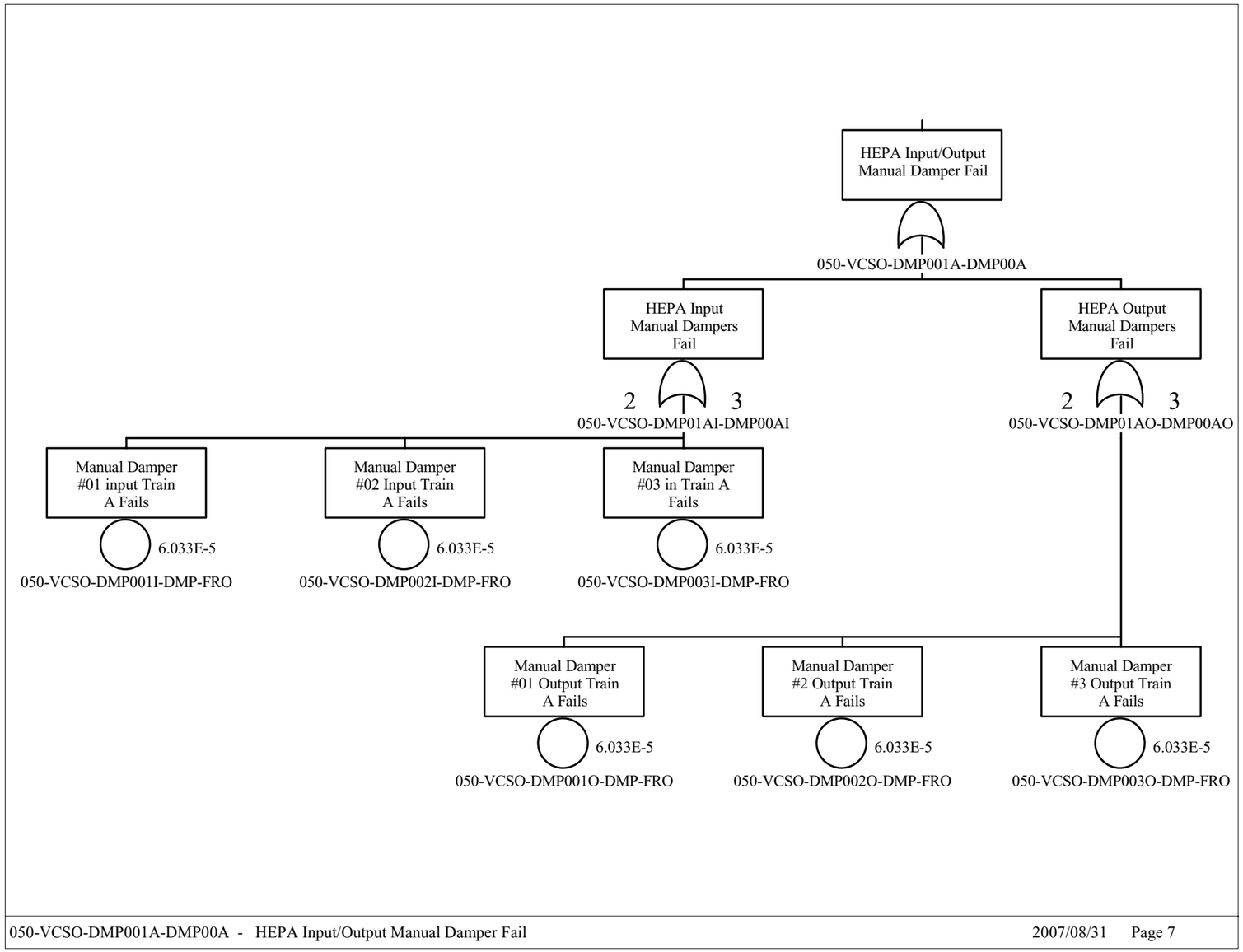
Source: Original

Figure B7.4-7. Exhaust Fan in Train A Fails



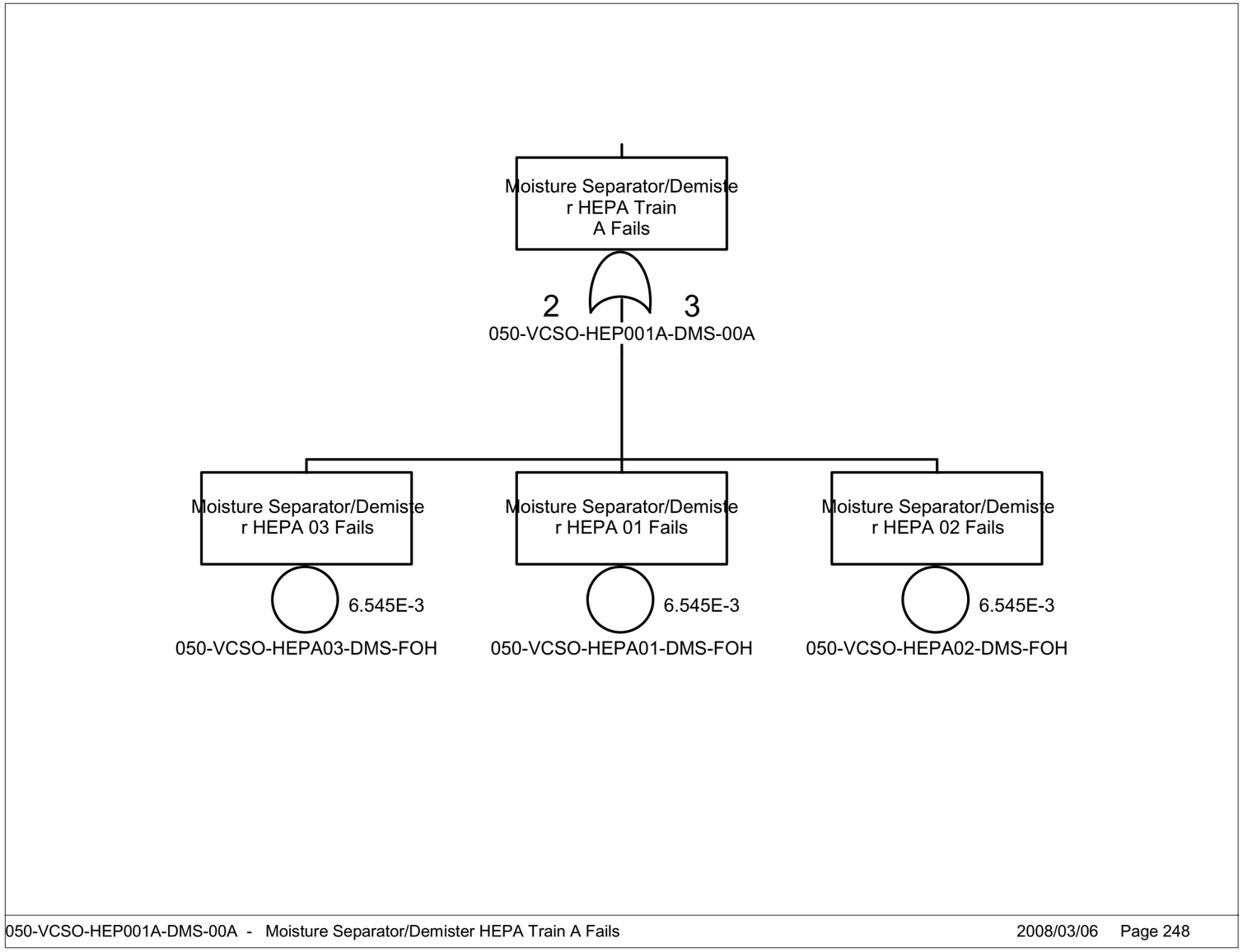
Source: Original

Figure B7.4-8. Exhaust HEPA Train A with Loss of Supply Fan



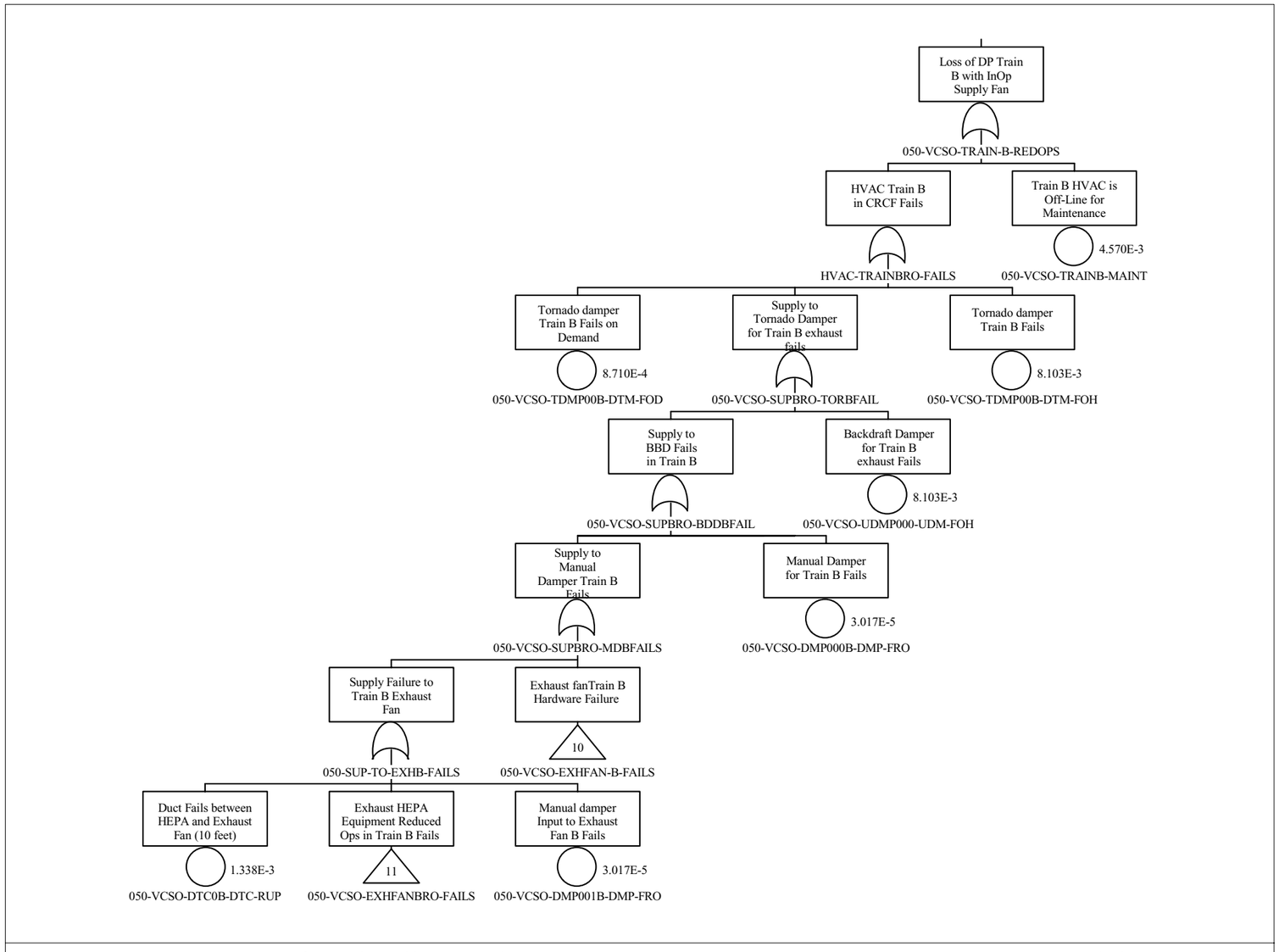
Source: Original

Figure B7.4-9. HEPA Input/Output Manual Damper Fail



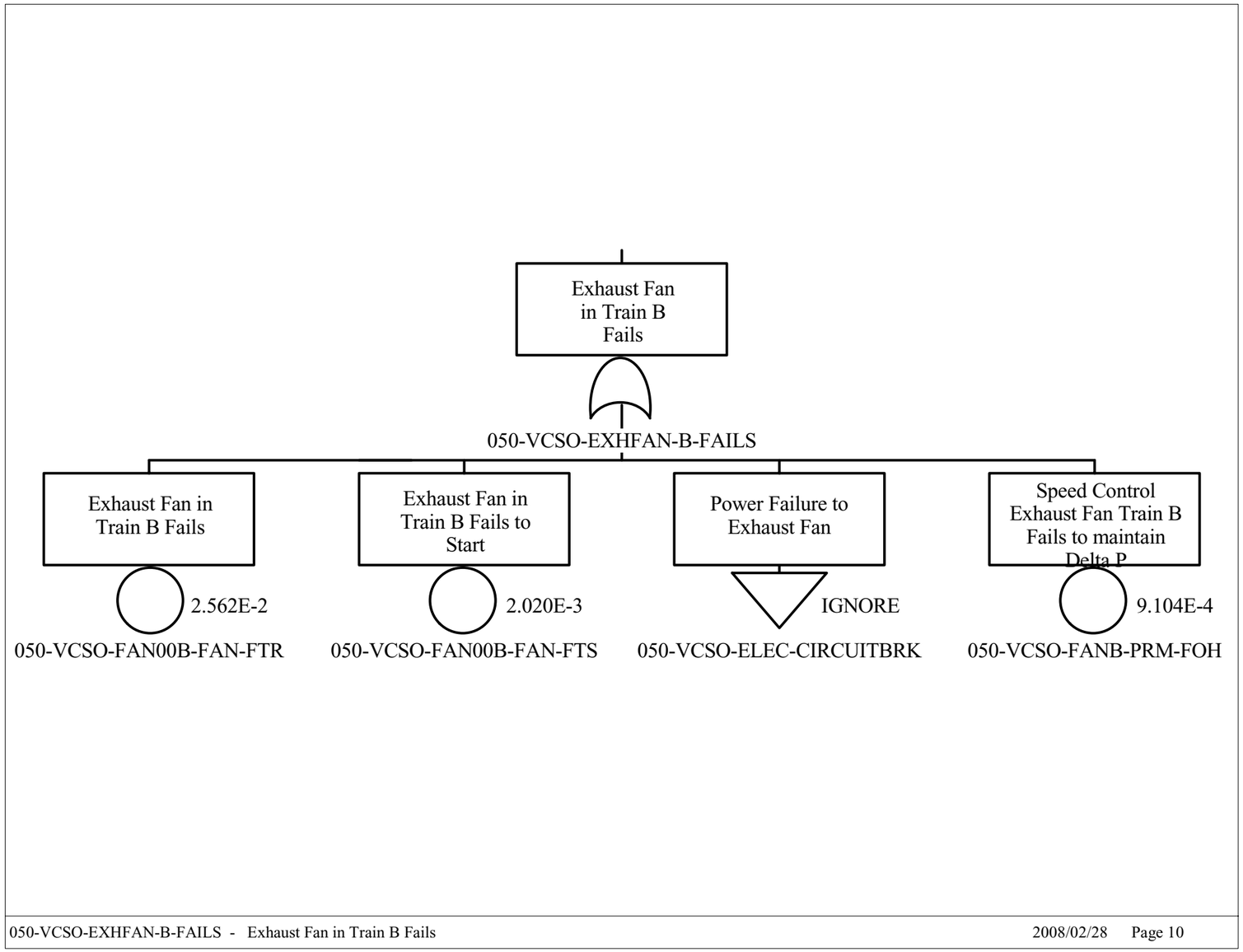
Source: Original

Figure B7.4-10. Moisture Separator/Demister HEPA Train A Fails



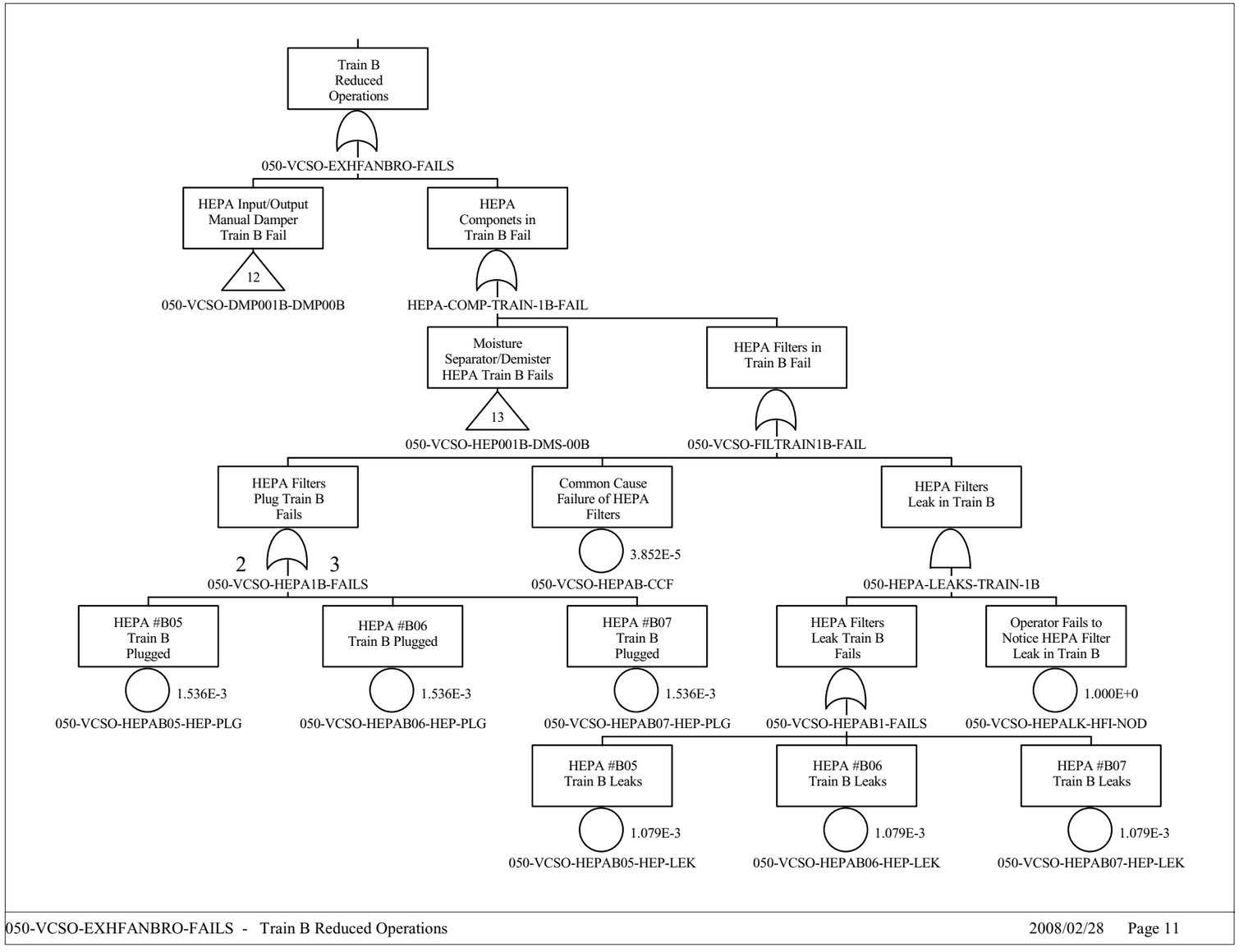
Source: Original

Figure B7.4-11. Loss of Delta Pressure in Train B with Inoperable Supply Fan



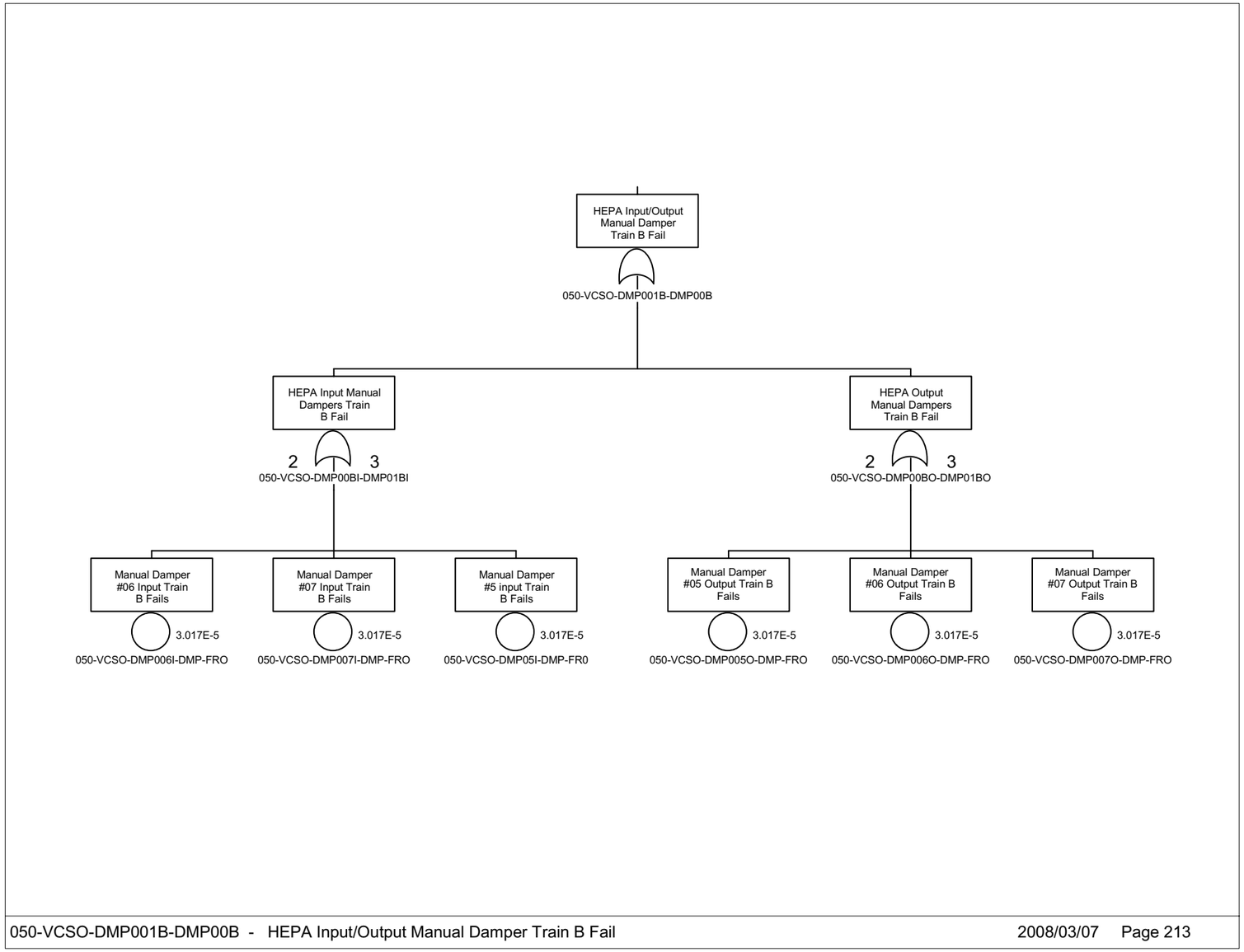
Source: Original

Figure B7.4-12. Exhaust Fan in Train B Fails



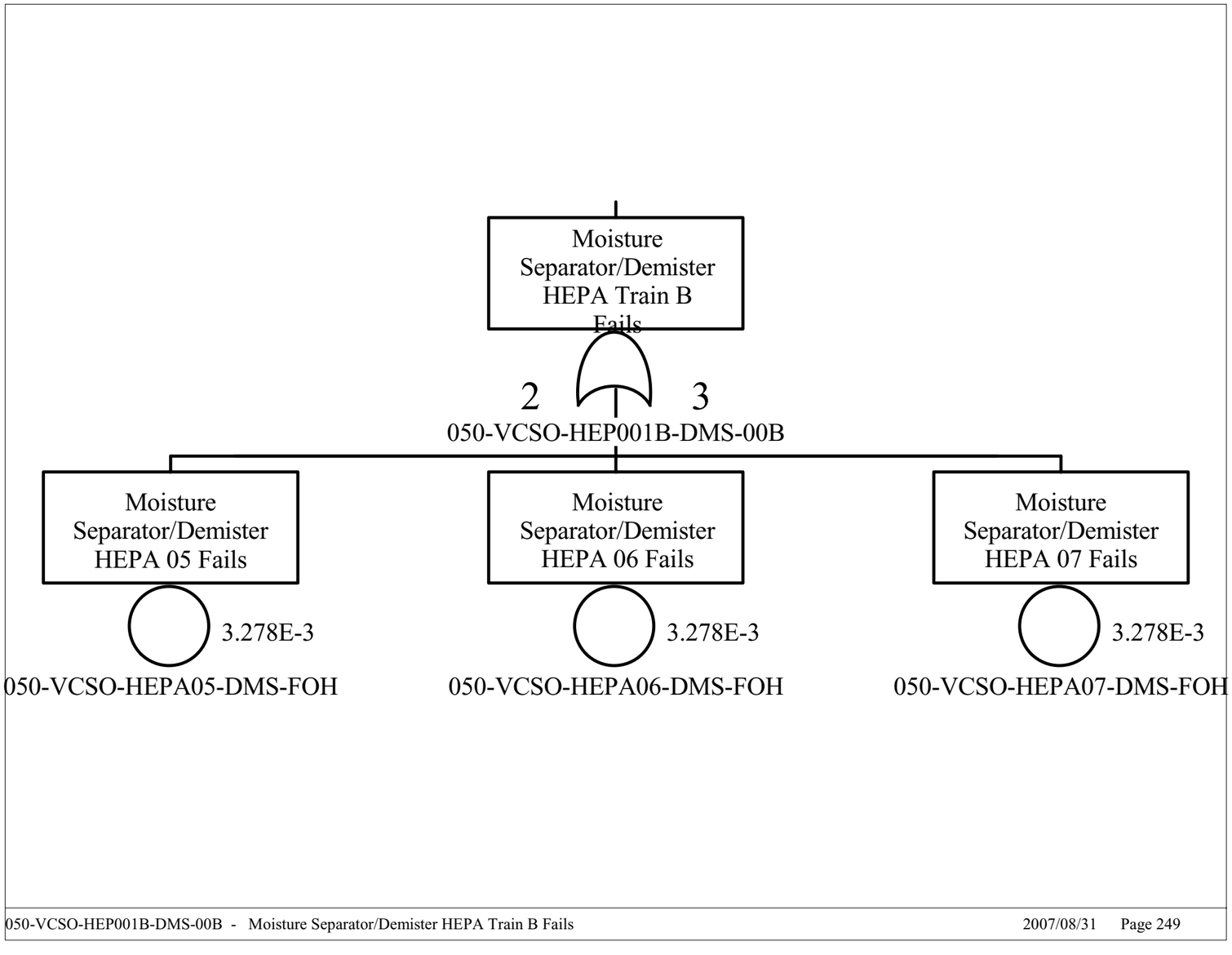
Source: Original

Figure B7.4-13. Train B Reduced Operations



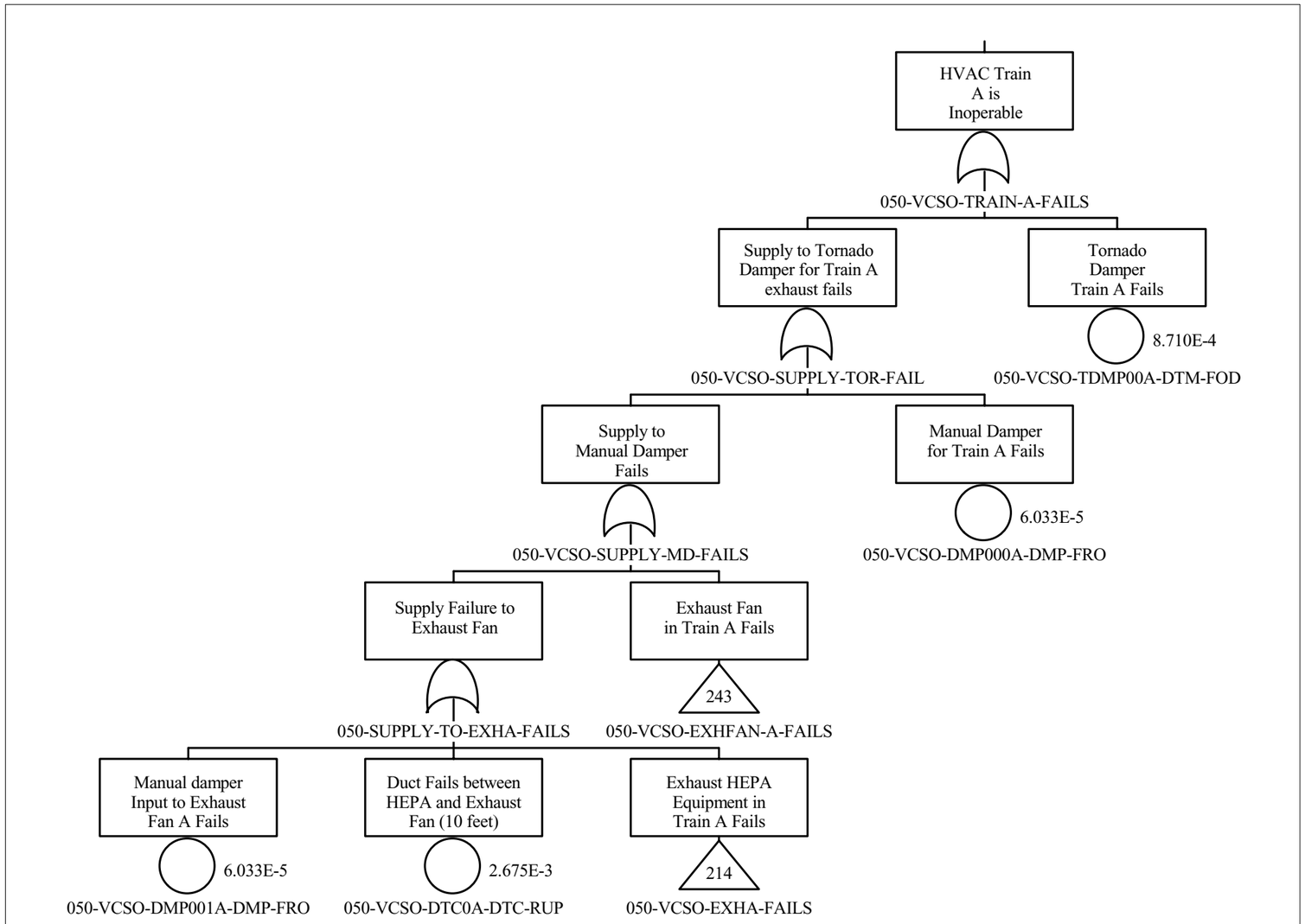
Source: Original

Figure B7.4-14. HEPA Input/Output Manual Damper Train B Fail



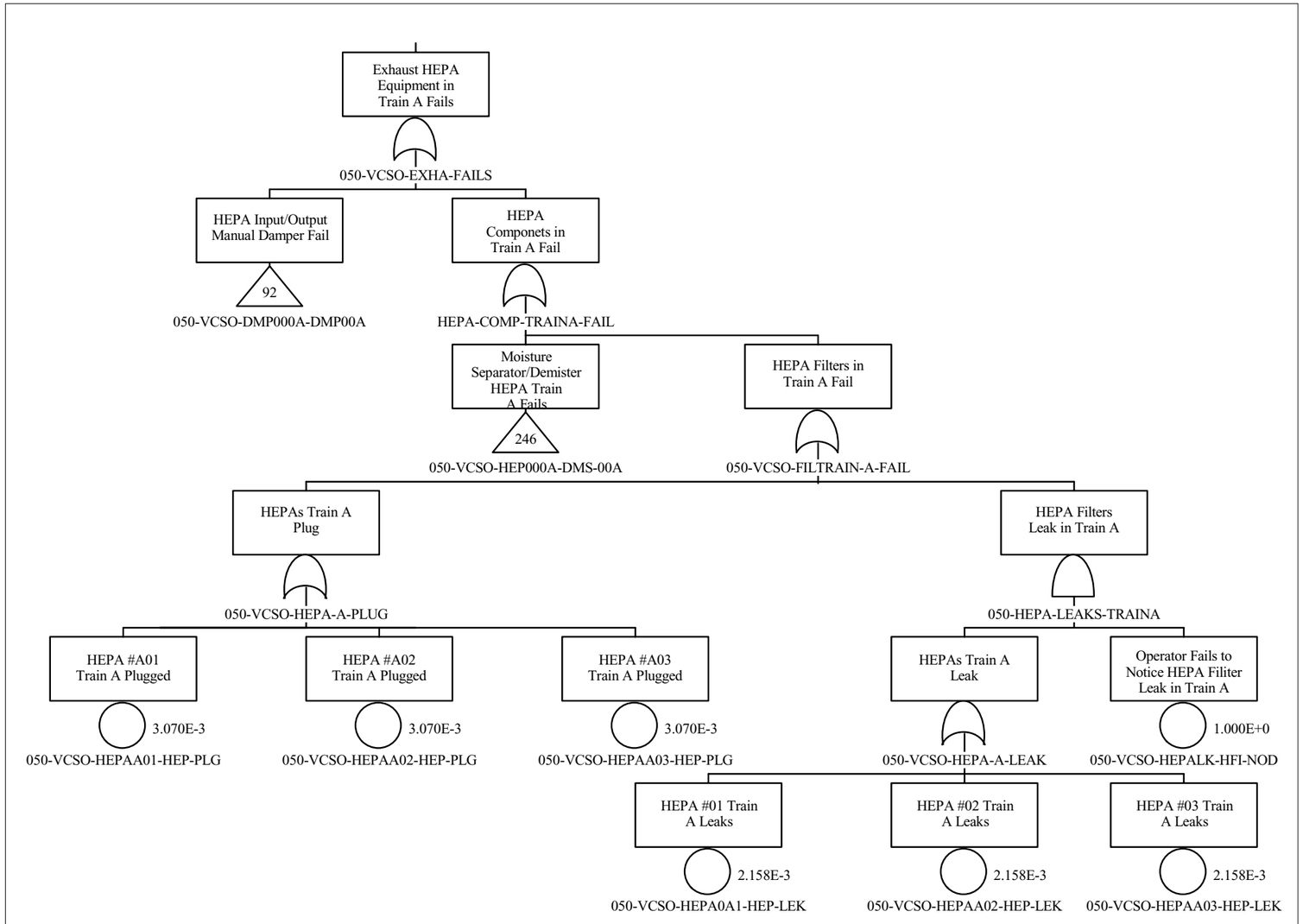
Source: Original

Figure B7.4-15. Moisture Separator/Demister HEPA Train B Fails



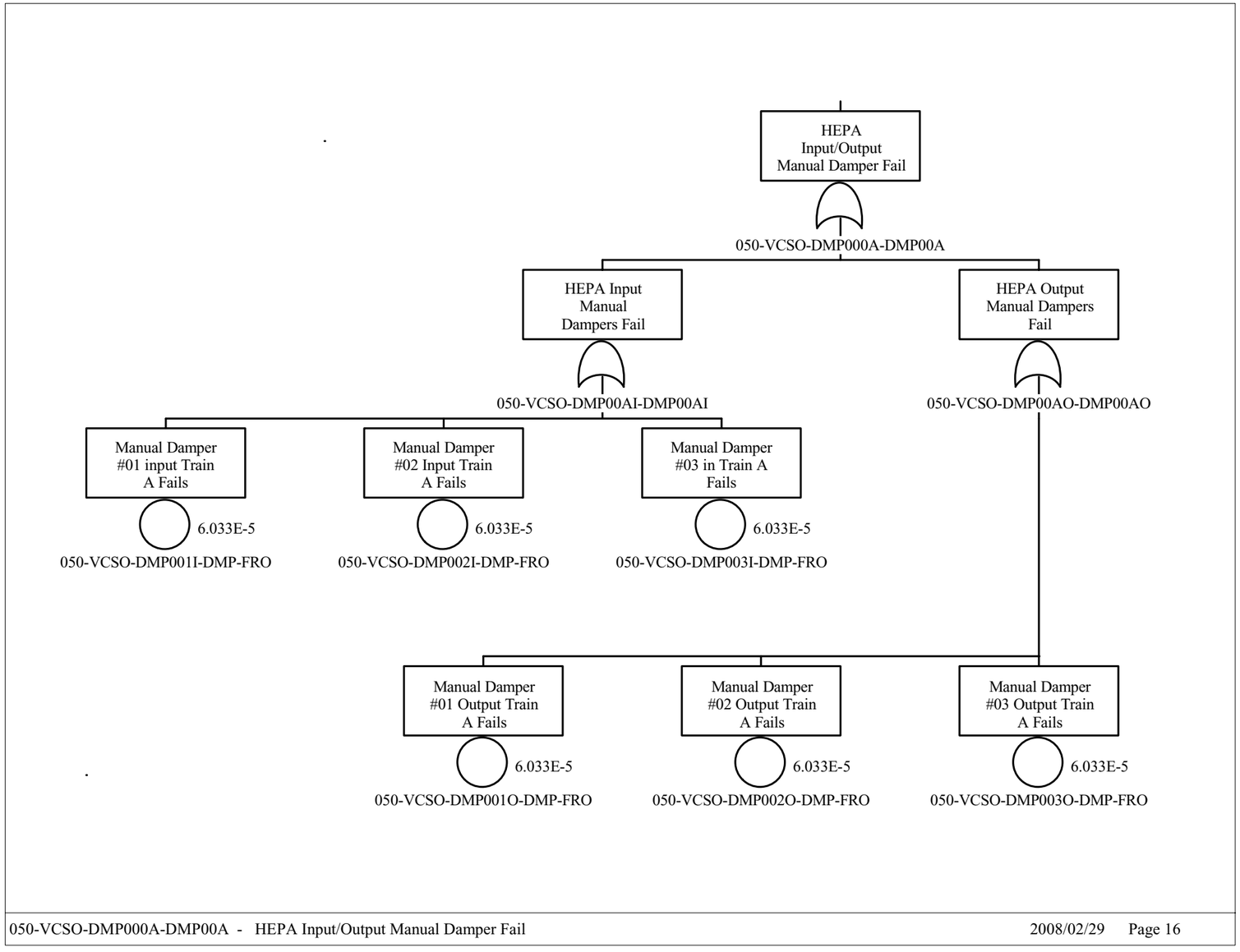
Source: Original

Figure B7.4-16. HVAC Train A is Inoperable



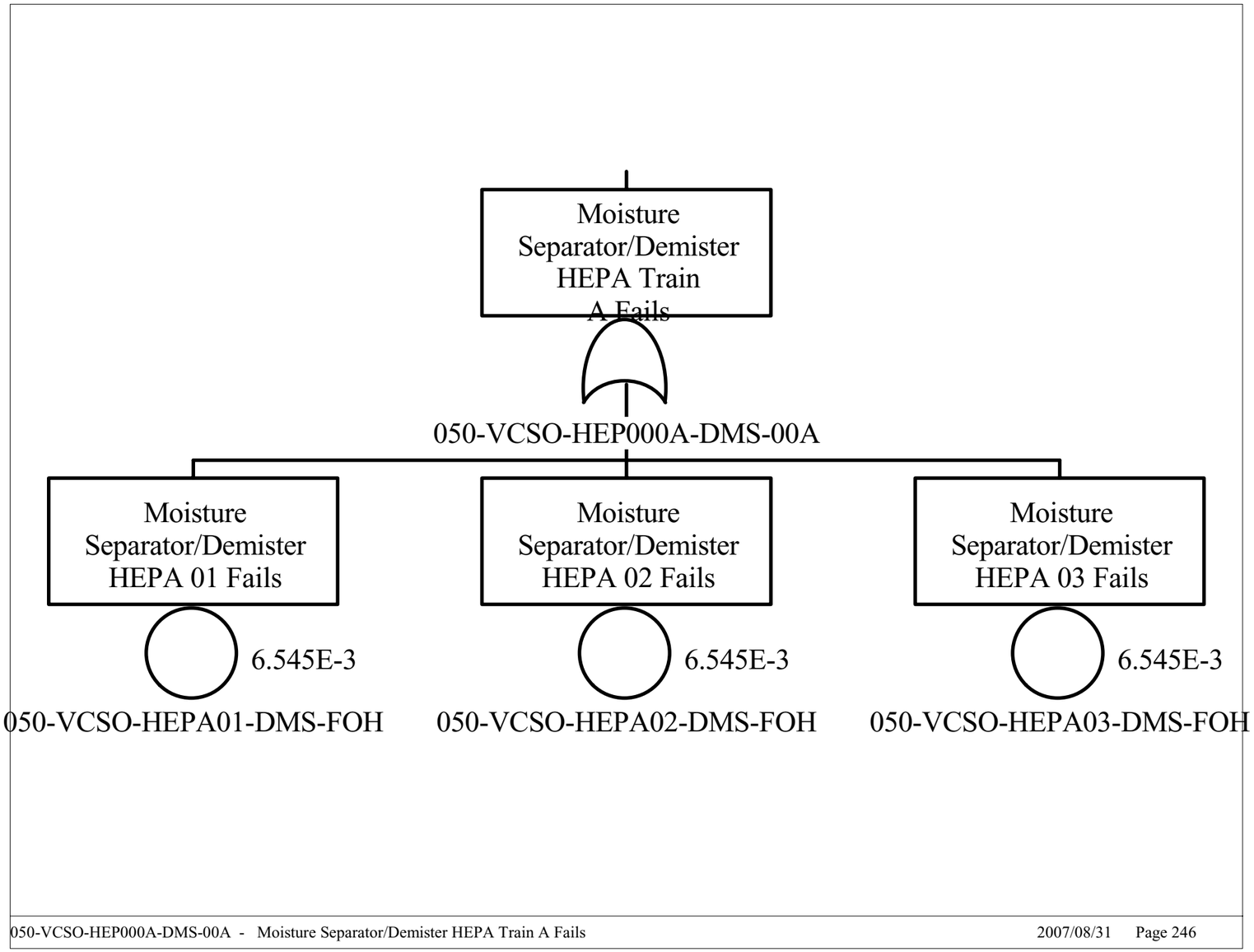
Source: Original

Figure B7.4-17. Exhaust HEPA Equipment in Train A Fails



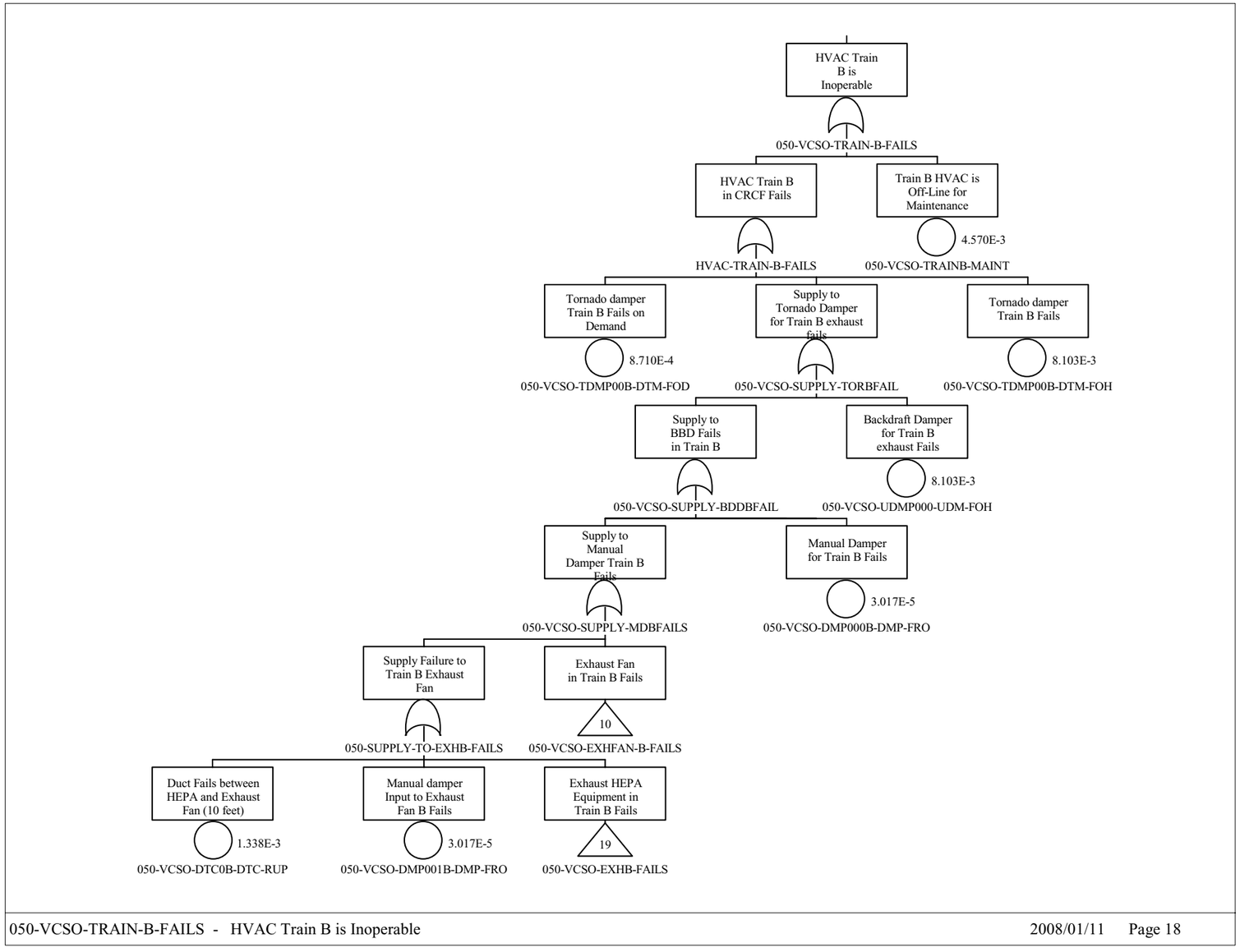
Source: Original

Figure B7.4-18. HEPA Input/Output Manual Damper Fail



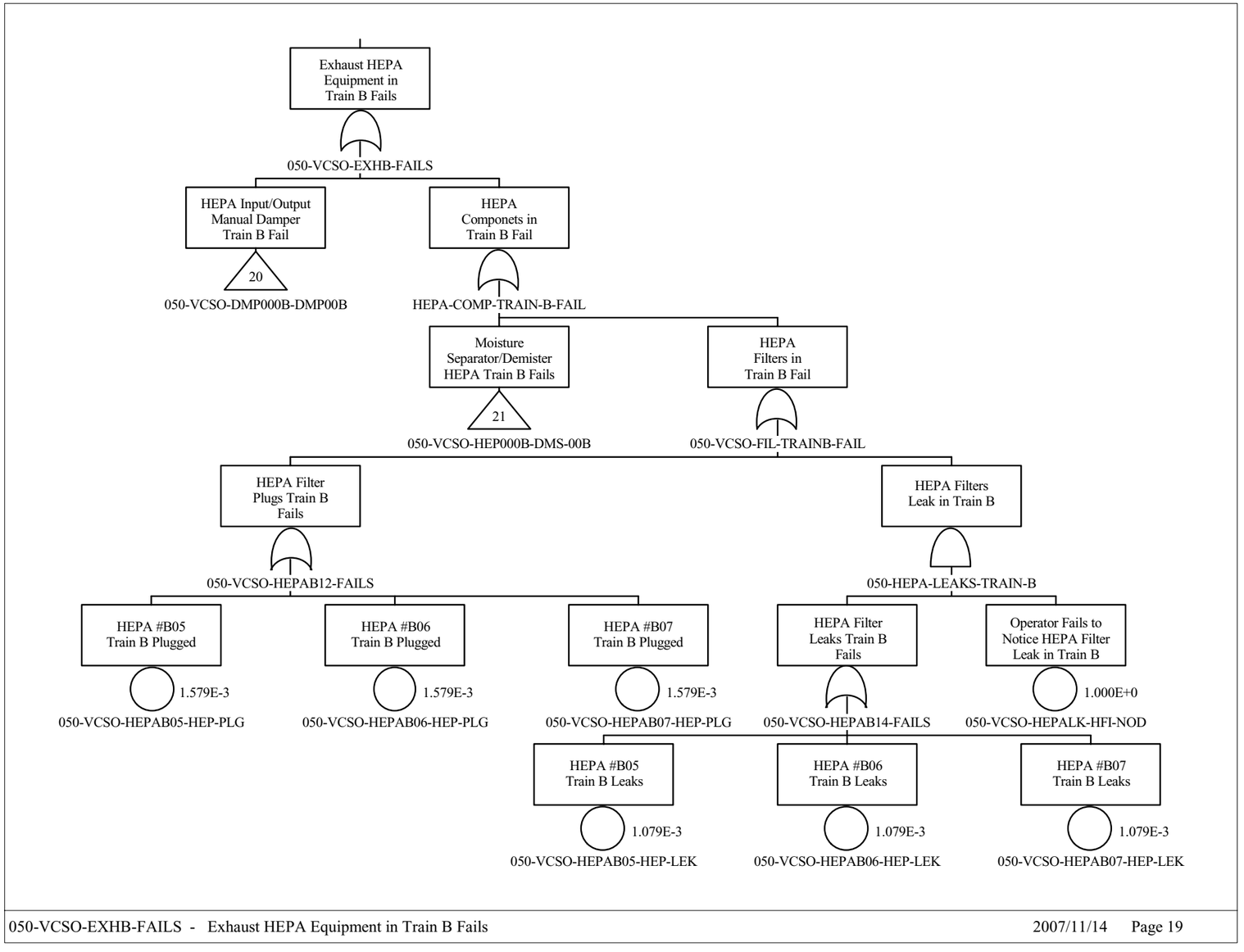
Source: Original

Figure B7.4-19. Moisture Separator/Demister HEPA Train A Fails



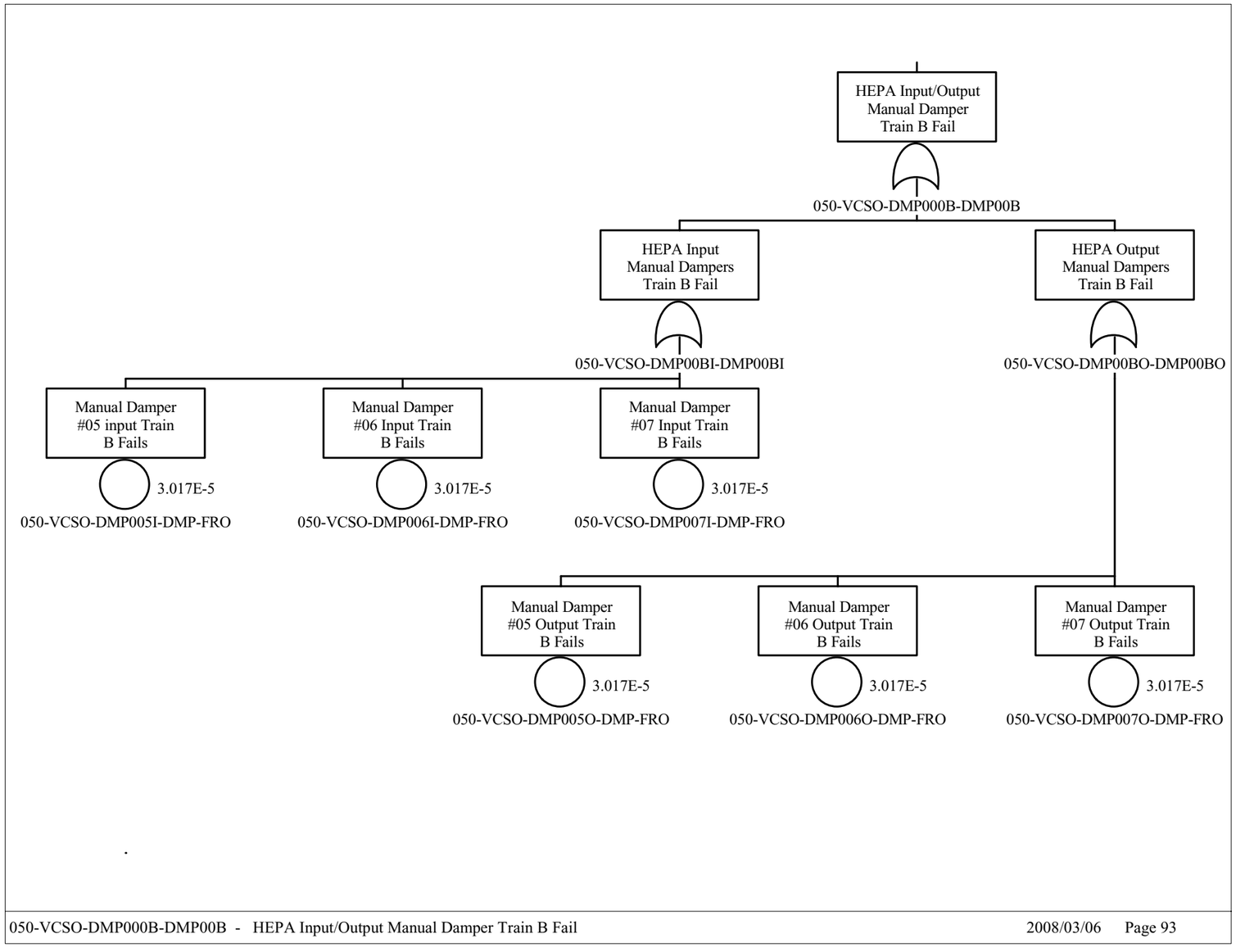
Source: Original

Figure B7.4-20. HVAC Train B is Inoperable



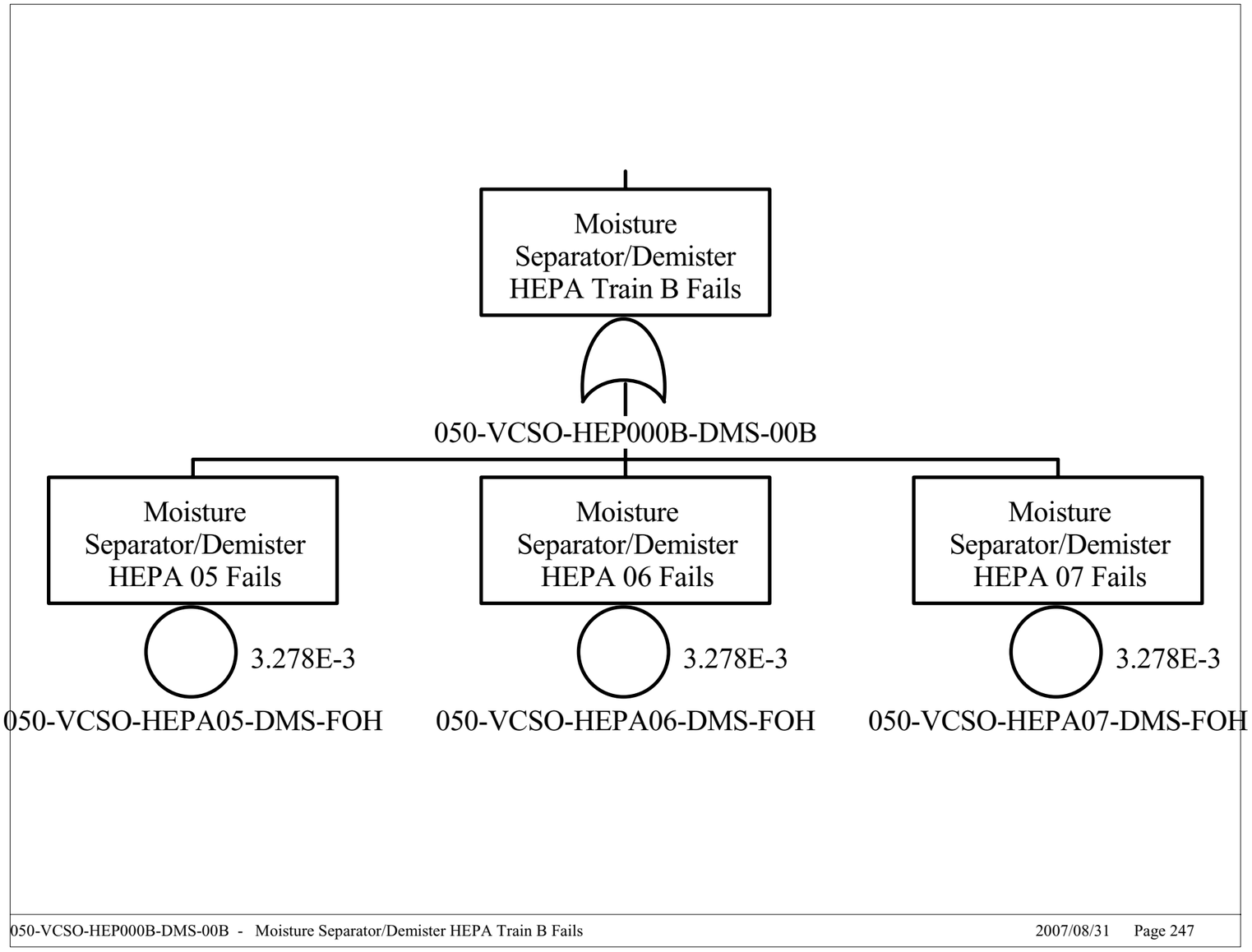
Source: Original

Figure B7.4-21. Exhaust HEPA Equipment in Train B Fails



Source: Original

Figure B7.4-22. HEPA Input/Output Manual Damper Train B Fail



Source: Original

Figure B7.4-23. Moisture Separator/Demister HEPA Train B Fails

B8 IMPORTANT TO SAFETY AC POWER FAULT TREE ANALYSIS

B8.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B8.1.1 BSC (Bechtel SAIC Company) 2008. *Normal Power System 13.8KV Site Distribution Overall Single Line Diagram*. 000-E10-EEN0-00202-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG. 20080206.0078.

B8.1.2 BSC 2008. *Emergency Diesel Generator Facility-13.8kV ITS Switchgear 26D-EEE0-SWGR-00001 Single Line Diagram (Train A)*. 26D-E10-EEE0-00101-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080204.0001.

B8.1.3 BSC 2008. *Emergency Diesel Generator Facility-13.8kV ITS Switchgear 26D-EEE0-SWGR-00002 Single Line Diagram (Train B)*. 26D-E10-EEE0-00201-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080204.0002.

B8.1.4 BSC 2007. *Emergency Diesel Generator Facility – 480V ITS MCC 26D-EEE0-MCC-00001 Single Line Diagram (Train A)*. 26D-E10-EEE0-00301-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0026.

B8.1.5 BSC 2007. *Emergency Diesel Generator Facility – 480V ITS MCC 26D-EEE0-MCC-00002 Single Line Diagram (Train B)*. 26D-E10-EEE0-00401-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0027.

B8.1.6 BSC 2007. *Emergency Diesel Generator Facility – ITS 125VDC System Single Line Diagram (Train A)*. 26D-E10-EED0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0015.

B8.1.7 BSC 2007. *Emergency Diesel Generator Facility – ITS 125V DC System Single Line Diagram (Train B)*. 26D-E10-EED0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0016.

B8.1.8 BSC 2007. *Emergency Diesel Generator Facility – Fuel Oil System Calculation*. 26D-M6C-EG00-00200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071025.0001.

B8.1.9 BSC 2007. *Emergency Diesel Generator Facility – Generator Room Ventilation System Calculation*. 26D-M5C-VNI0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071015.0018.

B8.1.10 BSC 2007. *Emergency Diesel Generator Facility – Switchgear and Battery Rooms Ventilation System Calculation.* 26D-M5C-VNI0-00200-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071022.0001.

B8.1.11 BSC 2007. *Wet Handling Facility 480V ITS Load Center 050-EEE0-LC-00001 Train A Single Line Diagram*. 050-E10-EEE0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0017.

B8.1.12 BSC 2007. *Wet Handling Facility 480V ITS Load Center 050-EEE0-LC-00002 Train B Single Line Diagram*. 050-E10-EEE0-00401-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0018.

B8.1.13 BSC 2007. *Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00001 Train A Single Line Diagram*. 050-E10-EEE0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0015.

B8.1.14 BSC 2007. *Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00002 Train B Single Line Diagram*. 050-E10-EEE0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0016.

B8.1.15 *BSC 2007. *Wet Handling Facility Confinement ITS Electrical Room HVAC System - Train A Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0001.

B8.1.16 *BSC 2007. *Wet Handling Facility Confinement ITS Electrical Room HVAC System - Train B Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00303-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0003.

B8.1.17 BSC 2008. *Wet Handling Facility Confinement ITS Battery Room Exhaust System - Train A Ventilation & Instrumentation Diagram*. 050-M80-VCT0-00302-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0018.

B8.1.18 BSC 2008. *Wet Handling Facility Confinement ITS Battery Room Exhaust System - Train B Ventilation & Instrumentation Diagram*. 050-M80-VCT0-00304-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0019.

B8.1.19 *Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Loss of Offsite Power Events: 1986-2004.* Volume 1 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants.* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0164. (DIRS 183908)

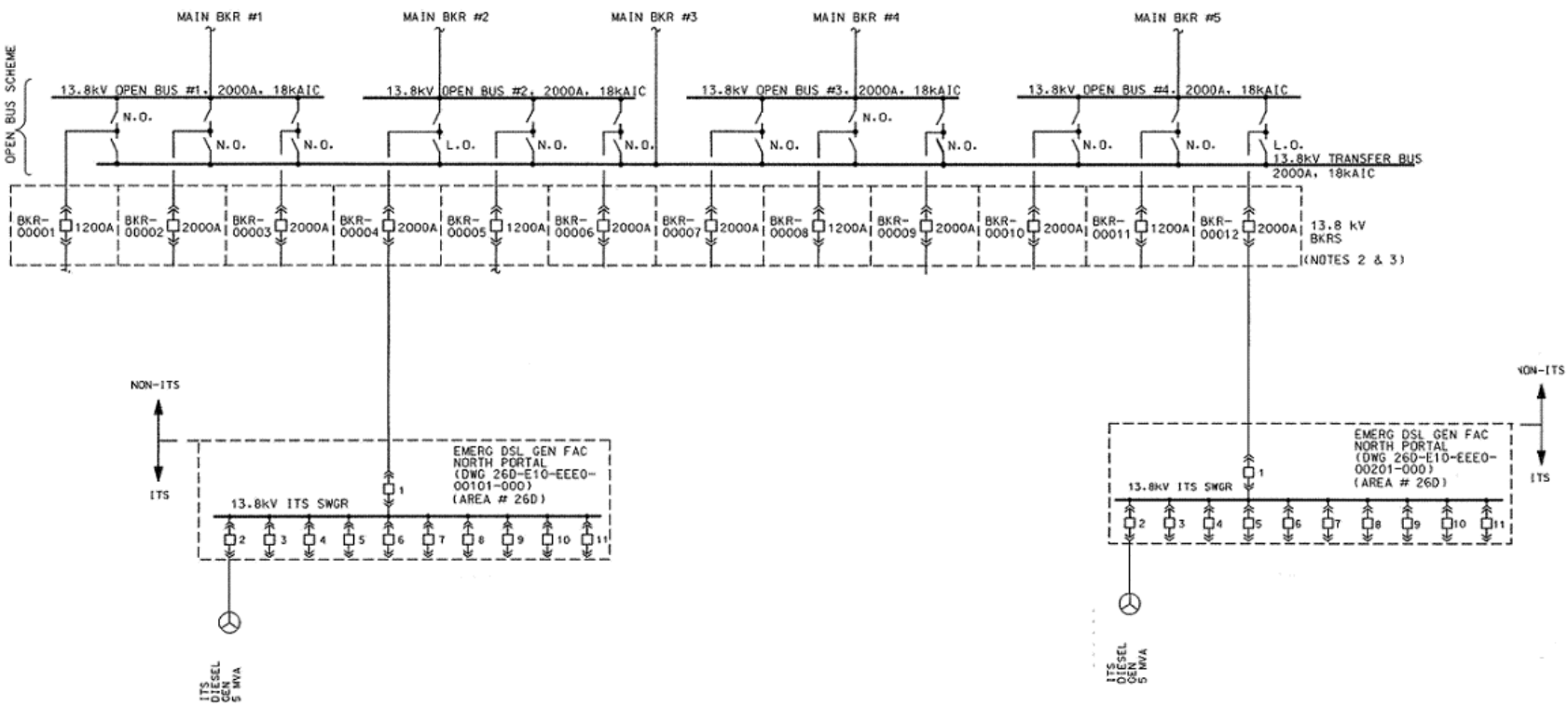
B8.2 ITS AC POWER DESCRIPTION

The ITS AC power system supplies power to the ITS HVAC systems in the three CRCFs, the WHF, and RF. The ITS power system makes use of two elements: (1) the onsite ITS power supply and (2) the ITS equipment needed to supply power from the onsite ITS power supply to the ITS loads in each of the site facilities. During normal operations AC power is supplied from two offsite 138kV power lines through the 138kV to 13.8kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site. Off-normal conditions for the distribution of AC power occur during a loss of offsite power (LOSP). A LOSP may be the result of problems on the power grid, or the result of failures within the plant AC power systems (most likely within the 138kV to 13.8kV switchyard). Under these conditions, the AC power source for the WHF ITS equipment is two onsite ITS diesel generators. (There are several diesel generators located onsite. However there are only two generators designated as ITS; the two that support each division of ITS equipment (A or B) in the three CRCFs, the WHF and the RF.) Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each ITS diesel generator supplies power to one division (A or B) of ITS systems. Each ITS diesel generator, its associate support systems and the power distribution system is independent, and electrically isolated, of the other diesel generator, its support systems and power distribution system.

B8.2.1 Normal AC Power Distribution

Normal AC power to the WHF ITS equipment is provided via two 13.8kV ITS switchgears (A and B), one supplying WHF train A ITS loads and the second supplying power to WHF train B ITS loads. These two 13.8kV ITS switchgears (Figures B8.2-1 through B8.2-3) are normally aligned to receive power from the site 138kV to 13.8kV switchyard though Open Buses 2 and 4.

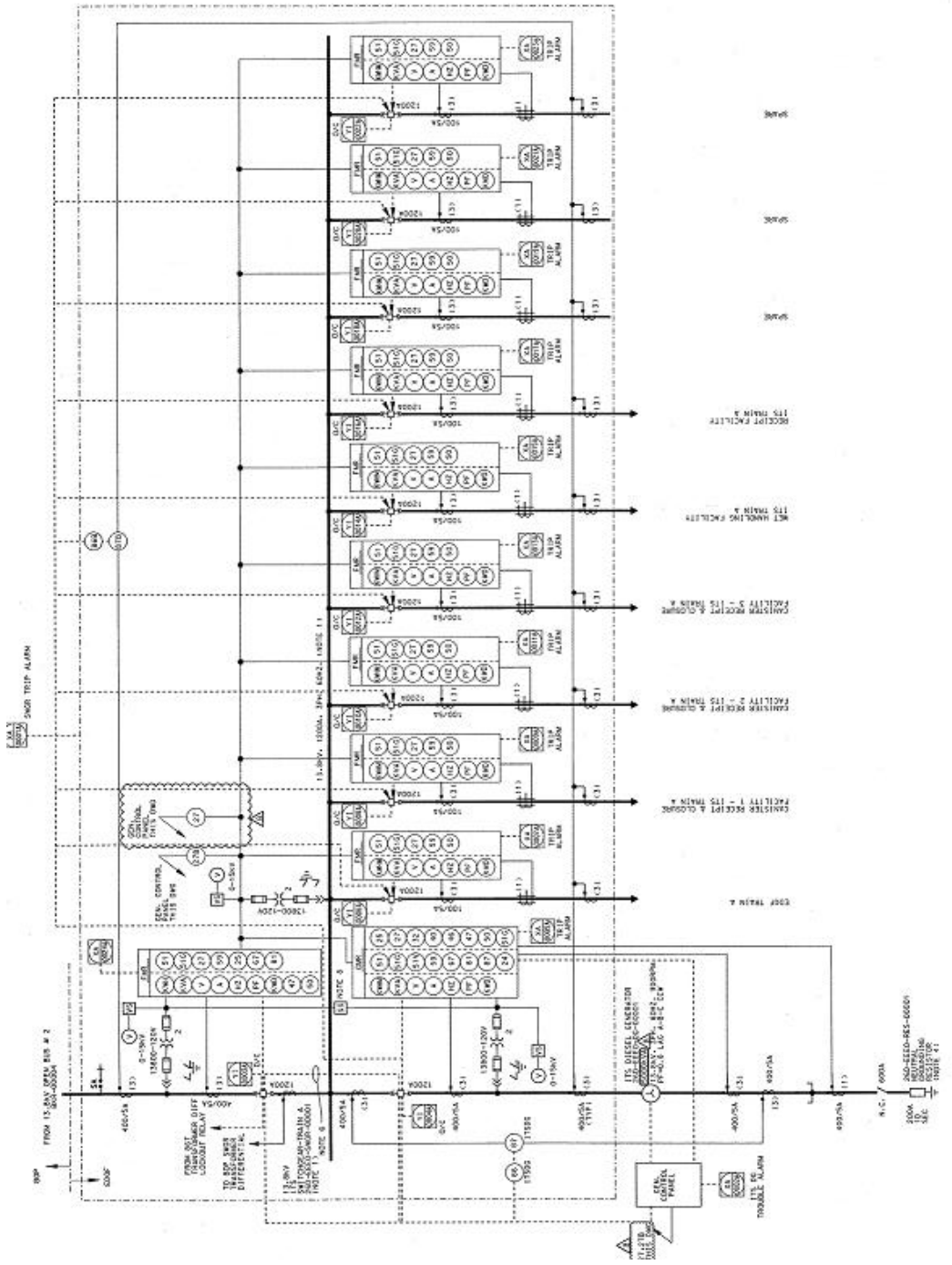
In addition to supplying power to the ITS loads in the WHF, the 13.8kV ITS switchgear supplies power to equipment in the EDGF required to support ITS diesel generator operation. These loads include the diesel generator room fans, 13.8kV ITS switchgear room and battery room air handling unit, the ITS diesel generator fuel oil pumps, and DC power (via a battery charger) to operate the ITS switchgear circuit breakers. (Figures B8.2-4 and B8.2-5 for ITS diesel generator train A and Figures B8.2-6 and B8.2-7 for ITS diesel generator train B).



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Modified from (Ref. B8.1.1)

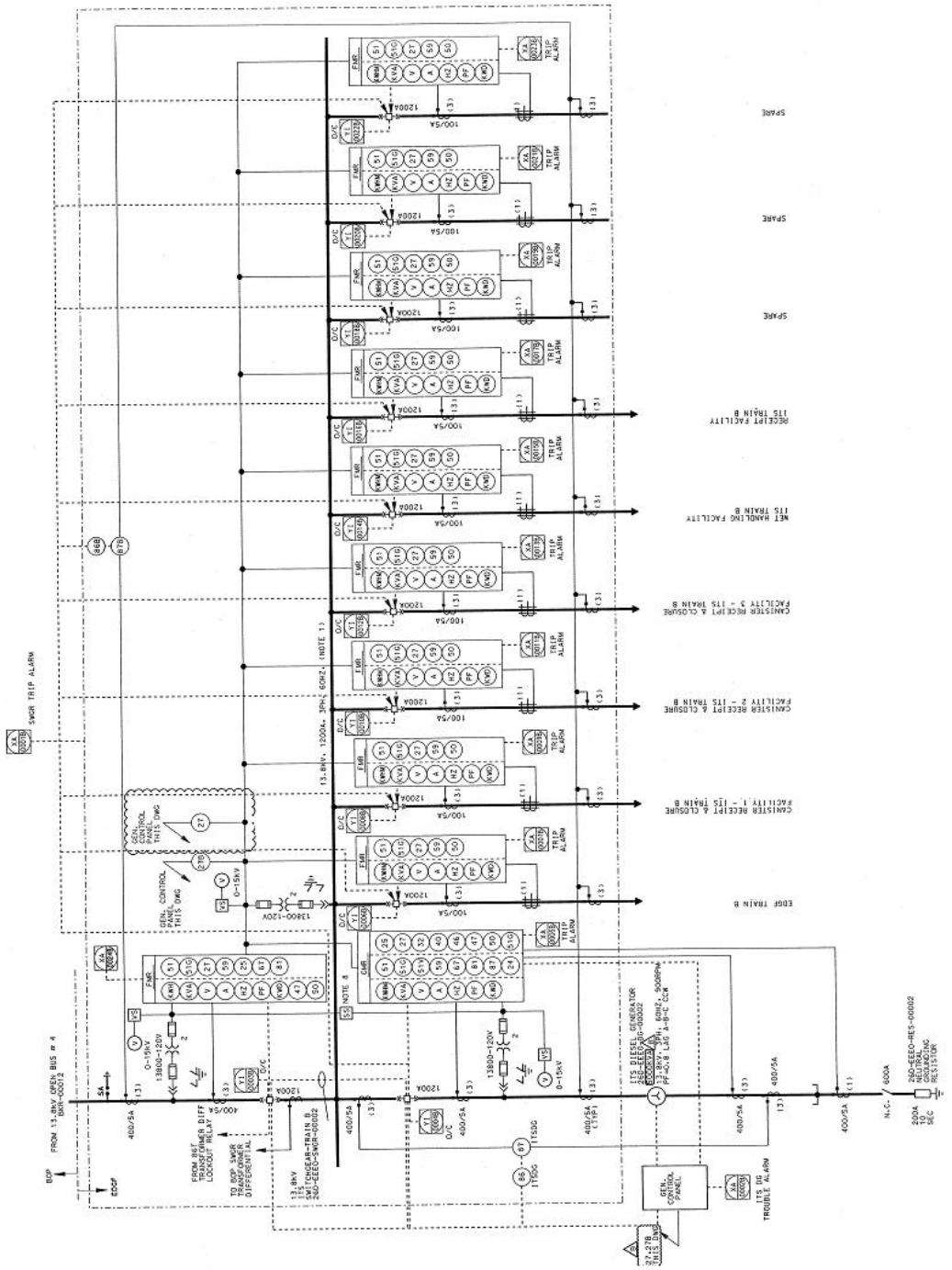
Figure B8.2-1. AC Power – Main Electrical Distribution



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: (Ref. B8.1.2)

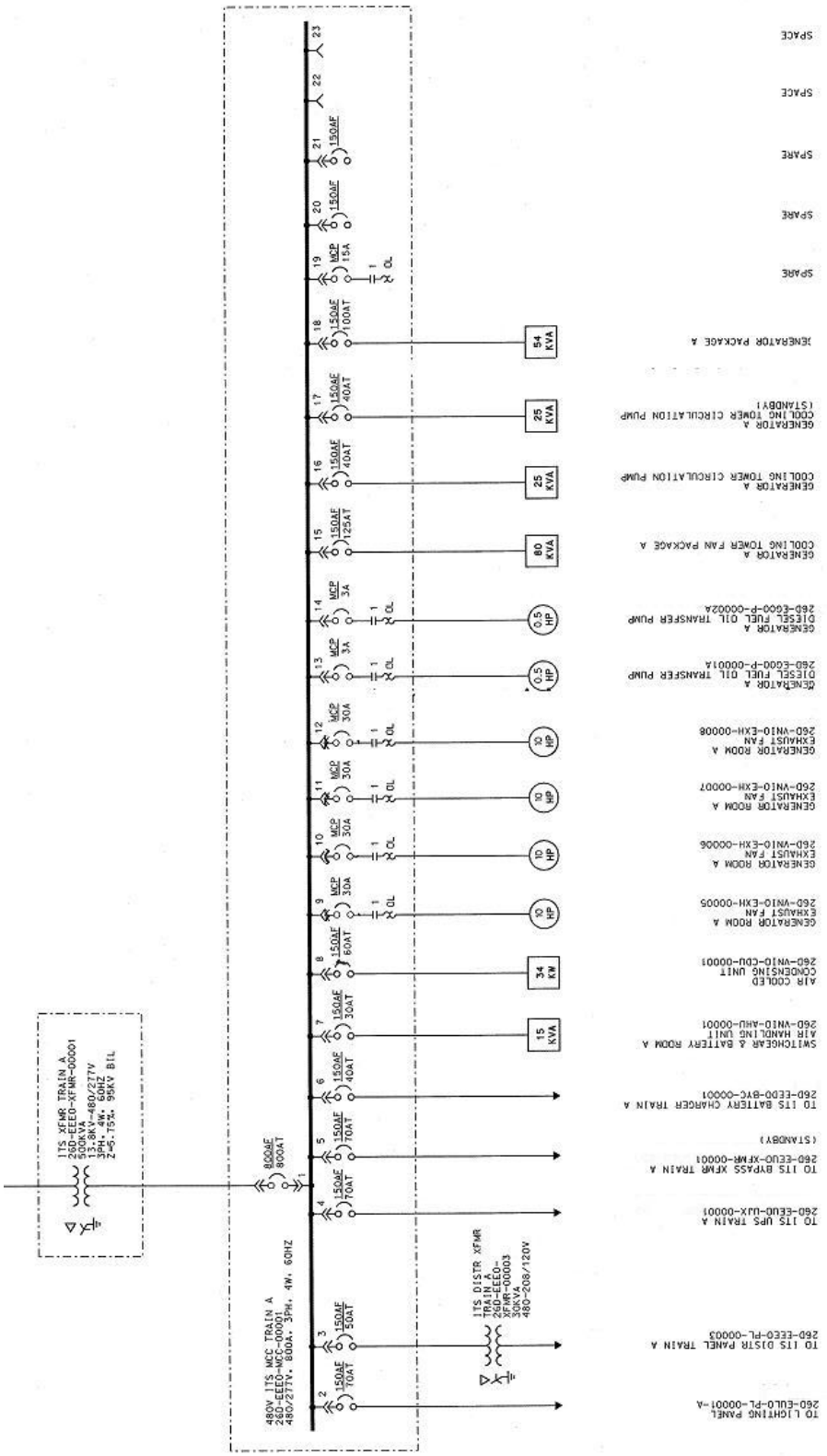
Figure B8.2-2. AC Power – 13.8kV ITS Switchgear Train A



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: (Ref. B8.1.3)

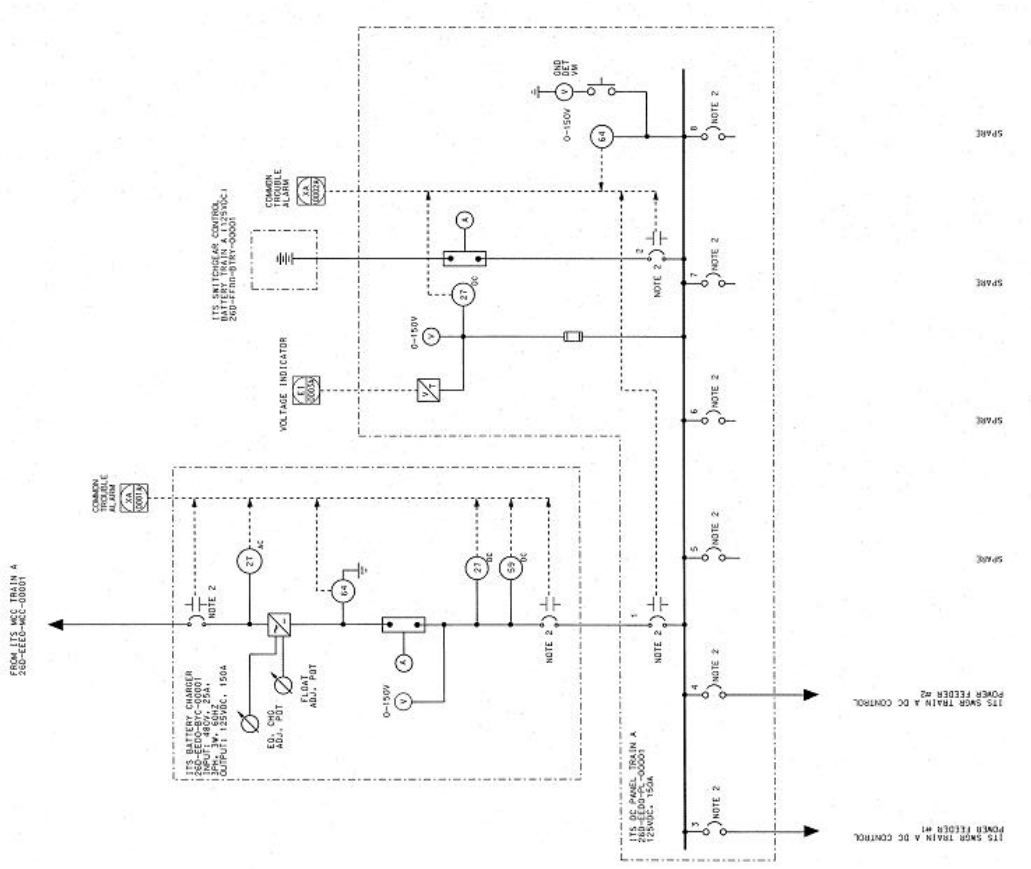
Figure B8.2-3. AC Power – 13.8kV ITS Switchgear Train B



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: (Ref. B8.1.4)

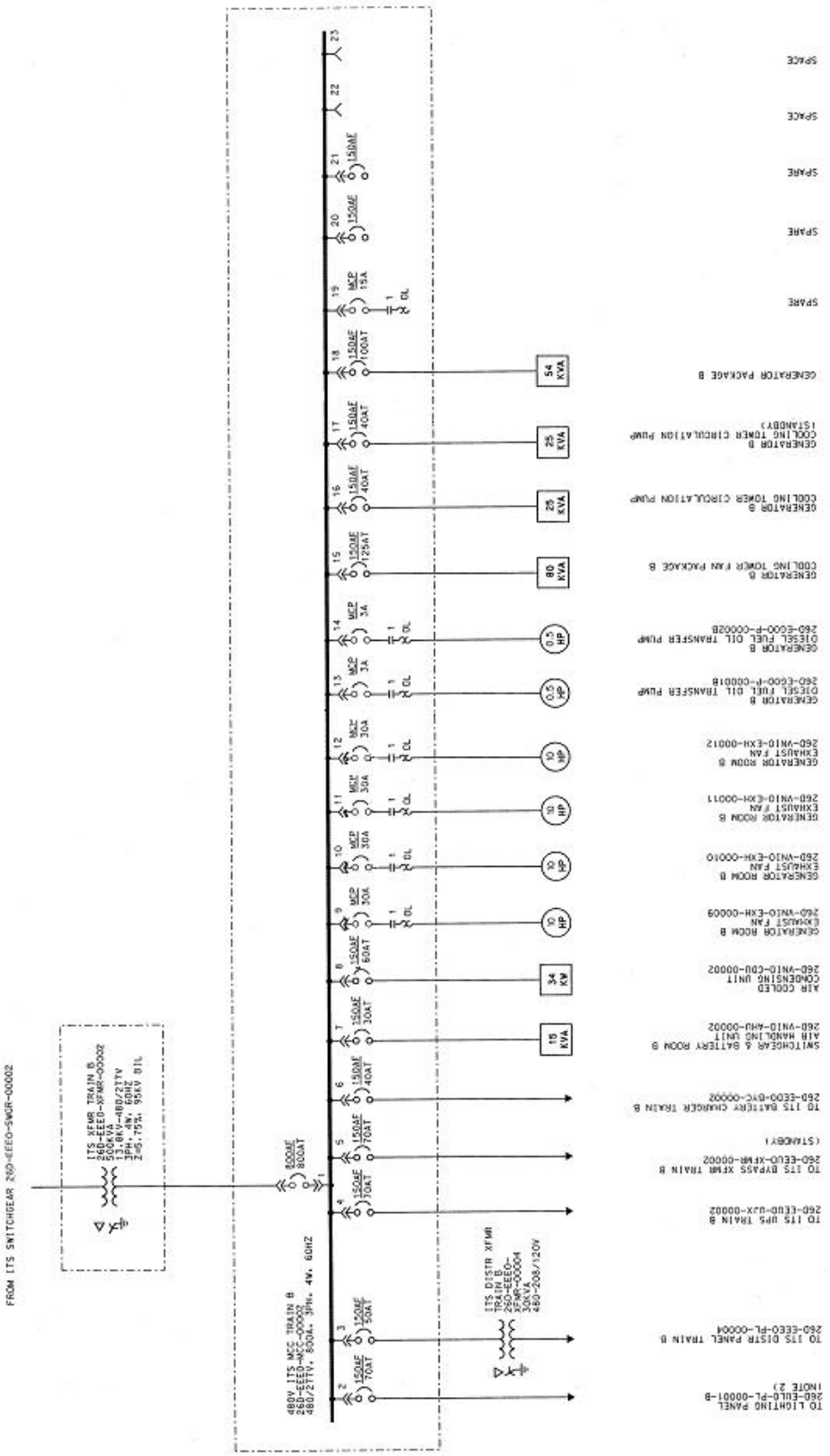
Figure B8.2-4. Emergency Diesel Generator Facility – 480V ITS MCC Train A



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: (Ref. B8.1.6)

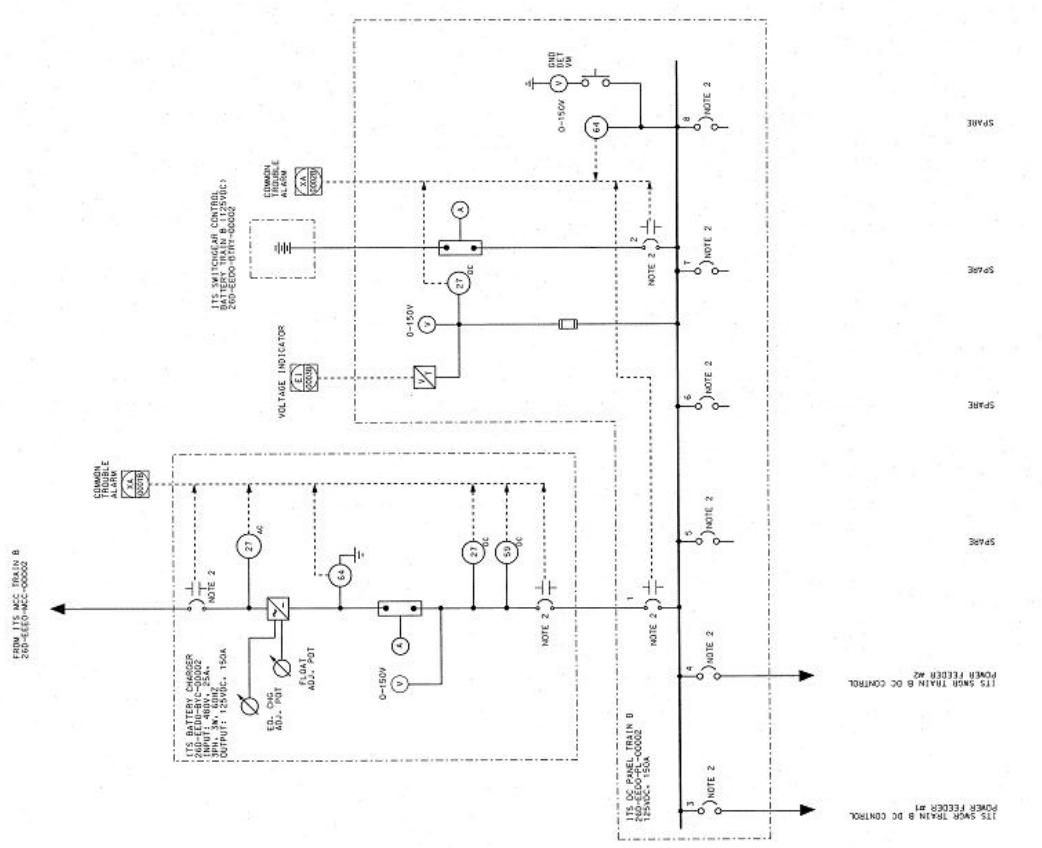
Figure B8.2-5. ITS 125 V DC System Train A



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: (Ref. B8.1.5)

Figure B8.2-6. Emergency Diesel Generator Facility – 480 V ITS MCC Train B



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: (Ref. B.8.1.7)

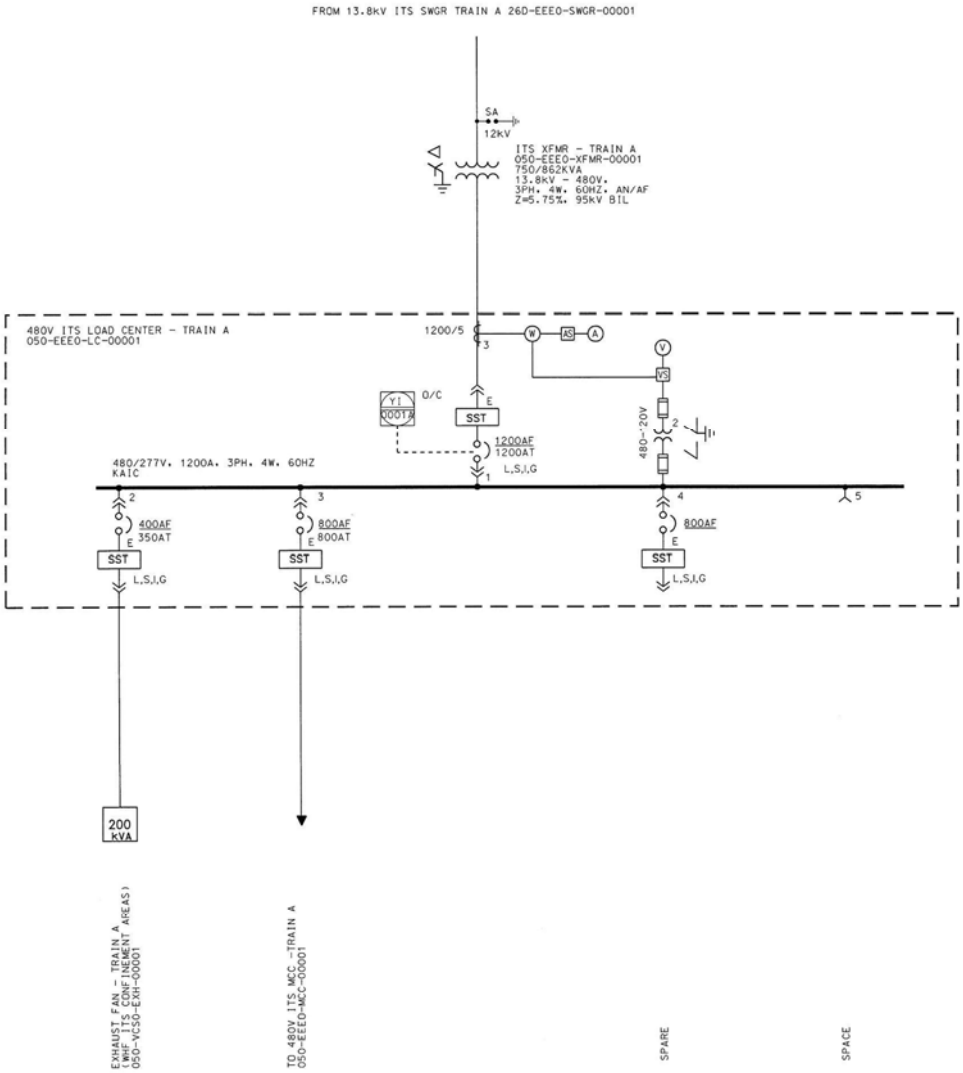
Figure B8.2-7. ITS 125 V DC System Train B

The ITS loads within the WHF are powered via two ITS 480/277V load centers and ITS 480/277V motor control centers (MCC) located within separate areas in the WHF. ITS 480/277V load center train A (Figure B8.2-8) and ITS 480/277V MCC train A (Figure B8.2-10) support train A of the WHF ITS HVAC.

For the remainder of this Attachment these will be referred to as ITS load center train A and ITS MCC train A.

The ITS 480/277V load center train B (Figure B8.2-9) and ITS 480/277V MCC train B (Figure B8.2-11) support train B of the WHF ITS HVAC.

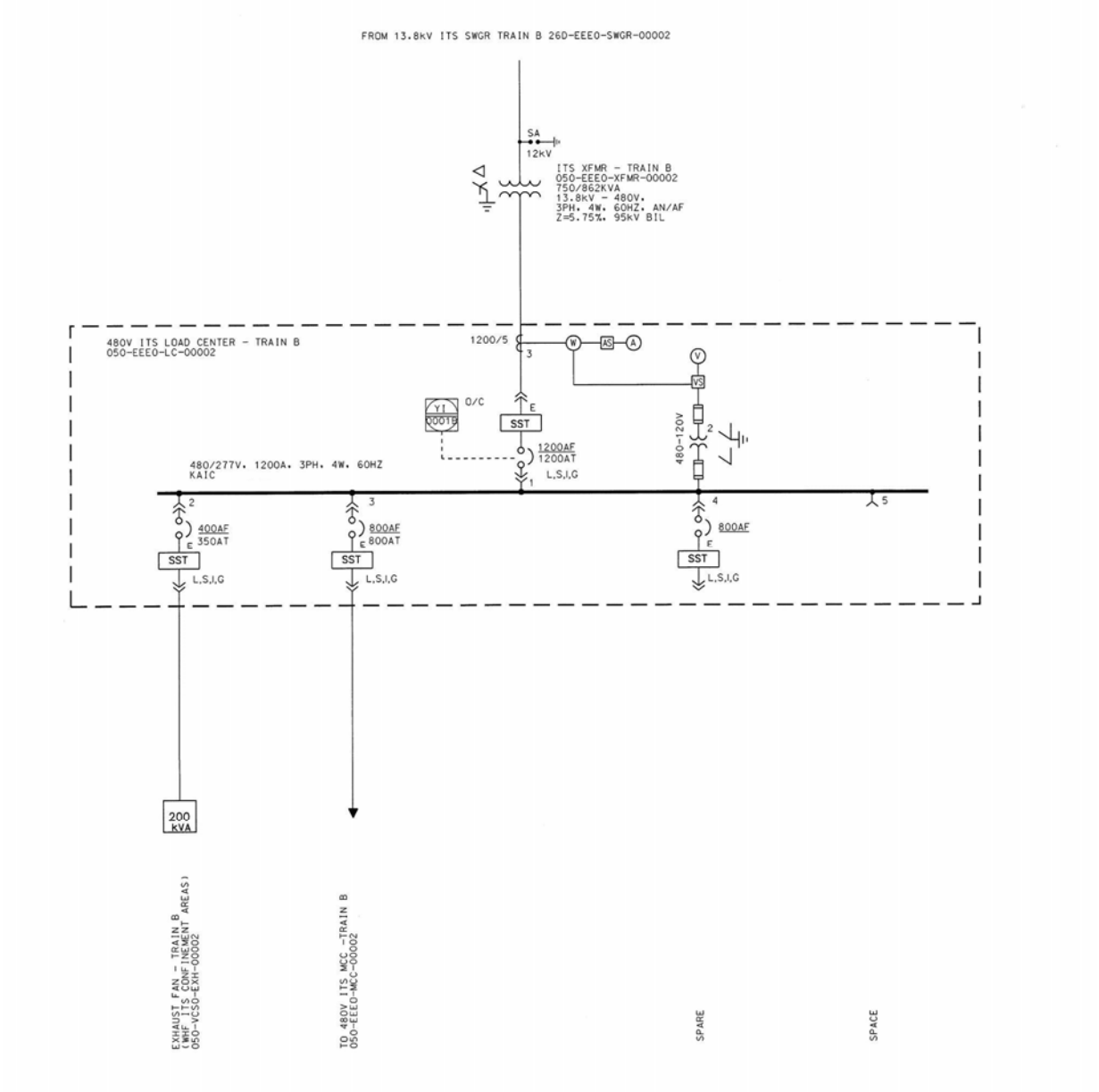
For the remainder of this Attachment these will be referred to as ITS load center train B and ITS MCC train B. Each division of the AC power supply from the 13.8kV ITS switchgears to the WHF ITS equipment passes through a 13.8kV to 480V transformer (Figures B8.2-8 through B8.2-11).



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document.

Source: Ref B8.1.11)

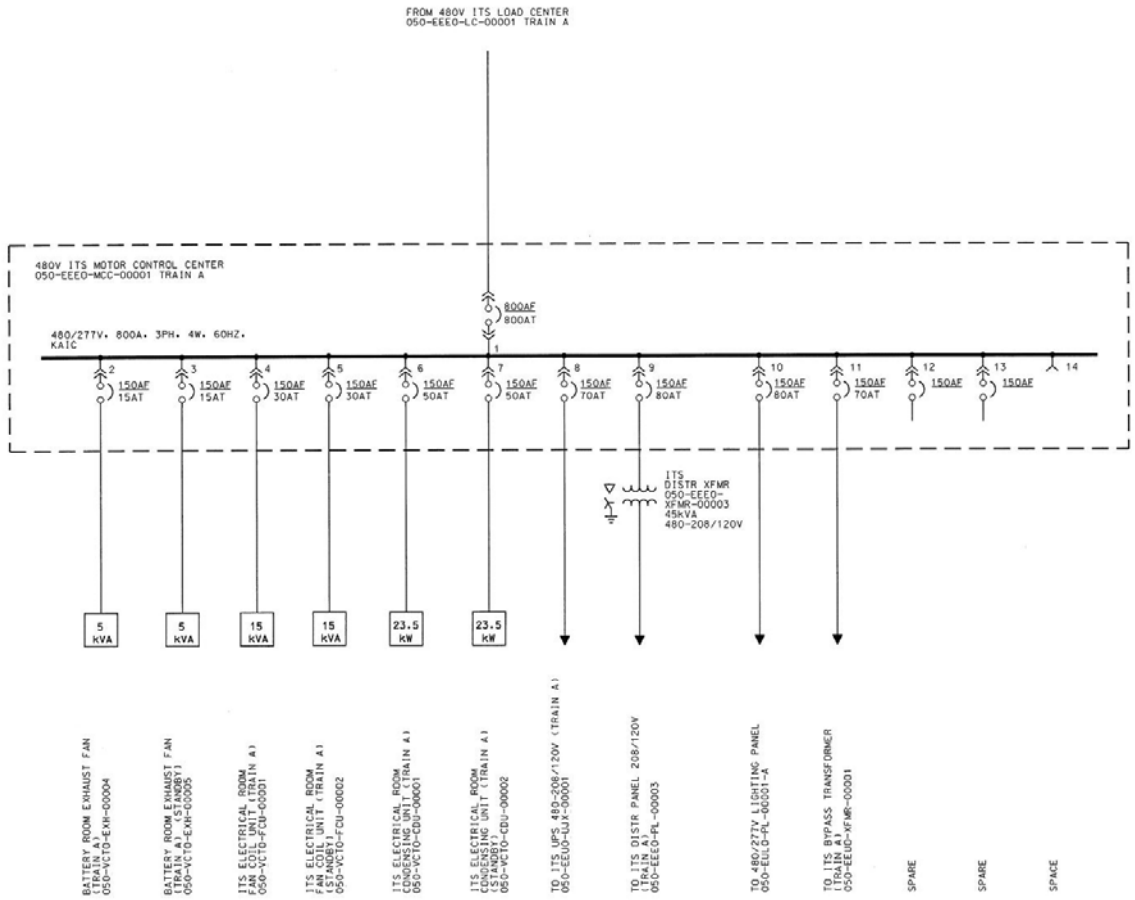
Figure B8.2-8. WHF 480 V ITS Load Center Train A



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: (Ref. B8.1.12

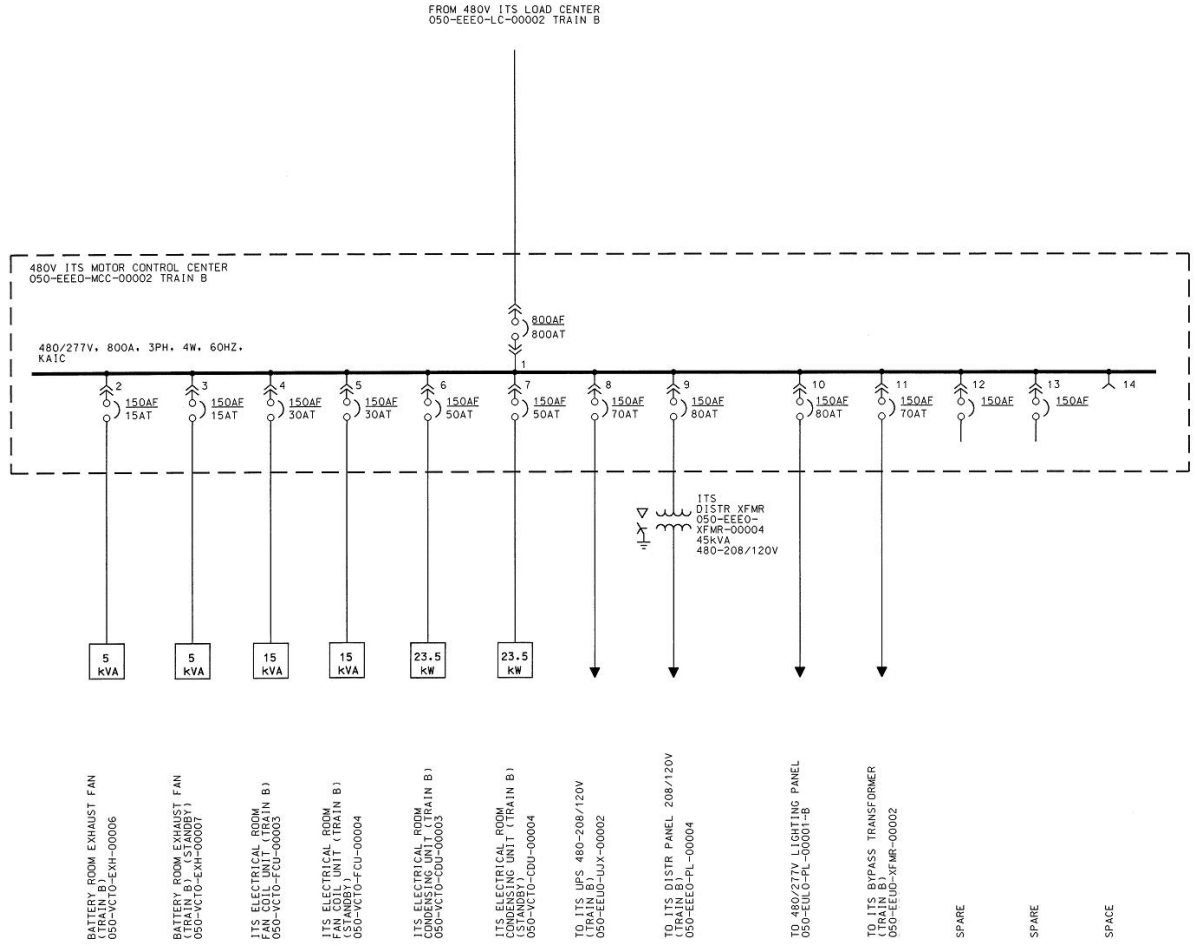
Figure B8.2-9. WHF 480 V ITS Load Center Train B



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: Ref. B8.1.13)

Figure B8.2-10. WHF 480 V ITS MCC Train A



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: Ref B8.1.14)

Figure B8.2-11. WHF 480 V ITS MCC Train B

B8.2.2 ITS Onsite AC Power

The ITS power supply system is intended to provide back-up power to selected buildings and operations in the event of LOSP. A LOSP could result from a loss of power on the offsite power grid or a failure within the site 138kV to 13.8kV switchyard. This portion of the ITS power supply system consists of two identical divisions of ITS diesel generator supplied AC power. The primary components in each division include: a diesel generator, support systems for the diesel generator, and a load sequencer.

Both ITS diesel generators are located in the EDGF. Each is sized to provide sufficient 13.8kV power to support all of the ITS loads in one ITS switchgear (A or B) in six facilities (three CRCFs, the WHF, the RF, and the EDGF). The ITS diesel generator starts upon detection of an under-voltage condition via an under voltage relay of the 13.8kV ITS switchgear. The

switchyard to switchgear feeder breaker also trips open upon detection of this undervoltage condition. Each ITS diesel generator is equipped with a complete set of support systems including HVAC systems, uninterruptible power supply (UPS) and DC power systems, a fuel oil system, diesel generator start subsystem, diesel generator cooling subsystem, and lube oil subsystem that are separate and independent from the support system for the other ITS diesel generator.

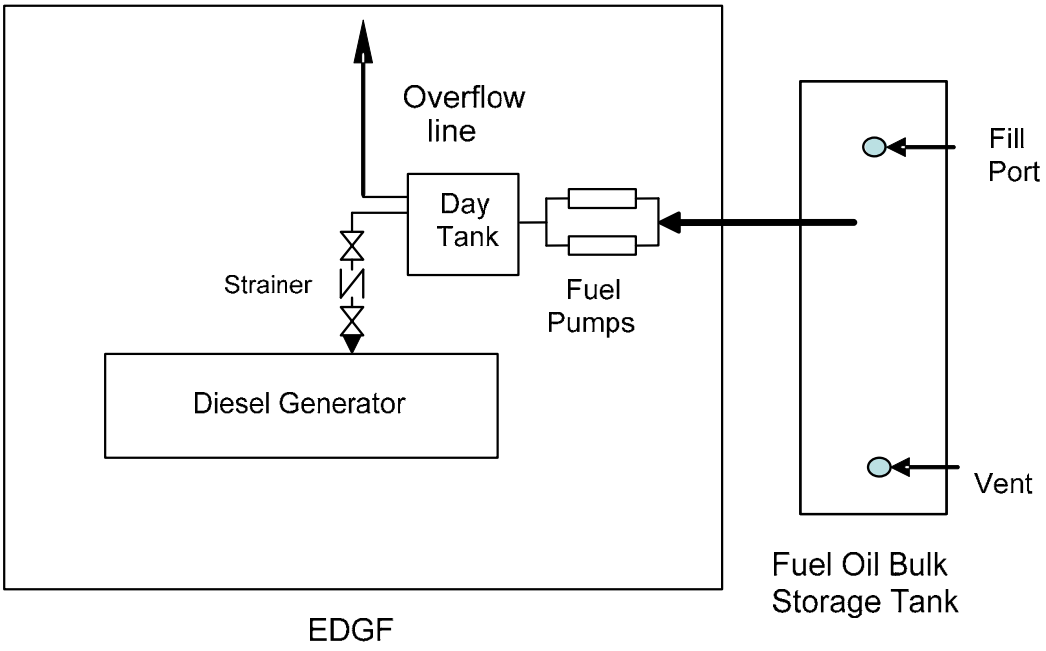
The EDGF is divided into several areas/rooms supporting the two trains of ITS AC power. Separate HVAC systems are provided for each room. The HVAC for the 13.8kV ITS Switchgear Room and Battery Room for each train of the ITS power system, includes an air handling unit and two exhaust fans for each battery room for both air flow and temperature control (Ref. B8.1.10). The system for each of the ITS diesel generator rooms consists of four exhaust fans, as maintaining air flow is sufficient to maintain room temperature within the ITS diesel generator operational limits. All four fans must operate to maintain an acceptable temperature within the ITS Diesel Generator Room (Ref. B8.1.9).

The 125 V DC power system (one for each ITS division) provides the essential power needed to operate (open/close) the medium voltage circuit breakers on the ITS switchgears. The UPS supports the ITS diesel generator control system. The UPS is not included in the ITS AC power model. A UPS is generally very reliable and the inclusion of this support system would not noticeably impact the ITS AC power system failure rate. The DC power for each division of the ITS power supply in the EDGF is supplied by a single battery. The battery is continuously charged through a single battery charger powered (through a transformer and the 480 V ITS MCC, 26D-EEE0-MCC-00001) from the 13.8 kV ITS switchgear (Figures B8.2-5 and B8.2-7).

Each ITS diesel generator fuel oil system consists primarily of a bulk storage tank, two fuel pumps, and a day tank (Figure B8.2-12). The bulk storage tank, located outside of the EDGF, has a capacity sufficient to operate the ITS diesel generator for two weeks. Each fuel pump is sized to be capable of providing sufficient makeup flow to the day tank once the level in the day tank has dropped to a one hour supply for the ITS diesel generator, and to refill the tank while the ITS diesel generator is running. The day tank, located within the EDGF, has a capacity to support four hours of ITS diesel generator operation (Ref. B8.1.8).

The lube oil subsystem, the diesel generator cooling subsystem, and the starting subsystem are considered to be part of the diesel generator and their failures are not modeled as separate events in the fault trees.

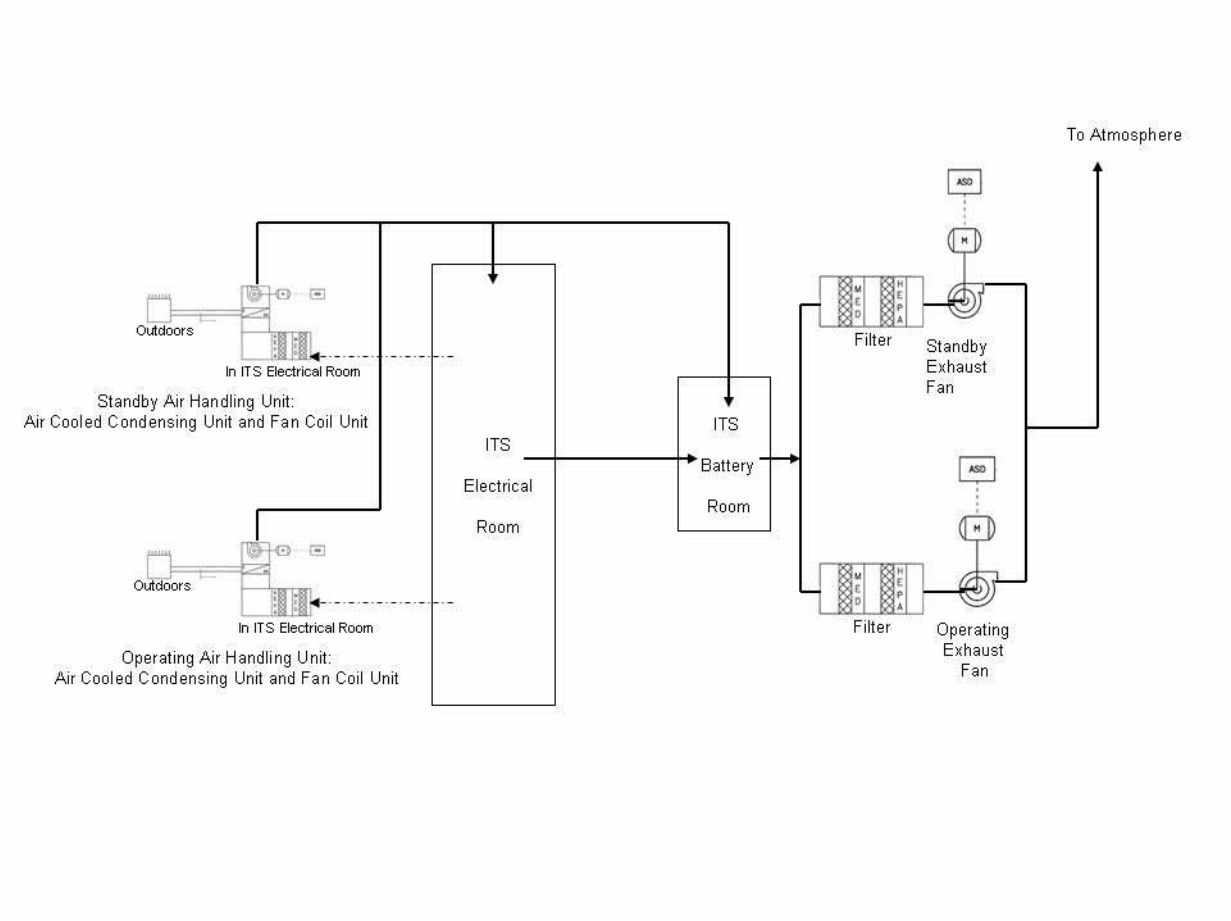
The load sequencer controls the sequence of events that occur after a LOSP and the diesel generator starts. Upon a LOSP, and after the diesel generator starts and reaches its rated capacity, the load sequencer connects the diesel generator to the 13.8kV ITS switchgear and then reconnects all division ITS loads, including the WHF ITS loads.



Source: Modified from Ref. B8.1.8

Figure B8.2-12. ITS Diesel Generator Fuel Oil System

Within the WHF, ventilation and cooling for the ITS Electrical Rooms and ITS Battery Rooms is provided by a dedicated ventilation system. A separate ventilation train is provided for each train of ITS Electrical/Battery Rooms. Each train consists of two air handling units (each consisting of an air cooled condensing unit and a fan coil unit), two exhaust fans and associated ducting and instrumentation (Fig B8.2-13). Each air handling unit and exhaust fan is rated at 100% capacity. Two air handling units, one in each train (air cooled condensing units 50-VCT0-CDU-00001 and 50-VCT0-CDU-00003 and fan coil units 50-VCT0-FCU-00001 and 50-VCT0-FCU-00003) are normally operating while the second one in each train (air cooled condensing units 50-VCT0-CDU-00002 and 50-VCT0-CDU-00004 and fan coil units 50-VCT0-FCU-00002 and 50-VCT0-FCU-00004) is normally in standby. Similarly, two exhaust fans, one in each train, (exhaust fan 50-VCT0-EXH-00004 and 50-VCT0-EXH-00006) are normally operating while the second one in each train (exhaust fan 50-VCT0-EXH-00005 and 50-VCT0-EXH-00007) is normally in standby (Ref. B8.1.15), (Ref. B8.1.16), (Ref. B8.17), and (Ref. B8.1.18).



NOTE: Legibility of figure does not affect technical content of the document. Details are found in the source document

Source: (Ref. B8.1.15), (Ref. B8.1.16), (Ref. B8.17), and (Ref. B8.1.18)

Figure B8.2-13. Simplified Diagram of Representative Train of WHF ITS Electrical and ITS Battery Rooms Ventilation System

B8.2.3 ITS AC Power Normal Operations

Under normal operating conditions, AC power is supplied from two 138kV offsite power lines. Power is passed through the 138kV to 13.8kV switchyard with the two independent 13.8kV ITS switchgears. From here, power is transmitted to two 13.8kV - 480V transformers, one supporting division A and one supporting division B of the WHF. Power to individual ITS equipment within each facility is provided via the ITS load centers and ITS MCCs (one of each for division A and division B).

The AC power system is normally operating, but one division at a time may be taken out of service for maintenance. With one division out of service, only one division of the supported ITS systems can be considered to be operable.

B8.2.4 ITS AC Power Off-Normal Operations

The off-normal condition of interest for the ITS AC power system is a LOSP. During a LOSP, both ITS diesel generators are required to start and accept loads in a timely manner. Upon a LOSP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8kV ITS switchgear and the switchyard in each division automatically opens. Both diesel generators start automatically and are connected to the 13.8kV ITS switchgear when the connecting breaker is closed by the load sequencer. The load sequencer then reconnects the WHF loads to the 13.8kV ITS switchgear. Both diesel generators continue to supply AC power until normal power is restored.

B8.2.5 ITS AC Power Testing and Maintenance

The normal AC power system is operated continuously. Maintenance would be performed on an as needed basis. The diesel generators and supporting subsystems are normally in a standby mode. Routine tests are performed to ensure that the ITS diesel generator can start and load, in the event of a loss of normal power, including during a LOSP event.

Requirements

The ITS diesel generators and their associated support components (start systems, lube oil, HVAC) are tested monthly on a staggered basis.

Features

Normal maintenance is performed in accordance with manufacturer's recommendations.

Maintenance outages that remove a division of ITS AC power from operation are limited to one week.

B8.2.5.1 Fault Trees

Requirements:

The fault tree model for the ITS AC power system includes: (1) those components that have been declared as ITS and (2) those AC power distribution system components whose failure would require the ITS AC power system to perform. The ITS power system includes components that are normally in standby (e.g., the diesel generator) and components that are normally in operation. The portions of the normal AC power distribution system modeled include the AC power distribution system from the 13.8kV ITS switchgear to the facility ITS load centers.

The mission time for the ITS AC power system is set to 720 hours. This is based on the mission time requirement for the WHF HVAC system following the potential breach of a waste canister.

B8.2.5.1.2 Design Feature:

Common-cause failures (CCF) have been included for fourteen events. Six are associated with ITS diesel generator operation: two for the ITS diesel generators (e.g., failure to start or run)

themselves and four for the pair of fuel pumps (e.g., failure to start and run for each pair) that support each ITS diesel generator. Three more are associated with the failure to open/close of the circuit breakers that disconnect the 13.8kV ITS switchgear from the normal offsite power supply, the ITS load center feed breakers, and the breakers that connect the ITS diesel generators to the 13.8kV ITS switchgear. Four are associated with the WHF Confinement ITS Electrical and Battery Rooms ventilation system: one for the failure to start and run the system standby exhaust fans, one for the failure to run the operating exhaust fans, one for the failure to start and run the standby air handling units, and one for the failure to run the operating air handling units. The final CCF event modeled is associated with the WHF 13.8kV to 480V ITS transformers. Additional detail about the treatment of CCF failures can be found in Attachment C.

Four human error conditions are incorporated into the model (details are provided in Section B.8.4 of this attachment). All four address the failure to properly restore portions of the system to operable status following maintenance.

The ITS diesel generator lube oil, cooling systems, and start subsystems are considered to be part of the diesel generator and are not modeled as separate systems.

B8.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B8.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B8.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
ITS Diesel Generators	Start systems, load sequencer	EDGF diesel Generator Room HVAC	—	Test and maintenance	—
13.8kV ITS Switchgear	ITS diesel generator, WHF 13.8kV to 480V ITS transformers	EDGF Switchgear Room HVAC	—	Test and maintenance	Offsite power
ITS Load Centers and MCCs	ITS diesel generator, 13.8kV ITS switchgear	WHF ITS AC Power Room Ventilation	—	Test and maintenance	Offsite power
AC Load Breakers	EDGF DC power system	—	—	Test and maintenance	
WHF 13.8kV to 480V ITS Transformers	ITS diesel generator, 13.8kV ITS switchgear	—	—	Test and maintenance	Offsite power
WHF ITS AC Power Room Ventilation	WHF ITS MCCs	—	—	Test and maintenance	—

NOTE: WHF = Wet Handling Facility; EDGF = Emergency Diesel Generator Facility; HVAC = heating, ventilation, and air conditioning (filter); ITS = important to safety; kV = kilovolt; MCC = motor control centers.

Source: Original

B8.4 ITS AC POWER FAILURE SCENARIOS

For the WHF the ITS AC power system has two credible failure scenarios:

1. Loss of AC Power to WHF ITS load center train A. Failure to provide power to the WHF ITS HVAC system train A powered by ITS load center train A.

2. Loss of AC Power to WHF ITS load center train B. Failure to provide power to the WHF ITS HVAC system train B powered by ITS load center train B.

B8.4.1 Loss of AC Power to WHF ITS Load Center Train A

B8.4.1.1 Description

WHF confinement following the potential breach of a waste canister is provided, in part, by the WHF ITS HVAC system. The ITS AC power system provides the power needed to operate the ITS HVAC system equipment. This fault tree models the components that are required to provide AC power from either the normal offsite power supplies or from ITS diesel generator A to ITS load center train A.

B8.4.1.2 Success Criteria

Success criteria for this train of the ITS AC power system is providing AC power from either the normal power system, or from the ITS diesel generator (diesel generator A) to the ITS HVAC division powered through WHF ITS load center train A. The AC power system must operate in support of the ITS HVAC system for as long as necessary to successfully provide confinement after the potential release of material from a breached canister. Therefore, the mission time (i.e., the period for which ITS AC power must be supplied to the ITS HVAC system) is the same for the ITS AC power system as it is for the ITS HVAC system, 720 hours.

B8.4.1.3 Design Features and Requirements

Requirements

Each ITS diesel generator has support systems that are independent from the support system for the other diesel generator. Independent support systems include:

- Fuel oil systems
- HVAC systems to include the ITS diesel generator room and 13.8kV ITS switchgear room systems
- Lube oil system
- ITS diesel generator cooling systems
- Diesel generator start system.

Features

The 13.8kV ITS switchgear is isolated from the main switchyard upon a loss of power in the switchyard, either due to a LOSP or from failures within the switchyard.

The WHF load is shed from the 13.8kV ITS switchgear upon a loss of power indication.

A load sequencer controls the loading of the diesel generator onto the 13.8kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the WHF loads onto the ITS AC power system

Environmental systems are provided to maintain the temperature in the various EDGF rooms within acceptable levels. This includes a fan system for the diesel generator room and an air handling unit for the 13.8kV ITS Switchgear and Battery Room.

B8.4.1.4 Fault Tree Model

The top event in this fault tree is “Loss of AC Power to WHF ITS Load Center Train A.” This is defined as a failure of normal and ITS on-site power at ITS load center train A. Faults considered in the evaluation of this top event include: failure of components in the normal AC

power system, failure of the ITS diesel generator, human events that can contribute to onsite system failures resulting in a power loss at the WHF and a LOSP. In this fault tree offsite power is not modeled as an initiating event, but as a system failure. The value used for this event represents the probability that offsite power would be lost in the 720 hours following a possible radioactive release from a damaged canister.

B8.4.1.5 Basic Event Data

Table B8.4-1 contains a list of basic events used in the "Loss of AC Power to WHF ITS Load Center Train A" fault tree. Included are component failures, maintenance errors and the human and CCF events identified in the previous two sections. The data, for both random and CCFs used to develop the failure probabilities associated with these basic events, comes from the component reliability data analysis (Attachment C). Human reliability analyses (Attachment E) provide the probabilities for the human events.

Mission times for the various components are based on the following:

- Fault exposure time (168 hours) for events limited to one week maintenance outages (train out of service (OOS) for maintenance).
- Mission time (360 hours) for operation of standby equipment that would operate after a LOSP (i.e., distribution of the occurrence of an LOSP is evenly distributed over the 720 hrs after a potential radiological release, average mission time is therefore 360 hours), and average fault-exposure time for standby components tested monthly.
- Mission time (720 hours) for operating components.

While some of the components are normally in operation, it is possible for any of the components to be OOS for maintenance. With train A of AC power OOS (resulting in train A of the facility ITS HVAC being OOS), train B provides support to an operable ITS HVAC train B. The intent of the maintenance events modeled is for the events to address maintenance on any component in that AC power division. This is true for the components normally in operation and the standby components. The maintenance unavailability represented by the ITS load center maintenance events model the unavailability of any component from the 13.8kV ITS switchgear through the ITS load center. The maintenance unavailability represented by the ITS diesel generator maintenance events represent the unavailability of any of the components or systems that would prevent the ITS diesel generator from starting and loading onto the 13.8kV ITS Switchgear. As noted earlier, all of the human events are associated with the failure to restore a component to operable or standby status after maintenance. The operator-related events shown in the following table are combinations events: they include the probability that the component has been taken OOS for maintenance and that site personnel have not restored the component to operable or standby status. A screening value of 0.1 has been used for the HEP in all cases.

Table B8.4-1. Basic Event Probability for the Loss of AC Power to WHF ITS Load Center Train A Fault Tree

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-#EEE-LDCNTRA-BUA-FOH	WHF load center A fails	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
050-#EEE-LDCNTRA-BUA-MTN	ITS load center train A OOS for maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
050-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS load center train A post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
050-#EEE-LDCNTRA-C52-FOD	Load Center A feed breaker fails to reclose	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
050-#EEE-LDCNTRA-C52-SPO	Load center A feed circuit breaker spurious operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
050-#EEE-LDCNTRB-BUA-MTN	ITS load center train B OOS for maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
050-#EEE-LDCNTRB-BUA-ROE	Failure to restore ITS load center train B post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
050-#EEE-LDCNTRS-C52-CCF	CCF of the ITS load center feed breakers to reclose	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
050-#EEE-WHFITSA-XMR-CCF	WHF ITS transformers CCF	1	4.450E-06	4.450E-06	0.000E+00	0.000E+00
050-#EEE-WHFITSA-XMR-FOH	WHF ITS transformer train B failure	3	2.095E-04	0.000E+00	2.910E-07	7.200E+02
050-#EEE-MCC0001-C52-SPO	WHF ITS MCC 0001 feed breaker spurious operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
050-#EEE-MCC0001-MCC-FOH	WHF ITS MCC 00001 fails	3	5.378E-03	0.000E+00	7.490E-06	7.200E+02
050-VCT0-AHU0001-AHU-FTR	WHF ITS elec AHU 00001 fails to run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
050-VCT0-AHU0001-CTL-FOD	WHF ITS elec AHU 00001 controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-AHU0002-AHU-FTR	WHF ITS elec AHU 00002 fails to run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
050-VCT0-AHU0002-CTL-FOD	WHF ITS elec AHU 00002 controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-AHU0002-FAN-FTS	WHF ITS elec AHU 00002 fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
050-VCT0-AHU0103-AHU-CCR	CCF of the running WHF ITS elec AHUs to continue to run	1	6.200E-05	6.200E-05	0.000E+00	0.000E+00
050-VCT0-AHU0202-AHU-CCR	CCF of standby WHF ITS elec AHUs to start/run	1	1.600E-04	1.600E-04	0.000E+00	0.000E+00
050-VCT0-EXH-004-CTL-FOD	WHF ITS elec exh fan 00004 controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-EXH-004-FAN-FTR	WHF ITS elec exhaust fan 00004 fails to run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
050-VCT0-EXH-005-CTL-FOD	WHF ITS elec exh fan 00005 controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-EXH-005-FAN-FTR	WHF ITS elec exhaust Fan 00005 fails to run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02

Table B8.4-1. Basic Event Probability for the Loss of AC Power to WHF ITS Load Center Train A Fault Tree (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-VCT0-EXH-005-FAN-FTS	WHF ITS elec exh Fan 00005 fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
050-VCT0-EXH-007-FAN-FTS	WHF ITS elec exh fan 00007 fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
050-VCT0-EXH0406-FAN-CCR	CCF of running exh fans for WHF ITS elec	1	1.200E-03	1.200E-03	0.000E+00	0.000E+00
050-VCT0-EXH0507-FAN-CCF	CCF to start/run: standby exh fans for the WHF ITS elec	1	1.300E-03	1.300E-03	0.000E+00	0.000E+00
26D-##EG-DAYTNKA-TKF-FOH	ITS DG A day tank (00002A) fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EG-FLITLKA-IEL-FOD	ITS DG A fuel transfer pumps interlock failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
26D-##EG-FTP1DGA-PMD-FTR	ITS DG A fuel transfer pump fails to run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP1DGA-PMD-FTS	ITS DG A fuel pump 1A fails to Start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FTP2DGA-PMD-FTR	ITS DG A fuel transfer pump 2A fails to run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP2DGA-PMD-FTS	ITS DG A fuel transfer pump 2A fails to start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FULPMPA-PMD-CCR	CCF of ITS DG A fuel pumps to run	1	2.900E-04	2.900E-04	0.000E+00	0.000E+00
26D-##EG-FULPMPA-PMD-CCS	CCF of ITS DG A fuel pumps to start	1	1.200E-04	1.200E-04	0.000E+00	0.000E+00
26D-##EG-STRTDGA-C72-SPO	ITS switchgear A battery circuit breaker (DC) spur op	3	3.851E-04	0.000E+00	1.070E-06	3.600E+02[d]
26D-##EG-WKTNK_A-TKF-FOH	ITS DG A bulk fuel tank (00001A) fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EGBATCHRGA-BYC-FOH	ITS switchgear A battery: battery charger failure	3	1.276E-03	0.000E+00	7.600E-06	1.680E+02[c]
26D-#EEE-SWGRDGA-BUA-FOH	13.8kV ITS switchgear A failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
26D-#EEESWGRDGA-AHU-FTR	13.8kV ITS switchgear room air handling unit fails	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room fan 1 (motor-driven) fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-#EEG-HVACFA1-FAN-FTS	ITS DG A room fan 1 (motor-driven) fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room fan 2 (motor-driven) fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-#EEG-HVACFA2-FAN-FTS	ITS DG A room fan 2 (motor-driven) fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room fan 3 (motor-driven) fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-#EEG-HVACFA3-FAN-FTS	ITS DG A room fan 3 (motor-driven) fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room fan 4 (motor-driven) fails to run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-#EEG-HVACFA4-FAN-FTS	ITS DG A room fan 4 (motor-driven) fails to start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-#EEU-208_DGA-BUD-FOH	ITS DC panel A DC bus failure	3	8.640E-05	0.000E+00	2.400E-07	3.600E+02[d]
26D-#EEY-DGALOAD-C52-FOD	ITS DG A load breaker (AC) fails to close	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00

Table B8.4-1. Basic Event Probability for the Loss of AC Power to WHF ITS Load Center Train A Fault Tree (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG load breakers to close	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-FTR	ITS diesel generator A fails to run	3	7.698E-01	0.000E+00	4.080E-03	3.600E+02
26D-#EEY-ITSDG-A-#DG-FTS	Diesel generator fails to start	1	8.380E-03	8.380E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly restore ITS DG-B to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A and B fail to run	1	1.800E-02	1.800E-02	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to start	1	3.900E-04	3.900E-04	0.000E+00	0.000E+00
26D-#EEY-OB-SWGA-C52-FOD	13.8kV ITS switchgear feed breaker (AC) fails to open	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS switchgear A feed breaker spurious operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
26D-#EEY-OB-SWGS-C52-CCF	CCF of 13.8 kV ITS switchgear feed breakers to open	1	1.040E-04	1.040E-04	0.000E+00	0.000E+00
26D-#EG-LCKOUTRL-RLY-FTP	13.8kV ITS switchgear feed breaker lockout relay fails to Open CB	3	3.152E-03	0.000E+00	8.770E-06	3.600E+02
26D-#EGLDSQNCRA-SEQ-FOD	DG A load sequencer fails	1	2.670E-03	2.670E-03	0.000E+00	0.000E+00
26D-EG-BATTERYA-BTR-FOD	ITS switchgear A battery no output given challenge	1	8.200E-03	8.200E-03	0.000E+00	0.000E+00
27A-#EEE-BUS2DGA-C52-SPO	13.8kV open bus 2 ITS load breaker spurious operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
27A-#EEN-OPENBS2-BUA-FOH	13.8kV open bus 2 bus failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
27A-#EEN-OPNBS1A-SWP-SPO	13.8kV open bus 2 to ITS Div A electric power switch spur. transfer	3	1.116E-04	0.000E+00	1.550E-07	7.200E+02

Table B8.4-1. Basic Event Probability for the Loss of AC Power to WHF ITS Load Center Train A Fault Tree (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
LOSP*	Loss of offsite power	1	2.990E-03	2.990E-03	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
[b] The designation of a circuit breaker as AC or DC refers to the system designation for the circuit breaker, it is not representative of the motive power for the circuit breaker.
[c] The failure of the battery charger would result in eventual depletion of the battery and a low power indication on both the battery and the DC bus. The 168 hr mission time was selected as a conservative estimation for the detection time of this failure.
[d] The mission times for the DC bus related failure rates do not take credit for any monitoring of bus status, which would provide nearly instantaneous indication of a bus failure or loss of power to the bus. The standby component mission time was used conservatively.
LOSP* represents the probability of losing offsite power during the 720 hours HVAC is required after any breach of a container releases radioactive material. It is based on a loss of offsite power frequency of 3.59E-02/year from NUREG/CR6890 Vol. 1 (Ref. B8.1.19). AC = alternating current; AHU = air handling unit; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator;
Div = division; elec = electrical EXH = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation;
Prob. = probability; Spur. = spurious; SWGR = switchgear.

Source: Original

B8.4.1.5.1 Human Failure Events

Four basic human failure events (HFEs) (Table B8.4-2) are associated with human error. All of the HFEs are associated with the failure to properly restore components to operable status following maintenance. The first two shown in Table B8.4-2 are associated with the failure to restore the normal power supply to the WHF ITS load centers after maintenance. The last two are representative of the failure to restore the ITS diesel generators (and any other components that would prevent the ITS diesel generator from starting or loading) to service after maintenance. These events are combination events consisting of the probability that a component was removed for maintenance and the failure of plant operators (assigned a screening value of 0.1) to restore the component after maintenance.

Table B8.4-2. Human Failure Events

Name	Description
050-#EEE-LDCNTRA-BUA-ROE	Failure to restore ITS load center train A post maintenance
050-#EEE-LDCNTRB-BUA-ROE	Failure to restore ITS load center train B post maintenance
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly return ITS DG-B to service

NOTE: DG = diesel generator; ITS = Important to Safety.

Source: Original

B8.4.1.5.2 Common-Cause Failures

Twelve of the fourteen CCFs identified earlier (Section B8.2.5.1.2) have been included in the analysis of the loss of ITS AC power to the ITS load center train A. Ten of the CCF events affect both trains of ITS AC power. Two affect only this train of the system. The remaining two affect only the other train of the system. Two are associated with the ITS diesel generators: CCF of the ITS diesel generators to start and CCF of the ITS diesel generators to run. The CCF of the ITS diesel generator fuel oil system incorporates two CCFs: CCF of the two fuel oil pumps to start and the CCF of the pumps to run. Three circuit breaker CCF events were considered. These are the CCF of: (1) 13.8 kV ITS switchgear feed breakers (from 13.8kV open buses) to open on loss of offsite power, (2) ITS diesel generator load breakers to close when commanded by the load sequencer, and (3) ITS load center feed breakers to close when commanded by the load sequencer. Four CCFs are associated with the WHF ITS Electrical and Battery Rooms' ventilation system, two for the CCF of exhaust fans to start and run, and two for the CCF of the air handling units to start and run. The last CCF event considered is the CCF of the 13.8kV to 480V ITS transformers.

Table B8.4-3. Common-Cause Basic Events

Name	Description	Alpha-factor
050-#EEE-LDCNTRS-C52-CCF	CCF of the ITS load center feed breakers to reclose	0.0235
050-#EEE-WHFITSA-XMR-CCF	CCF of WHF ITS transformers	0.047
26D-##EG-FULPMPA-PMD-CCR	CCF of ITS DG A fuel pumps to run	0.0235
26D-##EG-FULPMPA-PMD-CCS	CCF of ITS DG A fuel pumps to start	0.047
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG load breakers to close	0.047
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A and B fail to run	0.0235
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to start	0.047
26D-#EEY-OB-SWGS-C52-CCF	CCF of 13.8kV ITS switchgear feed breakers to open	0.047
050-VCT0-AHU0103-AHU-CCR	CCF of the running WHF ITS elec AHUs to continue to run	0.0235
050-VCT0-AHU0202-AHU-CCR	CCF of standby WHF ITS elec AHUs to start/run	0.047 start 0.0235 run
050-VCT0-EXH0406-FAN-CCR	CCF of running exh fans for WHF ITS elec.	0.0235
050-VCT0-EXH0507-FAN-CCF	CCF to start/run: standby exh fans for the WHF ITS elec	0.047 start 0.0235 run

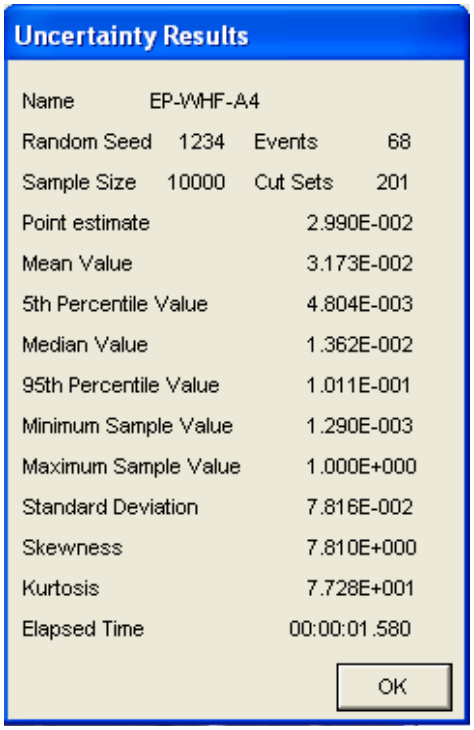
NOTE: AHU = air handling unit; CCF = common cause failure; DG = diesel generator; elec = electrical; exh = exhaust; ITS = important to safety.

Source: Original

All of the common cause successes modeled are used on pairs of components with one of two success criteria (i.e., two of two failure criteria). Alpha-factors used to determine the common cause failure probability are 0.047 for demand failures and 0.0235 for time dependent failures (see Attachment C, Table C3-1, CCCG=2, and the associated text). Two CCF in Table B8.4-3 are used to represent the CCF associated with the failure to start and failure to run for components. For these two CCFs, the appropriate alpha-factors were applied to the start and run portions of the random failure probability to develop a single CCF probability for the components.

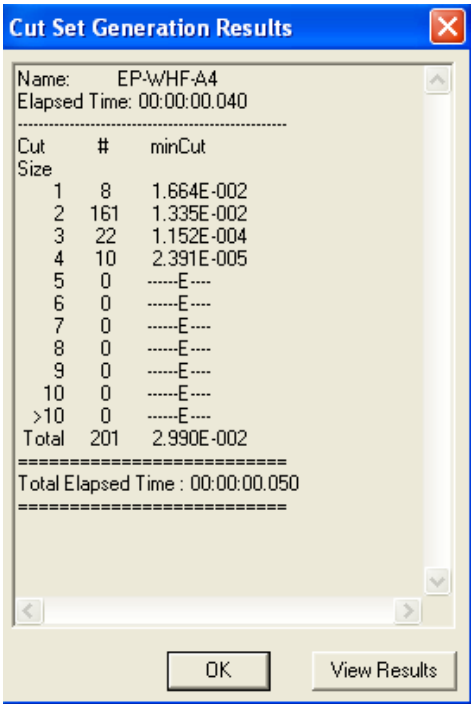
B8.4.1.6 Uncertainty and Cut Set Generation

Figure B8.4-1 contains the uncertainty results obtained from running the fault trees for the "Loss of AC Power to WHF ITS Load Center Train A". Figure B8.4-2 provides the cut set generation results for the "Loss of AC Power to WHF ITS Load Center Train A" fault tree.



Source: Original

Figure B8.4-1. Uncertainty Results of the Loss of AC Power to WHF ITS Load Center Train A Fault Tree



Source: Original

Figure B8.4-2. Cut Set Generation Results for the Loss of AC Power to WHF ITS Load Center Train A Fault Tree

B8.4.1.7 Cut Sets

Table B8.4-4 contains the top 25 cut sets accounting for 97% of the system failure probability for the "Loss of AC Power to WHF ITS Load Center Train A" fault tree.

Table B8.4-4. Dominant Cut Sets for the Loss of AC Power to WHF ITS Load Center Train A

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
17.99	17.99	5.378E-03	050-#EEE-MCC0001-MCC-FOH	WHF ITS MCC 00001 Fails	5.378E-03
30.75	12.76	3.816E-03	050-#EEE-LDCNTRA-C52-SPO	Load Center A Feed Circuit Breaker Spurious Operation	3.816E-03
43.51	12.76	3.816E-03	050-#EEE-MCC0001-C52-SPO	WHF ITS MCC 0001 Feed Breaker Spurious Operation	3.816E-03
53.33	9.82	2.937E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS Switchgear A Feed Breaker Spurious Operation	3.816E-03
63.15	9.82	2.937E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
72.00	8.85	2.646E-03	26D-#EEESWGRDGA-AHU-FTR	13.8kV ITS Switchgear Room Air Handling Unit Fails	2.646E-03
80.56	8.56	2.559E-03	050-VCT0-EXH-004-FAN-FTR	WHF ITS Elec Exhaust Fan 00004 Fails to Run	5.059E-02
			050-VCT0-EXH-005-FAN-FTR	WHF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-02
88.26	7.70	2.302E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			LOSP*	Loss of offsite power	2.990E-03
89.73	1.47	4.391E-04	050-#EEE-LDCNTRA-BUA-FOH	WHF Load Center A Fails	4.391E-04
91.20	1.47	4.391E-04	26D-#EEE-SWGRDGA-BUA-FOH	13.8kV ITS Switchgear A Failure	4.391E-04
92.33	1.13	3.380E-04	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			27A-#EEN-OPENBS2-BUA-FOH	13.8kV Open Bus 2 Bus Failure	4.391E-04
93.03	0.70	2.095E-04	050-#EEE-WHFITSA-XMR-FOH	WHF ITS Transformer Train B Failure	2.095E-04
93.37	0.34	1.027E-04	050-VCT0-EXH-004-FAN-FTR	WHF ITS Elec Exhaust Fan 00004 Fails to Run	5.059E-02
			050-VCT0-EXH-005-CTL-FOD	WHF ITS Elec Exh fan 00005 Controller Fails	2.030E-03
93.71	0.34	1.027E-04	050-VCT0-EXH-004-CTL-FOD	WHF ITS Elec Exh Fan 00004 Controller Fails	2.030E-03
			050-VCT0-EXH-005-FAN-FTR	WHF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-02

Table B8.4-4. Dominant Cut Sets for The Loss of AC Power to WHF ITS Load Center Train A (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
94.05	0.34	1.025E-04	050-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	1.025E-04
			/050-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	9.999E-01
			/050-#EEE-LDCNTRB-BUA-ROE	Failure to Restore ITS Load Center Train B post maintenance	1.000E+000
94.39	0.34	1.022E-04	050-VCT0-EXH-004-FAN-FTR	WHF ITS Elec Exhaust Fan 00004 Fails to Run	5.059E-02
			050-VCT0-EXH-005-FAN-FTS	WHF ITS Elec Exh Fan 00005 Fails to Start	2.020E-03
94.72	0.33	9.777E-05	26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS Switchgear A feed Breaker Spurious Operation	3.816E-03
95.05	0.33	9.777E-05	26D-#EEG-HVACFA2-FAN-FTR	ITS DG A Room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
95.38	0.33	9.777E-05	26D-#EEG-HVACFA3-FAN-FTR	ITS DG A Room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
95.71	0.33	9.777E-05	26D-#EEG-HVACFA4-FAN-FTR	ITS DG A Room Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8kV ITS Switchgear A feed Breaker Spurious Operation	3.816E-03
96.04	0.33	9.777E-05	26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
96.37	0.33	9.777E-05	26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
96.70	0.33	9.777E-05	26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
97.03	0.33	9.777E-05	26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
97.32	0.29	8.590E-05	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01

Table B8.4-4. Dominant Cut Sets for The Loss of AC Power to WHF ITS Load Center Train A (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
			27A-#EEN-OPNBS1A-SWP-SPO	13.8kV Open Bus 2 to ITS Div A Electric Power Switch Spur. Xfer	1.116E-04

NOTE: AC = alternating current; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator; Div = division elec = electrical; exh = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation; Prob. = probability; Spur. = spurious; SWGR = switchgear; WHF = Wet handling Facility; Xfer = transfer.

Source: Original

B8.4.2 Loss of AC Power to WHF ITS Load Center Train B

B8.4.2.1 Description

WHF confinement following the potential breach of a waste canister is provided, in part, by the WHF ITS HVAC system. The ITS AC power system provides the AC power needed to operate the ITS HVAC system equipment. This fault tree models the components that are required to provide AC power from either the normal offsite power supplies or from ITS diesel generator B to ITS load center train B.

B8.4.2.2 Success Criteria

Success criteria for this train of the ITS AC power system is to provide AC power from either the normal power system or from the ITS diesel generator (diesel generator train B) to the ITS HVAC division powered through WHF ITS load center train B. The AC power system must operate in support of the ITS HVAC system for as long as necessary to successfully provide confinement after the potential release of material from a breached canister. Therefore, the mission time (the period for which AC power must be supplied to the ITS HVAC system) is the same for the ITS AC power system as it is for the ITS HVAC system, 720 hours.

B8.4.2.3 Design Requirements and Features

Requirements

Each ITS diesel generator has support systems that are independent from the support system for the other diesel generator. Independent support systems include:

- Fuel oil systems
- HVAC systems to include the ITS diesel generator room and 13.8kV ITS switchgear room systems
- Lube oil system
- ITS diesel generator cooling systems
- Diesel generator start system.

Features

The 13.8kV ITS switchgear is isolated from the main switchyard upon a loss of power in the switchyard, either due to a LOSP or from failures within the switchyard.

The WHF load is shed from the 13.8kV switchgear upon a loss of power indication.

A load sequencer controls the loading of the diesel generator onto the 13.8kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the WHF loads onto the ITS AC power system.

Environmental systems are provided to maintain the temperature in the various EDGF rooms within acceptable levels. This includes a fan system for the diesel generator room and air handling units for the 13.8kV ITS switchgear and battery room.

B8.4.2.4 Fault Tree Model

The top event in this fault tree is "Loss of AC Power to WHF ITS Load Center Train B." This is defined as a failure of the normal and ITS onsite power supplies to provide power to ITS load center B. Faults considered in the evaluation of this top event include: failure of components in the normal AC power system, failure of the ITS diesel generator subsystem, human events that can contribute to onsite system failures resulting in a power loss at the WHF and a LOSP. In this fault tree offsite power is not modeled as an initiating event, but as a system failure. The value used for this event represents the probability that offsite power would be lost in the 720 hours following a possible radioactive release from a damaged canister.

B8.4.2.5 Basic Event Data

Table B8.4-5 contains a list of basic events used in the "Loss of AC Power to WHF ITS Load Center Train B" fault tree. Included are component failures, maintenance errors and the human events and the CCF events identified in the previous two sections. The data, for both random and CCFs used to develop the failure probabilities associated with these basic events comes from the component reliability data analysis (Attachment C). Human reliability analyses (Attachment E) provide the probabilities for the human events.

Mission times for the various components are based on the following:

- Fault exposure time (168 hours) for events limited to one week maintenance outages (train OOS for maintenance).
- Mission time (360 hours) for operation of standby equipment that would operate after a LOSP (distribution of the occurrence of an LOSP is evenly distributed over the 720 after a potential radiological release, average mission time is therefore 360 hours), and average fault exposure time for standby components tested monthly.
- Mission time (720 hours) for operating components.

While some of the components are normally in operation, it is possible for any of the components to be OOS for maintenance. With train A of AC power OOS (resulting in train B of the facility ITS HVAC being OOS) train A provides support to an operable ITS HVAC train A. The intent of the maintenance events modeled is for the events to address maintenance on any component in that AC power division. This is true for the components normally in operation and the standby components. The maintenance unavailability represented by the ITS load center maintenance events model the unavailability of any component from the 13.8kV ITS switchgear through the ITS load center. The maintenance unavailability represented by the ITS diesel generator maintenance events represent the unavailability of any of the components or systems that would prevent the ITS diesel generator from starting and loading onto the 13.8kV ITS switchgear. As noted earlier, all of the human events are associated with the failure to restore a component to operable or standby status after maintenance. The operator-related events shown in the following table are combination events: they include the probability that the component has been taken OOS for maintenance and that site personnel have not restored the component to operable or standby status. A screening value of 0.1 has been used for the HEP in all cases.

Table B8.4-5. Basic Event Probability for the Loss of AC Power to WHF ITS Load Center Train B Fault Trees

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
050-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
050-#EEE-LDCNTRB-BUA-FOH	WHF ITS Load Center B Fails	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
050-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
050-#EEE-LDCNTRB-BUA-ROE	Failure to Restore ITS Load Center Train B post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
050-#EEE-LDCNTRB-C52-FOD	13.8kV ITS SWGR to WHF ITS LC B Circuit Breaker Fails on Demand	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
050-#EEE-LDCNTRB-C52-SPO	WHF ITS Load Center Circuit Breaker (AC) Spur Op	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
050-#EEE-LDCNTRS-C52-CCF	CCF of the ITS Load Center feed breakers to reclose	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
050-#EEE-MCC0002-C52-SPO	WHF MCC-00002 Feed Breaker Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
050-#EEE-MCC0002-MCC-FOH	WHF ITS MCC00002 Failure	3	5.378E-03	0.000E+00	7.490E-06	7.200E+02
050-#EEE-WHFITSA-XMR-CCF	WHF ITS Transformers CCF	1	4.450E-06	4.450E-06	2.910E-07	3.400E+01
050-#EEE-WHFITSB-XMR-FOH	WHF ITS Transformer Train B Failure	3	2.095E-04	0.000E+00	2.910E-07	7.200E+02
050-VCT0-AHU0003-AHU-FTR	WHF ITS Elec AHU 00003 Fails to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
050-VCT0-AHU0003-CTL-FOD	WHF ITS Elec AHU 00003 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-AHU0004-AHU-FTR	WHF ITS ELec AHU 00004 Fails to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
050-VCT0-AHU0004-CTL-FOD	WHF ITS Elec AHU 00004 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-AHU0004-FAN-FTS	WHF ITS Elec AHU 00004 Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
050-VCT0-AHU0103-AHU-CCR	CCF of the running WHF ITS Elec AHUs to continue to run	1	6.200E-05	6.200E-05	0.000E+00	0.000E+00
050-VCT0-AHU0202-AHU-CCR	CCF of standby WHF ITS Elec AHUs to start/run	1	1.600E-04	1.600E-04	0.000E+00	0.000E+00
050-VCT0-EXH-006-CTL-FOD	WHF ITS Elec Exh Fan 0006 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-EXH-006-FAN-FTR	WHF ITS Elec Exh Fan Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
050-VCT0-EXH-007-CTL-FOD	WHF ITS Elec Exh fan 00007 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
050-VCT0-EXH-007-FAN-FTR	WHF ITS Elec Exhaust Fan 00007 Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
050-VCT0-EXH-007-FAN-FTS	WHF ITS Elec Exh fan 00007 Fails to Start	1	2.020E-03	2.020E-003	0.000E+00	0.000E+00
050-VCT0-EXH0406-FAN-CCR	CCF of Running Exh Fans for WHF ITS Elec.	1	1.200E-03	1.200E-003	0.000E+00	0.000E+00

Table B8.4-5. Basic Event Probability for The Loss of AC Power to WHF ITS Load Center Train B Fault Trees (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
050-VCT0-EXH0507-FAN-CCF	CCF to Start/Run: Standby Exh fans for the WHF ITS Elec	1	1.300E-03	1.300E-03	0.000E+00	0.000E+00
26D-##EGBATCHRGB-BYC-FOH	ITS DG B Battery Charger Failure	3	1.276E-03	0.000E+00	7.600E-06	1.680E+02[c]
26D-##EG-DAYTNKB-TKF-FOH	ITS DG B Day fuel tank fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EG-FLITLKB-IEL-FOD	ITS DG B fuel transfer pumps Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
26D-##EG-FTP1DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP1DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FTP2DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP2DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Start on Demand	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FULPMPB-PMD-CCR	CCF of ITS DG B Fuel Pumps to Run	1	2.900E-04	2.900E-04	0.000E+00	0.000E+00
26D-##EG-FULPMPB-PMD-CCS	CCF of ITS DG B Fuel Pumps to Start	1	1.200E-04	1.200E-04	0.000E+00	0.000E+00
26D-##EG-HVACFN1-FAN-FTR	ITS DG B Room Fan 1 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN1-FAN-FTS	ITS DG B Room Fan (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN2-FAN-FTR	ITS DG B Room Fan 2 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN2-FAN-FTS	ITS DG B Room Fan (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN3-FAN-FTR	ITS DG B Room Fan 3 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN3-FAN-FTS	ITS DG B Room Fan 3 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN4-FAN-FTS	ITS DG B Room Fan 4 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-STRTDGB-C72-SPO	13.8kV ITS Switchgear Battery B Circuit Breaker (DC) Spur Op	3	3.851E-04	0.000E+00	1.070E-06	3.600E+02[d]
26D-##EG-WKTNK_B-TKF-FOH	ITS DG B Bulk Fuel Tank Fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-#EEE-SWGRDGB-AHU-FTR	EDGF Switchgear Room Air Handling Unit Failure to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
26D-#EEE-SWGRDGB-BUA-FOH	13.8kV ITS Switchgear B Bus Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02

Table B8.4-5. Basic Event Probability for The Loss of AC Power to WHF ITS Load Center Train B Fault Trees (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
26D-#EEU-208_DGB-BUD-FOH	ITS Diesel Generator DC Panel Failure	3	8.640E-05	0.000E+00	2.400E-07	3.600E+02[d]
26D-#EEY-DGBLOAD-C52-FOD	ITS DG B load breaker fails to close	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG load breakers to close	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B Fail to Run	1	1.800E-02	1.800E-02	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to Start	1	3.900E-04	3.900E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	3	7.698E-01	0.000E+00	4.080E-03	3.600E+02
26D-#EEY-ITS-DGB-#DG-FTS	Diesel Generator Fails to Start	1	8.380E-03	8.380E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly restore ITS DG-B to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-OB-SWGB-C52-FOD	Circuit Breaker (AC) Fails on Demand	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
26D-#EEY-OB-SWGS-C52-CCF	CCF of 13.8kV ITS SWGR feed breakers to open	1	1.040E-04	1.040E-04	0.000E+00	0.000E+00
26D-#EG-BATTERYB-BTR-FOD	ITS SWGR Control Battery B No Output	1	8.200E-03	8.200E-03	0.000E+00	0.000E+00
26D-#EG-LDSQNCRB-SEQ-FOD	ITS DG B load sequencer fails	1	2.670E-03	2.670E-03	2.670E-03	0.000E+00
26D-#EG-LOCKOUTB-RLY-FTP	13.8kV ITS switchgear Lockout Relay (Power) Fails to Open CB	3	3.152E-03	0.000E+00	8.770E-06	3.600E+02
27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
27A-#EEN-OPENBS4-BUA-FOH	13.8kV Open Bus 4 Bus Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
27A-#EEN-OPNBS3B-SWP-SPO	13.8kV Open Bus 4 to ITS B Electric Power Switch Spur transfer	3	1.116E-04	0.000E+00	1.550E-07	7.200E+02

Table B8.4-5. Basic Event Probability for The Loss of AC Power to WHF ITS Load Center Train B Fault Trees (Continued)

Name	Description[b]	Calc. Type[a]	Calculation Probability	Failure Probability	Lambda	Mission Time[a]
LOSP*	Loss of offsite power	1	2.990E-03	2.990E-03	0.000E+00	0.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
[b] The designation of a circuit breaker as AC or DC refers to the system designation for the circuit breaker, it is not representative of the motive power for the circuit breaker.
[c] The failure of the battery charger would result in eventual depletion of the battery and a low power indication on both the battery and the DC bus. The 168 hr mission time was selected as a conservative estimation for the detection time of this failure.
[d] The mission times for the DC bus related failure rates do not take credit for any monitoring of bus status, which would provide nearly instantaneous indication of a bus failure or loss of power to the bus. The standby component mission time was used conservatively.
LOSP* represents the probability of losing offsite power during the 720 hours HVAC is required after any breach of a container releases radioactive material. It is based on a loss of offsite power frequency of 3.59E-02/year from NUREG/CR6890 Vol. 1 (Ref. B8.1.19).AC = alternating current; AHU = air handling unit; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator;
Div = division; elec = electrical EXH = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation;
Prob. = probability; Spur. = spurious; SWGR = switchgear.

Source: Original

B8.4.2.5.1 Human Failure Events

Four basic HFEs (Table B8.4-6) are associated with human error. All of the HFEs are associated with the failure to properly restore components to operable status following maintenance. The first two shown in Table B8.4-6 are associated with the failure to restore the normal power supply to the WHF ITS load centers after maintenance. The last two are representative of the failure to restore the ITS diesel generators (and any other components that would prevent the ITS diesel generator from starting or loading) to service after maintenance. These events are combination events consisting of the probability that a component was removed for maintenance and the failure of plant operators (assigned a screening value of 0.1) to restore the component after maintenance.

Table B8.4-6. Human Failure Events

Name	Description
050-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A Post Maintenance
050-#EEE-LDCNTRB-BUA-ROE	Failure to Restore ITS Load Center Train B Post Maintenance
26D-#EEY-ITSDG-A-#DG-RSS	Failure to Properly Return ITS DG A to Service
26D-#EEY-ITSDG-B-#DG-RSS	Failure to Properly Return ITS DG B to Service

NOTE: DG = diesel generator; ITS = Important to Safety.

Source: Original

B8.4.2.5.2 Common-Cause Failures

Twelve of the fourteen CCF identified earlier (Table B8.4-7) have been included in the analysis of the loss of ITS AC power to the ITS load center train B. Ten of the CCF events affect both trains of ITS AC Power. Two affect only this train of the system. The remaining two affect only the other train of the system. Two are associated with the ITS diesel generators: CCF of the ITS diesel generators to start and CCF of the ITS diesel generators to run.

The CCF of the ITS diesel generator fuel oil system incorporates two CCFs: CCF of the two fuel oil pumps to start and the CCF of the pumps to run. Three circuit breaker CCF events were considered. These are the CCF of the 1) 13.8kV ITS switchgear feed breakers (from 13.8kV open buses) to open on loss of offsite power, 2) ITS diesel generator load breakers to close when commanded by the load sequencer and 3) ITS load center feed breakers to close when commanded by the load sequencer. Four CCF are associated with the WHF ITS Electrical and Battery Rooms' ventilation system, two for the CCF of exhaust fans to start and run, and two for the CCF of the air handling units to start and run. The last CCF event considered is the CCF of the 13.8kV to 480V ITS transformers.

All of the CCFs modeled are used on pairs of components with one of two success criteria (i.e., two of two failure criteria). Alpha-factors used to determine the CCF probability are 0.047 for demand failures and 0.0235 for time dependent failures (see Attachment C, Table C3-1, CCCG=2, and the associated text). Two CCFs in Table B8.4-7 are used to represent the CCF associated with the failure to start and failure to run for components. For these two CCFs, the appropriate alpha-factors were applied to the start and run portions of the random failure probability to develop a single CCF probability for the components.

Table B8.4-7. Common-Cause Basic Events

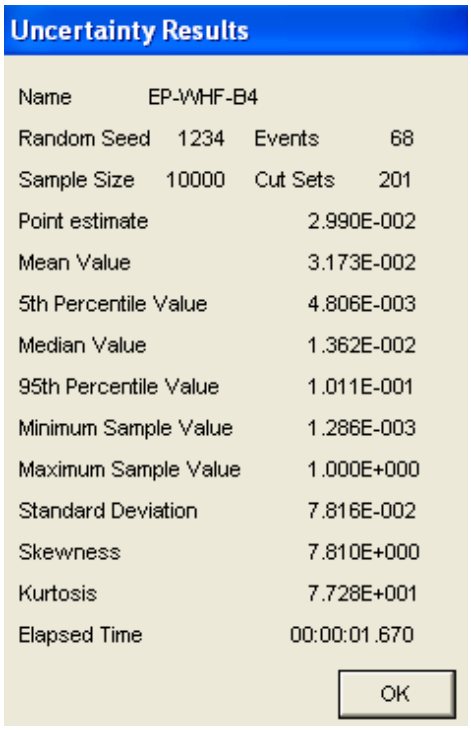
Name	Description	Alpha-factor
050-#EEE-LDCNTRS-C52-CCF	CCF of the ITS load center feed breakers to reclose	0.0235
050-#EEE-WHFITSA-XMR-CCF	CCF of WHF ITS transformers	0.047
26D-##EG-FULPMPB-PMD-CCR	CCF of ITS DG B fuel pumps to run	0.0235
26D-##EG-FULPMPB-PMD-CCS	CCF of ITS DG B fuel pumps to start	0.047
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG load breakers to close	0.047
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A and B fail to run	0.0235
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to start	0.047
26D-#EEY-OB-SWGS-C52-CCF	CCF of 13.8 kV ITS switchgear feed breakers to open	0.047
050-VCT0-AHU0103-AHU-CCR	CCF of the running WHF ITS elec AHUs to continue to run	0.0235
050-VCT0-AHU0202-AHU-CCR	CCF of standby WHF ITS elec AHUs to start/run	0.047 start 0.0235 run
050-VCT0-EXH0406-FAN-CCR	CCF of running exh fans for WHF ITS elec.	0.0235
050-VCT0-EXH0507-FAN-CCF	CCF to start/run: standby exh fans for the WHF ITS elec	0.047 start 0.0235 run

NOTE: AHU = air handling unit; CCF = common cause failure; DG = diesel generator; elec = electrical; exh = exhaust; ITS = important to safety; SWGR = switchgear; WHF = Wet Handling Facility.

Source: Original

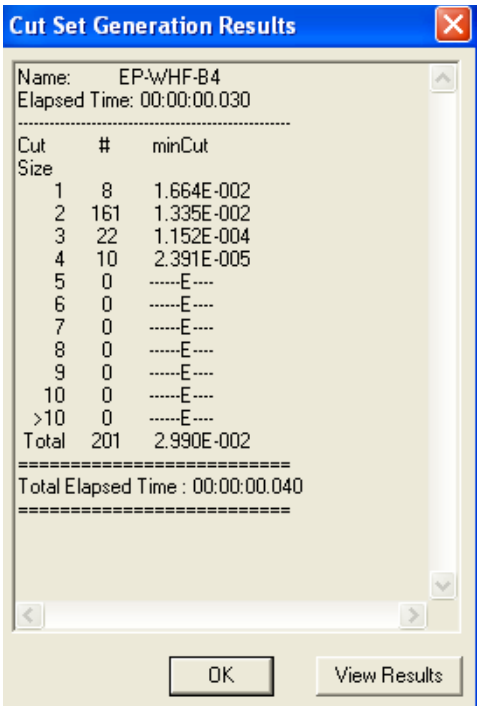
B8.4.2.6 Uncertainty and Cut Set Generation

Figure B8.4-3 contains the uncertainty results obtained from running the fault tree for "Loss of AC Power to WHF ITS Load Center Train B". Figure B8.4-4 provides the cut set generation results for the "Loss of AC Power to WHF ITS Load Center Train B".



Source:

Figure B8.4-3. Uncertainty Results of the Loss of AC Power to WHF ITS Load Center Train B Fault Tree



Source:

Figure B8.4-4. Cut Set Generation Results for the Loss of AC Power to WHF ITS Load Center Train B Fault Tree

B8.4.2.7 Cut Sets

Table B8.4-8 contains the top 25 cut sets that contribute 97% of the total system failure probability for the "Loss of AC Power to WHF ITS Load Center Train B" fault tree.

Table B8.4-8. Dominant Cut Sets for the Loss of AC Power to WHF ITS Load Center Train B

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
17.99	17.99	5.378E-03	050-#EEE-MCC0002-MCC-FOH	WHF ITS MCC00002 Failure	5.378E-03
30.75	12.76	3.816E-03	050-#EEE-LDCNTRB-C52-SPO	WHF ITS Load Center Circuit Breaker (AC) Spur Op	3.816E-03
43.51	12.76	3.816E-03	050-#EEE-MCC0002-C52-SPO	WHF MCC-00002 Feed Breaker Spurious Operation	3.816E-03
53.33	9.82	2.937E-03	26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.698E-01
			26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
63.15	9.82	2.937E-03	26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.698E-01
			27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
72.00	8.85	2.646E-03	26D-#EEE-SWGRDGB-AHU-FTR	EDGF Switchgear Room Air Handling Unit Failure to Run	2.646E-03

Table B8.4-8. Dominant Cut Sets for The Loss of AC Power to WHF ITS Load Center Train B (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
80.56	8.56	2.559E-03	050-VCT0-EXH-006-FAN-FTR	WHF ITS Elec Exh. Fan Fails to Run	5.059E-02
			050-VCT0-EXH-007-FAN-FTR	WHF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-02
88.26	7.70	2.302E-03	26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.698E-01
			LOSP*	Loss of Offsite Power	2.990E-03
89.73	1.47	4.391E-04	050-#EEE-LDCNTRB-BUA-FOH	WHF ITS Load Center B Fails	4.391E-04
91.20	1.47	4.391E-04	26D-#EEE-SWGRDGB-BUA-FOH	13.8kV ITS Switchgear B Bus Failure	4.391E-04
92.33	1.13	3.380E-04	26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.698E-01
			27A-#EEN-OPENBS4-BUA-FOH	13.8kV Open Bus 4 Bus Failure	4.391E-04
93.03	0.70	2.095E-04	050-#EEE-WHF ITSB-XMR-FOH	WHF ITS Transformer Train B Failure	2.095E-04
93.37	0.34	1.027E-04	050-VCT0-EXH-006-CTL-FOD	WHF ITS Elec Exh Fan 0006 Controller Fails	2.030E-03
			050-VCT0-EXH-007-FAN-FTR	WHF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-02
93.71	0.34	1.027E-04	050-VCT0-EXH-006-FAN-FTR	WHF ITS Elec Exh. Fan Fails to Run	5.059E-02
			050-VCT0-EXH-007-CTL-FOD	WHF ITS Elec Exh Fan 00007 Controller Fails	2.030E-03
94.05	0.34	1.025E-04	050-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	9.999E-01
			050-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post Maintenance	1.000E+00 0
			050-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	1.025E-04
94.39	0.34	1.022E-04	050-VCT0-EXH-006-FAN-FTR	WHF ITS Elec Exh. Fan Fails to Run	5.059E-02
			050-VCT0-EXH-007-FAN-FTS	WHF ITS Elec Exh fan 00007 Fails to Start	2.020E-03
94.72	0.33	9.777E-05	26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
95.05	0.33	9.777E-05	26D-##EG-HVACFN3-FAN-FTR	ITS DG B Room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
95.38	0.33	9.777E-05	26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03

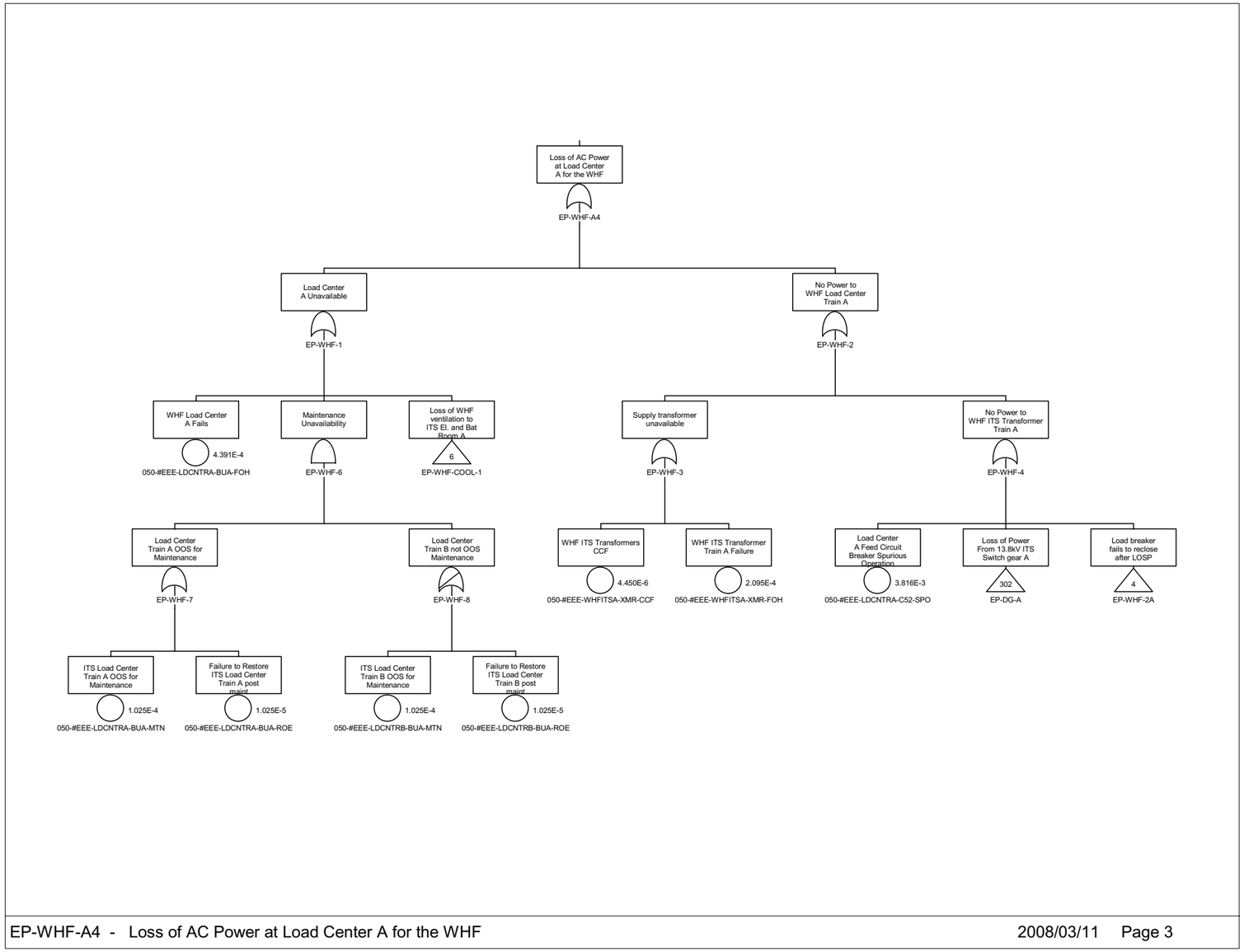
Table B8.4-8. Dominant Cut Sets for The Loss of AC Power to WHF ITS Load Center Train B (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
95.71	0.33	9.777E-05	26D-##EG-HVACFN1-FAN-FTR	ITS DG B Room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
96.04	0.33	9.777E-05	26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
96.37	0.33	9.777E-05	26D-##EG-HVACFN3-FAN-FTR	ITS DG B room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
96.70	0.33	9.777E-05	26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
97.03	0.33	9.777E-05	26D-##EG-HVACFN1-FAN-FTR	ITS DG B room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	Circuit Breaker (AC) Spurious Operation	3.816E-03
97.32	0.29	8.590E-05	26D-#EEY-ITSDGB-#DG-FTR	Diesel Generator Fails to Run	7.698E-01
			27A-#EEN-OPNBS3B-SWP-SPO	13.8kV Open Bus 4 to ITS B Electric Power Switch Spur Xfer	1.116E-04

NOTE: AC = alternating current; AHU = air handling unit; CB = circuit breaker; CCF = common cause failure; DC = direct current; DG = diesel generator; Div = division; elec = electrical; exh = exhaust; ITS ; important to safety; OOS = out of service; Xfer = transfer.

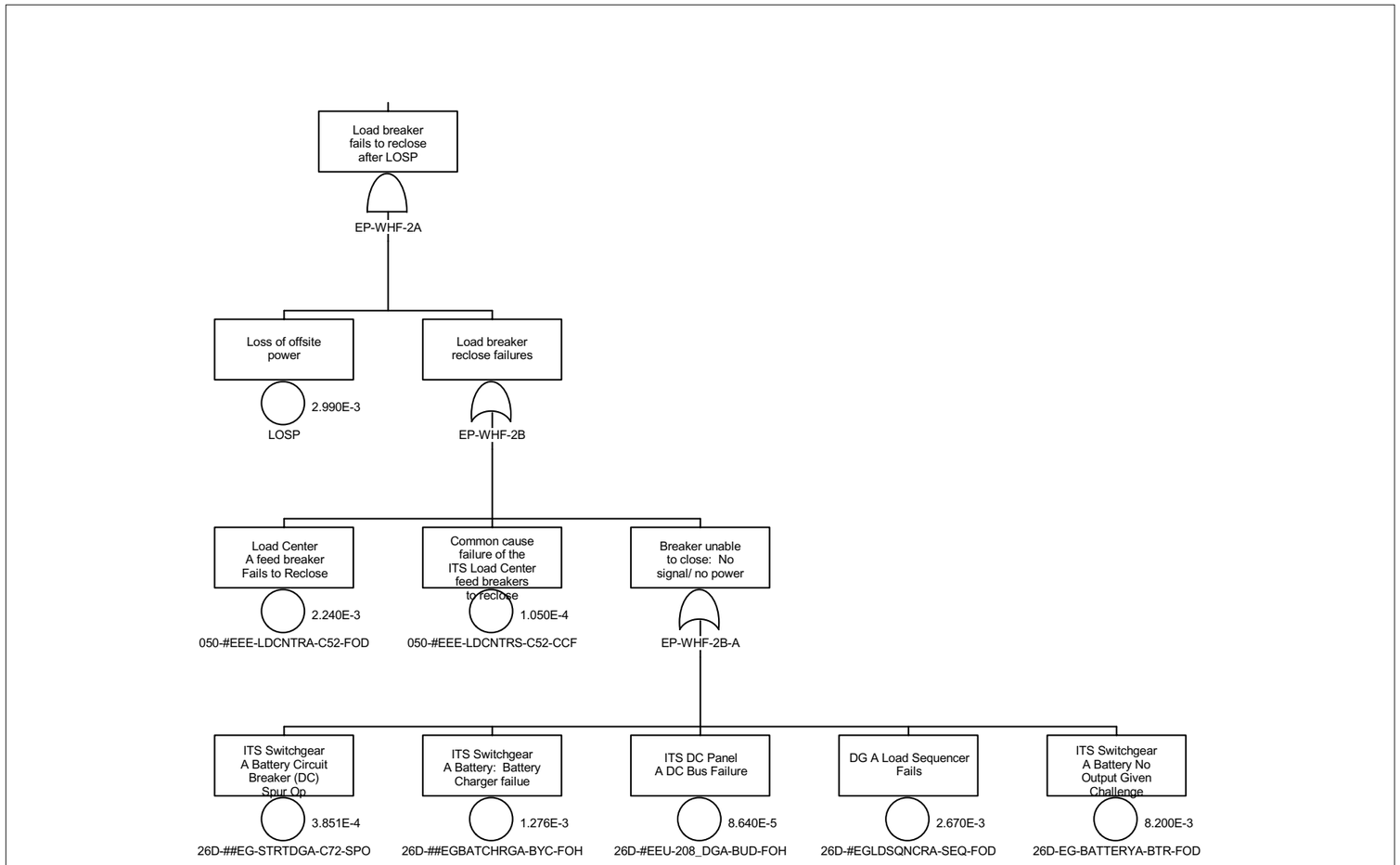
Source: Original

B8.4.2.8 AC Power Fault Trees



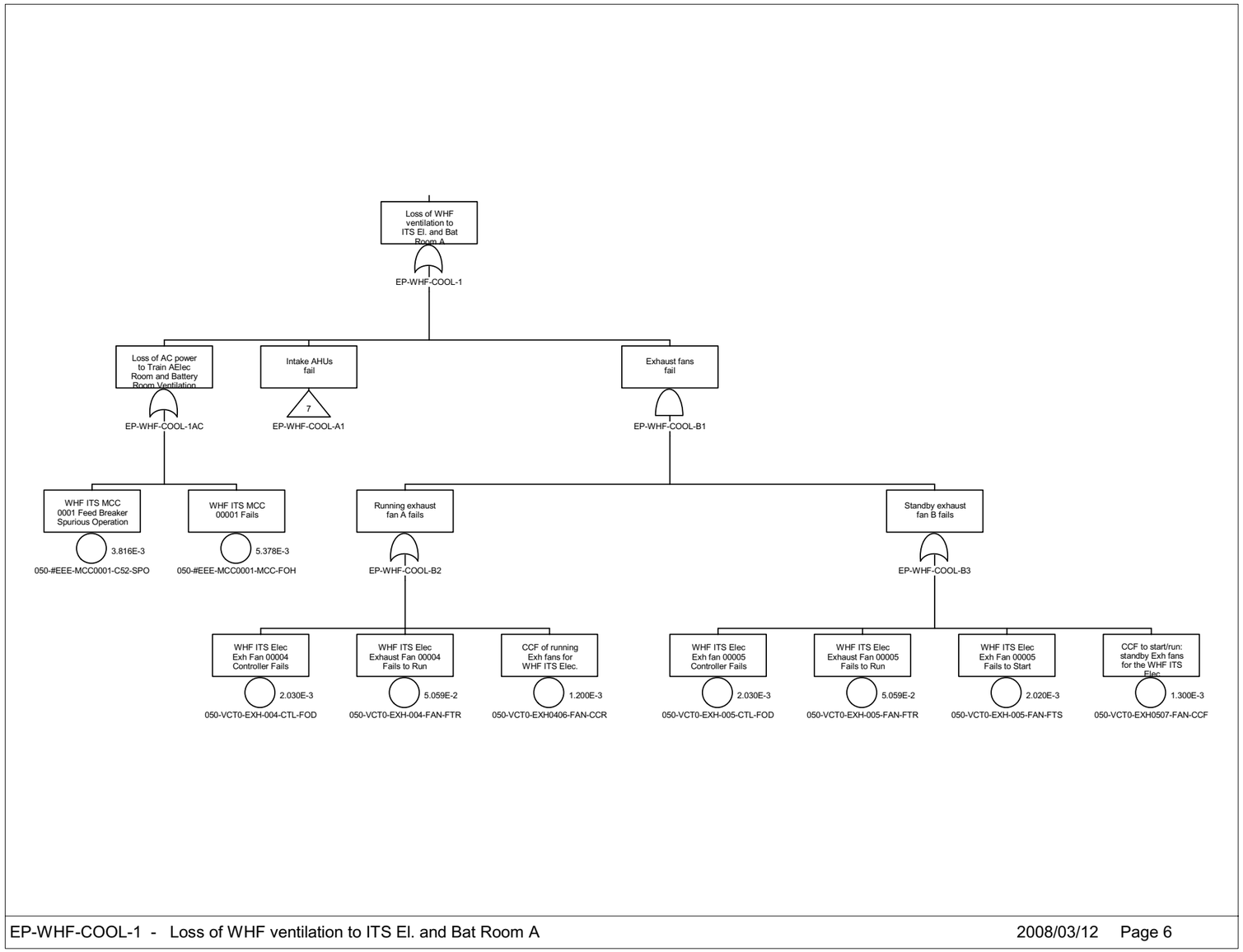
Source: Original

Figure B8.4-5. Loss of AC Power to WHF ITS Load Center Train A Sheet 1



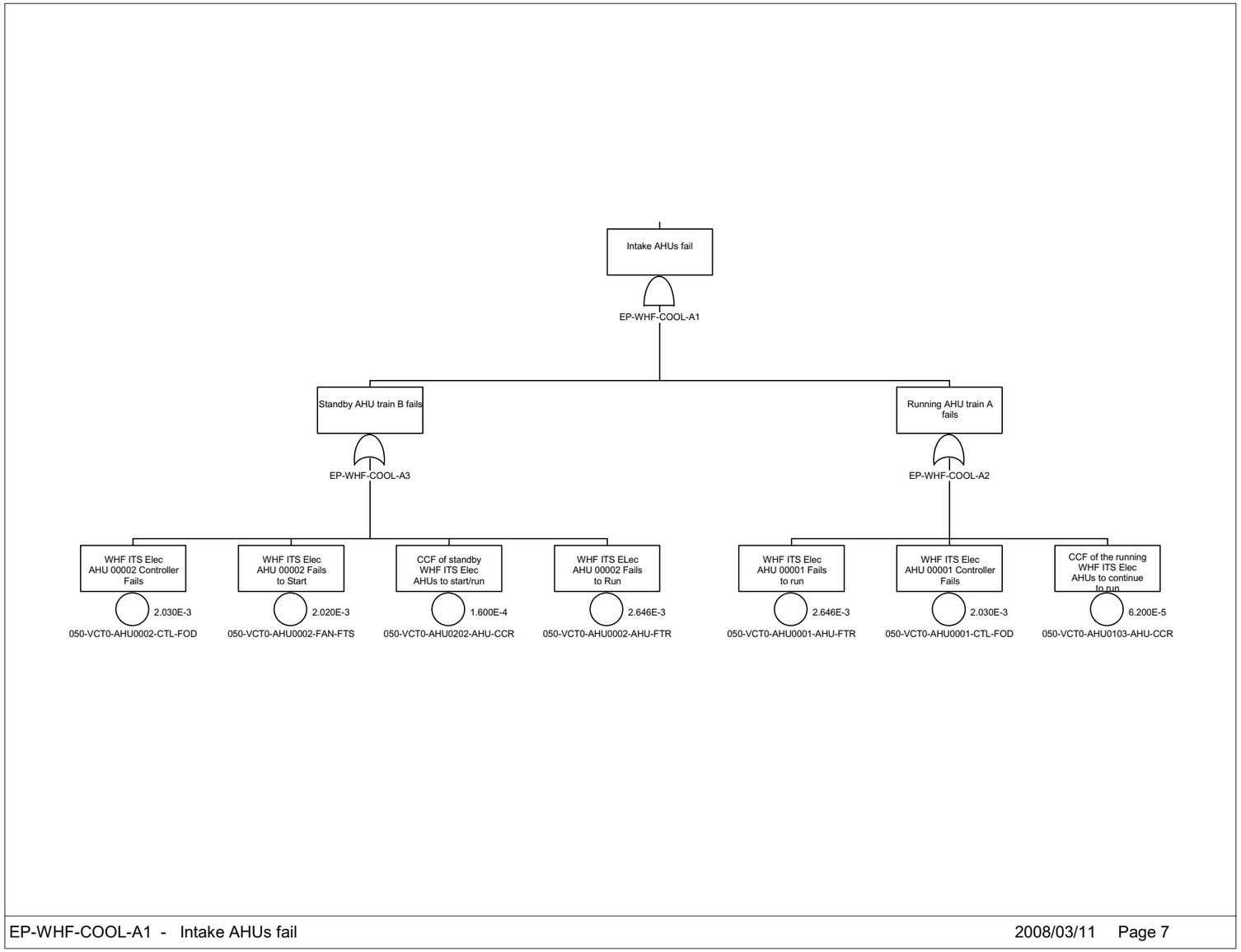
Source: Original

Figure B8.4-6. Loss of AC Power to WHF ITS Load Center Train A Sheet 2



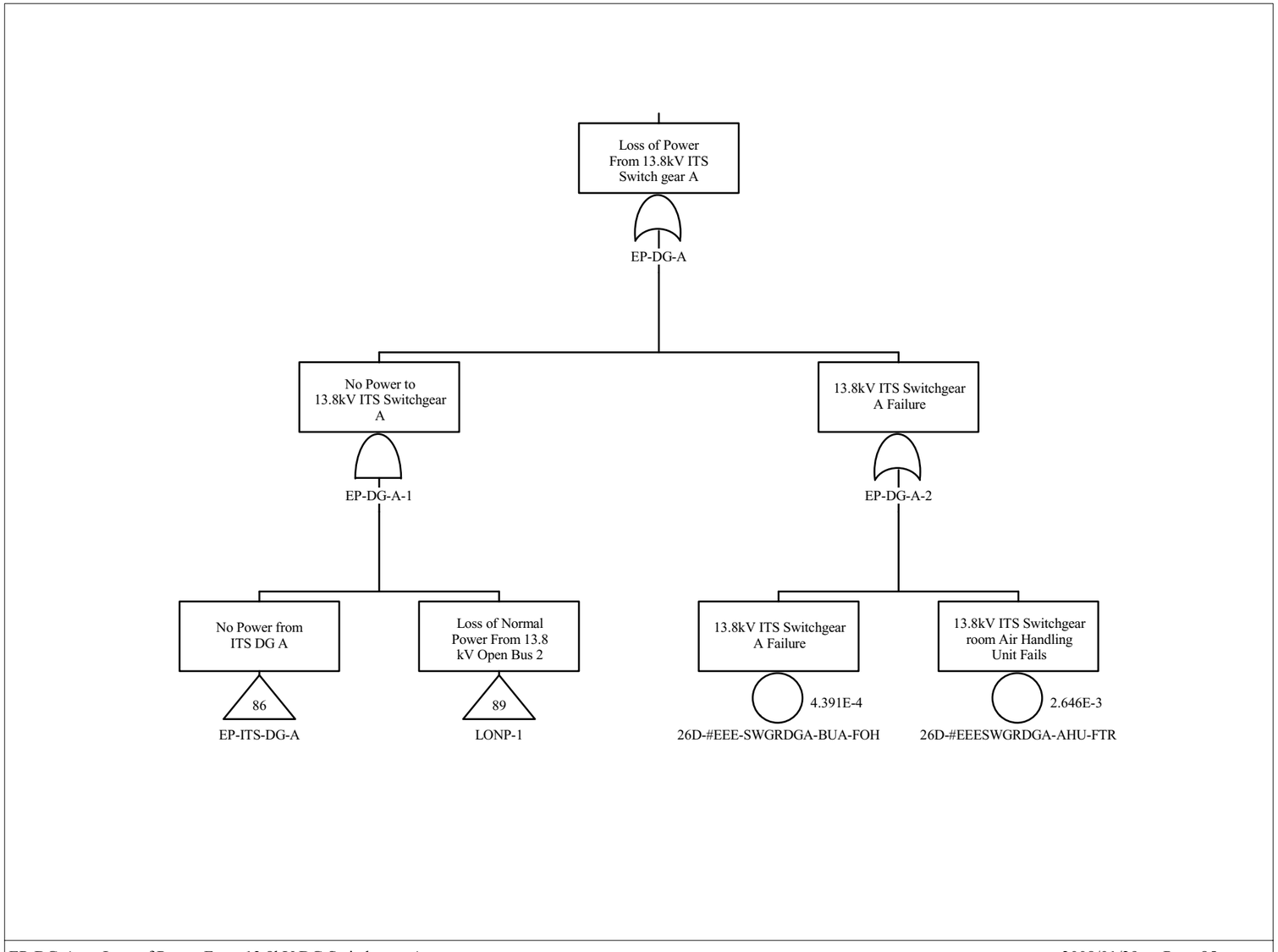
Source: Original

Figure B8.4-7. Loss of AC Power to WHF ITS Load Center Train A Sheet 3



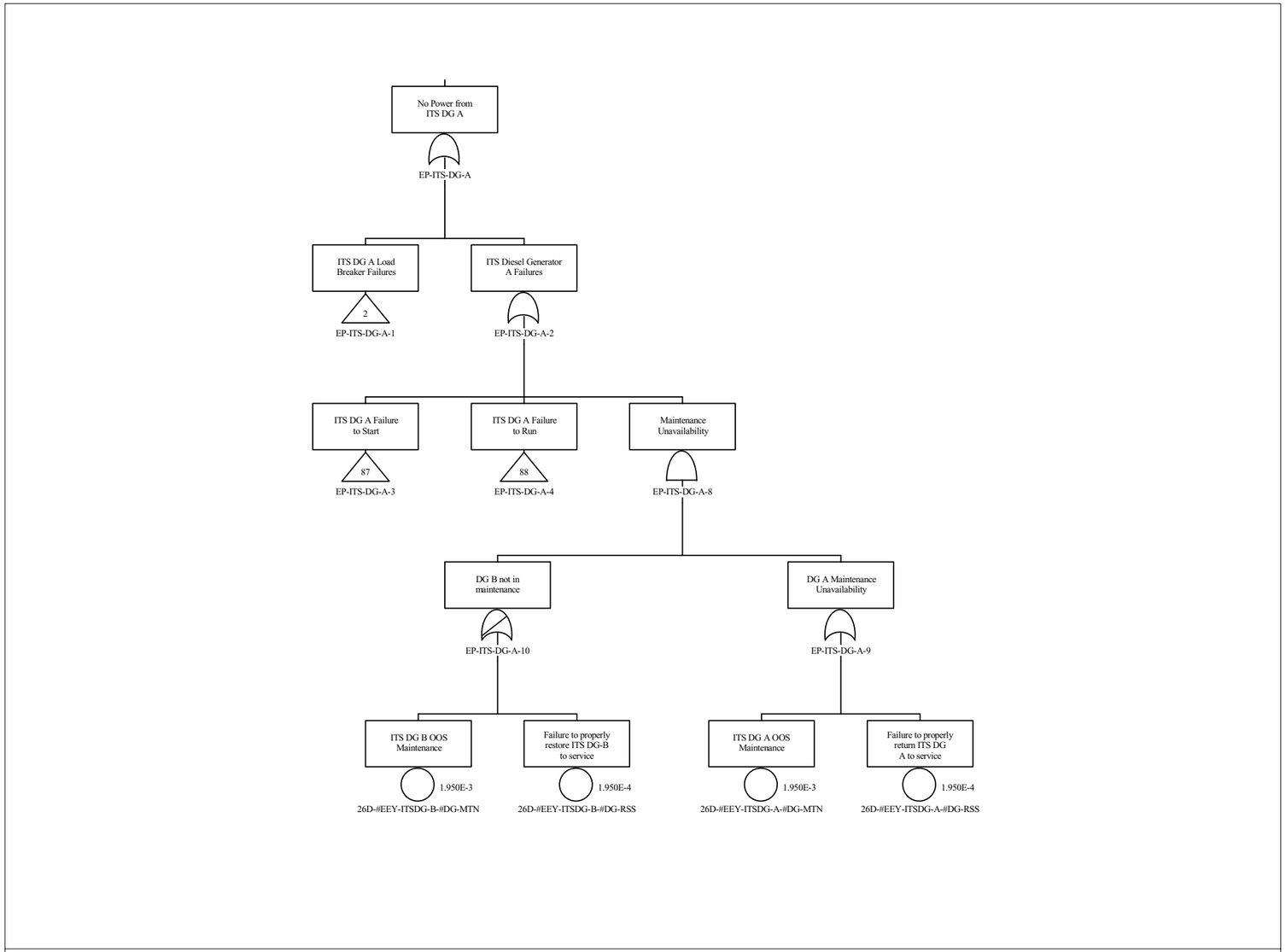
Source: Original

Figure B8.4-8. Loss of AC Power to WHF ITS Load Center Train A Sheet 4



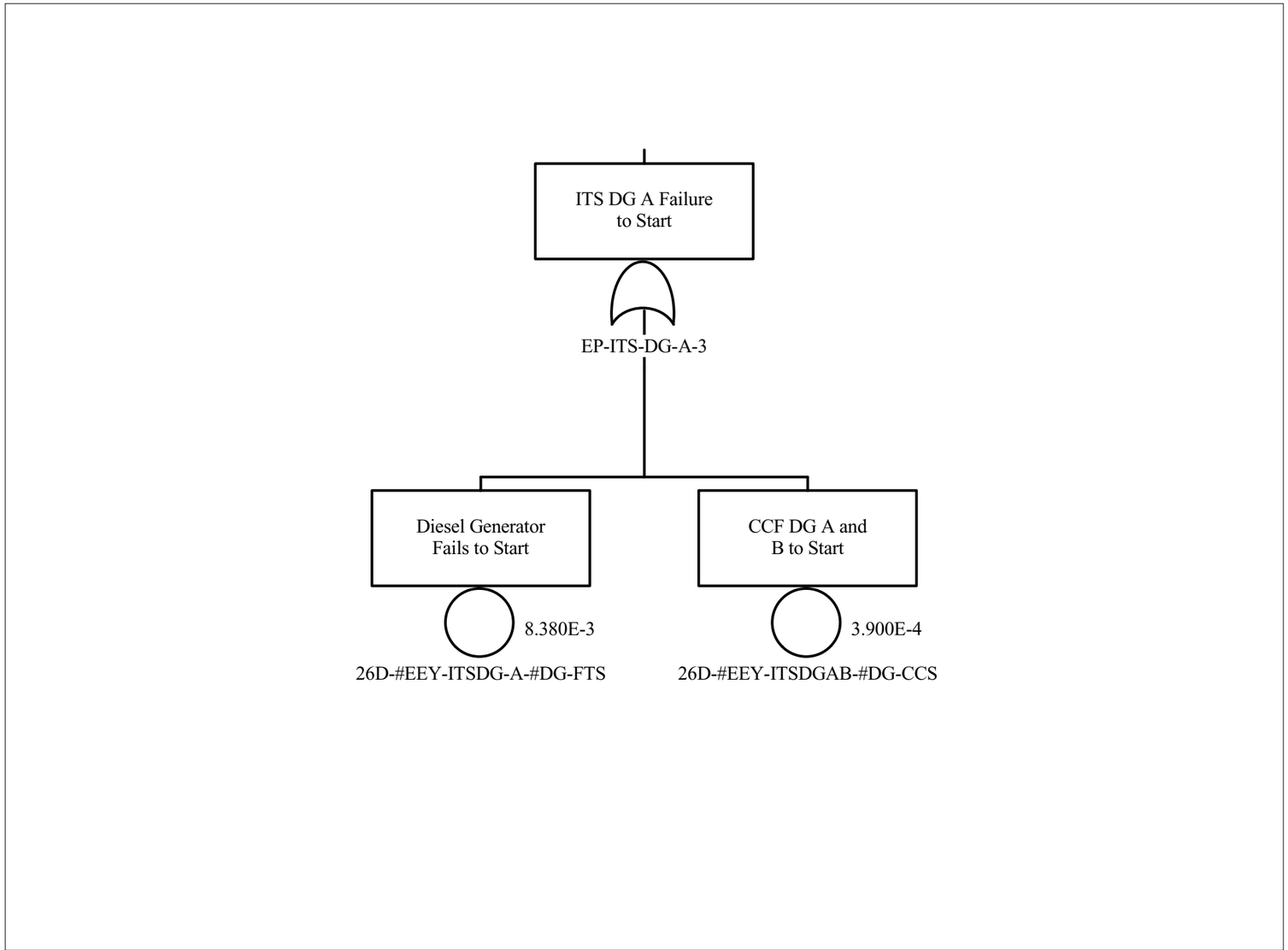
Source: Original

Figure B8.4-9. Loss of AC Power to WHF ITS Load Center Train A Sheet 5



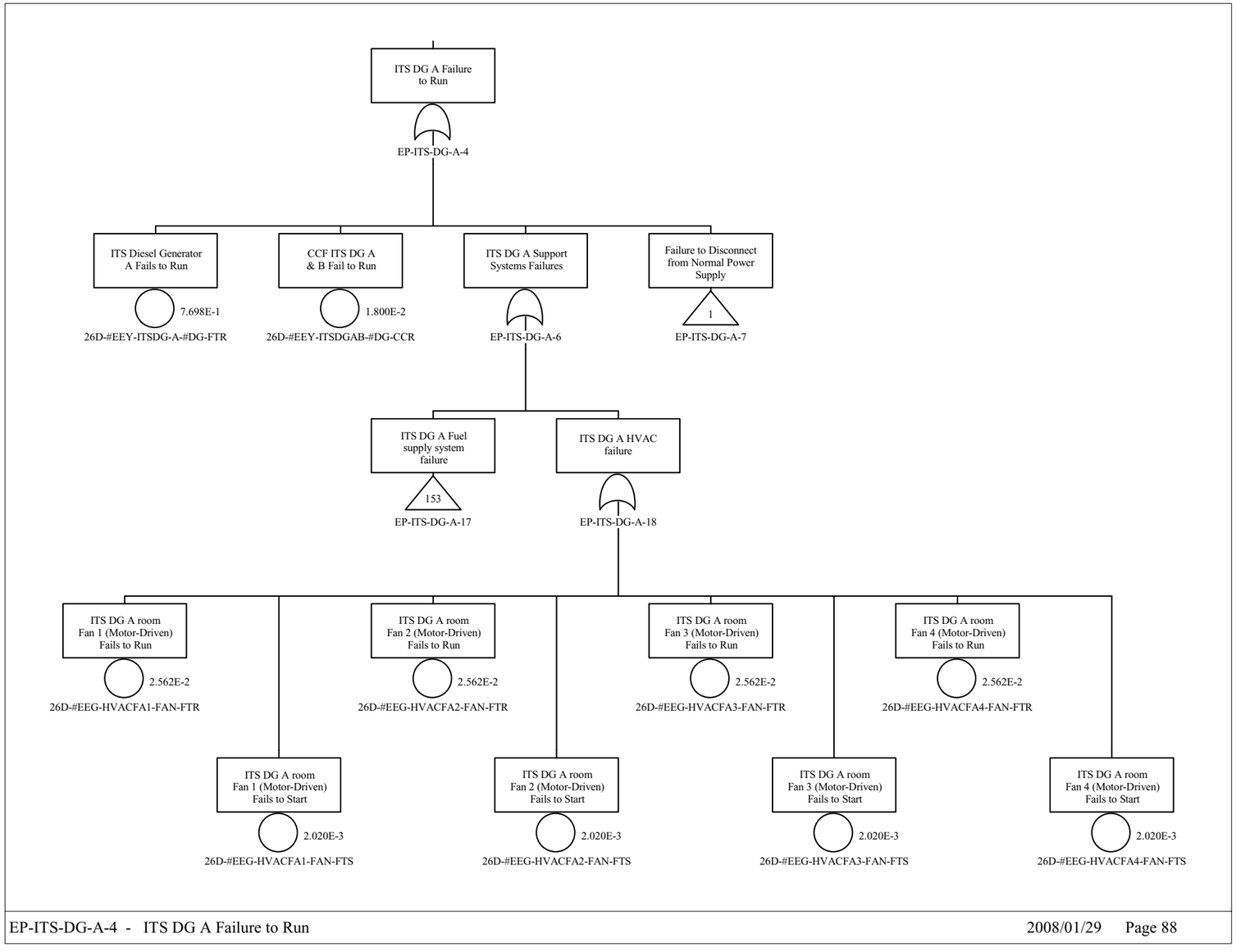
Source: Original

Figure B8.4-10. Loss of AC Power to WHF ITS Load Center Train A Sheet 6



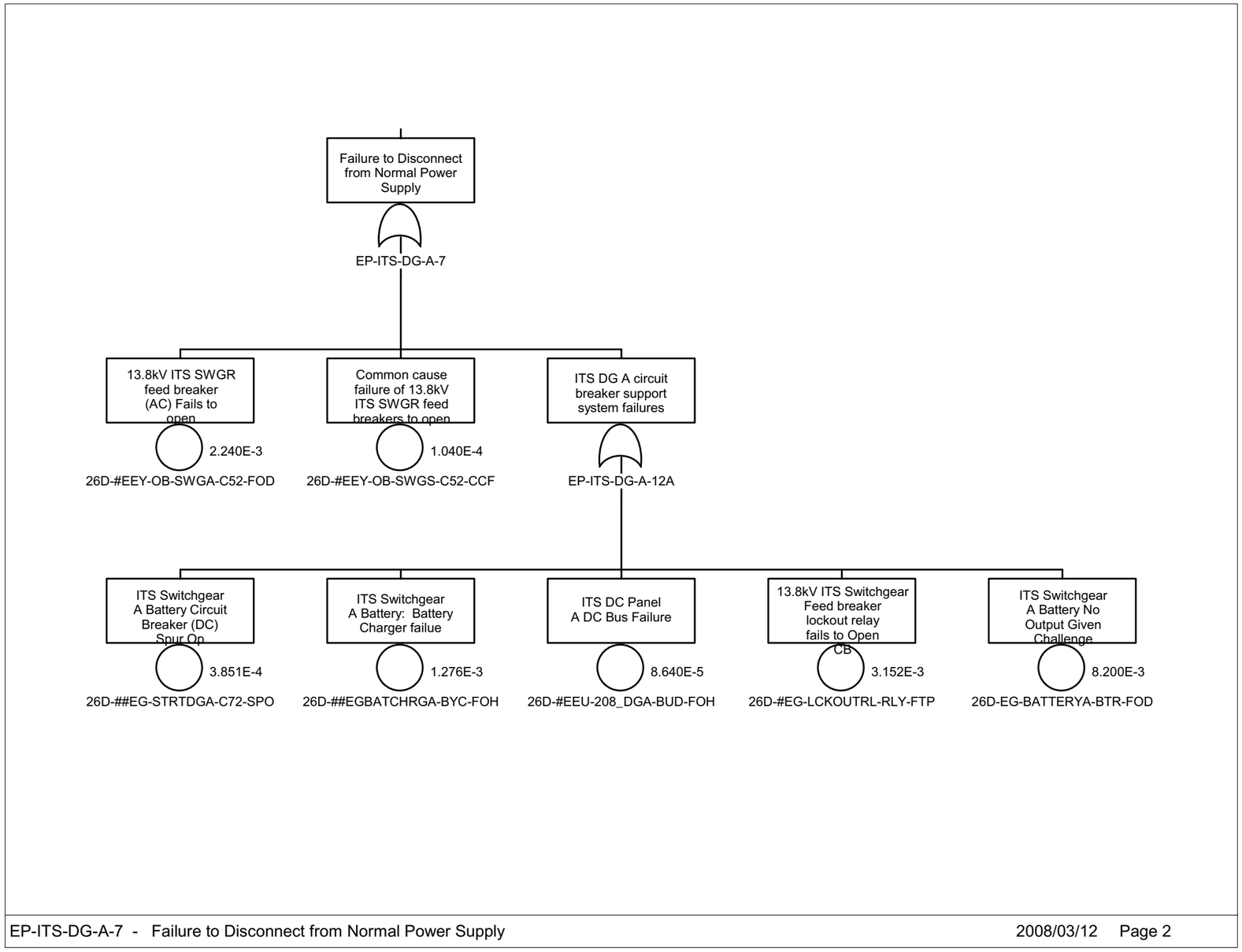
Source: Original

Figure B8.4-11. Loss of AC Power to WHF ITS Load Center Train A Sheet 7



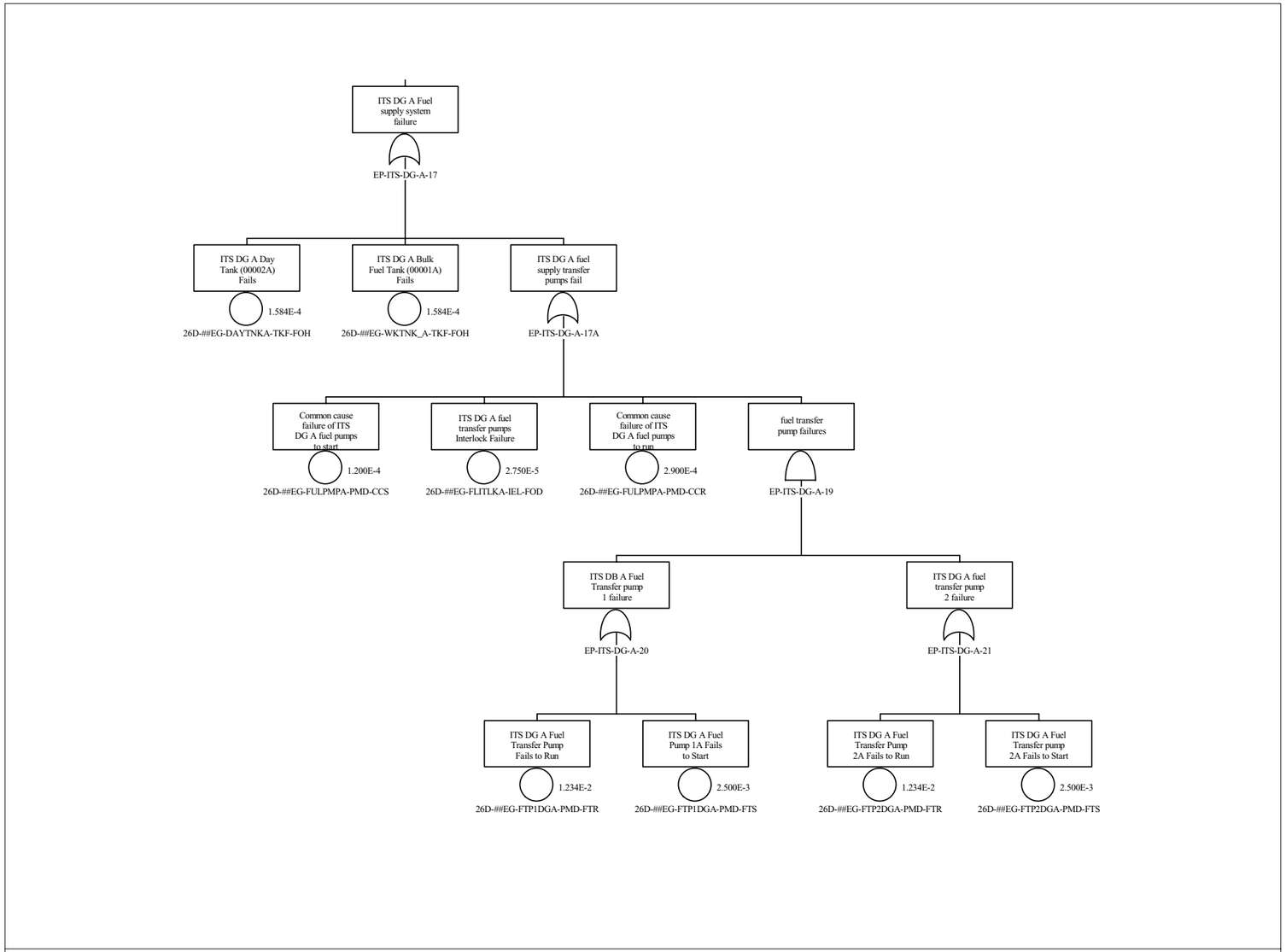
Source: Original

Figure B8.4-12. Loss of AC Power to WHF ITS Load Center Train A Sheet 8



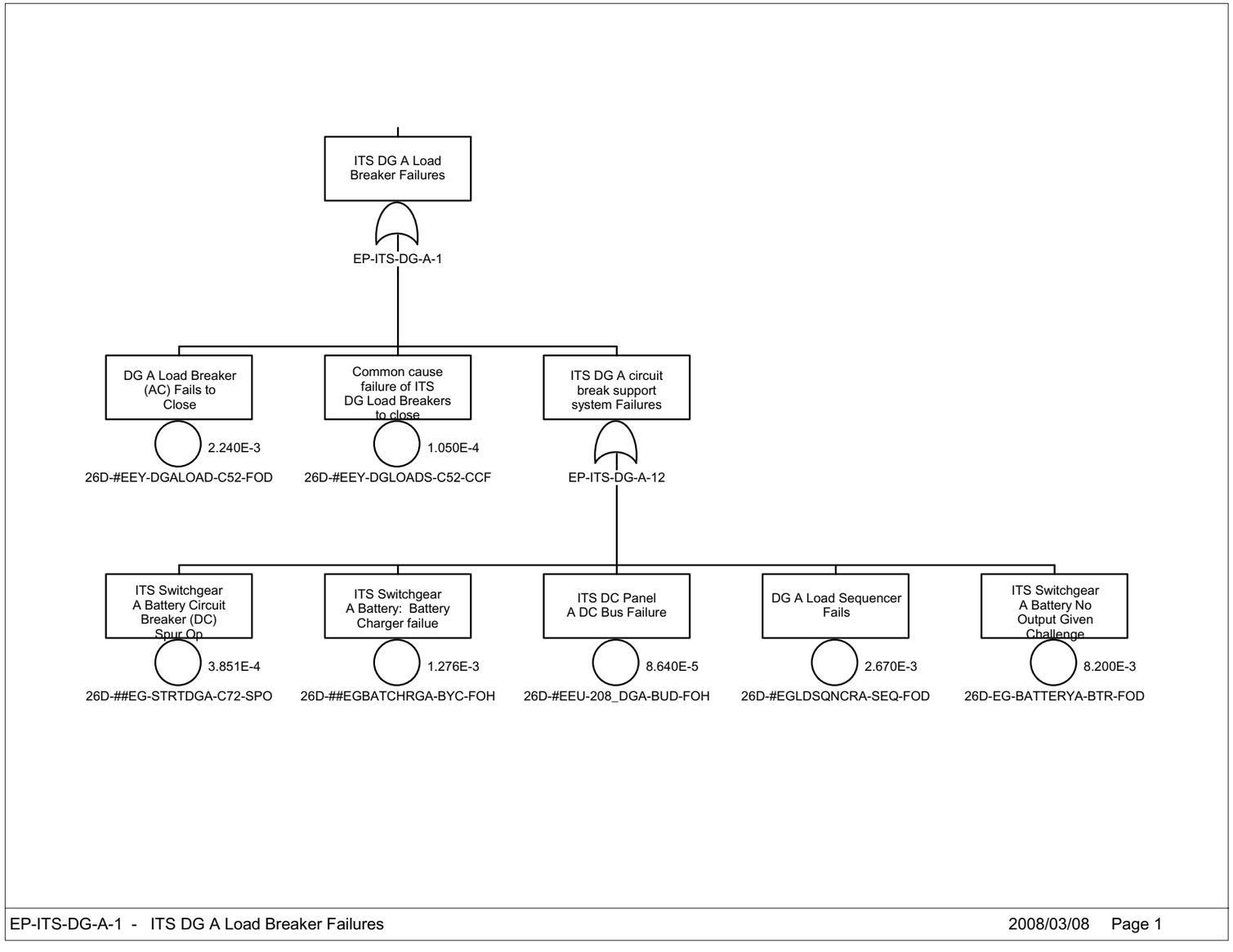
Source: Original

Figure B8.4-13. Loss of AC Power to WHF ITS Load Center Train A Sheet 9



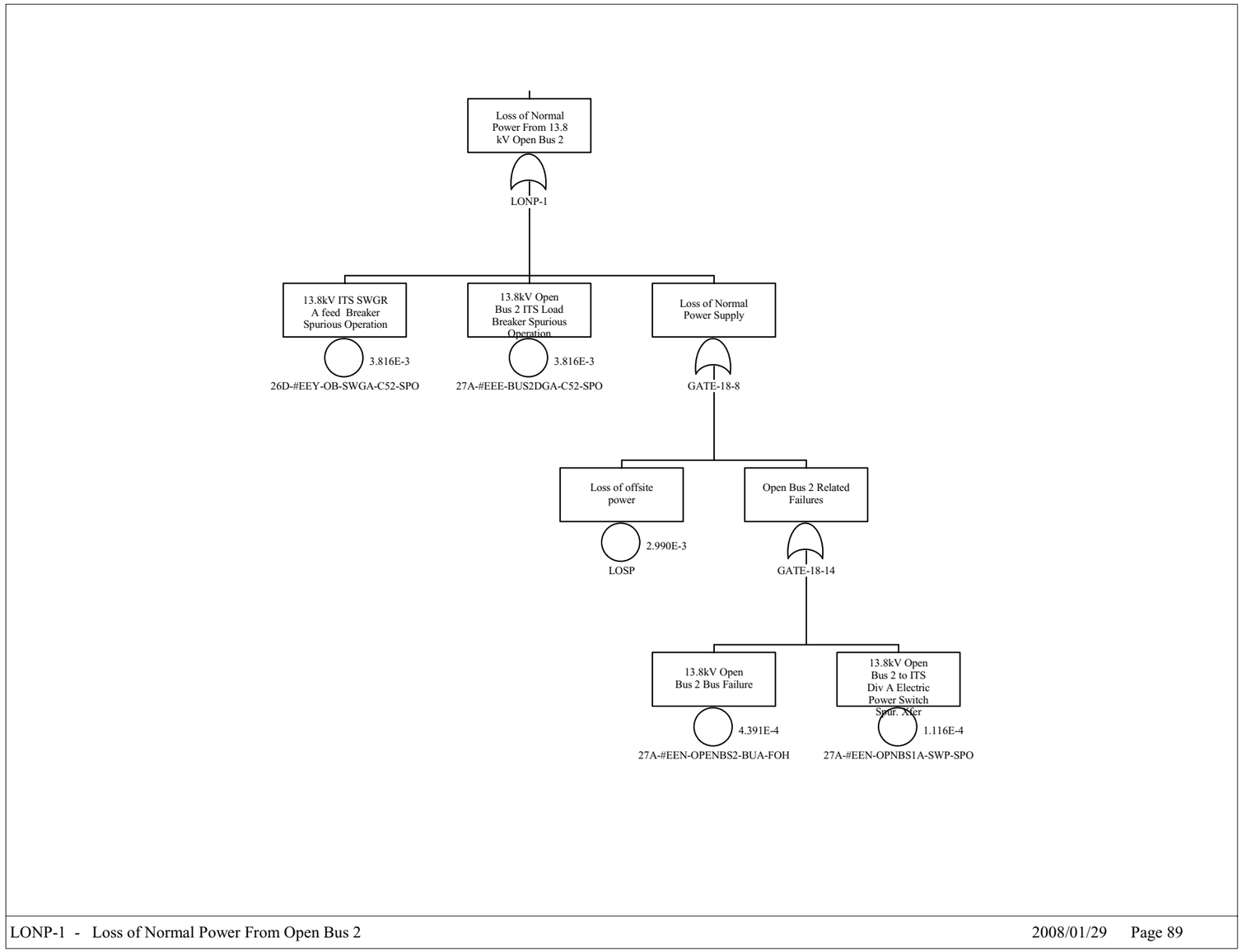
Source: Original

Figure B8.4-14. Loss of AC Power to WHF ITS Load Center Train A Sheet 10



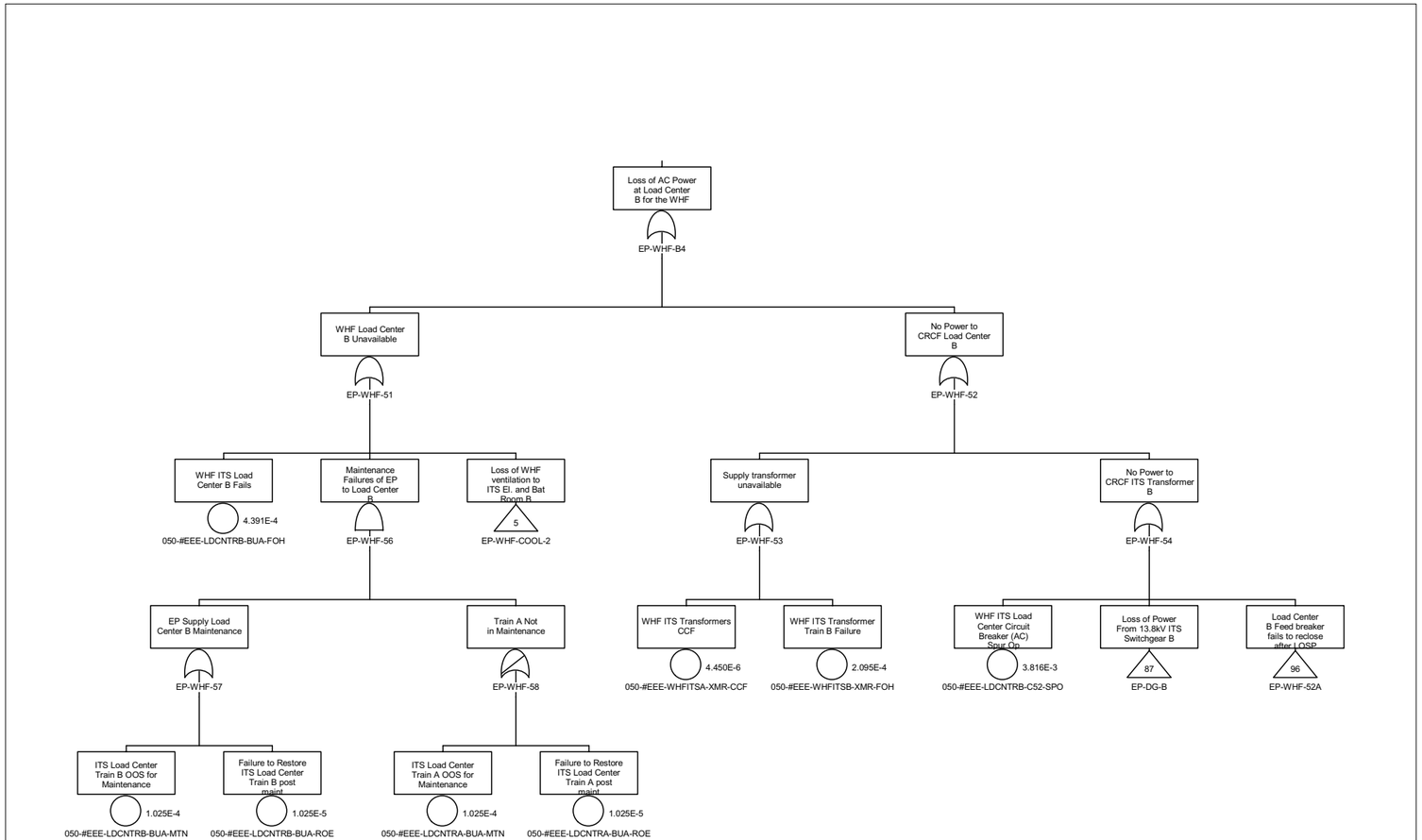
Source: Original

Figure B8.4-15. Loss of AC Power to WHF ITS Load Center Train A Sheet 11



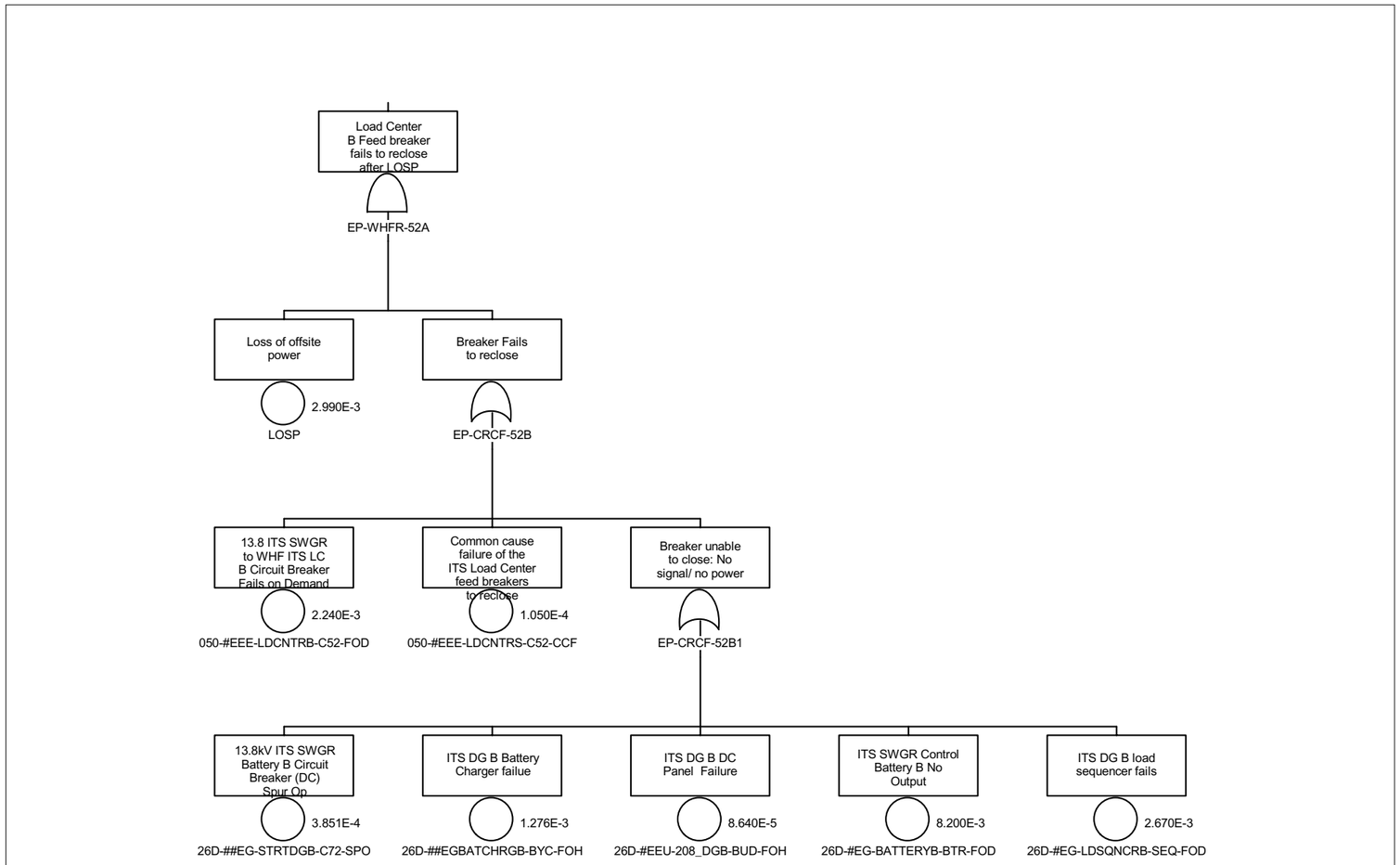
Source: Original

Figure B8.4-16. Loss of AC Power to WHF ITS Load Center Train A Sheet 12



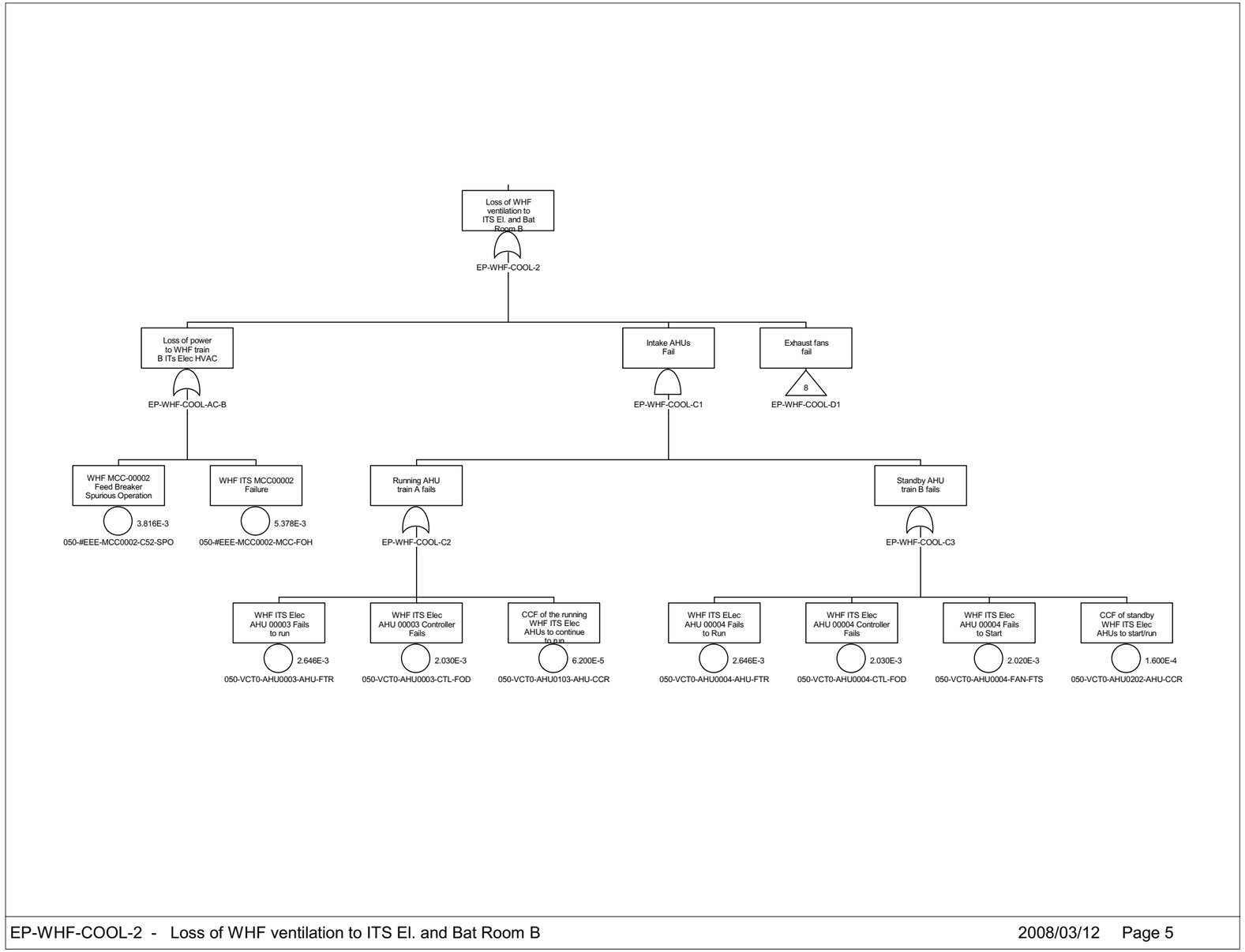
Source: Original

Figure B8.4-17. Loss of AC Power to WHF ITS Load Center Train B Sheet 1



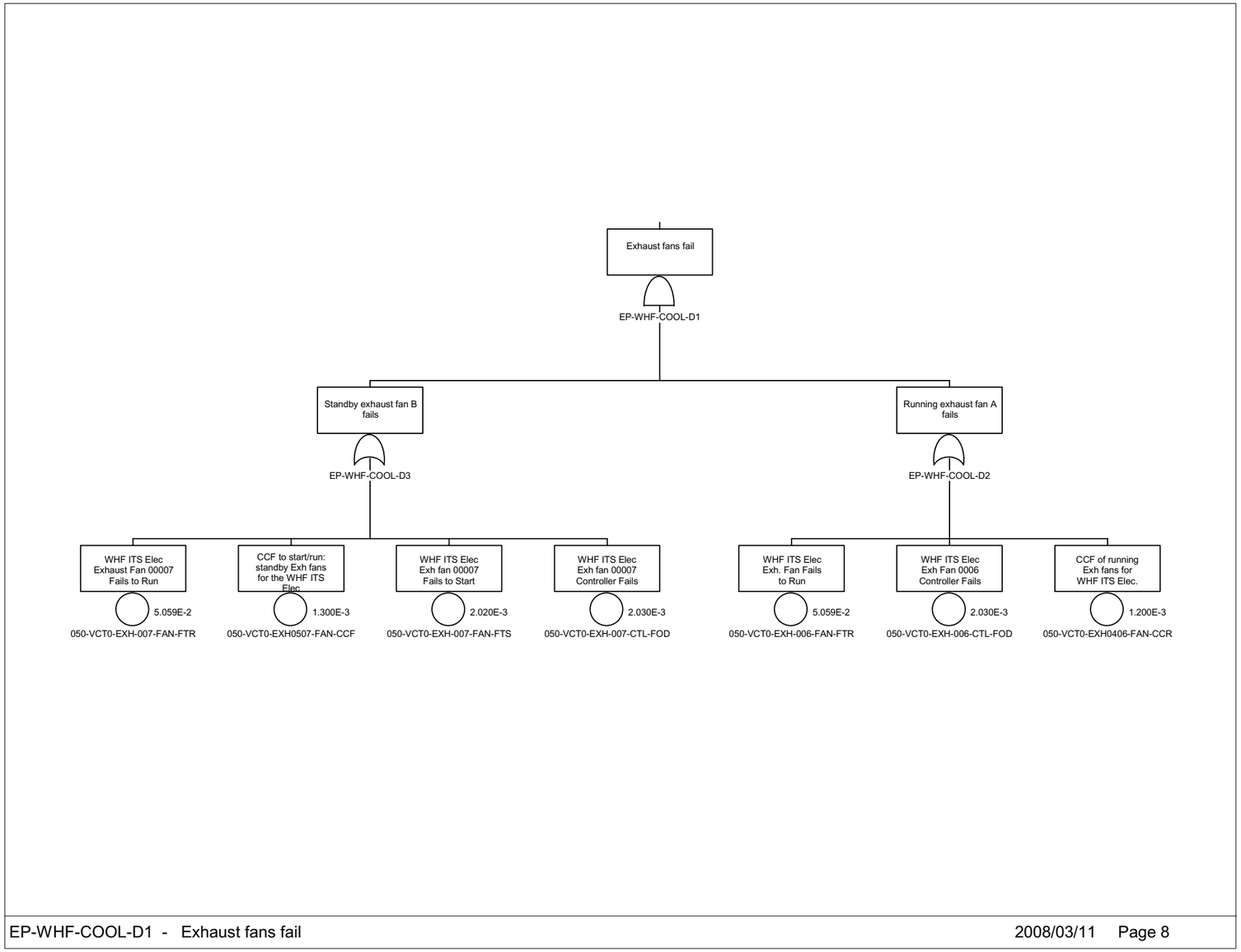
Source: Original

Figure B8.4-18. Loss of AC Power to WHF ITS Load Center Train B Sheet 2



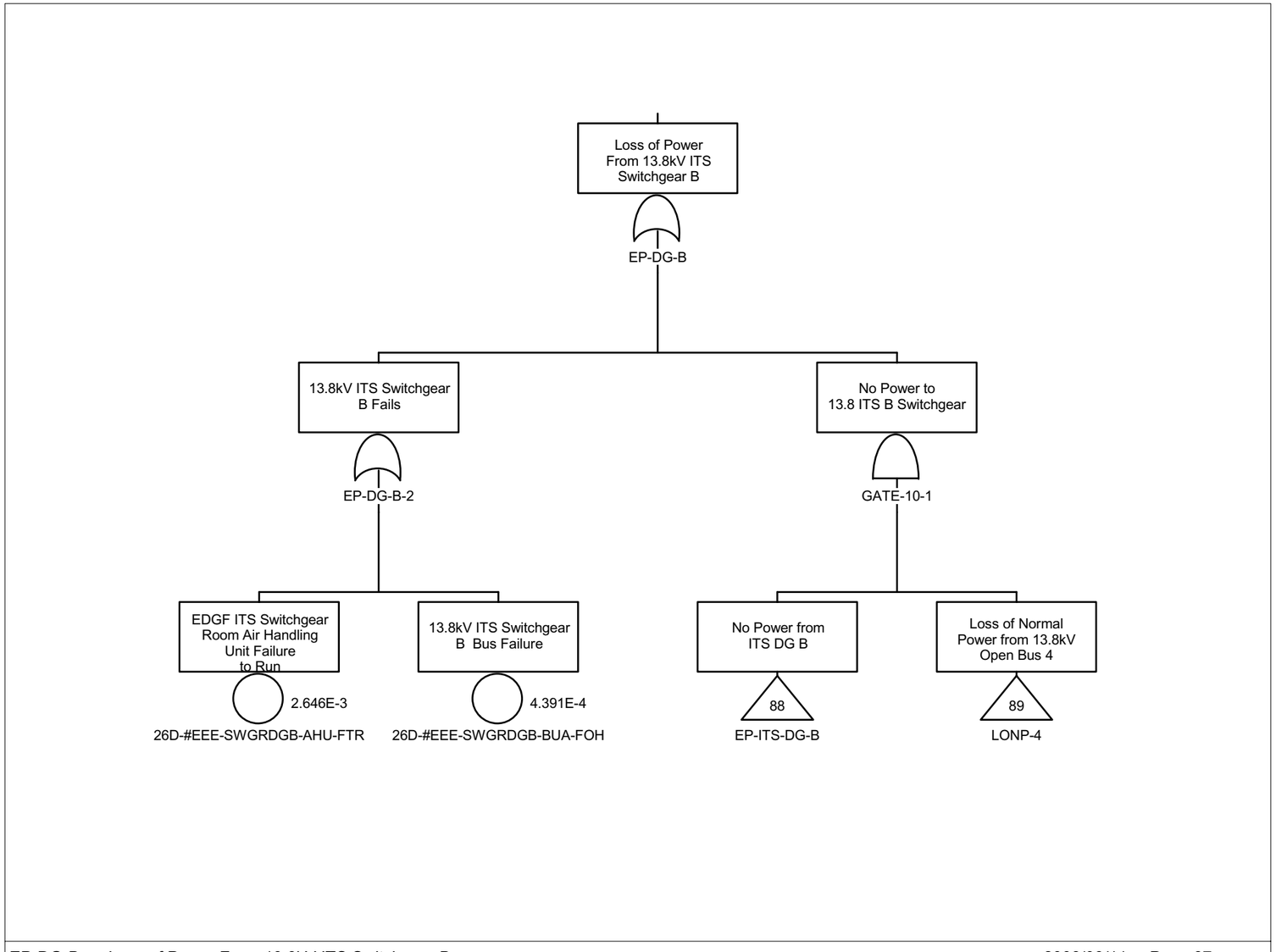
Source: Original

Figure B8.4-19. Loss of AC Power to WHF ITS Load Center Train B Sheet 3



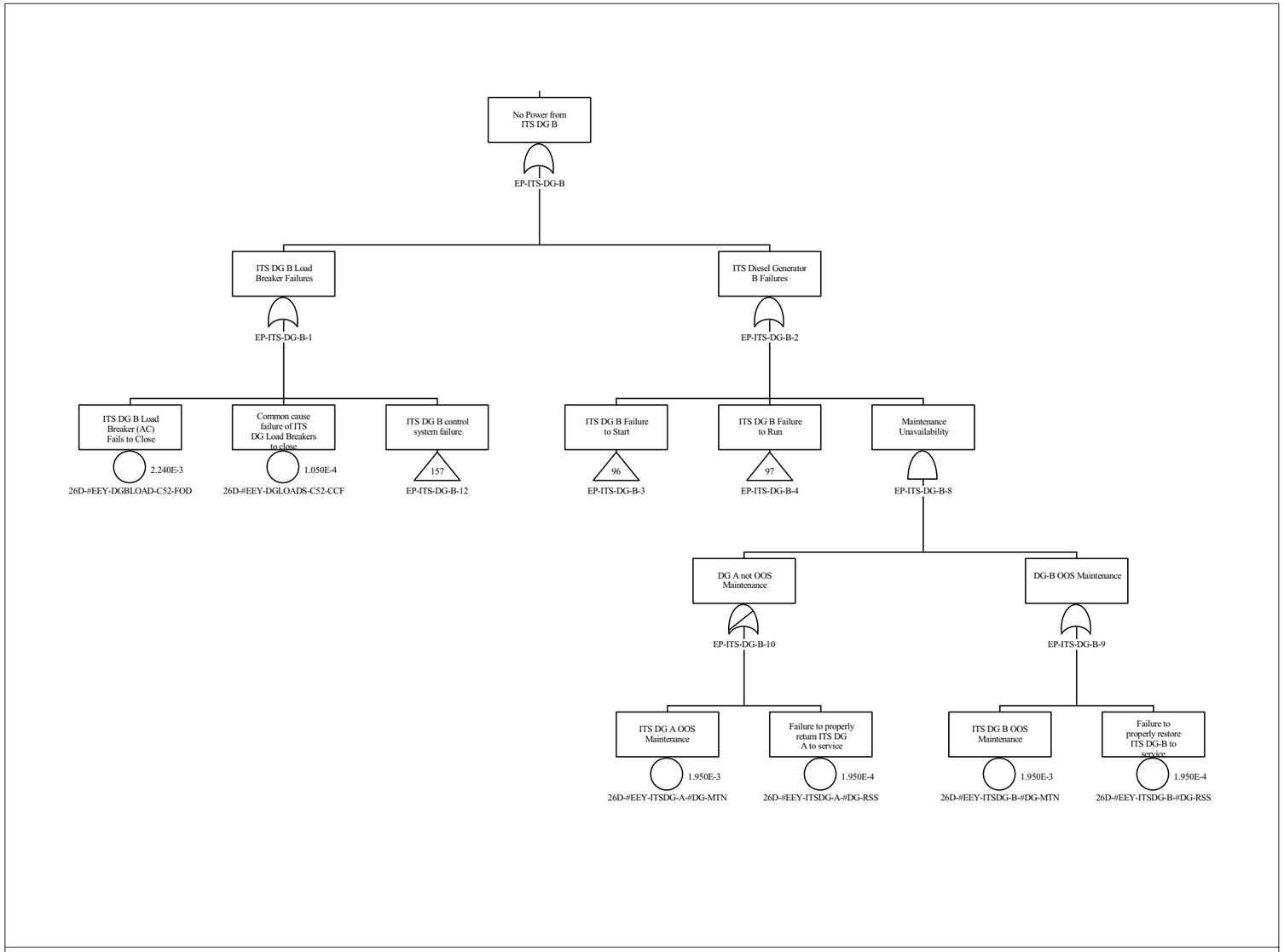
Source: Original

Figure B8.4-20. Loss of AC Power to WHF ITS Load Center Train B Sheet 4



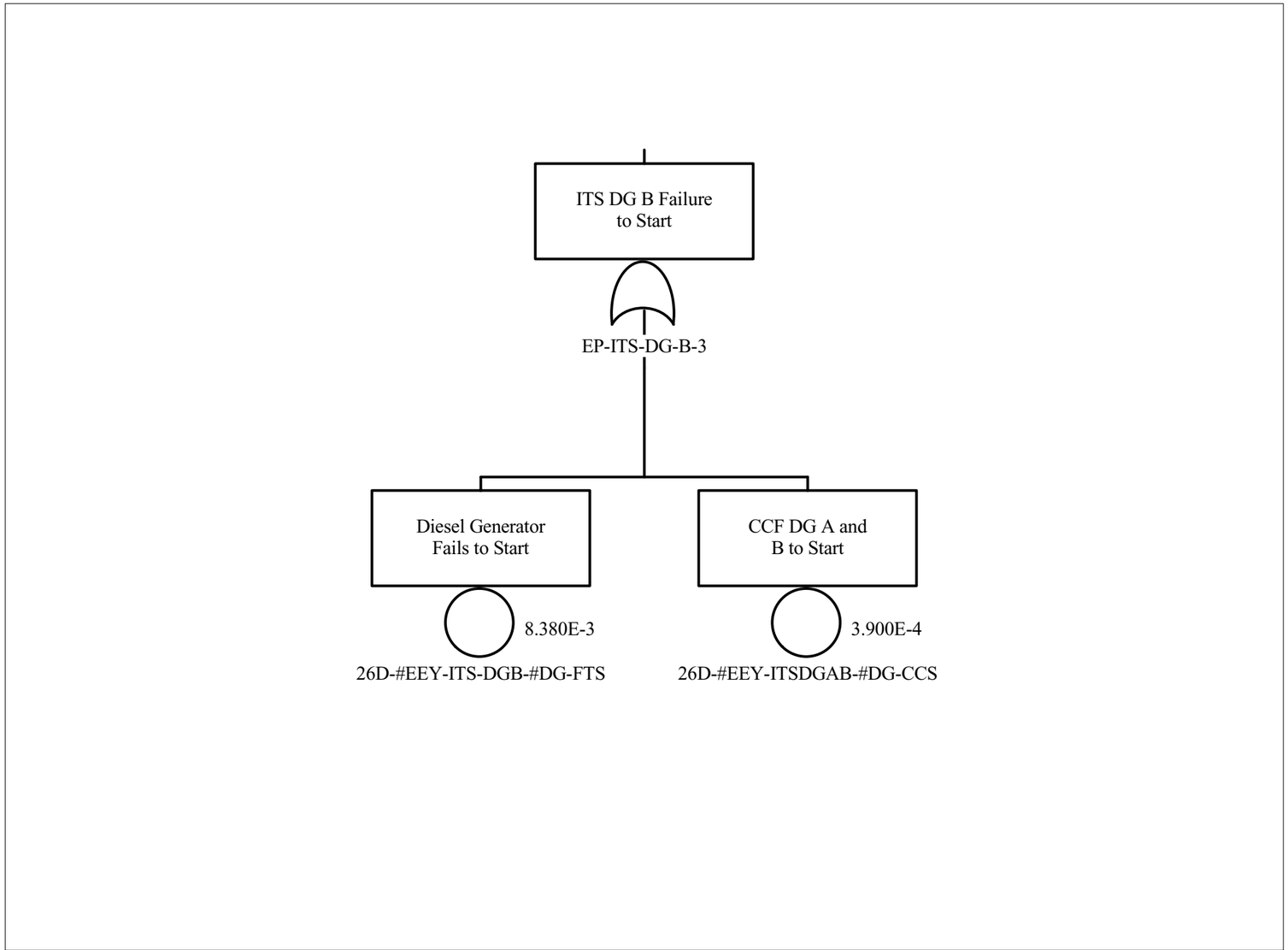
Source: Original

Figure B8.4-21. Loss of AC Power to WHF ITS Load Center Train B Sheet 5



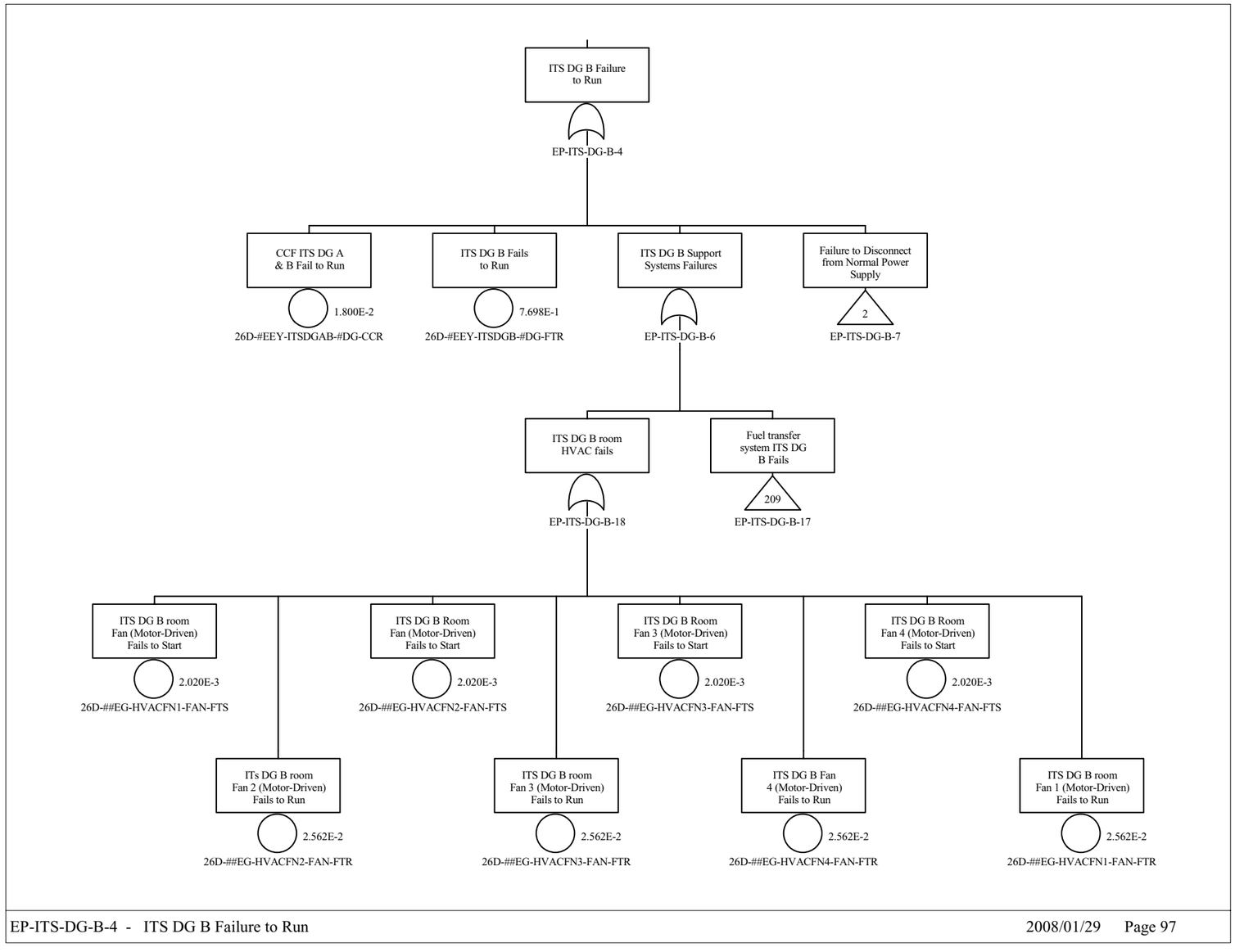
Source: Original

Figure B8.4-22. Loss of AC Power to WHF ITS Load Center Train B Sheet 6



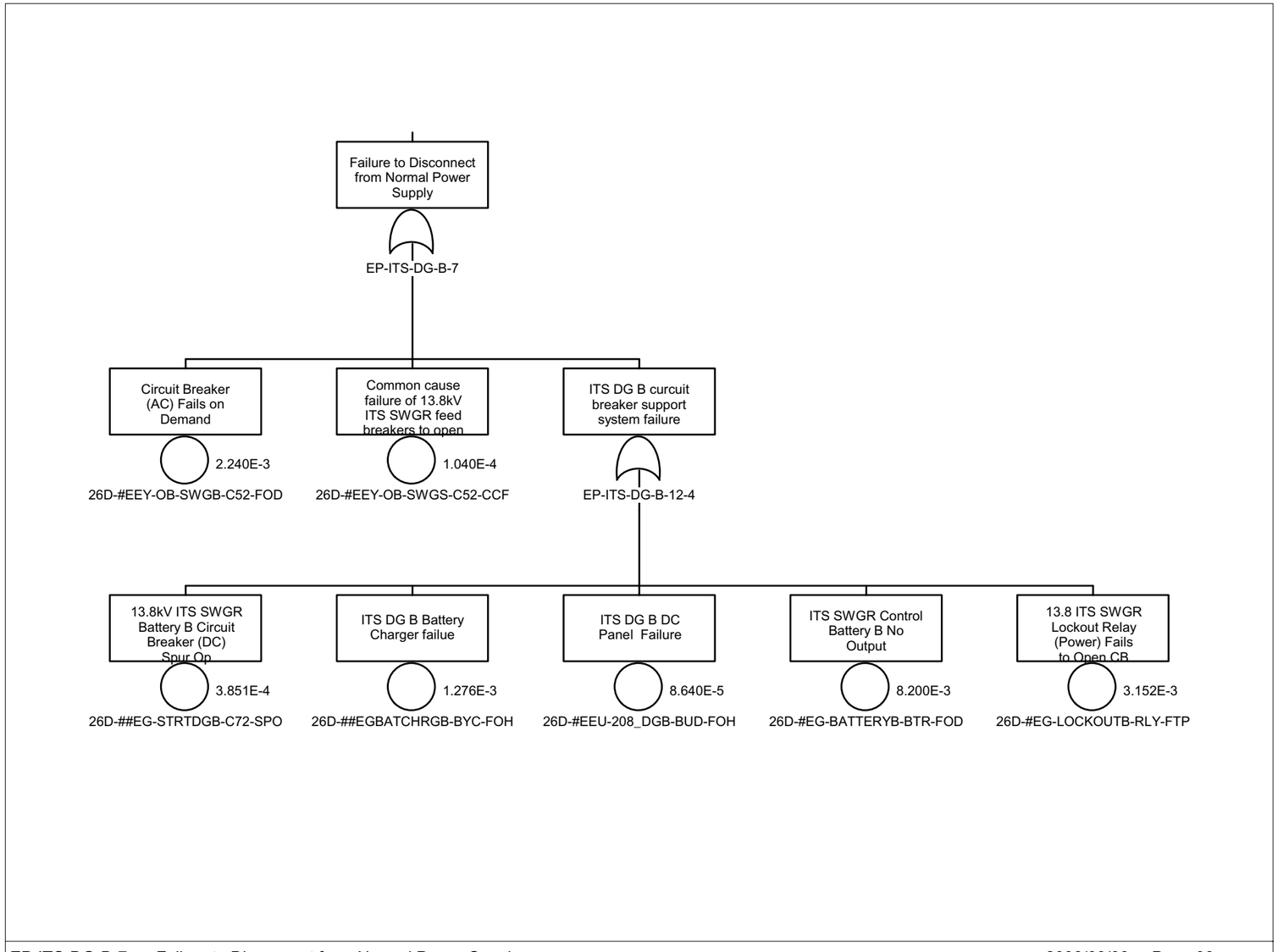
Source: Original

Figure B8.4-23. Loss of AC Power to WHF ITS Load Center Train B Sheet 7



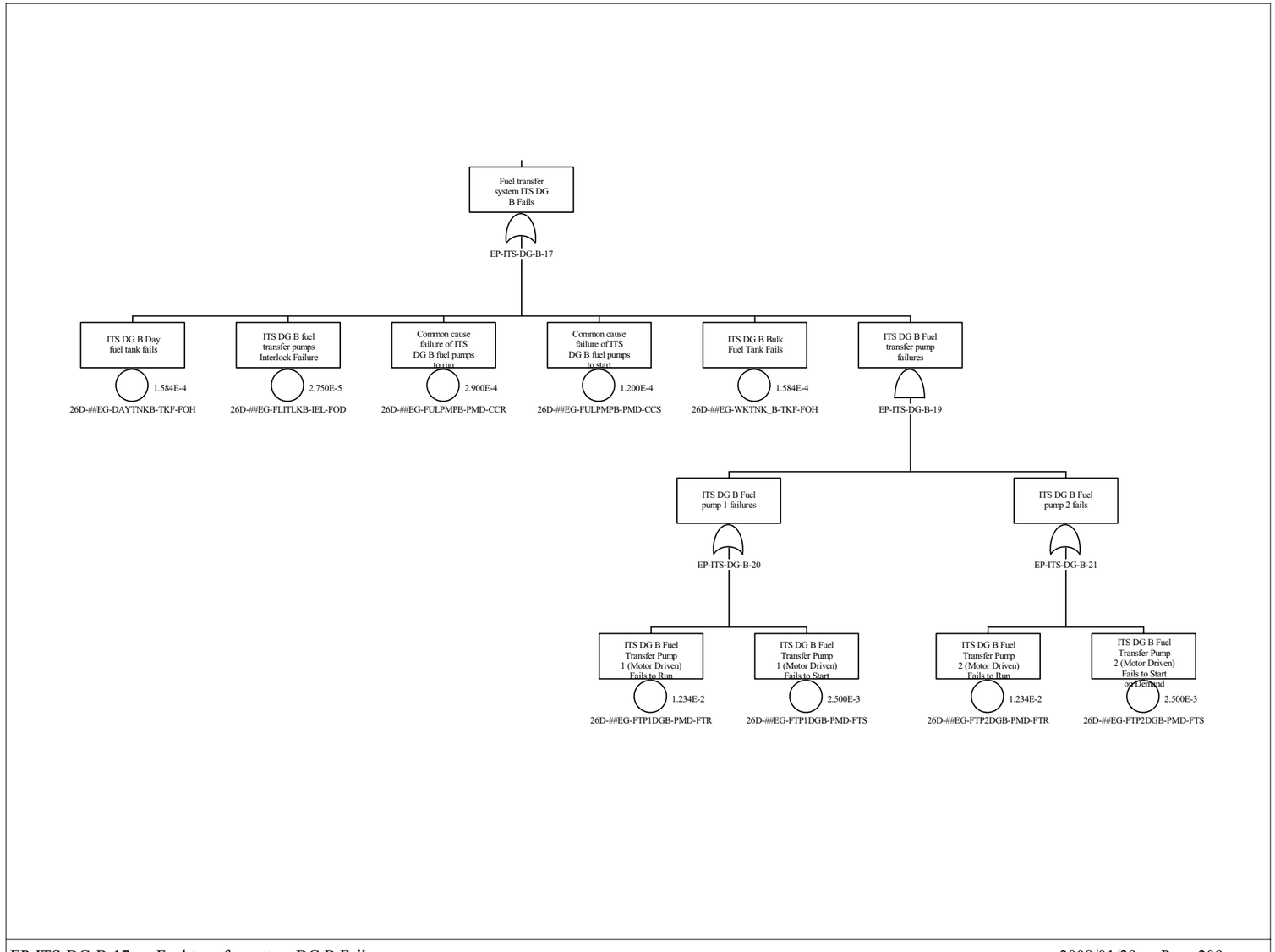
Source: Original

Figure B8.4-24. Loss of AC Power to WHF ITS Load Center Train B Sheet 8



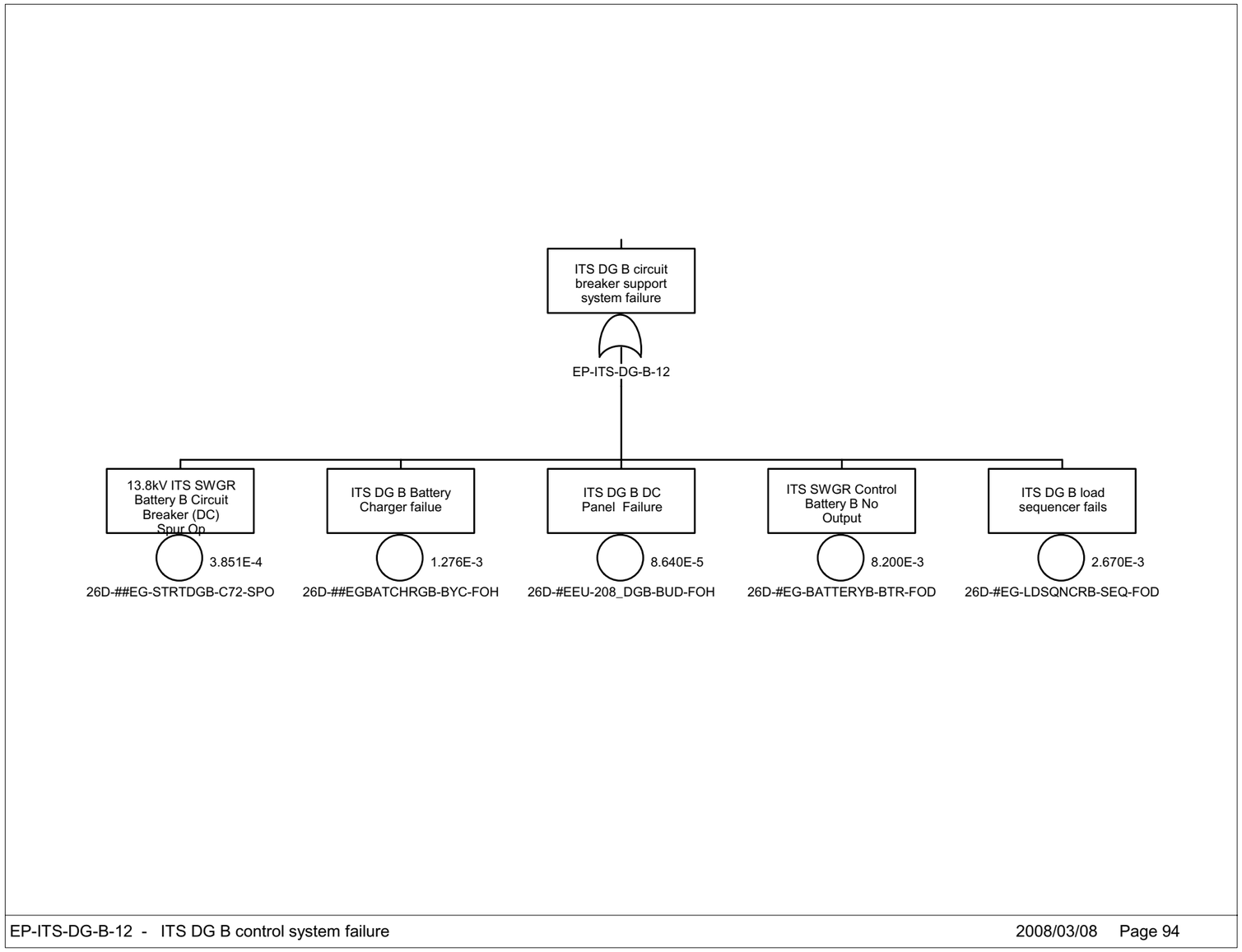
Source: Original

Figure B8.4-25. Loss of AC Power to WHF ITS Load Center Train B Sheet 9



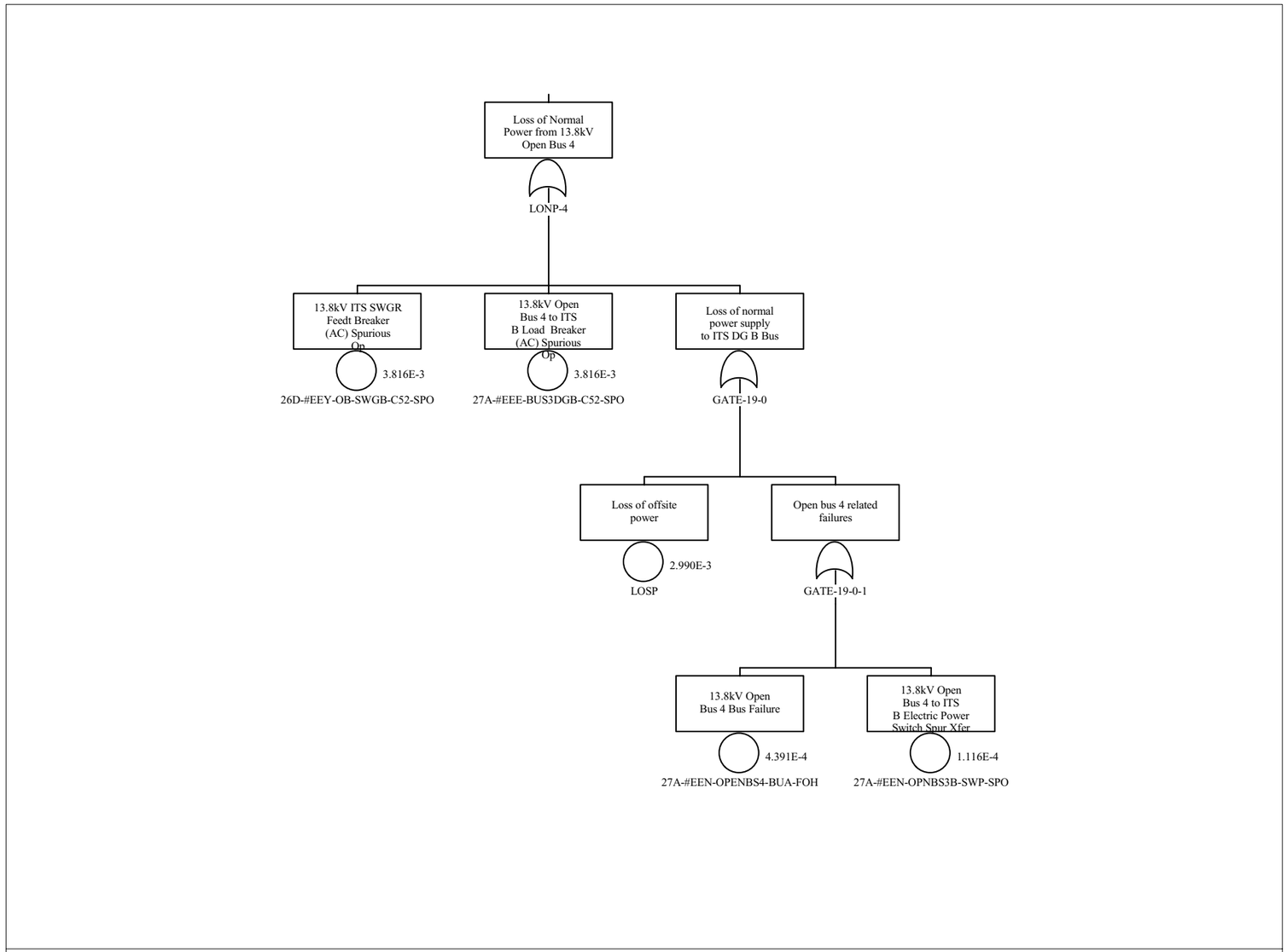
Source: Original

Figure B8.4-26. Loss of AC Power to WHF ITS Load Center Train B Sheet 10



Source: Original

Figure B8.4-27. Loss of AC Power to WHF ITS Load Center Train B Sheet 11



Source: Original

Figure B8.4-28. Loss of AC Power to WHF ITS Load Center Train B Sheet 12

B9 HORIZONTAL CASK TRACTOR AND TRAILER FAULT TREE ANALYSIS

B9.1 REFERENCES

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in the Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

Design Inputs

B9.1.1 BSC (Bechtel SAIC Company) 2007. *Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailers.* 000-3PS-HAT0-00300-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0004.

B9.1.2 BSC 2007. *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope.* 170-MJ0-HAT0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070518.0002.

B9.2 HORIZONTAL CASK TRACTOR AND TRAILER DESCRIPTION

B9.2.1 Overview

The horizontal cask tractor and trailer (HCTT) will provide the following functions as described in Section 3.1.1 of the HCTT specification (Ref. B9.1.1):

"The function of the cask tractor coupled with the cask transfer trailer is to:

- Move a transportation cask loaded with a horizontal dual-purpose canister (DPC) from the Wet Handling Facility (WHF) to a horizontal aging module (HAM) located on Aging Pad 17R.

- Retrieve a horizontal DPC from the HAM, place it into the horizontal shielded transfer cask, and transport it to the WHF."

B9.2.2 Physical Description

The tractor is a large, four-wheel drive, diesel tractor designed specifically for pulling the transfer trailer. The tractor has redundant brakes in addition to having a fail-safe emergency brake. The tractor has independently mounted non-driven hydraulic pendular axles with a minimum of four tires per axles that will ensure the cask remains level during transportation across uneven terrain. In addition to the pendular axles, the trailer has three other hydraulic

systems: (1) stabilizing jacks, (2) cask support skid and positioning system, and (3) hydraulic ram. Reference B5.1.1 depicts the tractor and trailer.

B9.3 DEPENDENCE AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with SSCs. The five areas considered are addressed in Table B9.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B9.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Hydraulic Pendular Axles	Vertical support and leveling during transport and load/unload	—	—	—	—
Hydraulic Stabilizing Jacks	Redundant vertical support during load/unload	—	—	—	—
Tractor brakes	Sufficient to stop conveyance with failed trailer brakes	—	—	—	—
Trailer brakes	Sufficient to stop conveyance on failed tractor brakes	—	—	—	—
Vehicle Steering, Control and Speed Limiter	Tractor/trailer control	—	—	Collision Overspeed	—

Source: Original

B9.4 HORIZONTAL CASK TRACTOR AND TRAILER FAILURE SCENARIOS

A HCTT collision is the only failure scenario modeled. A rollover scenario was also considered, but is screened out per Attachment E.

B9.4.1 Horizontal Cask Tractor and Trailer Collision (ESD04)

B9.4.1.1. Description

There are two situations modeled where a HCTT collision may occur and each has a unique vehicle configuration: (1) during the loading and unloading of the DPCs (the trailer is unhitched from the tractor), and (2) during transport between the facilities and HAMs when the tractor is pulling the trailer.

B9.4.1.2 Success Criteria

A collision is defined as any undesired contact with another vehicle, facility structure, or equipment. Any of the steering, braking and hydraulic system can cause this to occur, in addition to operator error.

B9.4.1.3 Design Features and Requirements

The tractor brakes are a redundant–brake design and include a backup system with a split master cylinder and an indicator light inside the cabin to warn an operator if one of the systems fails (Ref. B9.1.1, Section 3.9.1.8.b).

- The parking brakes are fail safe – The parking brake are designed as spring-applied, with hydraulically released calipers mounted on each axle input (Ref. B9.1.1, Section 3.9.1.9.b).

- The tractor and trailer brakes are redundant–either are capable of stopping the conveyance.

- The stabilizing jacks and pendular axles are redundant vertical support systems during loading and unloading operations.

- The trailer has four pendular axles and eight axle hydraulic actuators. The pendular axle hydraulic system can sustain one actuator failure and still function properly.

- There are four stabilizing jacks, failure of any one stabilizing jack results in the failure of the stabilizing jack system.

B9.4.1.4 Fault Tree Model

The top event in this fault tree is “Horizontal Tractor Trailer Collision”. This is defined as an undesired contact at any speed between the cask tractor and/or cask transfer trailer with another vehicle, facility structure, or equipment. Faults modeled in this tree include axle and stabilizing jack hydraulic failures as well as vehicle control failures.

B9.4.1.5 Basic Event Data

A number of basic events are used in this fault tree, including three common cause failure events and two human failure event as listed in Table B9.4-1.

Table B9.4-1. Basic Event Probabilities for Collision of Horizontal Cask Tractor and Trailer

Name	Description	Calc. Type	Calc Prob.	Fail. Prob.	Lambda	Miss. Time
050-CRWT-BRK001--BRK-FOD	Tractor brake A fails	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00
050-CRWT-BRK002--BRK-FOD	Tractor brake B fails	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00
050-CRWT-BRK003--BRK-FOD	Trailer brakes fail	1	1.46E-06	1.46E-06	0.00E+00	0.00E+00
050-CRWT-BRKCCF--BRK-FOD	CCF of both tractor brakes	3	6.86E-08	0.00E+00	6.86E-08	1.00E+00
050-CRWT-LPATH--ATH--CCF	CCF of pendular hydraulics during load/unload	3	9.80E-06	0.00E+00	9.80E-06	0.00E+00
050-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LSJATH1-ATH-FOH	Stabilizing jack 1 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LSJATH2-ATH-FOH	Stabilizing jack 2 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LSJATH3-ATH-FOH	Stabilizing jack 3 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-LSJATH4-ATH-FOH	Stabilizing jack 4 failure	3	1.78E-03	0.00E+00	8.91E-04	2.00E+00
050-CRWT-TRCT-STEER-FAIL	Tractor steering system failure	3	1.84E-05	0.00E+00	1.84E-05	1.00E+00
050-CRWT-TRLR-STEER-FAIL	Trailer steering system failure	3	1.84E-05	0.00E+00	1.84E-05	1.00E+00
050-HTTCOLLIDE---G65-FOH	Speed limiter fails	3	1.16E-05	0.00E+00	1.16E-05	1.00E+00
050-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HTT while leaving the WHF	1	3.00E-03	3.00E-03	0.00E+00	0.00E+00
050-OPHTINTCOL01-HFI-NOD	Operator causes collision of HTT due to over speed	1	1.00E-00	1.00E-00	0.00E+00	0.00E+00

NOTE: Calc. = calculation; CCF = common-cause failure; Fail. = failure; HTT = HTT = the cask tractor and cask transfer trailerreferred to as the HCTT in Section 6.2; Miss. = mission; Prob. = probability; RF = Receipt facility.

Source: Original

B9.4.1.5.1 Human Failure Events

Two HFEs are modeled in the HCTT collision failure scenario as follows:

1. Operator causes collision of HCTT while leaving the WHF.
2. Operator causes collision of HCTT due to overspeed condition.

Further description of these events can be found in Attachment E, Human Reliability Analysis.

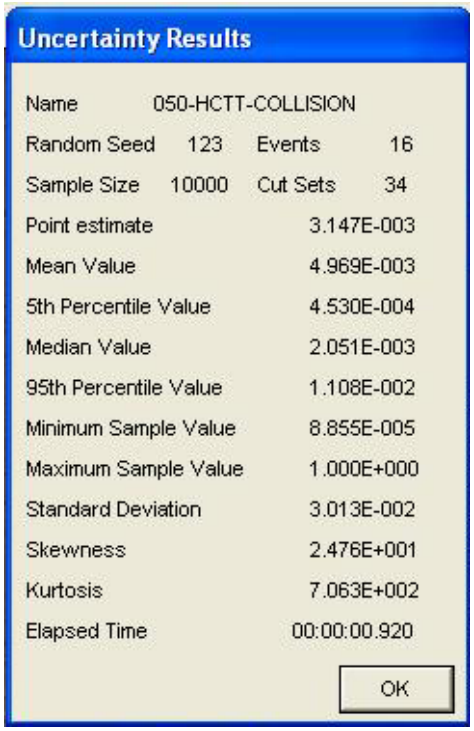
B9.4.1.5.2 Common-Cause Failures

Two CCF events are modeled in the HCTT collision failure scenario as follows:

1. Common-cause failure of the primary and redundant tractor brakes.
2. Common-cause failure of two or more pendular axle hydraulics.

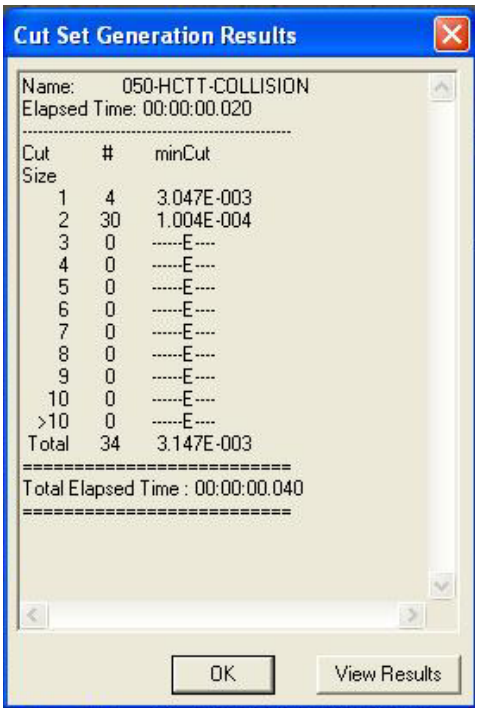
B9.4.1.6 Uncertainty and Cut Set Generation Results

Figure B9.4-1 contains the uncertainty results obtained from running the fault trees for "Horizontal Cask Tractor Trailer Collision". Figure B9.4-2 provides the cut set generation results for the "Horizontal Cask Tractor Trailer Collision" fault tree.



Source: Original

Figure B9.4-1. Uncertainty Results for the Horizontal Cask Tractor Trailer Collision Fault Tree



Source: Original

Figure B9.4-2. Cut Set Generation Results

B9.4.1.7 Cut Sets

Table B9.4-2 contains the cut sets for the collision of the HCTT.

Table B9.4-2. Cutset for Collision of Horizontal Cask Tractor and Trailer

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
050-HCTT-COLLISION	95.34	3.000E-003	050-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HTT while leaving the RF	3.0E-003
	0.58	1.840E-005	050-CRWT-TRCT-STEER-FAIL	Tractor Steering System Failure	1.8E-005
	0.58	1.840E-005	050-CRWT-TRLR-STEER-FAIL	Trailer Steering System Failure	1.8E-005
	0.37	1.160E-005	050-HTTCOLLIDE---G65-FOH	Speed Limiter Fails	1.2E-005
			050-OPHTINTCOL01-HFI-NOD	Operator Causes Collision of HTT due to Overspeed	1.0E+000
	0.31	9.800E-006	050-CRWT-LPATH--ATH--CCF	CCF of Pendular Axle Hydraulics During Load/Unload	9.8E-006
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003

Table B9.4-2. Cutset for Collision of Horizontal Cask Tractor and Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003

Table B9.4-2. Cutset for Collision of Horizontal Cask Tractor and Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
	0.10	3.170E-006	050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
			050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
			050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
			050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
			050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
			050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
			050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003

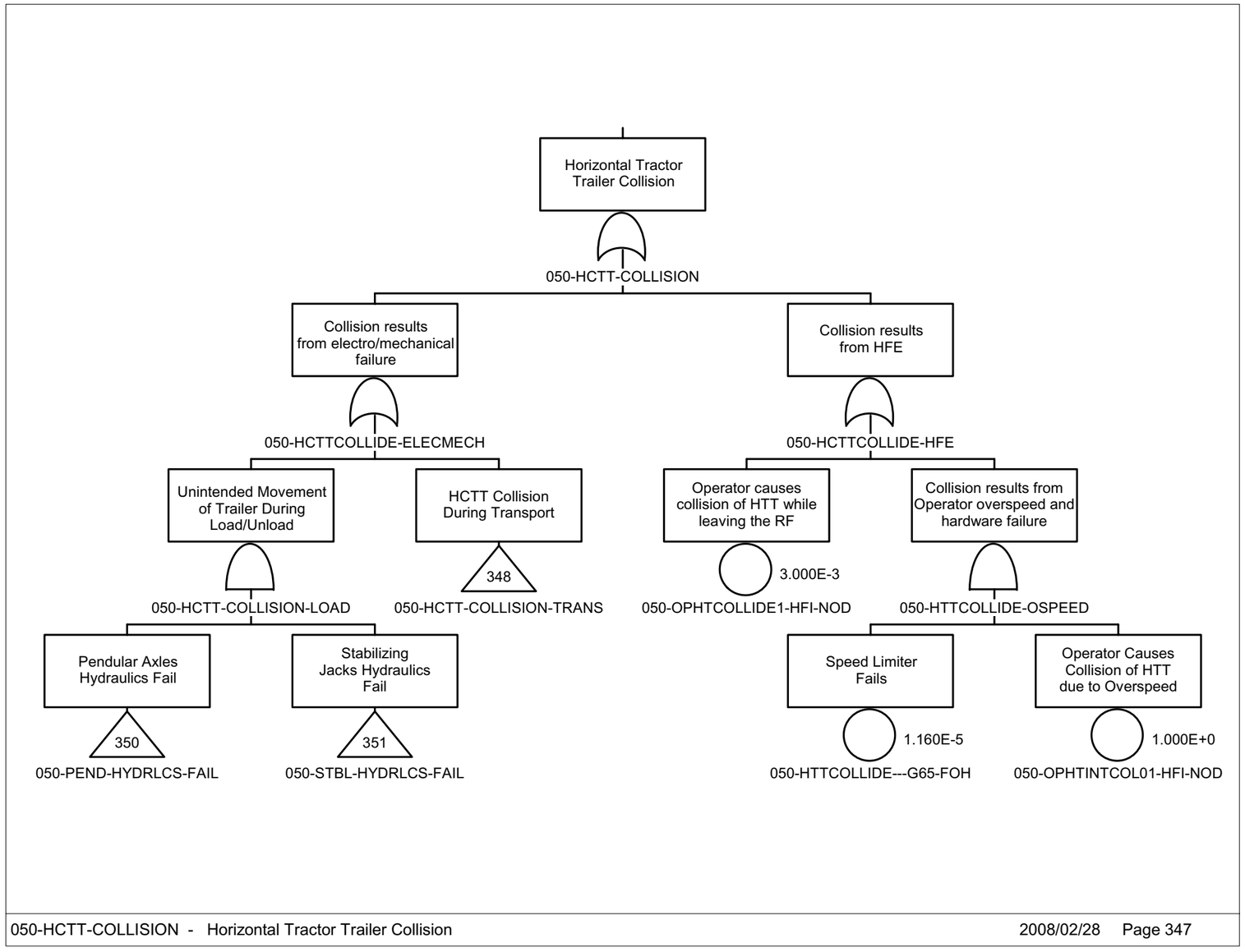
Table B9.4-2. Cutset for Collision of Horizontal Cask Tractor and Trailer (Continued)

Fault Tree	% Cut Set	Prob./Frequency	Basic Event	Description	Event Prob.
	0.10	3.170E-006	050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
			050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003
	0.10	3.170E-006	050-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.8E-003
			050-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.8E-003
	0.00	1.002E-013	050-CRWT-BRK003--BRK-FOD	Trailer Brakes Fail	1.5E-006
			050-CRWT-BRKCCF--BRK-FOD	CCF of Both Tractor Brakes	6.9E-008
		3.147E-003	= Total		

NOTE: CCF = common-cause failure; No. = number; Prob. = probability; RF = Receipt Facility.

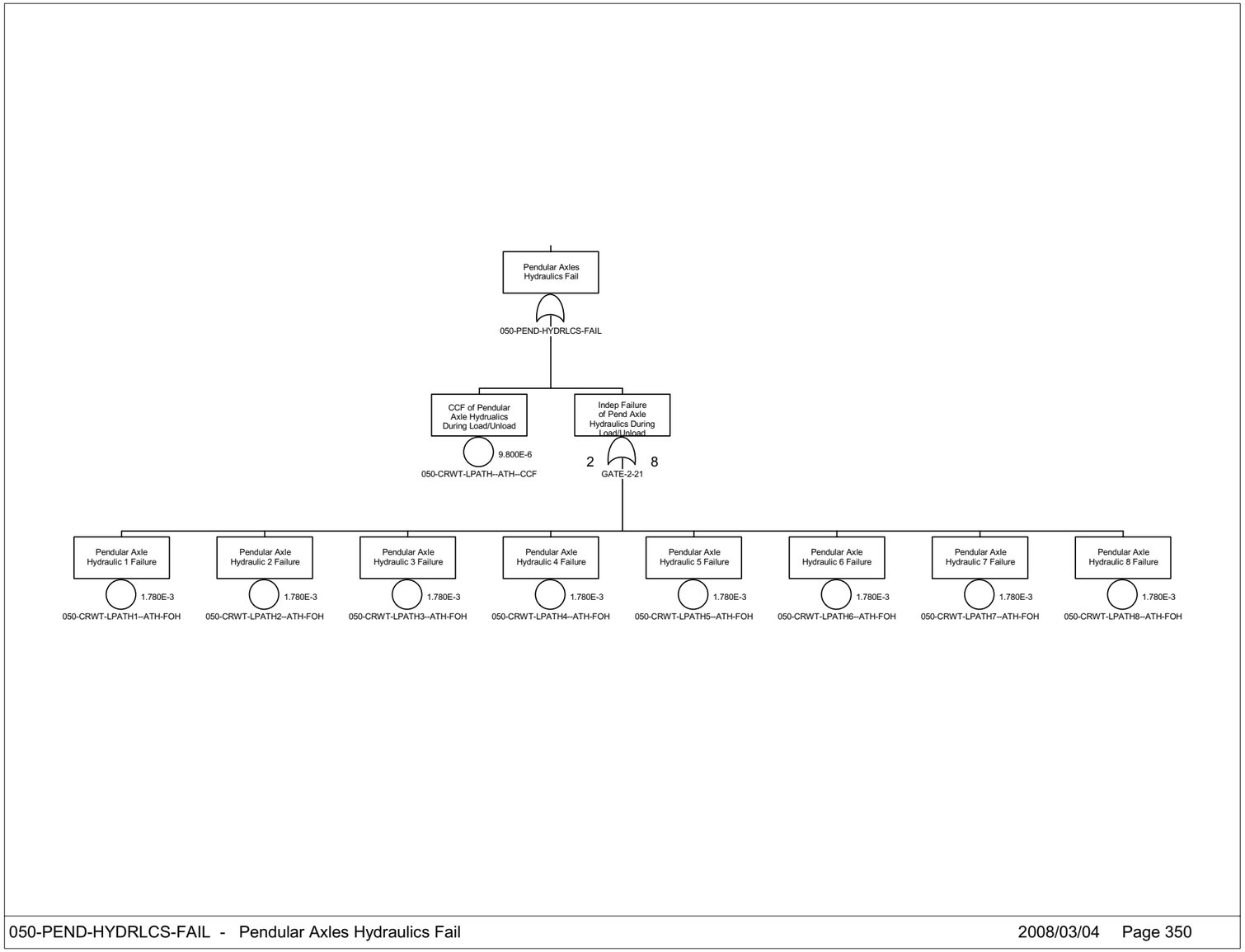
Source: Original

B9.4.1.8 Fault Trees



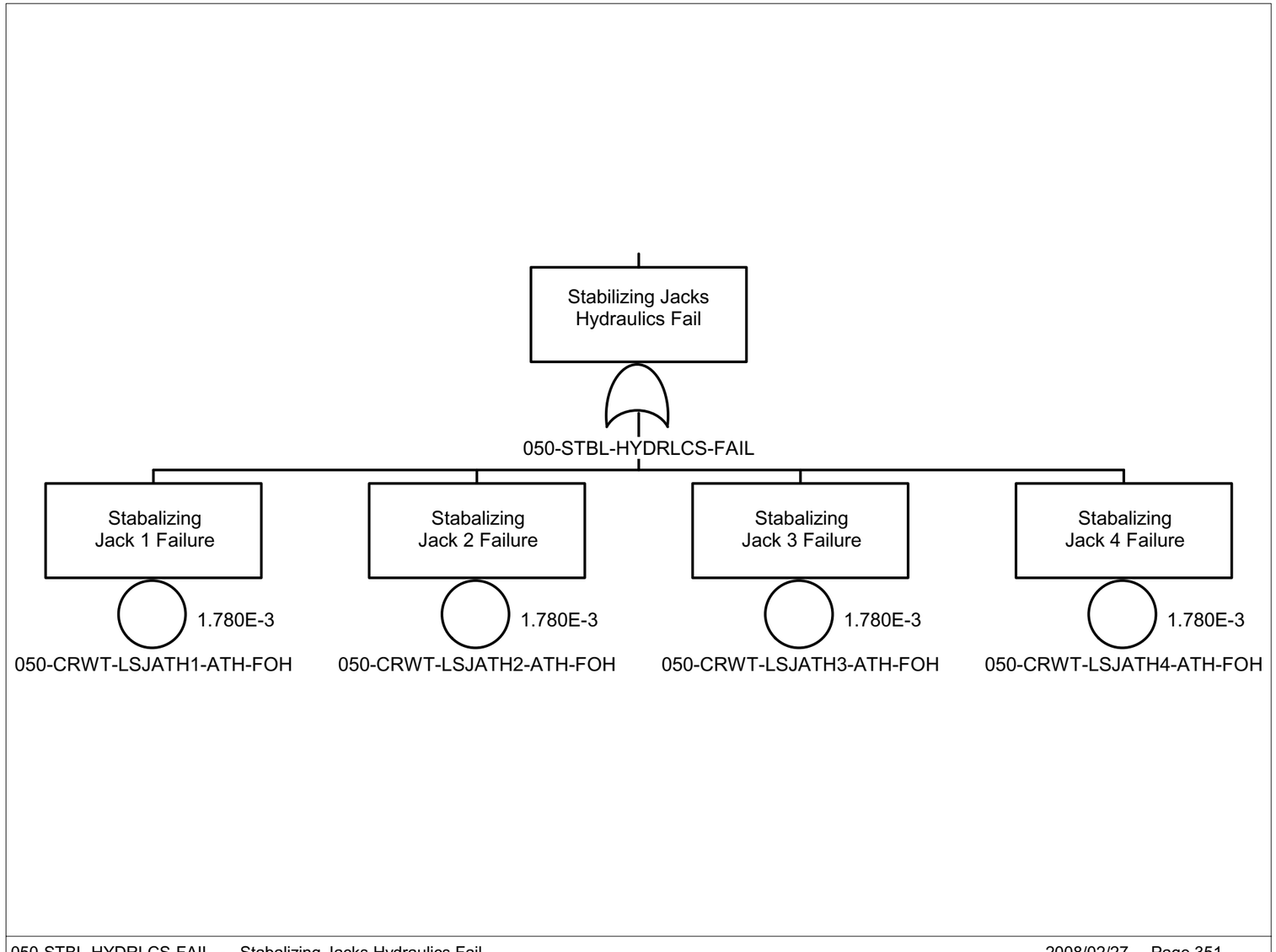
Source: Original

Figure B9.4-3. Fault Tree for Horizontal Cask Tractor Trailer Collision



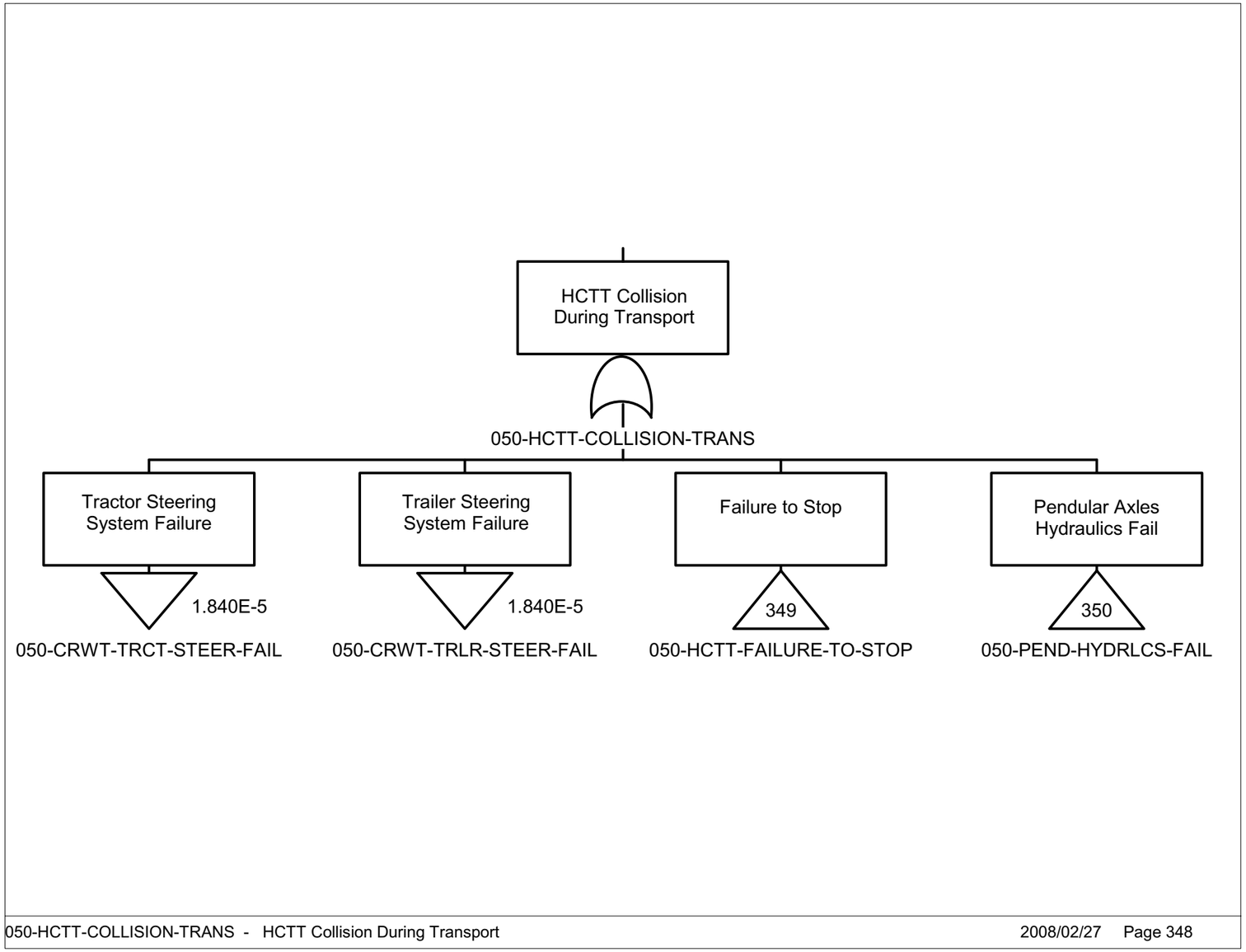
Source: Original

Figure B9.4-4. Fault Tree for Pendular Axles Hydraulics Fail



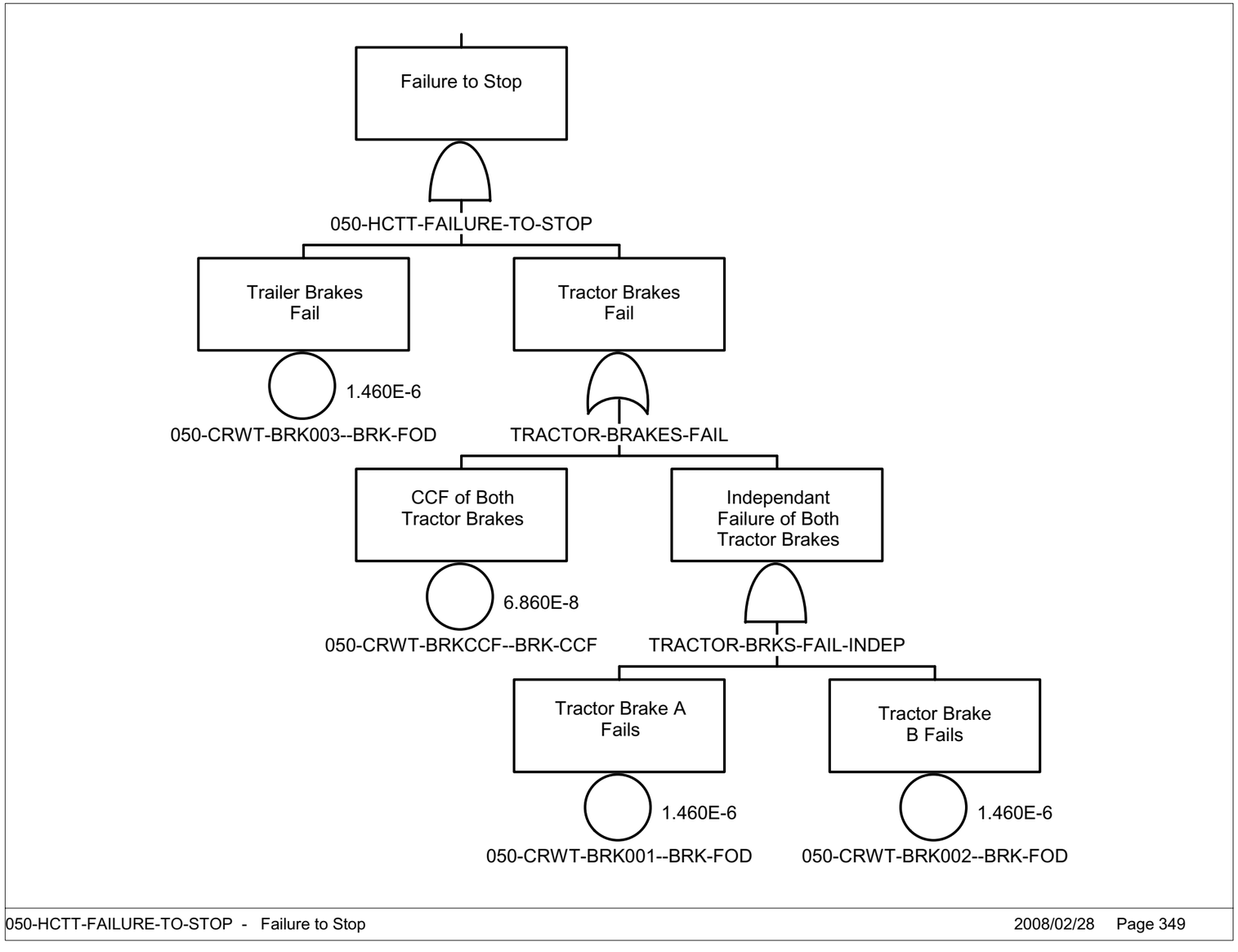
Source: Original

Figure B9.4-5. Fault Tree for Stabilizing Jacks Hydraulics Fail



Source: Original

Figure B9.4-6. Fault Tree for HCTT Collision during Transport



Source: Original

Figure B9.4-7. Fault Tree for Failure to Stop

B10 PIVOTAL EVENT ANALYSIS

Miscellaneous linking fault trees that were not discussed in Attachment A are described in this section. Attachment A describes fault trees that provided links between the event trees and basic events, fault trees containing split fractions, and initiating event fault trees described in Attachment B. This section describes the remaining types of initiating event fault trees that do not fit into these categories.

There are eight types of fault trees discussed in this section:

1. Dropping an object onto a cask or canister.
2. Impact to a cask by another vehicle or object.
3. Spurious movement of a crane causing impact to or tipping-over of a cask.
4. Loss of shielding leading to direct exposure.
5. Potential moderator sources.
6. Valve impacts on transportation casks.
7. Shield door impact to conveyance.
8. Crane drop of high star canister.

B10.1 FAULT TREES INVOLVING DROPPING AN OBJECT

These “drop on” fault trees address the events associated with dropping an object onto a cask or a canister. Table B10.1-1 identifies the applicable ESDs, a specific fault tree associated with the event sequence and the affected cask or canister. A typical fault tree for drop of an object onto a transportation cask is shown in Figure B10.1-1.

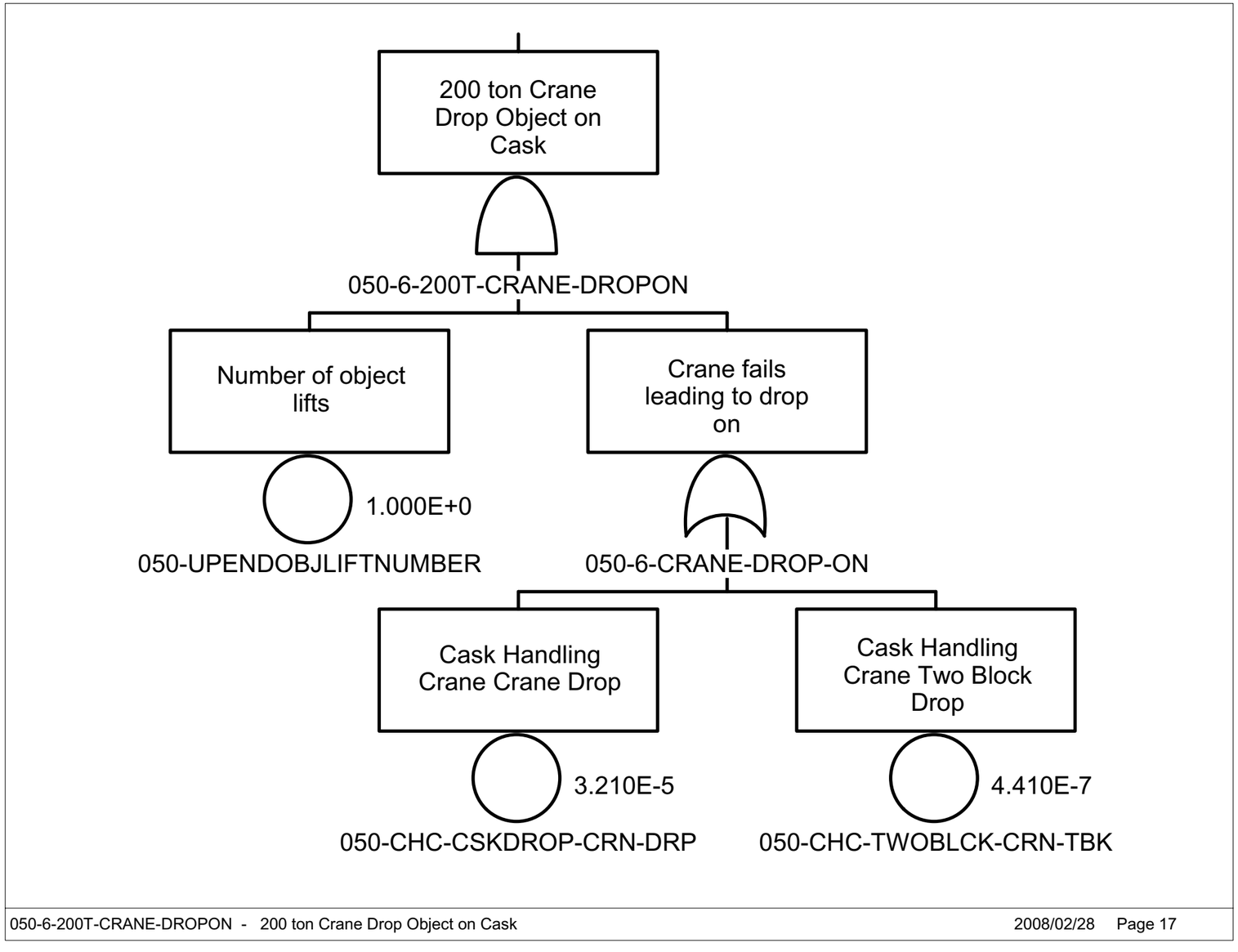
Table B10.1-1. Drop-On Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD05-UPEND-DROPON-CASK	050-5-200T-CRANE DROPON	CSNF in Transportation Cask
ESD06-TTC-UPDROPON	050-6-200T-CRANE-DROPON	Horizontal STC/DPC in Transportation Cask
ESD06-VTC-UPDROPON	050-6-200T-CRANE-DROPON	DPC in Rail Transportation Cask
ESD07-CPREP-DROPON*	ESD07-CPREP-DROPON	DPC in Transportation Cask
ESD08-CPREP-DROPON*	ESD08-CPREP-DROPON	CSNF in Transportation Cask
ESD09-DPREP-DROPON*	ESD09-DPREP-DROPON	DPC in Transportation Cask
ESD13-DPC-DROPON	CTM-DROP-ONTO-CASK	DPC Canisters (Details in Attachment B)
ESD13-TAD-DROPON	CTM-DROP-ONTO-CASK	TAD Canisters (Details in Attachment B)
ESD15-PREP-DROPON*	ESD15-PREP-DROPON	STC/DPC Casks
ESD18-DPC-DROPON*	ESD18-DPC-DROPON	DPC in Canister
ESD19-FLOOR-DROPON*	ESD19-FLOOR-DROPON	DPC Casks
ESD19-POOL-DROPON*	ESD19-POOL-DROPON	DPC Casks
ESD20-FLOOR-DROPON*	ESD20-FLOOR-DROPON	CNSF Casks
ESD20-POOL-DROPON*	ESD20-POOL-DROPON	CNSF Casks
ESD21-CSNF-LOWER-DROPON	ESD21-CSNF-LOWER-DROPON	CNSF Casks
ESD21-DPC-LOWER-DROPON	ESD21-DPC-LOWER-DROPON	STC/DPC in Cask
ESD21-TAD-LOWER-DROPON*	ESD21-TAD-LOWER-DROPON*	STC/TAD in Cask
ESD24-FLOOR-DROPON*	ESD24-FLOOR-DROPON*	STC/TAD in Cask
ESD24-POOL-DROPON*	ESD24-POOL-DROPON	STC/TAD Cask
ESD25-TAD-DROPON	ESD25-TAD-DROPON	TAD in STC
ESD28-TAD-DROPON*	ESD28-TAD-DROPON	STC/TAD Cask

NOTE: CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; ESD = event sequence diagram; STC = shielded transfer cask; TAD = transportation, aging, and disposal.
Entries in "ESD Designator column marked with "*" are described in applicable sections in Attachment A.

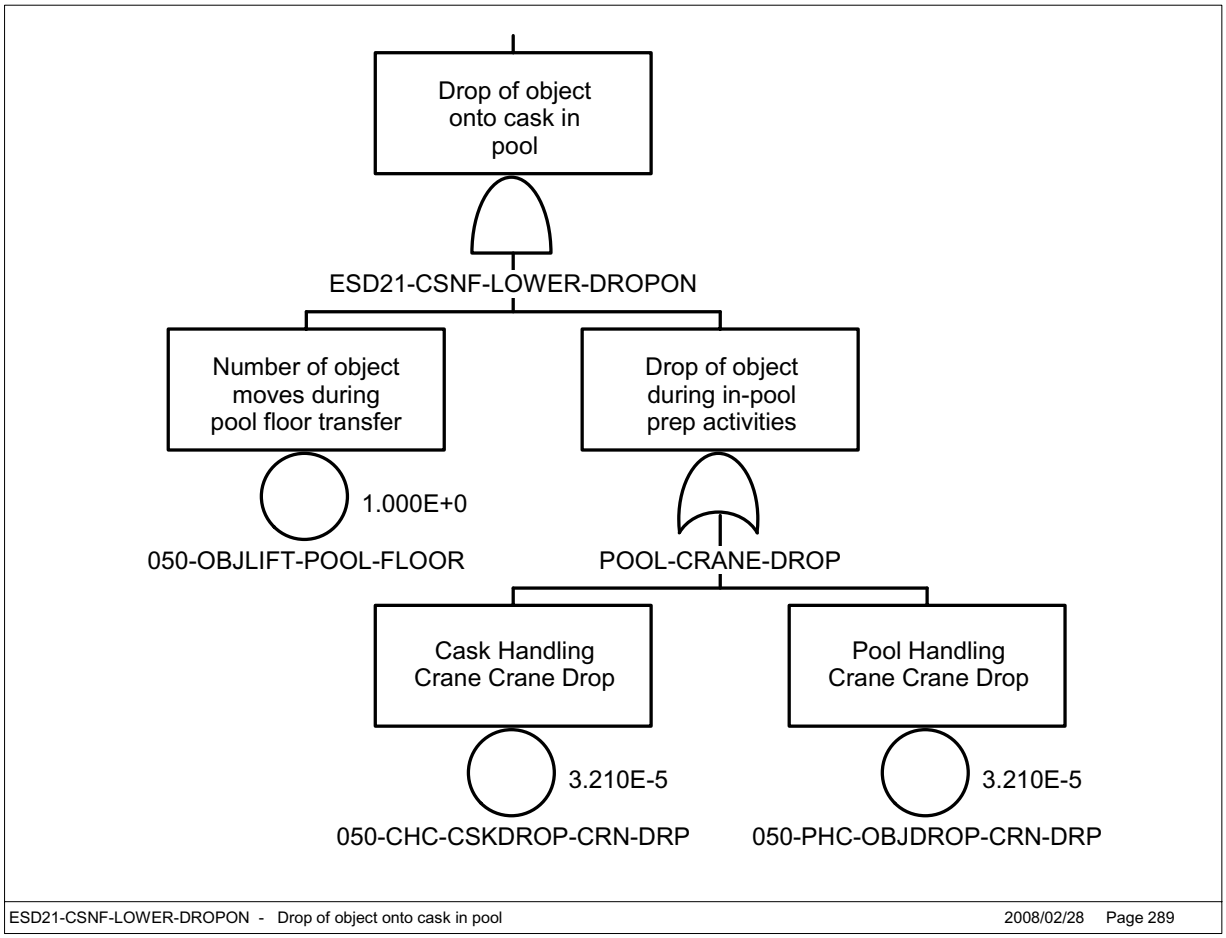
Source: Original

In Figure B10.1-1, the 200-ton crane may drop a lifting fixture onto a transportation cask or transportation, aging and disposal (TAD) canisters from a normal height or from a much higher than normal height due to a two-blocking event. In Figure B10.1-2 the cask or pool handling cranes may drop a handling fixture during in-pool preparation activities. The probabilities of crane drops are based on historical data discussed in Section 6.3 and Attachment C.



Source: Original

Figure B10.1-1. Typical 200-Ton Crane Drop-On Fault Tree



Source: Original

Figure B10.1-2. Typical Crane Drop-On Fault Tree for In-Pool Preparation Activities

ESD13-DPC-DROPON and ESD13-TAD-DROPON fault trees are addressed in section B4 of this Attachment.

B10.2 IMPACT TO A CASK BY ANOTHER VEHICLE OR OBJECT

These trees involve side impacts to the transportation cask by another vehicle or object. Table B10.2-1 lists the ESD fault trees that describe these impacts.

Table B10.2-1. Transportation Cask Impact Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD05-UPEND-SIDE-IMPACT	050-5-CSNF-IMPACT	CSNF
ESD06-TTC-UP-IMPACT	050-6-HS-TC-IMPACT	HS
ESD06-VTC-UP-IMPACT	050-6-VTC-IMPACT	VTC
ESD07-CPREP-SIMPACT	ESD07-CPREP-SIMPACT	DPC
ESD08-CPREP-IMPACT	ESD08-CPREP-SIMPACT	CSNF
ESD09-DPREP-IMPACT	ESD09-DPREP-SIMPACT	DPC
ESD11-TAD-IMPACT	ESD11-TAD-IMPACT	TAD
ESD13-DPC-CANIMPACT	ESD13-DPC-CANIMPACT	DPC
ESD13-DPC-SIDEIMPACT	ESD13-DPC-SIDEIMPACT	DPC
ESD13-TAD-SIDEIMPACT	ESD13-TAD-SIDEIMPACT	TAD

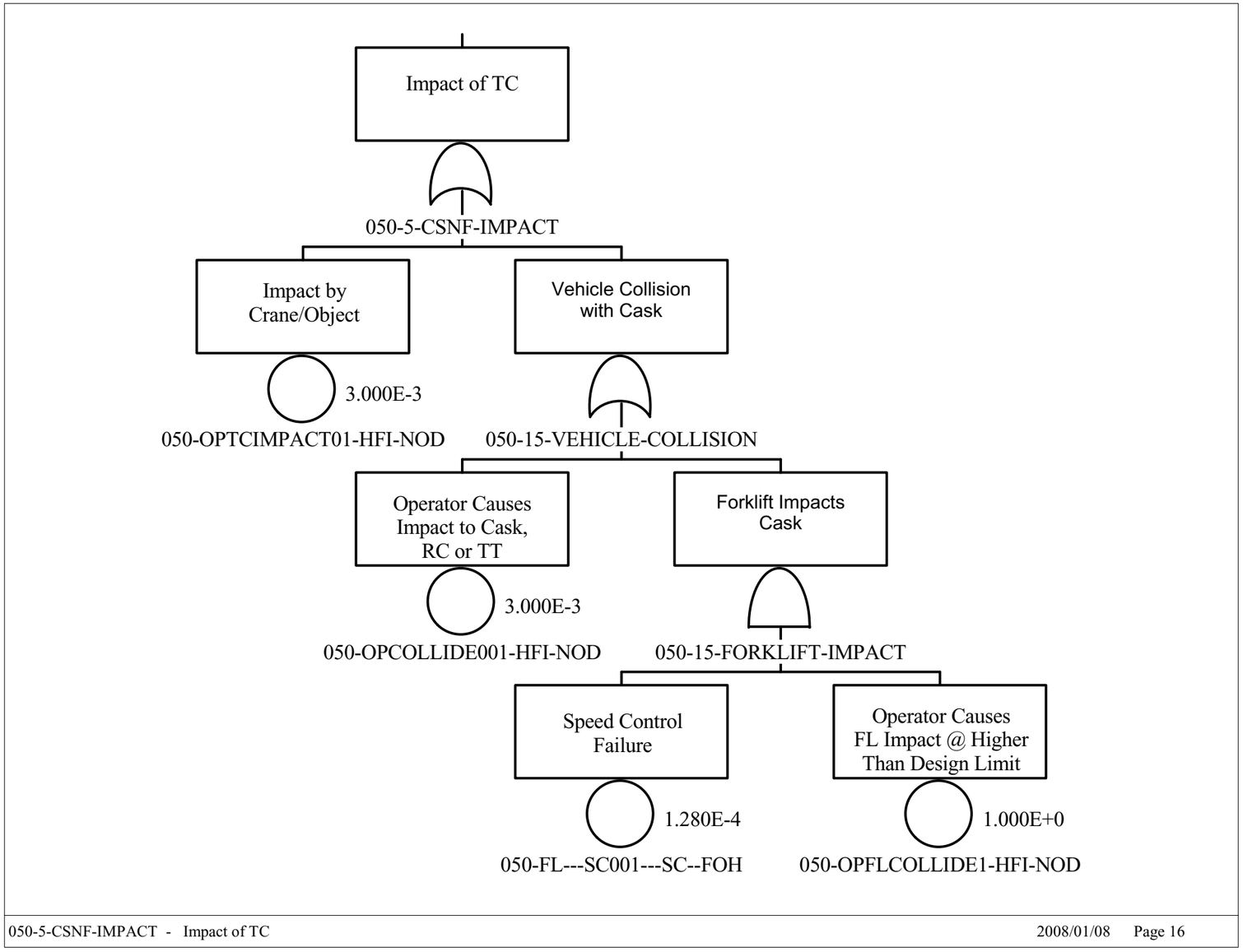
NOTE: CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; ESD = event sequence diagram; HS = High Star canister; TAD = transportation, aging, and disposal canister.

Source: Original

Figure B10.2-1 illustrates a side impact to a transportation cask for ESD05 and ESD06 that may occur due to the following operator errors:

- Operator causing impact by the crane or object being carried by the crane
- Operator impacting a vehicle (such as a forklift) into the cask at the design speed
- Operator causing a forklift impact at higher than the design speed coupled with failure of the forklift speed control.

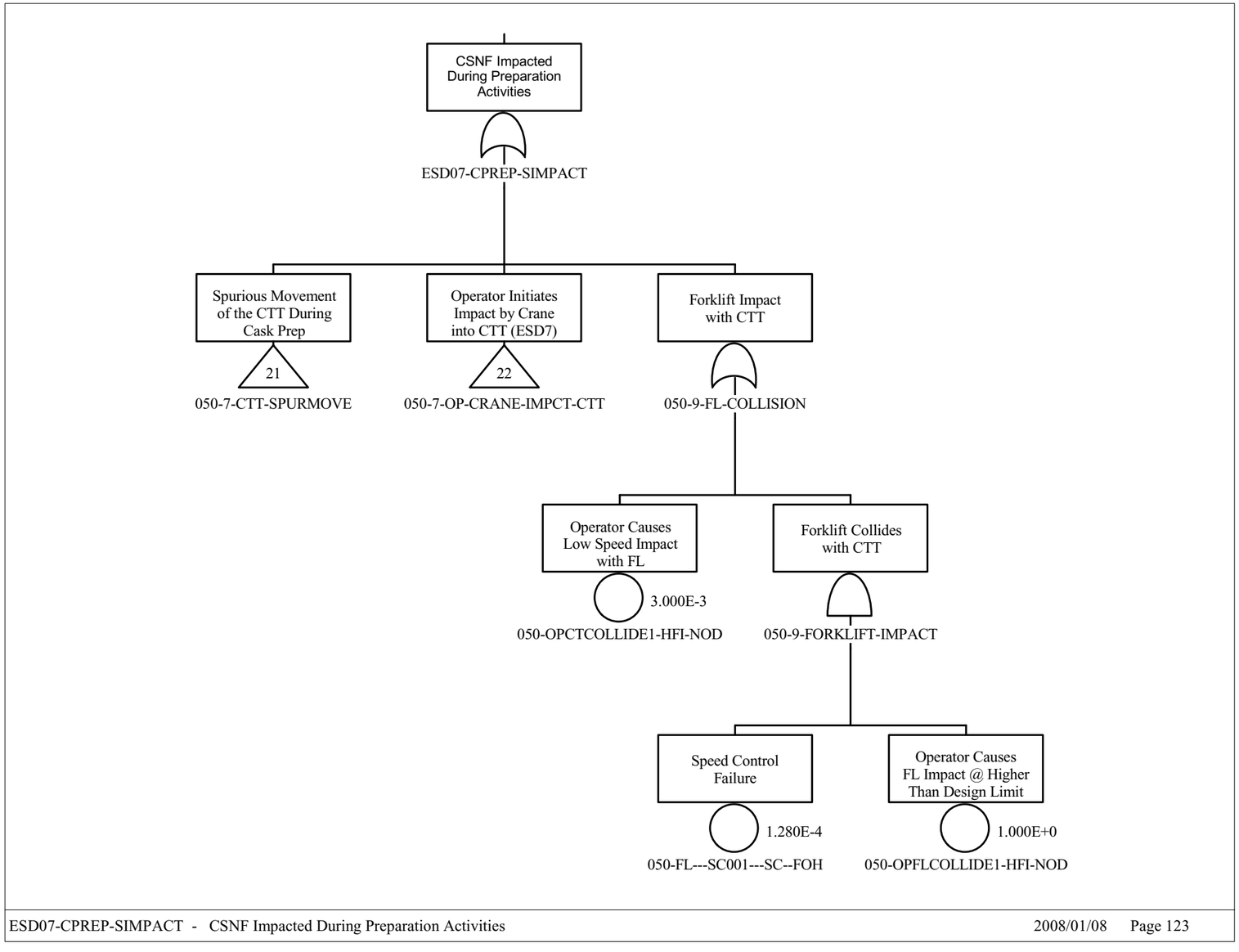
Detailed analysis on human errors is contained in Section 6.4 and Attachment E.



Source: Original

Figure B10.2-1. Typical Side Impact Fault Tree

Figure B10.2-2 is a typical fault tree developed for impact events associated with for ESD07, ESD08, and ESD09. Details on spurious movement of the cask transfer trolley (CTT) are contained in Attachment B2. Human error events are described in Section 6.4 and Attachment E.

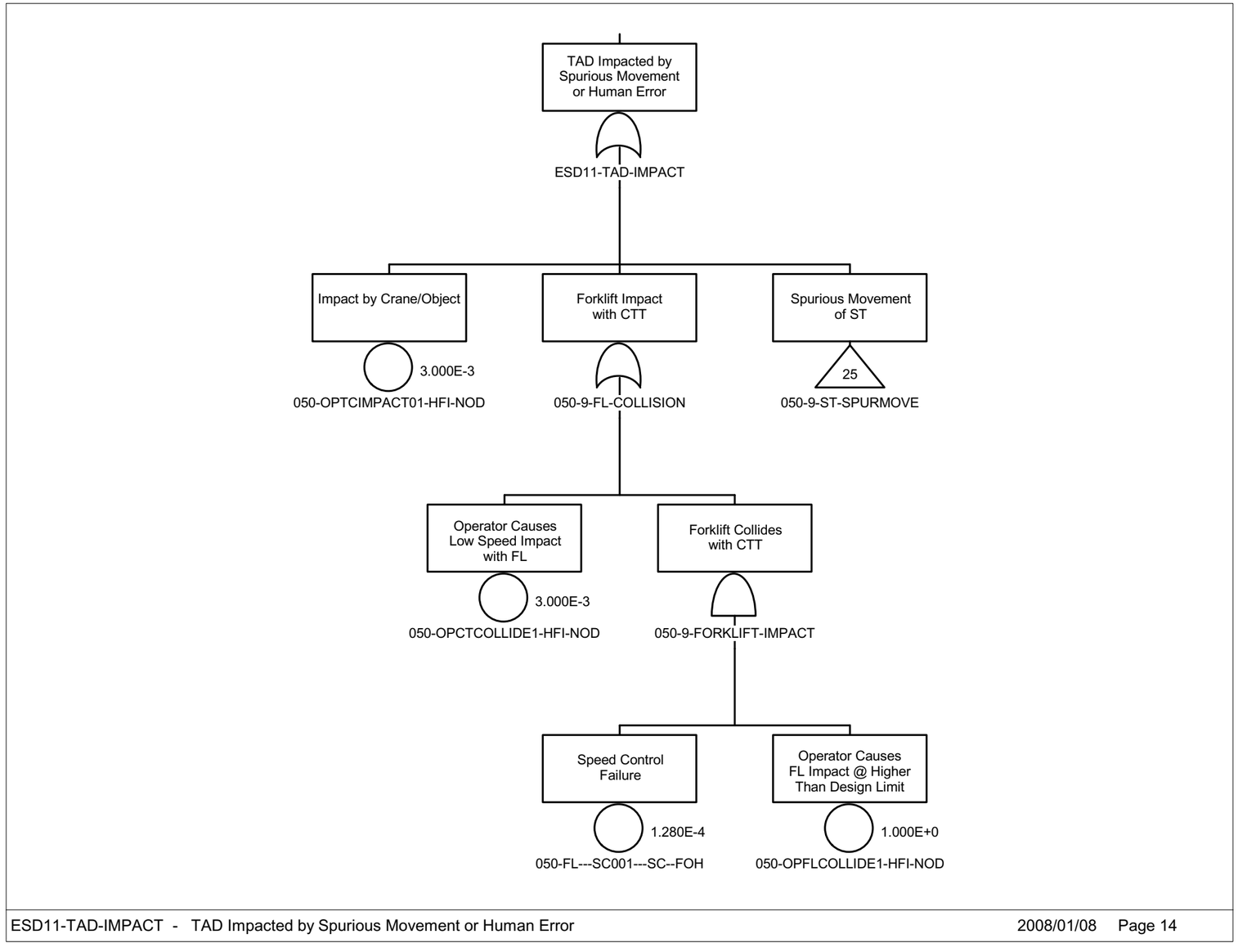


Source: Original

Figure B10.2-2. Typical Side Impact with Spurious Movement of CTT Fault Tree

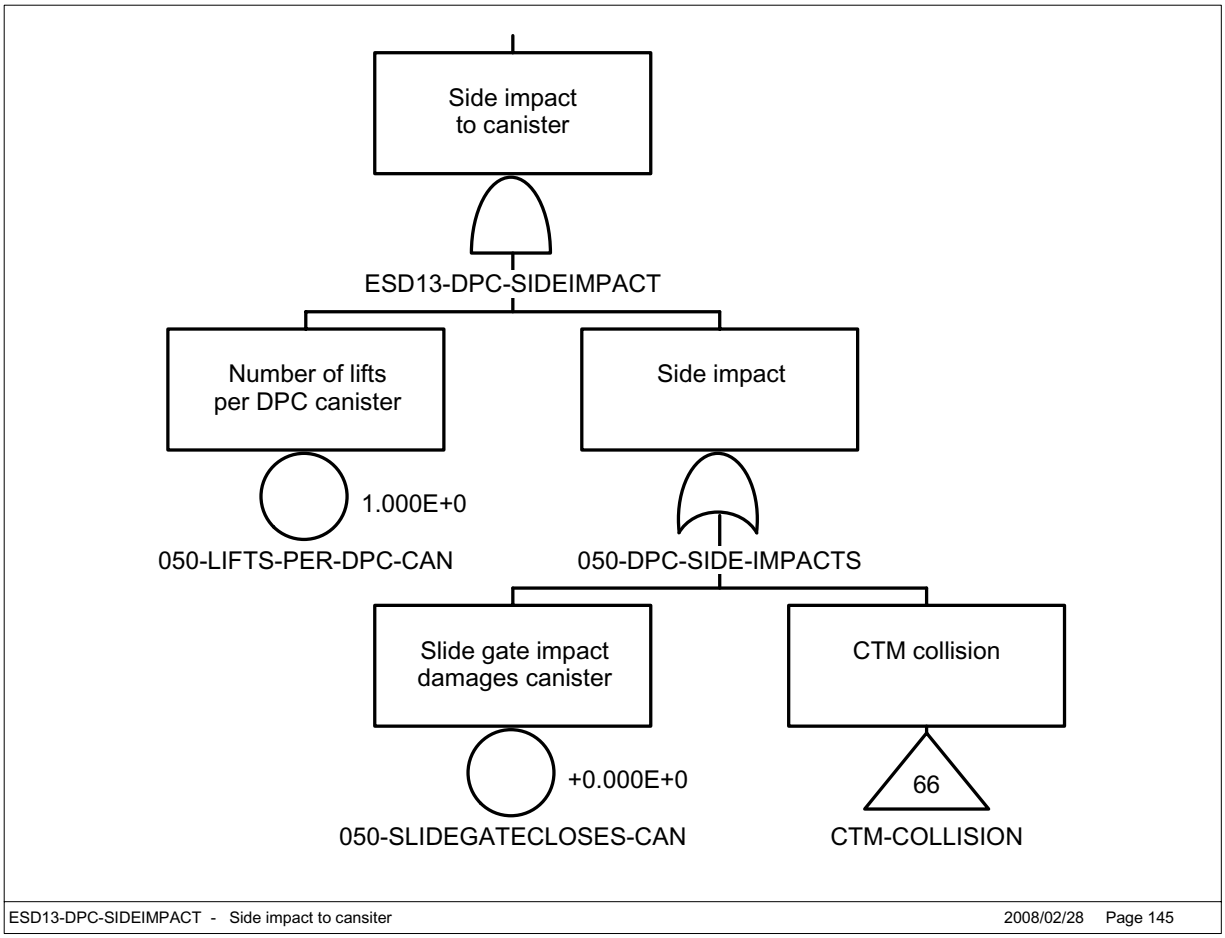
Figure B10.2-3 for ESD11 addresses impact events caused by spurious movements of conveyances and human error. ESD11 addresses the spurious movement of the site transporter and human errors. Figure B10.2-4 for ESD13 addresses spurious canister transfer machine movements and human errors. Details on human errors are contained in Section 6.4 and Attachment E. Details on spurious movements of the site transporter, CTT and CTM are contained in Sections B6, B2, and B4, respectively.

Figure B10.2-5 for ESD13 addresses canister impacts during CTM operations.



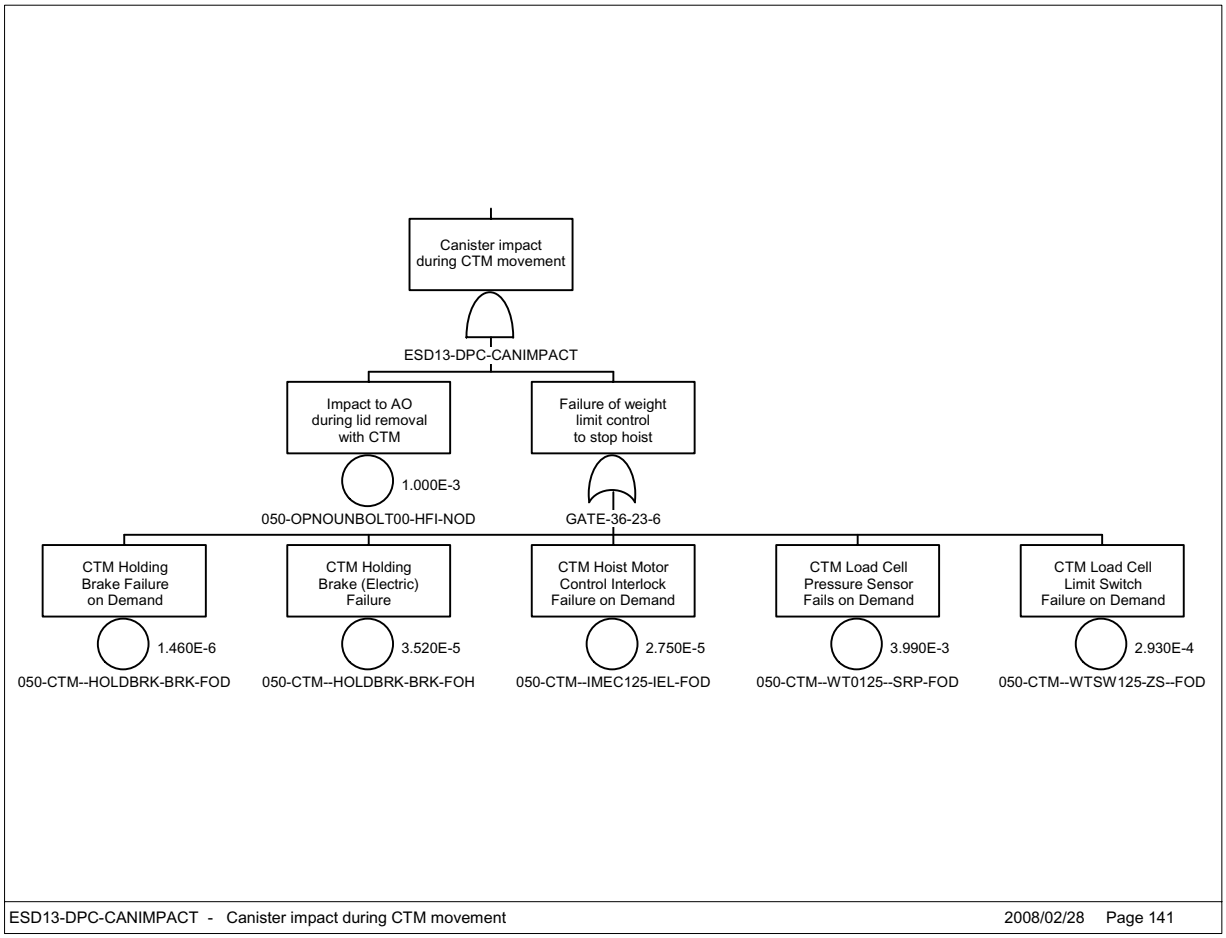
Source: Original

Figure B10.2-3. Typical Side Impact with Spurious Movement of Site Transporter Fault Tree



Source: Original

Figure B10.2-4. Typical Side Impact with Spurious Movement of Canister Transfer Machine Fault Tree



Source: Original

Figure B10.2-5. Canister Impact during Canister Transfer Machine Operations Fault Tree

B10.3 IMPACT TO A CASK DUE TO SPURIOUS MOVEMENT (TIP-OVER)

The ESD contained in Table B10.3-1 address impacts to or tip-over of the transportation cask due to spurious movements of the crane, CTT, or site transporter.

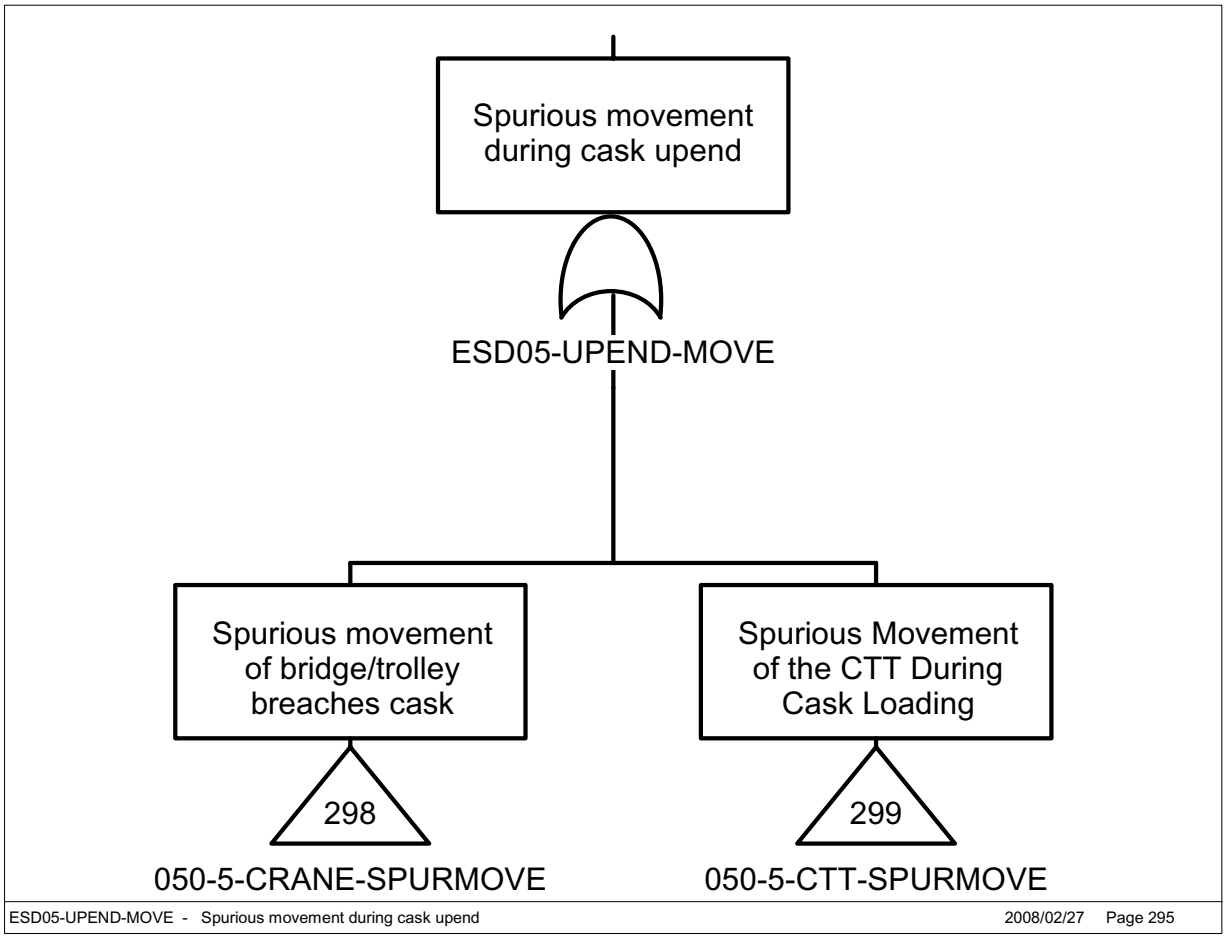
Table B10.3-1. Transportation Cask Impacts or Tip-over Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD05-UPEND-MOVE	ESD05-UPEND-MOVE	CSNF in TC
ESD06-TTC-UP-MOVE	ESD06-TTC-UP-MOVE	TTC
ESD06-VTC-UP-MOVE	ESD06-VTC-UP-MOVE	VTC
ESD07-CPREP-CASKTIP	ESD07-CPREP-CASKTIP	DPC
ESD08-CPREP-TIP	ESD08-CPREP-TIP	CSNF
ESD11-DPC-TIP	050-11-ST-ROLLOVER	DPC
ESD11-TAD-TIP	050-11-ST-ROLLOVER	TAD
ESD13-DPC-SPURMOVE	ESD13-DPC-SPURMOVE	DPC
ESD13-TAD-SPURMOVE	ESD13-TAD-SPURMOVE	TAD

NOTE: CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; ESD = event sequence diagram; TAD = transportation, aging, and disposal; VTC = vertical transportation cask.

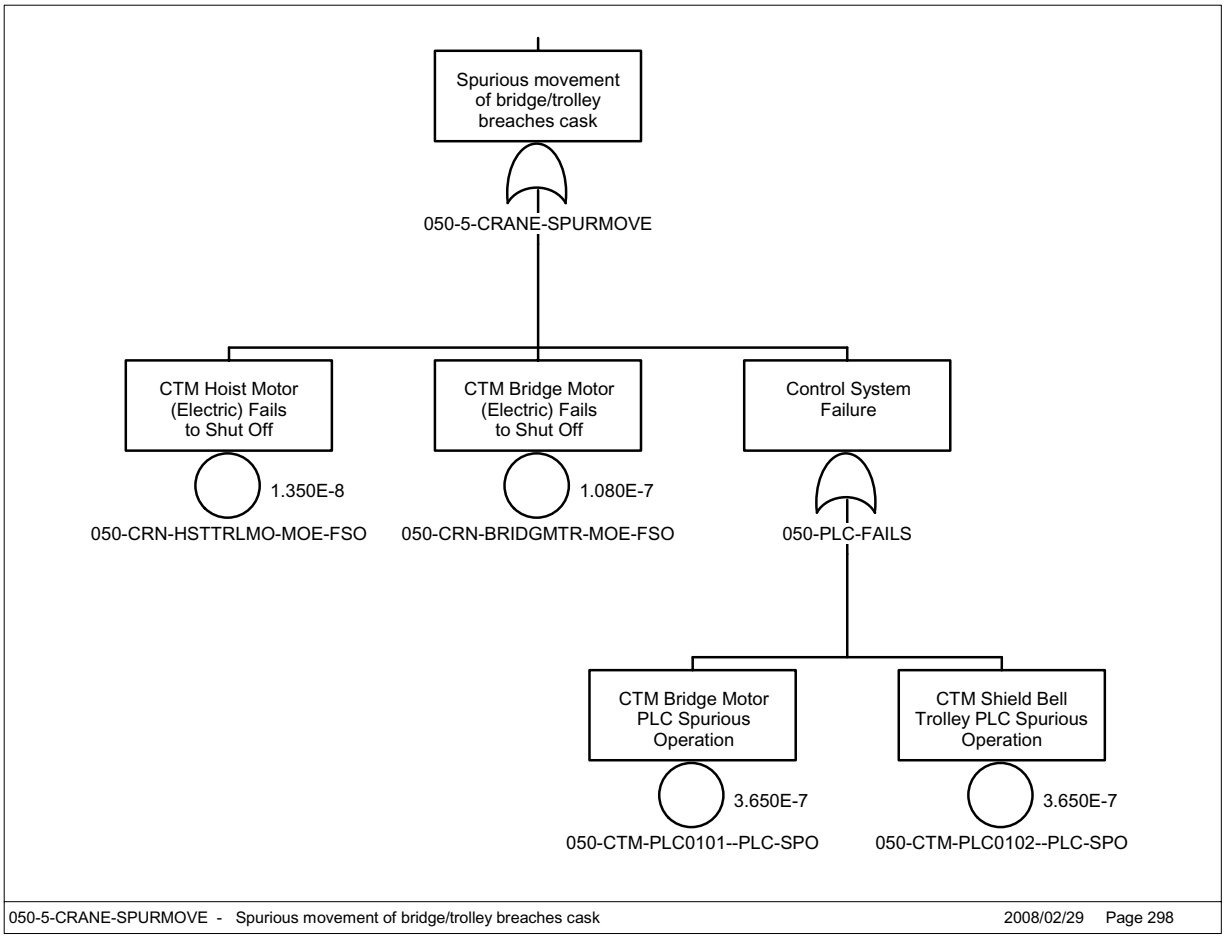
Source: Original

Figure B10.3-1 describes an impact to a cask due to spurious movement of the crane or a CTT that could result in an impact or tip over. The fault tree for spurious movement of the crane (identified as transfer gate 050-5-CRANE-SPURMOVE) detailed in Figure B10.3-2. Spurious movement of the CTT is detailed in Attachment B2. Spurious movement of the crane may occur due to failure of either the crane bridge or hoist motor to shut off, or spurious signals from the system controls.



Source: Original

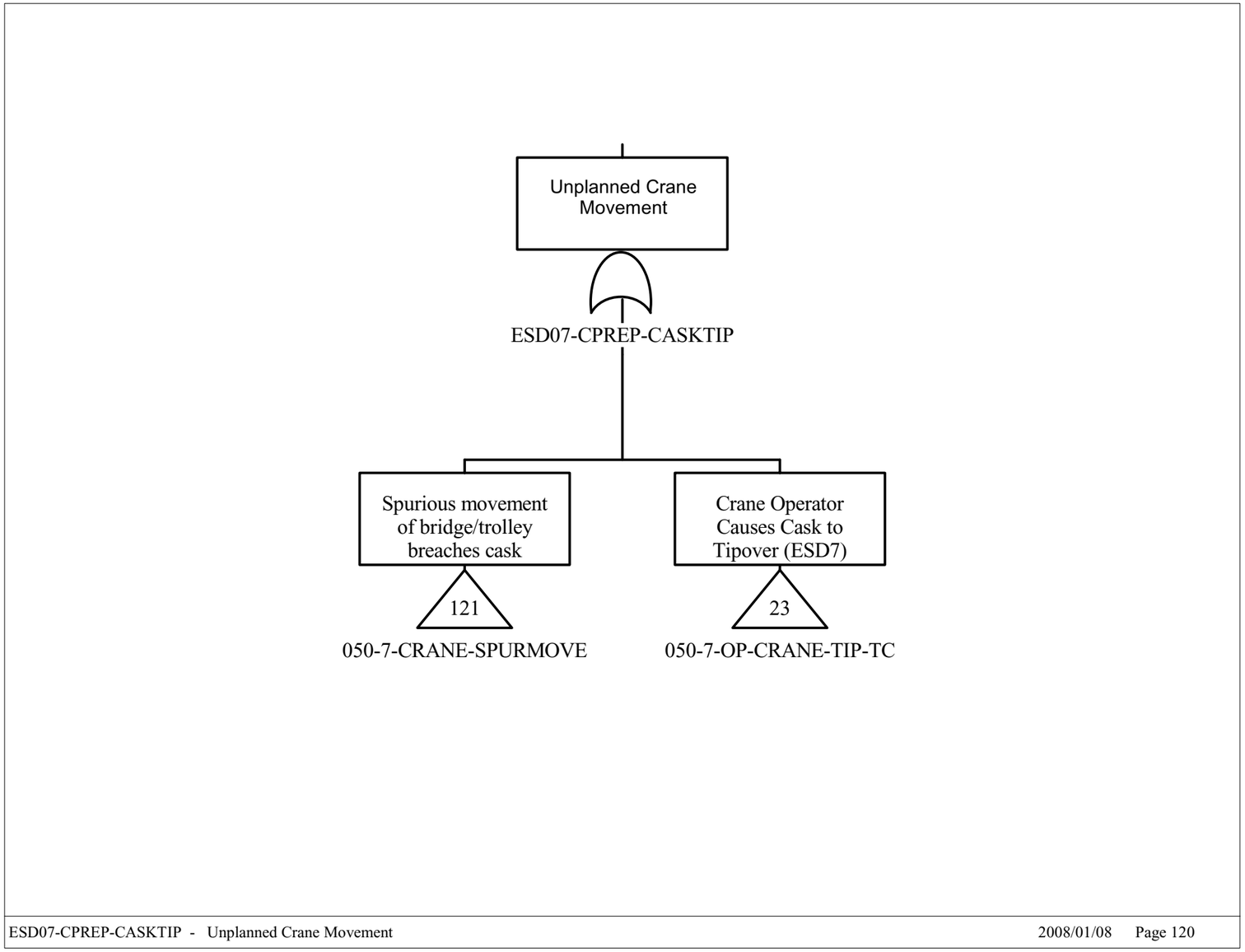
Figure B10.3-1 Spurious Movement during Cask Upending



Source: Original

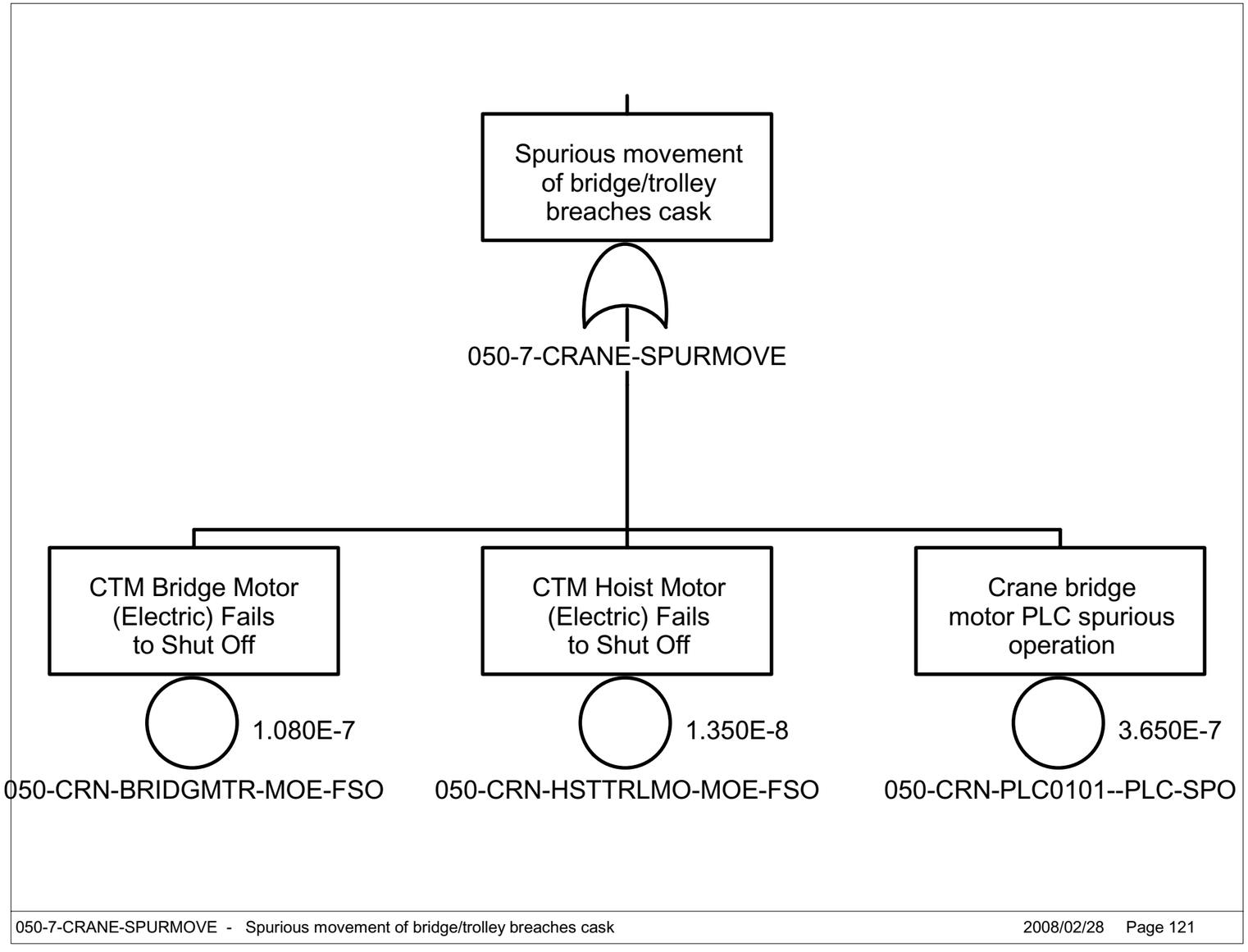
Figure B10.3-2. Spurious Movement of the Crane during Cask Upending

Figure B10.3-3 describes an impact to a cask due to spurious movement of the crane and a crane operator human error (050-OPTIPOVER001-HFI-NOD) that could result in a cask tip-over. The fault tree for spurious movement of the crane (identified as transfer gate 050-7-CRANE-SPURMOVE) detailed in Figure B10.3-4. Spurious movement of the crane may occur due to failure of either the crane bridge or hoist motor to shut off, or spurious signals from the crane bridge motor PLC. Details on the human error are contained in Section 6.4 and Attachment E. Details on site transporter rollover are contained in Attachment B6.



Source: Original

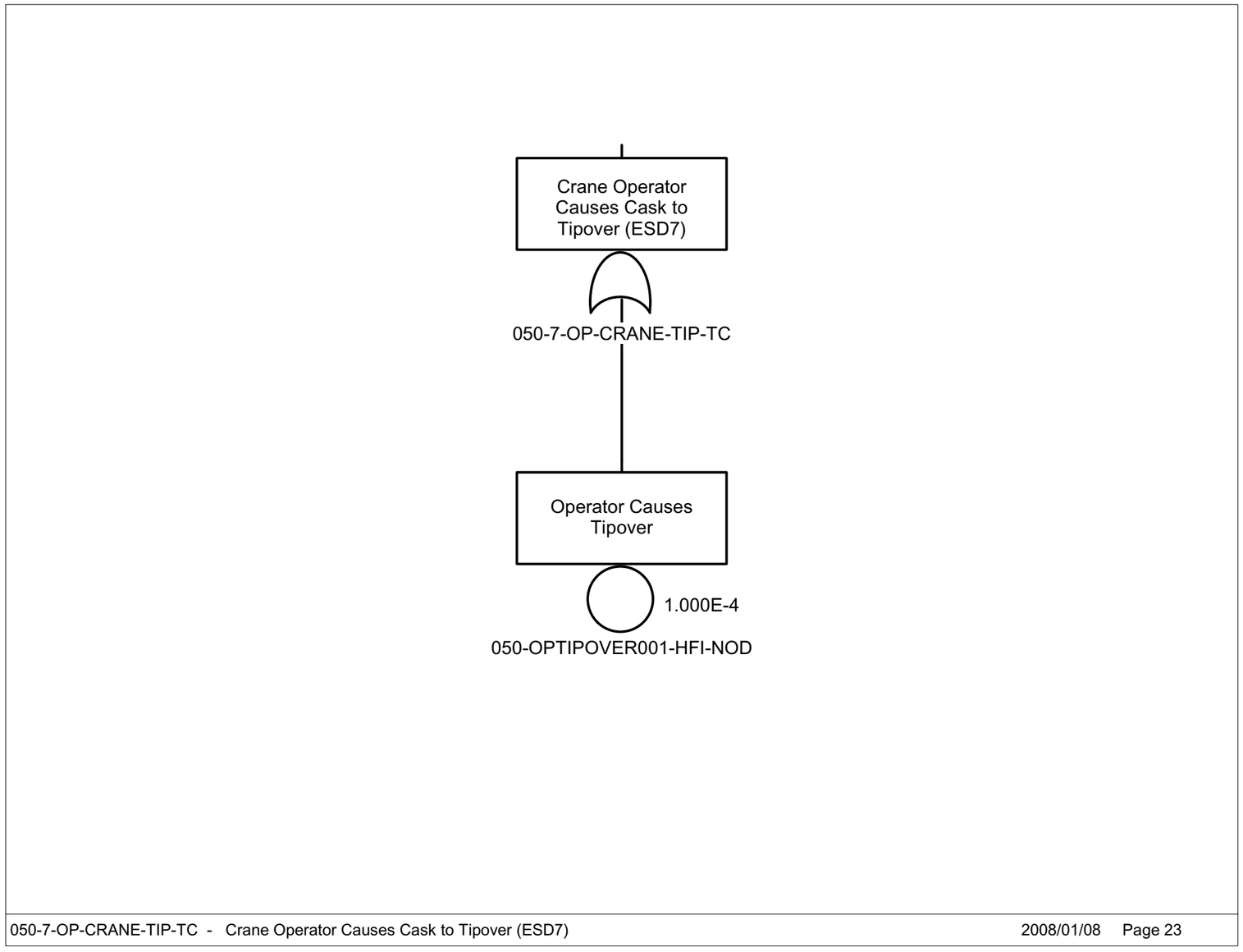
Figure B10.3-3. Spurious Movement of the Crane Fault Tree



Source: Original

Figure B10.3-4. Spurious Movement of the Bridge/Trolley Breaches Cask

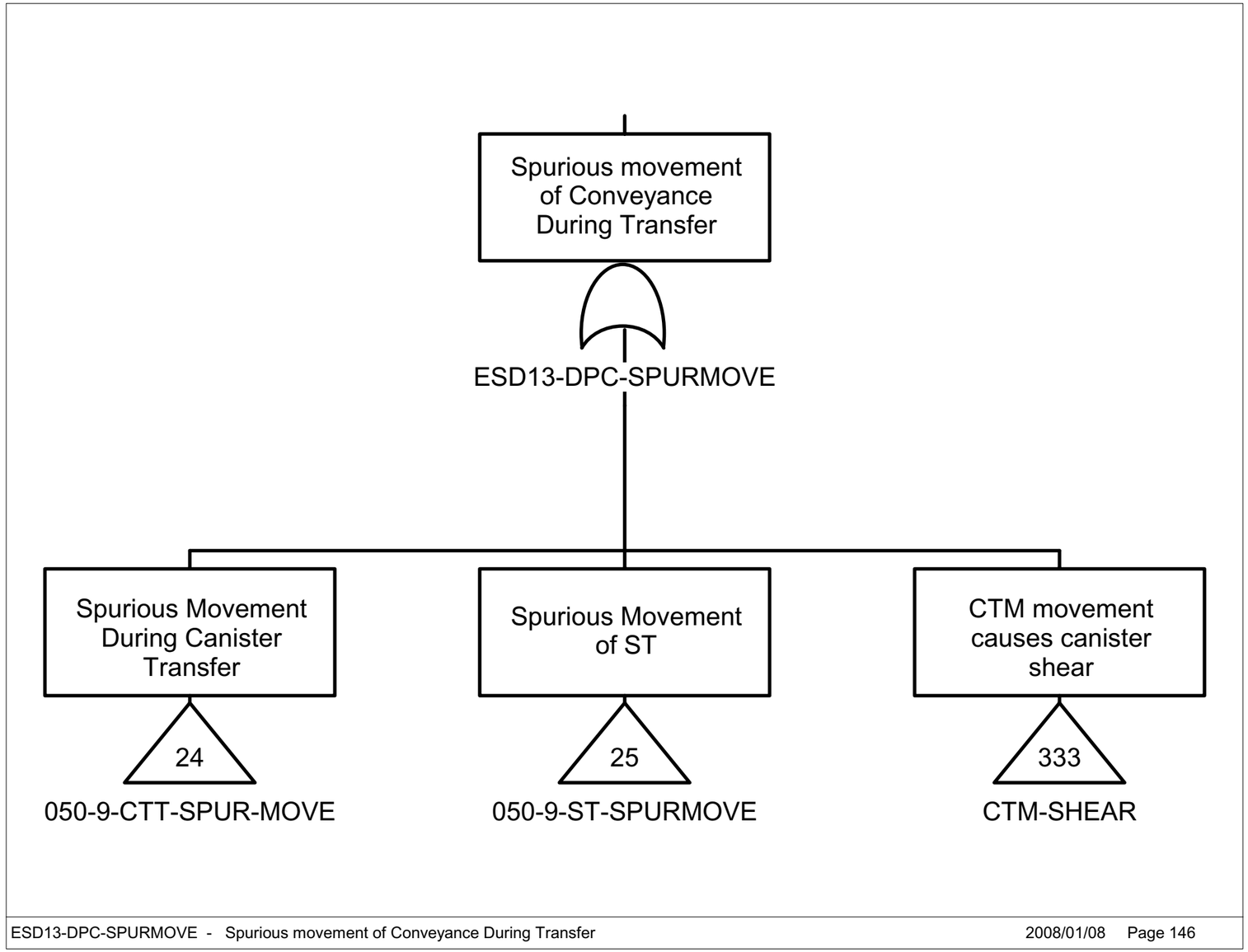
Tip-over in ESD7 addresses a potential operator error as shown in Figure B10.3-5.



Source: Original

Figure B10.3-5. Human Error Tip-Over Fault Tree

ESD-13 addresses spurious movement of conveyances and the possibility of impacts to the cask during movements on the CTT, site transporter, and CTM (Figure B10.3-6). Details on 050-9-CTT-SPUR-MOVE are addressed in Attachment B2; 050-9--ST-SPURMOVE in Attachment B6; and CTM-SHEAR in Attachment B4.



Source: Original

Figure B10.3-6. Spurious Conveyance Movement Fault Tree

B10.4 LOSS OF SHIELDING LEADING TO DIRECT EXPOSURE

These fault trees describe direct exposure during canister transfer operations in the WHF. Table B10.4-1 lists the fault trees that describe these direct exposures.

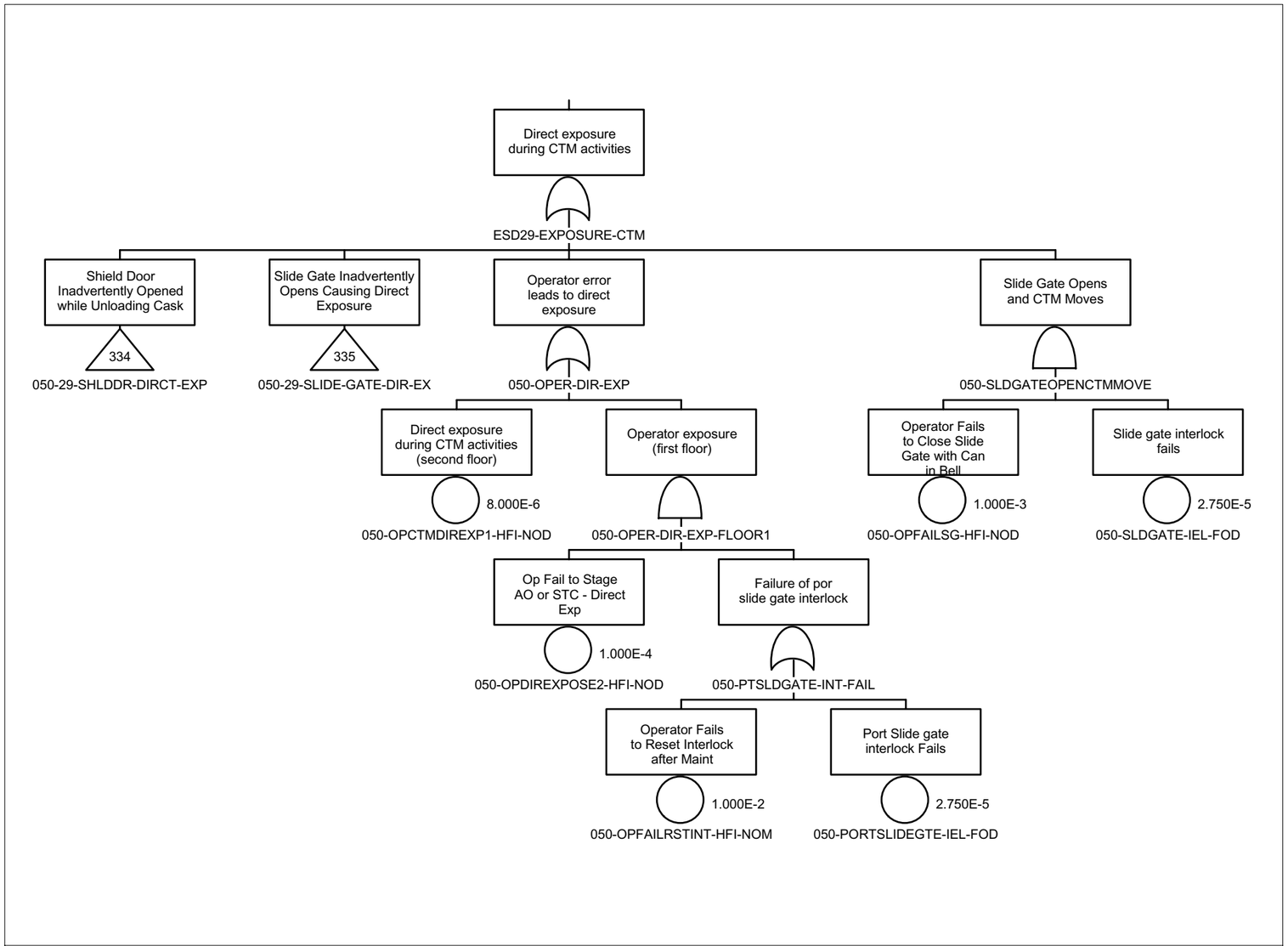
Table B10.4-1. Direct Exposure Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD29-EXPOSURE-CTM	ESD29-EXPOSURE-CTM	DPC
ESD29-EXPOSURE-LIFT	ESD29-EXPOSURE-LIFT	DPC
ESD29-TAD-CTM	ESD29-TAD-CTM	TAD
ESD30-EXPOSURE-SPLASH	ESD30-EXPOSURE-SPLASH	DPC

NOTE: CTM = canister transfer machine; DPC = dual-purpose canister; TAD = transportation, aging, and disposal canister.

Source: Original

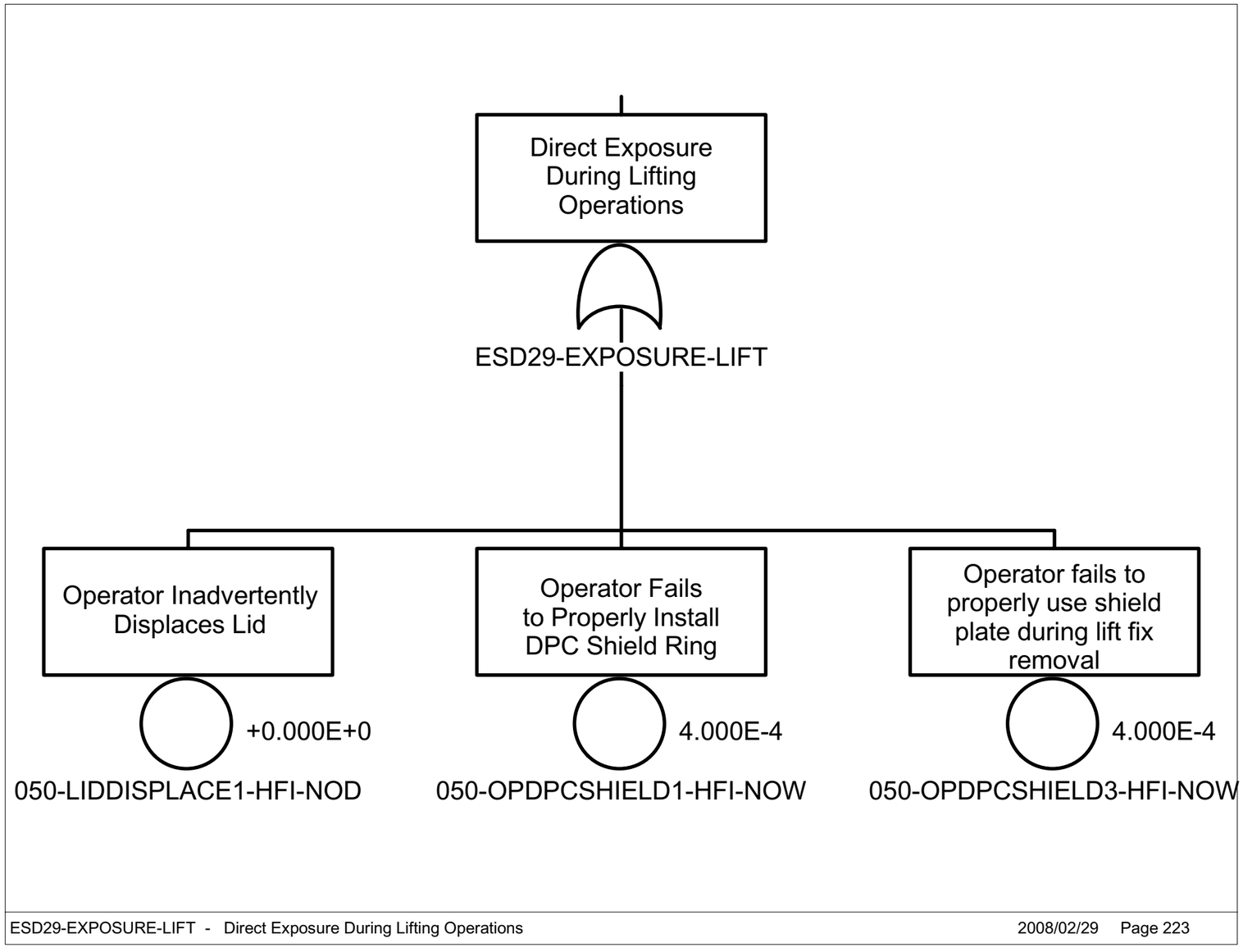
Figure B10.4-1 illustrates the potential causes of direct exposure during canister transfer. The potential causes include operator error coupled with interlock failures, and inadvertent opening of the shield door or slide gate. Fault trees for inadvertent opening of the shield door or slide gate are described in "Loading/Unloading Room Shield Door and Slide Gate Fault Tree Analysis" in Attachment B3.



Source: Original

Figure B10.4-1. Typical Direct Exposure Fault Tree due During CTM Activities

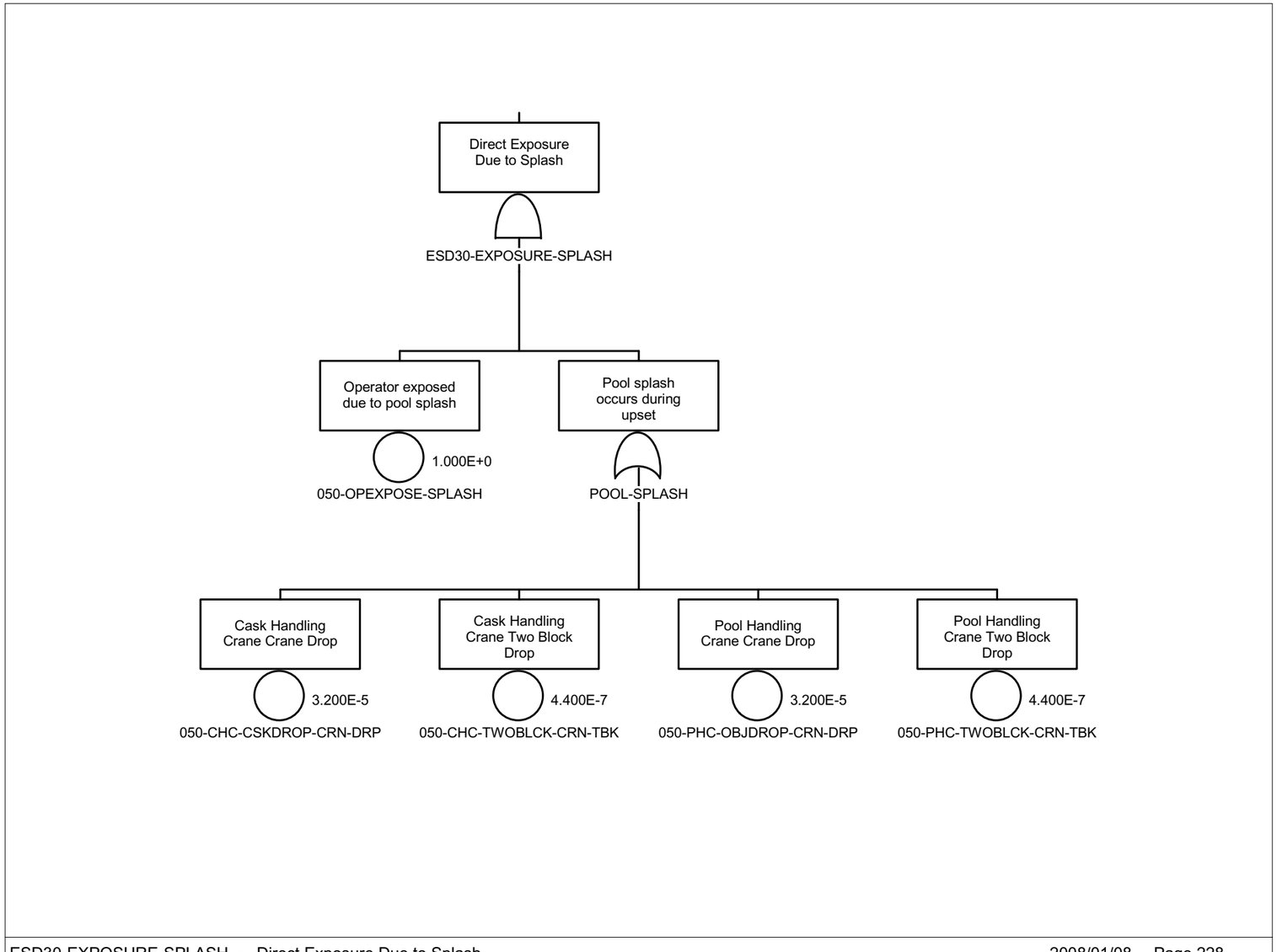
Figure B10.4-2 addresses the potential of a direct exposure resulting from human errors associated with transportation cask preparation activities for lid removal. The events are documented in Section 6.4 and Attachment E.



Source: Original

Figure B10.4-2. Human Errors Resulting in Direct Exposure during Cask Preparation Activities

Figure B10.4-3 illustrates the potential causes of direct exposure resulting from cask and pool handling crane drops from both normal and above normal heights associated with two blocking which could result in dropping of the cask into the pool. The human error event is described in Section 6.4 and Attachment E.



Source: Original

Figure B10.4-3. Direct Exposure Due to Splash from Pool

B10.5 MODERATOR SOURCE

Internal floods are potential sources of moderator addition into a canister associated with pivotal events in the event sequences included in Section 6.1. Moderator addition into a canister can occur following a breach of the canister and a subsequent internal flooding. Table B10.5-1 lists the fault trees that describe the moderator events during WHF operations.

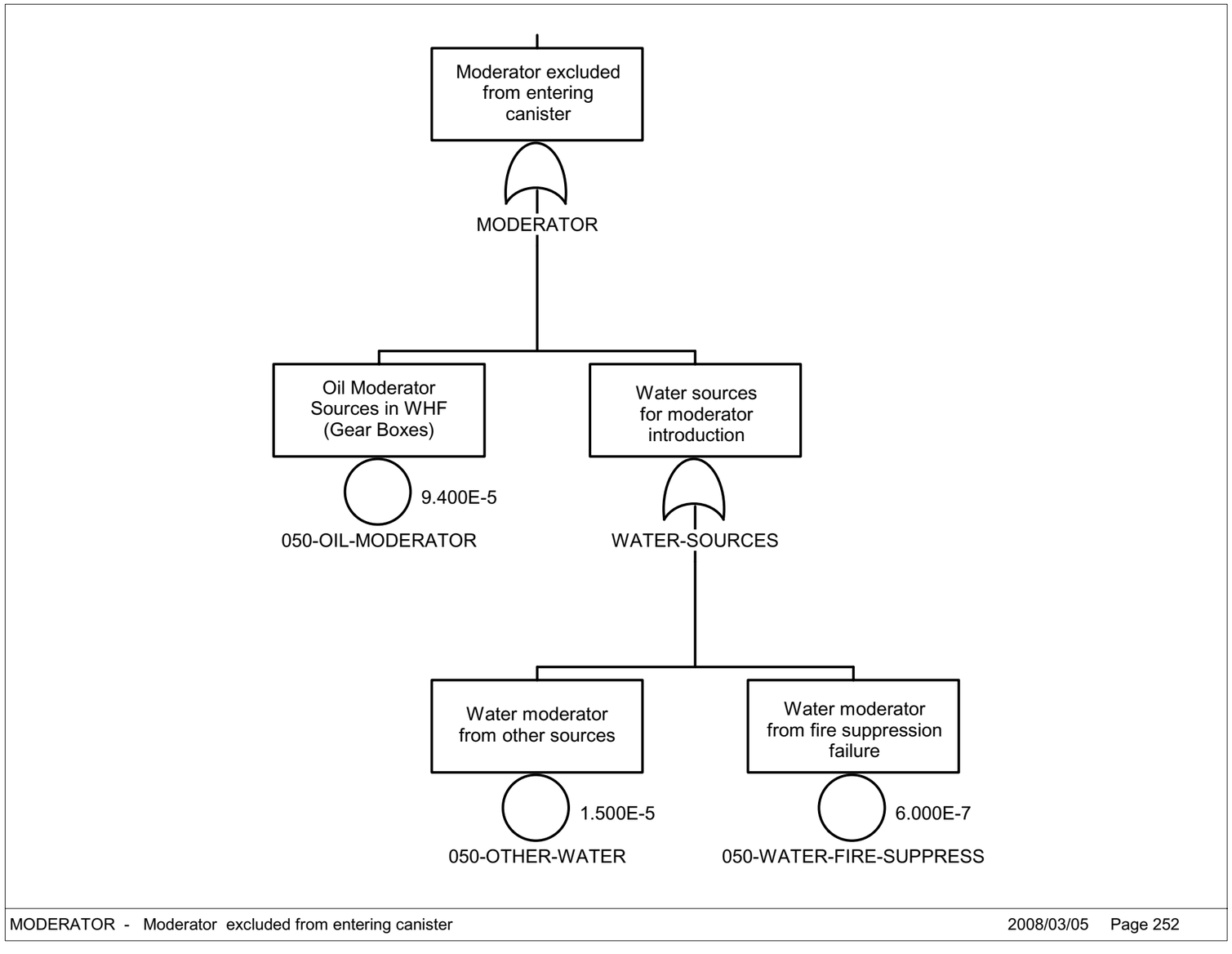
Table B10.5-1. Moderator Fault Trees

Fault Tree Name	Applies To
MODERATOR	DPC, TAD, STC, CSNF
MODERATOR-FIRE	DPC, TAD, STC, CSNF

NOTE: CSNF = Commercial Spent NuclearFuel; DPC = dual-purpose canister; STC = shielded transfer cask; TAD = transportation, aging, and disposal canister.

Source: Original

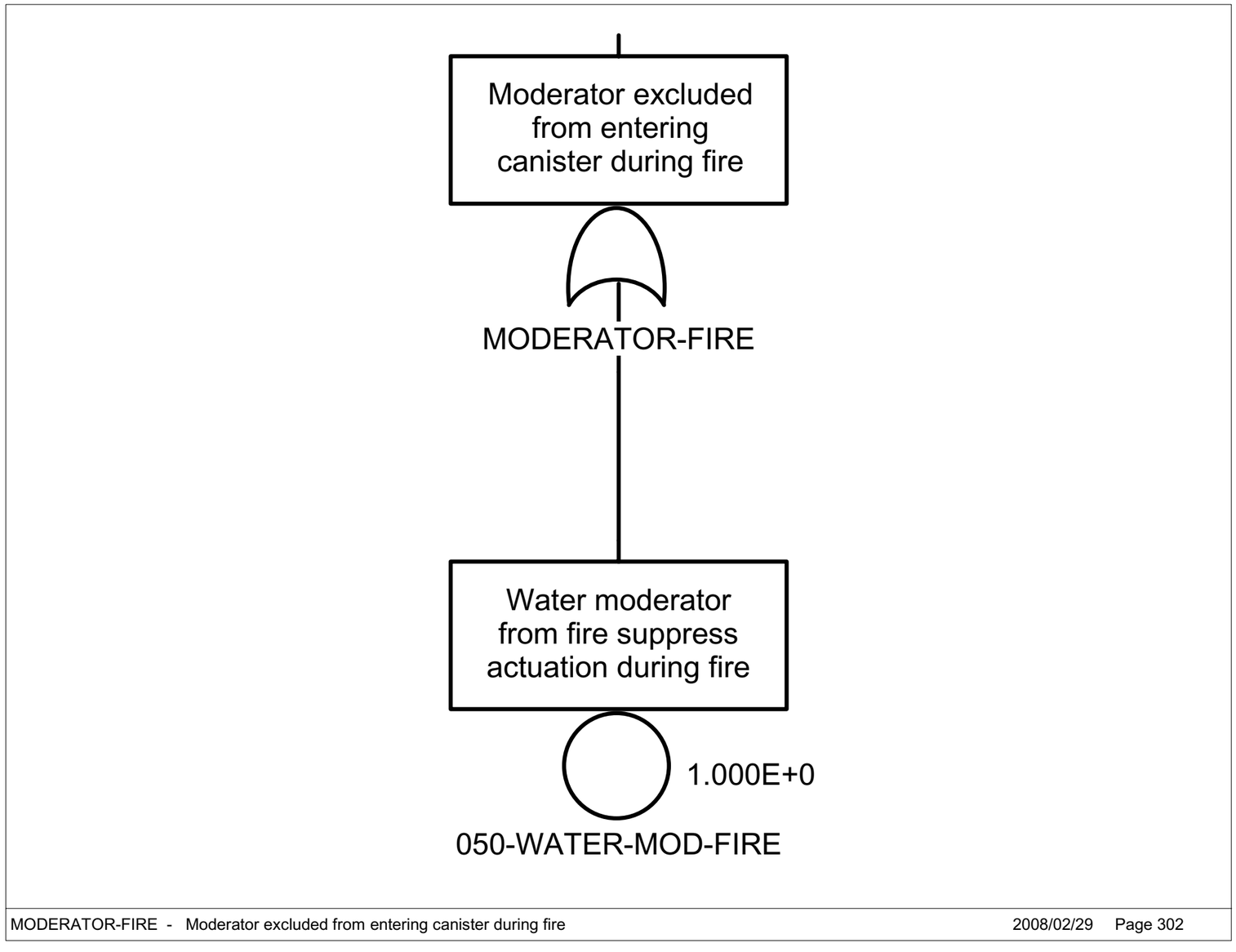
Figure B10.5-1 illustrates the possibility of a moderator source during normal operations in the WHF. Potential sources are: oil from the 200-ton crane gear box, water from an inadvertent activation of the fire suppression system, and other water sources in the facility (e.g., water pipes). Details on moderator source failures are addressed in Section 6.2.2.9.



Source: Original

Figure B10.5-1. Moderator Source (no fire)

Figure B10.5-2 addresses the possibility of a moderator entering a cask during a facility fire in the WHF.



Source: Original

Figure B10.5-2. Moderator Source (Fire)

B10.6 IMPACT TO CASK VALVE DURING PREPARATION ACTIVITIES

There is a valve on the outside of transportation casks that is used to inject cooling water. During cask preparation activities, the valve may be damaged either by dropping equipment on it from the jib crane or from direct impacts. Table B10.6-1 lists the fault trees that describe the cask valve impact events during WHF operations.

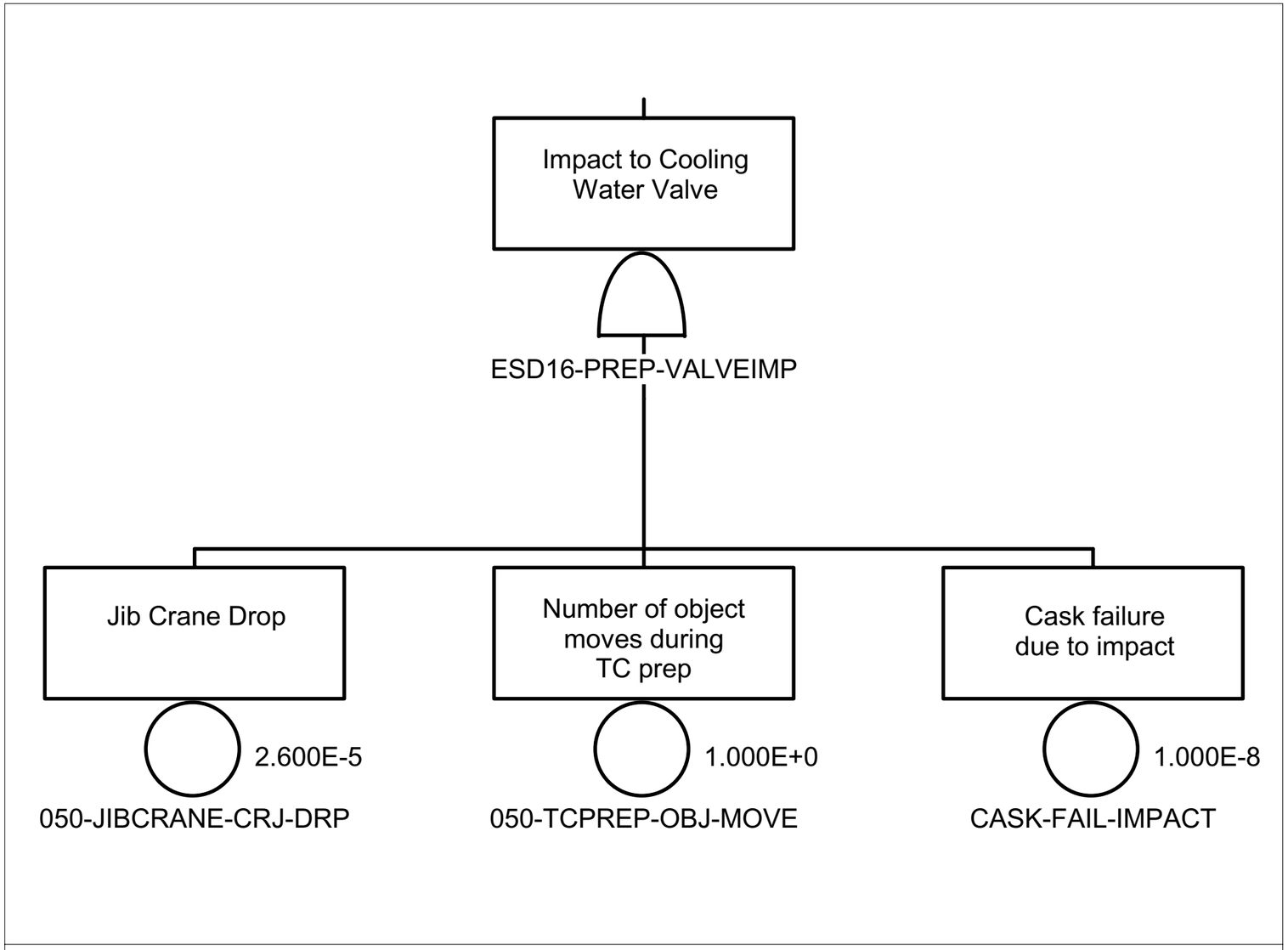
Table B10.6-1. Cask Valve Impact Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD16-PREP-VALVEIMP	ESD16-PREP-VALVEIMP	CSNF
ESD17-PREP-VALVEIMP	ESD17-PREP-VALVEIMP	DPC

NOTE: CSNF = Commercial Spent Nuclear Fuel; DPC = dual-purpose canister.

Source: Original

Figure B10.6-1 is a typical fault tree that addresses the events that could result in an impact to valve on the CSNF or DPC transportation cask during cask preparation activities in the WHF.



Source: Original

Figure B10.6-1. Typical Fault Tree for Cask Valve Impact During Cask Preparation Activities

B10.7 IMPACT OF SHIELD DOOR INTO CONVEYANCE

These fault trees describe collision of a moving shield door with the CTT or site transporter. Table B10.7-1 lists the fault trees that describe these impacts. The DPCs and TAD canisters may be transported in the WHF in transportation casks on a CTT or in aging overpacks on a site transporter

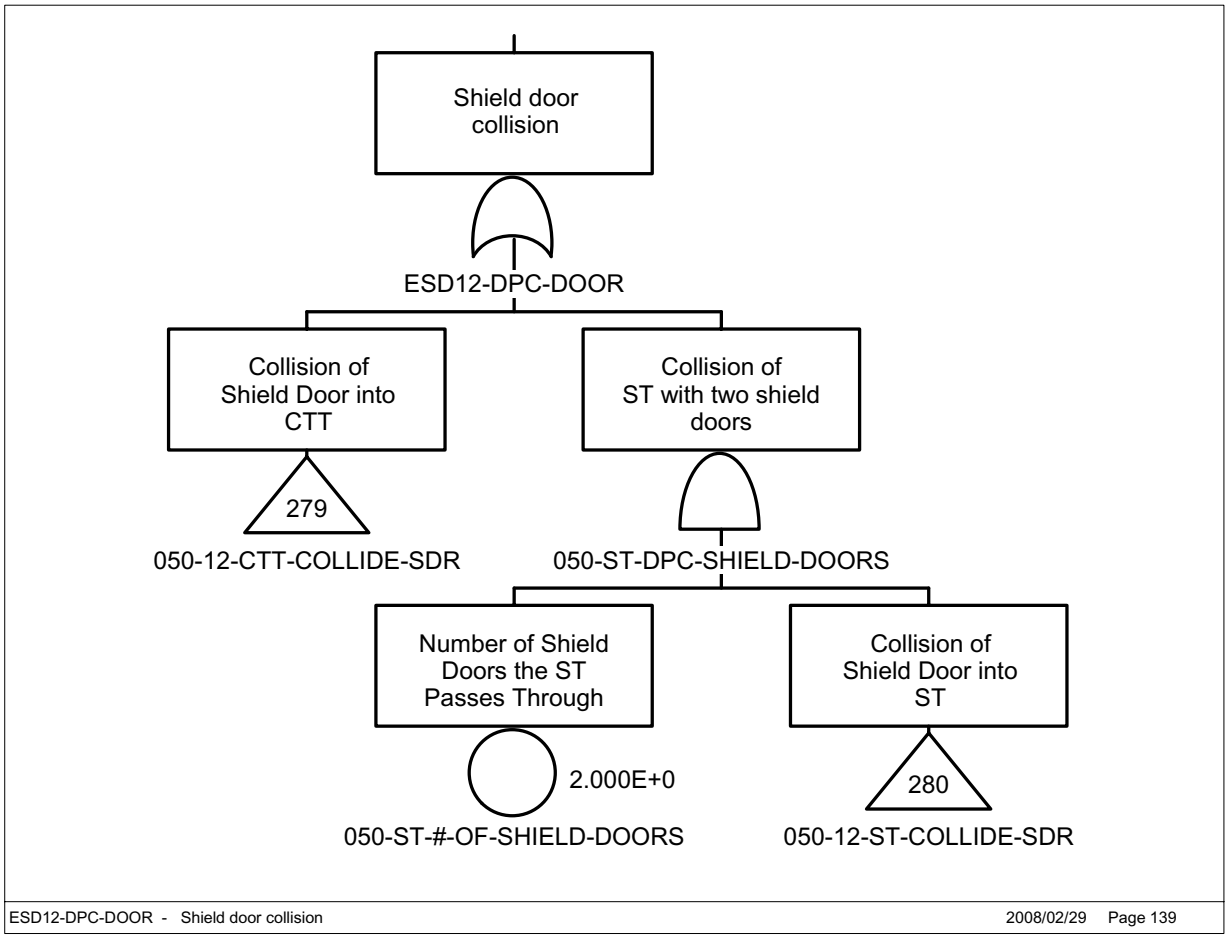
Table B10.7-1. Impact of Shield Door Fault Trees

ESD Designator	Fault Tree Name	Applies To
ESD12-DPC-DOOR	ESD12-DPC-DOOR	DPCs in transportation casks or AOs
ESD12-TAD-DOOR	ESD12-TAD-DOOR	TADs in transportation casks or AOs

NOTE: AO = aging overpack; DPC = dual-purpose canister; TAD = transportation, aging, and disposal canister.

Source: Original

Figure B10.7-1 illustrates the fault tree for shield door impact to a conveyance carrying a DPC. The DPC may be carried on a CTT or a site transporter where the site transporter passes through two shield doors and the CTT passes through one door. The same number of DPCs that are carried on a CTT are also carried on a site transporter. The fault trees for collision of the shield door into a CTT or ST are described in Attachment B3.



Source: Original

Figure B10.7-1. Impact of Shield Door into Conveyance with DPC

B10.8 DROP IF HIGH STAR CANISTER

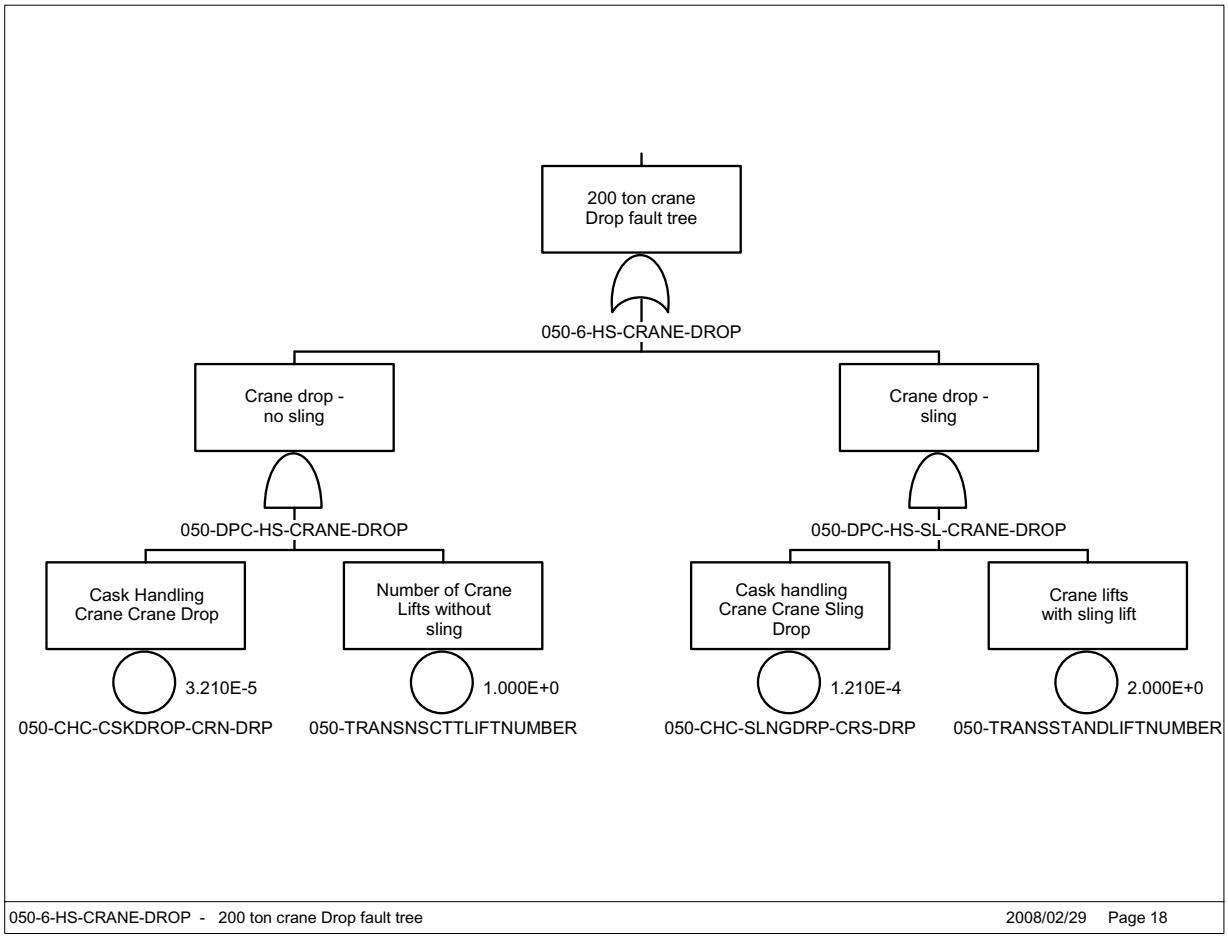
This fault tree describes dropping of a high star canister containing a DPC from a 200 ton handling crane with and without a sling lift. Table B10.8-1 lists the fault tree that describes this drop. Figure B10.8-1 illustrates the fault tree for dropping a high star canister.

Table B10.8-1. Drop of a High Star Canister Fault Tree

ESD Designator	Fault Tree Name	Applies To
ESD06-TTC-UP-DROP	050-6-HS-CRANE-DROP	DPCs in HSs

NOTE: DPC = dual-purpose canister; HS = High Star canister

Source: Original



Source: Original

Figure B10.7-2. Drop of High Star Canister

ATTACHMENT C
ACTIVE COMPONENT RELIABILITY DATA ANALYSIS

CONTENTS

Page

FIGURES

Page

TABLES

Page

ACRONYMS AND ABBREVIATIONS

Acronyms

CCF	common-cause failure
CTM	canister transfer machine
CTT	cask transfer trolley
DOE	U.S. Department of Energy
GROA	geologic repository operations area
HEPA	high-efficiency particulate air filter
HLW	high-level radioactive waste
HVAC	heating, ventilation, and air conditioning
MCC	motor control centers
MCO	multicanister overpack
NRC	U.S. Nuclear Regulatory Commission
PCSA	Preclosure Safety Analysis
PRA	probabilistic risk assessment
SFTM	spent fuel transfer machine
SNF	spent nuclear fuel
TEV	transport and emplacement vehicle
TYP	component type code
TYP-FM	component type and failure mode code
UPS	uninterruptible power supply
YMP	Yucca Mountain Project

Abbreviations

AC	alternating current
DC	direct current
hr	hour

ATTACHMENT C
ACTIVE COMPONENT RELIABILITY DATA ANALYSIS

The purpose of component-level reliability data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. In this report, the term data is taken to mean reliability data analyzed as part of the preclosure safety analysis (PCSA) from published sources. The fault tree models described in Section 4.3.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. This attachment provides a summary of the approach for developing these active component reliability estimates by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represented the range of the industry-wide information. The discussion also addresses the method used for estimating the probability of common-cause failures among multiple components. Finally, a table is given showing the template data values input to the Yucca Mountain Project (YMP) PCSA SAPHIRE models (Section 4.2).

C1 INDUSTRY-WIDE COMPONENT RELIABILITY DATA

While data from the facility being studied is the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP activities are atypical of nuclear power plant activities and no operating history exists, it was necessary to develop the required data from the experience of other industries.

C1.1 COMPONENT DEFINITION

The purpose of component-level data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. To do this, it is necessary to clearly define component types, boundaries, and failure modes. The system analysis fault tree basic events identify the component and failure mode combinations requiring data, and the analysts' descriptions provide an understanding of the component operating environments. In response to these identified data needs, the data analysts compile data at the component failure mode level for input to the SAPHIRE models. However, this is best achieved via an iterative process between the system and data analysts to ensure that all basic events are properly quantified with appropriate failure data estimates.

1. Component Type. Corresponds to the category of equipment at the level for which data is required by the logic model and at which data will be developed by the data analyst. Examples of such component types are motor-driven pumps, cameras, diesel generators, and heat exchangers. For certain complex components, a larger component type such as the canister transfer machine (CTM) is likely to be broken down by the system analyst in the logic model into constituent component types including motors and brakes, not only to facilitate the data analysis but to evaluate the contribution of various subcomponents to the overall component failure.

2. Component Boundaries. The boundary definition task is closely connected with the tasks of defining systems boundaries and fault tree construction. Therefore this task is performed jointly with the system analysts.

3. Failure Mode. Failure mode is defined as an undesirable component state (e.g., normally closed motor operated valve doesn't open on demand because of valve mechanical damage that occurred before the demand itself).

4. Selection of Model and Parameters. Stochastic models of failures of different systems component are defined for component failure probability estimation depending on the system operational mode. A set of available models is given in SAPHIRE for Windows and includes the following:

   A. Components of stand-by systems. The main parameter of stand-by system is the unavailability upon demand. Such system unavailability can be modeled by fault tree, where basic events probabilities are equal to system components unavailabilities averaged by time. This model treats the time to failure as a random value with exponential distribution. Such component unavailability is the function of time. In case of periodic test, unavailability is a periodic function of time. For simplifying the calculation, time dependency is usually replaced by the average value over the considered interval. For periodically tested components, the interval average is the average value for the test interval.

      Three types of stand-by system components are identified:

      1) Periodically tested stand-by components. For such components it is necessary to estimate following parameters: failure rate, probability of failure per demand, average restoring time (for repair), and average outage time due to test and maintenance.

      2) Non-tested stand-by component. For such components, the exposure time is set to unit projected operation time for calculation of unavailability. But often the component is tested indirectly or replaced. For example, if the system gets a real actuation signal, the state of the non-tested component can be determined. In this case, the average time to failure for a component is set to the average interval between system actuations. In some instances, the component can be replaced along with the tested components. In this case, test interval for non-tested component is set to average time to failure of tested component.

      3) Monitored components. State of some stand-by components is tested continuously (monitoring). In this case component failure is revealed immediately.

B. Components of systems in operation. For systems in operation, the most important parameter is the probability of failure during the defined mission time. This probability may be estimated based on fault trees or another logic model, where basic event probabilities are set to unavailabilities of components over the interval mission time. Failures of operating components are modeled using an exponentially distribution with a failure rate different from the failure rate in stand-by mode.

   Operating systems contain two main types of components: restorable and non-restorable.

   1) Non-restorable components. Components that cannot be restored in case of failure. Exponential distribution of time between failures for such components is characterized by failure rate, λ.

   2) Restorable components. Components that may be restored in case of failure. In this case restoration means restoration without outage of operation.

C. Stand-by systems following demand. Stand-by systems must fulfill a specific function during the defined time after successful start. During this time such systems are described in the same way as operating systems.

D. Constant probability per demand. The model treats component failure probability as a fixed probability for every demand. For such components, tests are excluded from consideration.

For YMP, the operational mode of failure and standby failures predominate; therefore, constant failure rates and constant probabilities per demand were constructed.

Component types and failure modes were initially identified based upon a listing of the components considered to be likely to be encountered in the analysis. This list was compiled from expertise in database development and familiarity with general component requirements in a variety of facilities. As the fault tree modeling progressed, this list was augmented and tailored to the specific active components included in the PCSA models based on the YMP design.

Correspondingly, it was necessary to develop an active component and failure mode coding scheme that would be consistent with the fault tree model basic events, the needs of the SAPHIRE models, as well as with standard repository naming conventions for YMP equipment types.

The YMP PCSA basic event naming convention was therefore developed to incorporate the following information in the 24 character basic event (BE) name (consistent with the BE field in SAPHIRE):

- Area code – physical design or construction area where a component would be installed
- System locator code – operational systems and processes

- Component function identifiers – component function
- Sequence code – numeric sequence and train assignment
- Component type code – three character identifier for general component type, such as battery, actuator, or pump
- Failure mode code – three character identifier for the way in which the component is considered in the fault tree models to have failed, (e.g., FTS for fails to start or FOD for fails on demand).

The area, system locator, and component function codes were obtained from engineering standards from the YMP repository as a whole to be consistent with overall site naming conventions. The sequence codes were taken from the component identification numbers on project drawings, if the design had progressed to that point at the time of the data development and modeling.

Active component type codes were developed to be consistent with the component function identifiers, but since the type codes were limited to three digits and the function identifiers were occasionally four-characters long, in some instances it was necessary to truncate the identifier to construct the type code.

Failure mode (FM) codes were developed using prior database conventions or abbreviations that would be as intuitively obvious as possible.

Both type (TYP) and FM were limited to three characters each in order to be consistent with the input constraints and conventions of the SAPHIRE template database feature, which allows the same component failure data to be applied to all items in the model.

A list of the component type and failure mode combinations is provided in Table C1.1-1.

Industry-wide data sources were then collected and reviewed to identify failure rates per hour or failure probabilities per demand that would be relevant to each of the 146 TYP-FM combinations.

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM)

TYP-FM	Component Name and Failure Mode
AHU-FTR	Air Handling Unit Failure to Run
ALM-SPO	Alarm/Annunciator Spurious Operation
AT-FOH	Actuator (Electrical) Failure
ATH-FOH	Actuator (Hydraulic) Failure
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation
AXL-FOH	Axle Failure
B38-FOH	Bearing Failure
BEA-BRK	Lifting Beam/Boom Breaks
BLD-RUP	Air Bag Ruptures

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name and Failure Mode
BLK-FOD	Block or Sheaves Failure on Demand
BRH-FOD	Brake (Hydraulic) Failure on Demand
BRK-FOD	Brake Failure on Demand
BRK-FOH	Brake (Electric) Failure
BRP-FOD	Brake (Pneumatic) Failure on Demand
BRP-FOH	Brake (Pneumatic) Failure
BTR-FOD	Battery No Output Given Challenge
BTR-FOH	Battery Failure
BUA-FOH	AC Bus Failure
BUD-FOH	DC Bus Failure
BYC-FOH	Battery Charger Failure
C52-FOD	Circuit Breaker (AC) Fails on Demand
C52-SPO	Circuit Breaker (AC) Spurious Operation
C72-SPO	Circuit Breaker (DC) Spurious Operation
CAM-FOH	Cam Lock Fails
CBP-OPC	Cables (Electrical Power) Open Circuit
CBP-SHC	Cables (Electrical Power) Short Circuit
CKV-FOD	Check Valve Fails on Demand
CKV-FTX	Check Valve Fails to Check
CON-FOH	Electrical Connector (Site Transporter) Failure
CPL-FOH	Coupling (Automatic) Failure
CPO-FOH	Control system Onboard (TEV or Trolley) Failure
CRD-FOH	Badge/Card Reader Failure
CRJ-DRP	Jib Crane Load Drop
CRN-DRP	200-Ton Crane Load Drop
CRN-TBK	200-Ton Crane Two-Blocking Load Drop
CRS-DRP	Crane using Slings Load Drop
CRW-DRP	Waste Package Crane Load Drop
CRW-TBK	Waste Package Crane Two-Blocking Load Drop
CSC-FOH	Cask Cradle Failure
CT-FOD	Controller Mechanical Jamming
CT-FOH	Controller Failure
CT-SPO	Controller Spurious Operation
CTL-FOD	Logic Controller Fails on Demand
DER-FOM	Derailment Failure per Mile
DG-FTR	Diesel Generator Fails to Run
DG-FTS	Diesel Generator Fails to Start
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days
DM-FOD	Drum Failure on Demand
DM-MSP	Drum Mis-spooling (Hourly)
DMP-FOH	Damper (Manual) Fails to Operate
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name and Failure Mode
DMS-FOH	Demister (Moisture Separator) Failure
DRV-FOH	Drive (Adjustable Speed) Failure
DRV-FSO	Drive (Adjustable Speed) Failure to Stop on Demand
DTC-RUP	Duct Ruptures
DTM-FOD	Damper (Tornado) Failure on Demand
DTM-FOH	Damper (Tornado) Failure
ECP-FOH	Position Encoder Failure
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)
FAN-FTR	Fan (Motor-Driven) Fails to Run
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand
FRK-PUN	Forklift Puncture
G65-FOH	Governor Failure
GPL-FOD	Grapple Failure on Demand
GRB-FOH	Gear Box Failure
GRB-SHH	Gear Box Shaft/Coupling Shears
GRB-STH	Gear Box Stripped
HC-FOD	Hand Held Radio Remote Controller Fails to Stop (on Demand)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation
HEP-LEK	Filter (HEPA) Leaks [Bypassed]
HEP-PLG	Filter (HEPA) Plugs
HOS-LEK	Hose Leaking
HOS-RUP	Hose Ruptures
IEL-FOD	Interlock Failure on Demand
IEL-FOH	Interlock Failure
LC-FOD	Level Controller Failure on Demand
LRG-FOH	Lifting Rig or Hook Failure
LVR-FOH	Lever (Two Position; Up-Down) Failure
MCC-FOH	Motor Control Centers (MCCs) Failure
MOE-FOD	Motor (Electric) Fails on Demand
MOE-FSO	Motor (Electric) Fails to Shut Off
MOE-FTR	Motor (Electric) Fails to Run
MOE-FTS	Motor (Electric) Fails to Start (Hourly)
MOE-SPO	Motor (Electric) Spurious Operation
MSC-FOH	Motor Speed Control Module Failure
MST-FOH	Motor Starter Failure
NZL-FOH	Nozzle Failure
PIN-BRK	Pin (Locking or Stabilization) Breaks
PLC-FOD	Programmable Logic Controller Fails on Demand
PLC-FOH	Programmable Logic Controller Fails to Operate
PLC-SPO	Programmable Logic Controller Spurious Operation
PMD-FTR	Pump (Motor Driven) Fails to Run
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name and Failure Mode
PPL-RUP	Piping (Lined) Catastrophic
PPM-PLG	Piping (Water) Plugs
PPM-RUP	Piping (Water) Ruptures
PR-FOH	Passive Restraint (Bumper) Failure
PRM-FOH	eProm (HVAC Speed Control) Failure
PRV-FOD	Pressure Relief Valve Fails on Demand
PV-SPO	Pneumatic Valve Spurious Operation
QDV-FOH	Quick Disconnect Valve Failure
RCV-FOH	Air Receiver Fails to Supply Air
RLY-FTP	Relay (Power) Fails to Close/Open
SC-FOH	Speed Control Failure
SC-SPO	Speed Control Spurious Operation
SEL-FOH	Speed Selector Fails
SEQ-FOD	Sequencer Fails on Demand
SFT-COL	Spent Fuel Transfer Machine Collision/Impact
SFT-DRP	Spent Fuel Transfer Machine Fuel Drop
SFT-RTH	Spent Fuel Transfer Machine Fuel Raised Too High
SJK-FOH	Screw jack (TEV) Failure
SRF-FOH	Flow Sensor Failure
SRP-FOD	Pressure Sensor Fails on Demand
SRP-FOH	Pressure Sensor Fails
SRR-FOH	Radiation Sensor Fails
SRS-FOH	Over Speed Sensor Fails
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand
SRT-FOH	Temperature Sensor/Transmitter Fails
SRT-SPO	Temperature Sensor Spurious Operation
SRU-FOH	Ultrasonic Sensor Fails
SRV-FOH	Vibration Sensor (Accelerometer) Fails
SRX-FOD	Optical Position Sensor Fails on Demand
SRX-FOH	Optical Position Sensor Fails
STU-FOH	Structure (Truck or Railcar) Failure
SV-FOD	Solenoid Valve Fails on Demand
SV-FOH	Solenoid Valve Fails
SV-SPO	Solenoid Valve Spurious Operation
SWA-FOH	Switch, Auto-Stop Fails (CTT end of Hose Travel)
SWG-FOH	13.8kV Switchgear Fails
SWP-FTX	Electric Power Switch Fails to Transfer
SWP-SPO	Electric Power Switch Spurious Transfer
TD-FOH	Transducer Failure
TDA-FOH	Transducer (Air Flow) Failure
TDP-FOH	Transducer (Pressure) Fails
TDT-FOH	Transducer (Temperature) Fails

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name and Failure Mode
THR-BRK	Third Rail Breaks
TKF-FOH	Fuel Tank Fails
TL-FOH	Torque Limiter Failure
TRD-FOH	Tread (Site Transporter)
UDM-FOH	Damper (Backdraft) Failure
UPS-FOH	Uninterruptible Power Supply (UPS) Failure
WNE-BRK	Wire Rope Breaks
XMR-FOH	Transformer Failure
XV-FOD	Manual Valve Failure on Demand
ZS-FOD	Limit Switch Failure on Demand
ZS-FOH	Limit Switch Fails
ZS-SPO	Limit Switch Spurious Operation

NOTE: AC = alternating current; DC = direct current; CTT = cask transfer trailer; HEPA = high efficiency particulate air (filter); HVAC = heating, ventilation, and air conditioning; MCC = motor control center; TEV = transport and emplacement vehicle; UPS = uninterruptible power supply.

Source: Original

C1.2 INDUSTRY-WIDE RELIABILITY DATA

Industry-wide data sources are documents containing industrial or military experience on component performance. Usually they are previous safety/risk analyses and reliability studies performed nationally or internationally, but they can also be standards or published handbooks. For the YMP PCSA, an industry-wide database was constructed using a library of industry-wide data sources of reliability data from nuclear power plants, equipment used by the military, chemical processing plants, and other facilities. The sources used are listed in Table C1.2-1.

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
Guidelines for Process Equipment Reliability Data with Data Tables. [CCPS] (Ref. C5.1)
Savannah River Site, Generic Data Base Development (U) [SRS Reactors] (Ref. C5.5)
The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve Component. NUREG/CR-3154 (Ref. C5.6)
Waste Form Throughputs for Preclosure Safety Analysis.[BSC 2007](Ref. C5.7)
Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report. [EPRI PRA] (Ref. C5.8)
Component Failure and Repair Data for Coal-Fired Power Units. EPRI AP-2071 [EPRI Pipe Failure Study] (Ref. C5.10)
Mechanical Reliability: Theory, Models and Applications. [AIAA] (Ref. C5.11)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
Military Handbook, Reliability Prediction of Electronic Equipment. MIL-HDBK-217F [MIL-HDBK-217F] (Ref. C5.12)
The In-Plant Reliability Data Base for Nuclear Power Plant Components - Pump Component. NUREG/CR-2886. (Ref. C5.13)
Some Published and Estimated Failure Rates for Use in Fault Tree Analysis [DuPont] (Ref. C5.14)
Analysis of Station Blackout Risk. Volume 2 of Reevaluation of Station Blackout Risk at Nuclear Power Plants. NUREG/CR-6890 (Ref. C5.15)
Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants. NUREG/CR-6928. (Ref. C5.16)
"Train Accidents by Cause from Form FRA F 6180.54." [Federal Railroad Administration] (Ref. C5.17)
Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999. [McKenna] (Ref. C5.20)
Ruggedized Card Reader/Ruggedized Keypad Card Reader. [HID] (Ref. C5.21)
IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. [IEEE-493] (Ref. C5.22)
IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations. [IEEE-500] (Ref. C5.23)
The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report- Diesel Generators, Batteries, Chargers and Inverters. NUREG/CR-3831 (Ref. C5.24)
Instruments and Software Solutions (for Emergency Response and Health Physics [LAURUS] (Ref. C5.25)
A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002. NUREG-1774. (Ref. C5.26)
Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980. NUREG/CR-1363 (Ref. C5.28)
The Reliability Data Handbook. [Moss] (Ref. C5.32)
Control of Heavy Loads at Nuclear Power Plants. NUREG-0612. (Ref. C5.35)
Handbook of Reliability Prediction Procedures for Mechanical Equipment [NSWC-98-LE1] (Ref. C5.37)
"Using the EDA to Gain Insight into Failure Rates" [Rand] (Ref. C5.38)
Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data. NUREG/CR-4639, (Ref. C5.39)
Nonelectronic Parts Reliability Data 1995. NPRD-95. [NPRD -95] (Ref. C5.40)
Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment. [SAIC Umatilla] (Ref. C5.41)
Offshore Reliability Data Handbook. 2nd Edition [OREDA-92] (Ref. C5.42)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
Offshore Reliability Data Handbook. 4th Edition. [OREDA-2002] (Ref. C5.43)
Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1972-April 30, 1980. NUREG/CR-1205. (Ref. C5.45)
N-Reactor Level 1 Probabilistic Risk Assessment: Final Report. [N-Reactor] (Ref. C5.46)

NOTE: The code in brackets [XXXX] is used to aid the reader in identifying references in Table C4-1.

Source: Original

It was necessary to analyze the industry-wide data to compare the relevancy of the component data selected from the industry-wide data sources with the equipment in the YMP PCSA models.

The data source scope had to be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might have been used for electronics data versus mechanical data, so long as its use was justified by the detail and the applicability of the information provided. Lastly, the quality of the data source was considered to be a measure of the source's credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort was made to use the highest quality data source available for each active component type and failure mode.

Data were selected from the industry-wide data sources using the following criteria:

- The component type (TYP) and FM identified in the data source had to match those in the basic events specified in the fault tree. For every component modeled, a comparison was made between the modeled component and the component found in the data source to ensure its suitability for the PCSA. Also, every attempt was made to match the failure modes. Often, the source described the failure mode as "all modes," whereas the fault tree required "fails to operate." In cases such as this, sources with more general failure modes were not used unless they were the only available sources.

- The data source had to be widely available, not proprietary. This ensured traceability and accessibility.

- Mid level or low level quality data sources were used only when high level sources were not available.

- The operating environment is an important factor in the selection of data sources. The environment of a component refers not only to its physical state, but also its operational state. The operating conditions of a component include the plant's maintenance policy and testing policy. If either of these states differed from the modeled facility's state, then the data were reconsidered and usually rejected (unless no alternative existed).

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, was to evaluate the similarity between the YMP operating environment and that represented in each generic data source to ensure data appropriateness.

An example of how data were retrieved from the various data sources is described in the following example for check valves. The failure modes modeled in the PCSA for the check valve are fails per hour (FOH), fails to check (FTX), leaks (LEK), and spurious operation (SPO).

Table C1.2-2 shows a comparison between the failure rates for the check valve and its failure modes from three different industry-wide data sources.

Table C1.2-2. Data Source Comparison for Check Valve

Data Source	Equipment Description	Failure Modes	Data Values Provided	Equipment Boundary Given?	Taxonomy Given?
(Ref. C5.1)	Valve-non-operated, Check	• Fails to Check • Significant Back Leakage	Lower, Mean, Upper	Yes	Yes
(Ref. C5.23)	Driven Equipment Valves, Check	"All Modes"	Low, Recommended, High	No	Yes
(Ref. C5.5)	Check	• Fails to Open • Fails to Close • Plugs • Internal Leakage • Internal Rupture • External Leakage • External Rupture	Mean	No	No

NOTE: AIChE = American Institute of Chemical Engineers; IEEE = Institute of Electrical and Electronics Engineers.

Source: Original

Table C1.2-3 shows actual numbers extracted from industry-wide data sources for five failure modes for check valves.

Table C1.2-3. Failure Rates Extracted from Various Data Sources for Check Valve

Failure Mode Description	Failure Mode Code	Data Source	Lower	Median	Upper	EF
Fails to Close (Hourly)	FOH	(Ref. C5.5)	1.27 × 10-7	7.74 × 10-7	4.70 × 10-6	6.1
Leaks	LEK	(Ref. C5.5)	6.98 × 10-7	3.49 × 10-6	1.75 × 10-5	5.0
Fails to Open (Hourly)	FOH	(Ref. C5.5)	1.27 × 10-7	7.74 × 10-7	4.70 × 10-6	6.1
Transfers Closed	SPO	(Ref. C5.23)	8.00 × 10-8	7.81 × 10-7	3.27 × 10-4	5.0
Transfers Open	SPO	(Ref. C5.23)	8.00 × 10-8	7.81 × 10-7	3.27 × 10-4	5.0

NOTE: EF = error factor.

Source: Original

At this stage of the analysis, it remains to decide which data is appropriate to keep and include in the data pool and which are discarded. The criteria for this process are discussed below.

The guidelines shown in Table C1.2-4 are based on observations of the analysts of their preferences and rationales during the data selection process among the data available at the time.

Table C1.2-4. Guidelines for Industry-wide Data Selection

Data Selection Guidelines	
1.	Preference for greater than zero failures (but not always able to exclude on this basis)
2.	Population of at least 5
3.	Denominator greater than 1,000 hours or 100 demands
4.	If mean or median values, some expression of uncertainty surrounding these values (either upper or lower bounds or lognormal error factor)
5.	Data analyst's confidence in the applicability of the data to the YMP based on: • Component design • Driver/operator • Size • Component application • Active versus passive service • Materials/fluids moved (e.g., water versus caustic versus viscous) • Component boundary • What's included and excluded in component definition (e.g., motor, electrical connections) • Failure modes • Operating environment • Physical (e.g., heat, humidity, corrosive) • Functional (e.g., operation, maintenance, and testing frequency)

NOTE: YMP = Yucca Mountain Project.

Source: Original

Given the fact that the YMP will be a relatively unique facility (although portions will be similar to the spent fuel handling and aging areas of commercial nuclear plants), the data development perspective was to collect as much relevant industry-wide failure estimate information as possible to cover the spectrum of equipment operational experience. It is assumed that the YMP equipment would fall within this spectrum (Assumption 3.2.1). The scope of the sources

selected for this data set was deliberately broad to increase the probability that YMP operational experience would fall within the bounds. A combined estimate that reflected the uncertainty ranges defined by the data source values was developed. This process is addressed further in the Bayesian estimation Section C2.

Every attempt was made to find more than one data source for each TYP-FM, although the unique nature of many equipment types made this difficult. Data was extracted from several sources in many cases, then combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs were quantified with one data source, 8% with two data sources, 8% with three data sources, and 31% with four or more data sources.

C1.3 CRANE AND SPENT FUEL TRANSFER MACHINE DROP ESTIMATES

Industry-wide data was used to quantify the likelihood of experiencing a drop from the 200-ton crane while handling waste forms and their associated containers and for estimating drop probability for jib cranes and cranes used to maneuver waste packages. In addition, drop likelihoods for the spent fuel transfer machine (SFTM) were estimated using industry-wide data.

The rationale for using industry-wide data for these estimates was that a significant amount of crane experience exists within the commercial nuclear power industry and other applications and that this experience could be used to bound the anticipated crane performance at YMP. Further, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants.

Handling incidents that resulted in a drop were included in the drop probability regardless of cause; they may have been caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

The industry-wide data for cranes was taken from NUREG-0612 (Ref. C5.35), *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774 (Ref. C5.26), and the *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8). NUREG-0612 (Ref. C5.35) has several appendices that contain crane data from the Occupational Safety and Health Act Administration, the U.S. Navy, Waste Isolation Pilot Plant, Licensee Event Reports, and from the results of a fault tree analysis. The *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8) provides estimates from Savannah River Site crane experience in addition to fault tree analysis. Crane failure information was also obtained from quantitative risk study performed for the U.S. Army chemical weapons destruction program (Ref. C5.41).

The information from each of these sources was evaluated in terms of quality, applicability to YMP, and to ensure that the events cited included both equipment failures and human failures. For the industry-wide data provided in terms of the number of events, another major factor was the ability to reasonably and justifiably estimate a meaningful denominator of number of lifts

(demands) conducted by the crane population considered in the data source. If this could not be done, the source information could not be used.

A key consideration in evaluating the industry-wide crane data for the 200-ton cranes was the NOG-1 (Ref. C5.3) design requirements that will be placed upon the YMP cranes versus the crane design features reflected in the input data sources. NUREG-1774 (Ref. C5.26, Table 12, pp. 61 to 63) provides a list of the nuclear power plants that had upgraded their cranes to single-failure-proof status consistent with licensee response to U.S. Nuclear Regulatory Commission (NRC) *NRC Bulletin 96-02* (Ref. C5.9) which requested specific information relating to their heavy loads programs and plans consistent with the recommendations of NUREG-0554 (Ref. C5.34). This information was used to constrain the denominator of the number of very heavy load lifts from NUREG-1774 (54,000) by using a percentage of percent of nuclear power plants reporting single failure proof cranes out of total plants (42/110).

Conversely, a separate category of non-single-failure-proof cranes for the waste package manipulating cranes was developed using the remaining percentage (68/110) to adjust the number of lifts. The jib crane lifts were estimated using the NUREG-1774 (Ref. C5.26, Appendix D) table of the types of cranes involved in accidents; mobile and tower cranes using jibs are cited as being involved in ~76% of accidents while bridge and gantry (used for very heavy loads) are ~19%. The percentage of accidents that did not involve jib cranes was therefore believed to reside somewhere between 19% and 24% (100% to 76%). So, the 20,620 lifts estimated for very heavy loads by single failure proof cranes was divided by 21.2% to yield a round number estimate of 97,250 jib crane lifts.

The number of crane drop incidents used as the numerator of the 200-ton crane drop estimate from NUREG-1774 (Ref. C5.26) was also restricted to those involving very heavy loads (defined in NUREG-1774 as >30 tons) of single-failure-proof cranes. Drops occurring during sling lifts were parsed into a separate category and used to estimate the sling lift-related drop likelihood.

Load drop likelihood due to two-blocking was also estimated using industry-wide data. NUREG-0612 (Ref. C5.35) describes a two-blocking event as: "The act of continued hoisting to the extent that the upper head block and the load block are brought into contact, and unless additional measures are taken to prevent further movement of the load block, excessive loads will be created in the rope reeving system, with the potential for rope failure and dropping of the load." Two-blocking events in the various data sources were evaluated based upon the type of crane involved, as was done for the drop likelihood estimates.

As a result, several categories of crane drop estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

CRN-DRP	200-ton Crane Load Drop	3.2E-05/demand
CRN-TBK	200-ton Crane Two Block Causing Load Drop	4.4E-07/demand
CRS-DRP	200-ton Crane using Slings Load Drop	1.2E-04/demand
CRJ-DRP	Jib Crane Load Drop	2.6E-05/demand
CRW-DRP	Waste Package Crane (Not Single Failure Proof) Load Drop	1.1E-04/demand

CRW-TBK	Waste Package Crane (Not Single Failure Proof) Two Block Causing Load Drop	4.5E-05/demand

In each of these cases, as with the other active component reliability estimates, an effort was made to include a variety of operating experience and combine it together using a parametric empirical Bayes approach. However, for the CRS, CRJ and CRW estimates, since only NUREG-1774 (Ref. C5.26), data was considered to be applicable, a Jeffrey's non-informative prior approach for the Beta distribution was used, since the estimates were per lift (demand).

These crane incident estimates were combined in the SAPHIRE models with the number of estimated YMP crane lifts.

One potential issue regarding the applicability of the industry-wide crane data was the inclusion of hard-wired interlock features on the YMP cranes that might not exist at the nuclear power plants or naval installations from which the industry-wide experience resulted. In other instances, there was concern that interlocks included in the design for use in normal operations, on grapples to verify installation or engagement, could be defeated during maintenance actions where bypasses are permitted to move tools or pallets, since a particular grapple interlock is not standard in industry but is unique to YMP. Further, PCSA is not crediting the grapple interlock function and it was considered that having such interlocks in place would not make the estimated failure probability worse. Therefore the estimates from industry-wide data were considered to be reasonable in that they provided experience-based and perhaps somewhat pessimistic measures of anticipated crane performance.

Estimates were also developed from industry-wide data source information for the likelihood of SFTM drop, collision, and raising the fuel too high but not dropped (for potential personnel exposure considerations). The primary source for this information was NUREG-1774 (Ref. C5.26, Table 4), which provides brief descriptions of SFTM incidents at U.S. nuclear power plants from 1968 through 2002. A separate study (McKenna/Framatome) (Ref. C5.20) was reviewed, which also included SFTM incidents at U.S. nuclear power plants categorized in terms of Human Error, Equipment Failure, or Misload. Some of these were the same incidents included in NUREG-1774 (Ref. C5.26) so care was taken not to double-count any events. Each of the incidents described was reviewed in detail to evaluate their relevance to the failure modes of interest to the study and their applicability to spent fuel transfers. Incidents related to all types of fuel transfers, such as refueling or new fuel receipt, were used to estimate upper bounds (95th percentiles of a lognormal distribution) and to develop the error factor uncertainty information input to SAPHIRE along with the mean value.

It should be noted that events prior to 1985 were removed from consideration since the number of plants in operation (and therefore the number of lifts per year) would significantly differ from that cited in McKenna/Framatome (Ref. C5.20). Also, McKenna/Framatome stated that reporting practices were inconsistent prior to 1985.

The number of fuel movements used as the denominator of the SFTM estimates was based upon information from McKenna/Framatome (Ref. C5.20), which gave 1,198,723 fuel movements for the 15 year study data window, from 1985 through 1999, or a rough estimate of 79,914.87 per year. Since the numerator information from NUREG-1774 (Ref. C5.26) was based upon

17 years of data, from 1985 through 2002, the estimated denominator was calculated for consistency as 79,914.87×17 or 1,358,553 SFTM lifts.

As a result, several categories of SFTM event estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

SFT-COL	SFTM Collision/Impact	2.9E-06/demand
SFT-DRP	SFTM Load Drop	5.2E-06/demand
SFT-RTH	SFTM Fuel Raised Too High (but not dropped)	7.4E-07/demand

These SFTM incident estimates were combined in the SAPHIRE models with the number of estimated YMP fuel assembly transfers, specifically: 66,188 based on two transfers each of 33,094 assemblies (Ref. C5.7, Table 4, pg. 27).

The results of the industry-wide data search are documented, organized by component type and failure mode, and can be found in the Excel spreadsheet file "YMP Active Comp Database.xls", located on the CD in Attachment H.

C2 BAYESIAN DATA COMBINATION

The application of industry-wide data sources or expert elicitation introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes' theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

A typical application of Bayes' theorem is illustrated as follows: a failure rate for a given component is needed for fault tree (e.g., a fan motor in the heating, ventilation, and air conditioning (HVAC) system). There is no absolute value but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying λj data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.

2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trial if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur in over a certain exposure, operational, or test duration.

3. Update the probability distribution for the failure rate based on the new body of evidence using the mathematical expression of Bayes' theorem.

The mathematical expression for applying Bayes' theorem to data analysis is briefly described here. Let λ_j be one failure rate of a set of possible failure rates of the fan motor (component j). Initially, the state of knowledge of the "true value" of λ_j is expressed by the probability distribution $P(\lambda)$, the "prior." The choice of the analytic or discrete form of the prior distribution is made by the data analyst. Let E be a new body of evidence, e.g., a new set of test data or field observations. The new evidence improves the data analyst's state of knowledge. The revised, or "updated," probability distribution for the "true value" of λ_j is represented as $P(\lambda_j|E)$. Bayes' theorem gives:

$$P(\lambda_j \mid E) \quad \frac{P(\lambda_j)L(E \mid \lambda_j)}{\sum_j P(\lambda_j)P(E \mid \lambda_j)} \qquad \text{(Eq. C-1)}$$

In summary, Equation C-1 states that the knowledge of the "updated" probability of λ_j, given the new information E, equals the "prior" probability of λ_j before any new information times the likelihood function, $L(E/\lambda_j)$. The likelihood function expresses the probability of observing the number of failures in the evidence if the failure rate λ_j has a certain value. The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The numerator in Equation C-1 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of λ_j equals unity.

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in NUREG/CR-6823 (Ref. C5.4). For the YMP PCSA, the method known as "parametric empirical Bayes" was used. This permitted a variety of different sources to be statistically combined and compared, whether the inputs were expressed as the number of failures and exposure time or demands, or as a mean and error factor. Examples of the methods used for several combinatorial cases are provided below.

C2.1 PARAMETER ESTIMATION USING DATA FROM DIFFERENT SOURCES

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution, *g*, representing the source-to-source variability, also called population variability, of the component reliability (Ref. C5.4, Section 8.1). The objective of this section is to outline the methodology for developing the population-variability distribution of active components in the preclosure safety analysis. In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. This distribution is to be updated, as operating experience becomes available, to produce a reliability distribution specific to the component operated under geologic repository operations area (GROA) conditions. For the time being however, the components anticipated for use at the GROA are yet to be procured and operated. As a consequence, the population-variability distributions developed in this section both aim at and are limited to encompassing the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the preclosure safety analysis. As indicated in "Bayesian Parameter Estimation in Probabilistic Risk Assessment." (Ref. C5.44, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example, the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

Applying the parametric empirical Bayes method requires first to categorize the reliability data sources into two types: those that provide information on exposure data (i.e., the number of failures that were recorded over an exposure time (in case of a failure rate) or over a number of demands (in case of a failure probability), and those that do not provide such information). In the latter case, reliability estimates for a failure rate or failure probability are provided in the form of a mean or a median value, along with an uncertainty estimate, typically an error factor.

For each data source, the reliability information about a component's failure rate of failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. C5.44, Section 4.2). When no exposure data are available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution ((Ref. C5.44, Section 4.4) and (Ref. C5.27, pp. 312, 314, and 315)).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. C5.4, Section 8.2.1), which have the advantage of resulting in relatively simpler

calculations. This technique however is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of "The Combined Use of Data and Expert Estimates in Population Variability Analysis,"(Ref. C5.27, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the population-variability distribution in its lognormal form is noted $g(x,\nu,\tau)$, where x is the reliability parameter for the component (failure rate or failure probability), and ν and τ, the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided in the latter case that any tail truncation above $x = 1$ has a negligible effect (Ref. C5.44, p. 99). The validity of this can by confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98 percent of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

To determine ν and τ, it is first necessary to express the likelihood for each data source as a function of ν and τ only (i.e., unconditionally on *x)*. This is done by integrating, over all possible values of x, the likelihood function evaluated at x, weighted by the probability of observing x, given ν and τ. For example, if the data source *i* indicates that r failures of a component occurred out of n demands, the associated likelihood function $L_i(\nu,\tau)$, unconditional on the failure probability x, is as follows:

$$L_i(\nu,\tau) \quad \int_0^1 Binom(x,r,n) \times g(x,\nu,\tau)dx \qquad \text{(Eq. C-2)}$$

where $Binom(x,r,n)$ represents the binomial distribution evaluated for r failures out of n demands, given a failure probability equal to x, and $g(x,\nu,\tau)$ is defined as previously indicated. This equation is similar to that shown in "Bayesian Parameter Estimation in Probabilistic Risk Assessment." (Ref. C5.44, Equation 37). If the component reliability was expressed in terms of a failure rate and the data source provided exposure data, the binomial distribution in Equation C-2 would be replaced by a Poisson distribution. If the data source provided expert opinion only (no exposure data), the binomial distribution in Equation C-2 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine ν and τ (Ref. C5.44, p. 101). The maximum likelihood estimators for ν and τ are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each data source (Ref. C5.27, Equation 4). To find the maximum likelihood estimators for ν and τ, it is equivalent

and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of ν and τ completely determines the population-variability distribution *g* for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution *g*, which are calculated using the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to $\exp(\nu + \tau^2/2)$ and the error factor is equal to $\exp(1.645 \times \tau)$.

The selection of the parametric empirical Bayes method to determine the population-variability distribution is now discussed. This method provides a single "best" solution, while other techniques, such as the hierarchical Bayes method (Ref. C5.4, Section 8.3) differ by using a weighted mix of distributions of the chosen model, which incorporate epistemic (state of knowledge) uncertainty about the model. The parametric empirical Bayes method does not embed epistemic uncertainty but was nevertheless employed because of its satisfactory results for the majority of active components modeled in the preclosure safety analysis. The general adequacy of the method was confirmed by comparing its results to those obtained based on an example using a state-of-knowledge-informed approach (Ref. C5.27). The example involves twelve hypothetical data sources, each documenting the failure rate of motor-driven pumps either in terms of expert judgment or exposure data (Ref. C5.27, Table 1). Table C2.1-1 compares the percentiles predicted by the parametric empirical Bayes method and those found in "The Combined Use of Data and Expert Estimates in Population Variability Analysis." (Ref. C5.27, Table 4). Overall, the percentiles appear to be similar, with a key metric of the distributions, their mean, being nearly identical, and the medians being comparable. Percentiles at the tails of the distributions show more differences, the parametric empirical Bayes method yielding a population-variability distribution more spread out overall than the state-of-knowledge-informed distribution (Ref. C5.27).

Table C2.1-1. Comparison of Results of Parametric Empirical Bayes and Results Reported by Lopez Droguett et al.

Population-Variability Value	Parametric Empirical Bayes Method[a]	Lopez Droguett Results[b]
Mean	6.00×10^{-5}	6.05×10^{-5}
1st percentile	1.32×10^{-7}	3.16×10^{-7}
5th percentile	4.75×10^{-7}	1.38×10^{-6}
10th percentile	9.38×10^{-7}	2.67×10^{-6}
50th percentile (median)	1.04×10^{-5}	1.61×10^{-5}
90th percentile	1.14×10^{-4}	7.79×10^{-5}
95th percentile	2.26×10^{-4}	1.36×10^{-4}
99th percentile	8.10×10^{-4}	4.85×10^{-4}

NOTE: [a] Derivation of the results is given in the following section, Example of Development of Population-Variability Distribution.

[b] "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety, 83* (Ref. C5.27, Table 1)

Source: (Ref. C5.27, Table 1).

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom," *Reliability Engineering and System Safety, 47* (Ref. C5.19, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between 2×10^{-8}/hr (5th percentile) and 6×10^{-5}/hr (95th percentile). Using the definition of the error factor given in NUREG/CR-6823, (Ref. C5.4, Section A.7.3), this corresponds to an error factor of $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} \quad 55$. Therefore, in the preclosure safety analysis, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55 are too diffuse to adequately represent the population-variability distribution of a component. In such instances (two such cases in the entire PCSA database, when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution and therefore is unaffected by the value taken by the error factor. Based on NUREG/CR-6823, (Ref. C5.4, Section A.7.3), the median is calculated as exp(ν), where ν is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the preclosure safety analysis is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in NUREG/CR-6823, (Ref. C5.4, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for a component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using a data source that yields a more diffuse likelihood. In the other cases, the lognormal distribution approximately encompasses the likelihood functions yielded by the data sources, showing that the parametric empirical Bayes method is adequate. An illustration of a graph plotting the population-variability distribution along with the likelihood functions from data, based on the example of the Lopez Droguett et al. paper (Ref. C5.27) is provided below.

Example of Development of Population-Variability Distribution

Mathcad is used to calculate the population-variability distribution of active components. An illustration of such a calculation is given using the example in "The Combined Use of Data and Expert Estimates in Population Variability Analysis." (Ref. C5.27, Table 1). In this example, several data sources supply information about the reliability of motor-driven pumps, as follows:

Four data sources supply point estimates of the failure rates, along with a range (error) factor. This information is given in the following matrix, where the first column contains the estimated hourly failure rate (considered to be a median value) and the second column the associated error factor:

$$A := \begin{pmatrix} 3.0 \cdot 10^{-5} & 5 \\ 2.1 \cdot 10^{-5} & 3 \\ 2.0 \cdot 10^{-5} & 10 \\ 2.53 \cdot 10^{-5} & 10 \end{pmatrix}$$

In addition, eight data sources supply exposure data, which are given in the following matrix, where a recorded number of failures is shown in the first column, and the associated operating time (in hours) is shown in the second.

$$B := \begin{pmatrix} 0 & 76000 \\ 0 & 152000 \\ 0 & 74000 \\ 2 & 74000 \\ 0 & 48000 \\ 3 & 76000 \\ 9 & 10200 \\ 2 & 48000 \end{pmatrix}$$

The population-variability distribution g of the failure rate x is approximated by a lognormal distribution whose unknown parameters, ν and τ, respectively the mean and standard deviation of the associated normal distribution, are to be determined. Calculating ν and τ involves calculating the likelihood function associated with the reliability information in each data source. This is done as follows:

For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate x, and characterized by its median value and associated error factor shown in the matrix A. In Mathcad, the parameters required for defining a lognormal distribution are the mean and standard deviation of the associated normal distribution. Based on the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3), the mean of the associated normal distribution is the natural logarithm of the median failure rate, and the standard deviation of the associated normal distribution is $\ln(EF)/1.645$, where EF is the error factor.

Because the unknowns to be determined are ν and τ, the likelihood function is expressed as a function unconditional on the value of x. This is done by integrating the likelihood function over all possible values of x (i.e., theoretically, from 0 to infinity) and weighting by the probability of having a value of x, conditional on observing ν and τ. In practice, to facilitate the numerical integration on Mathcad, the integration is performed on a range that encompasses credible values

for x. In this example, the failure rate range considered varies from 10^{-8}/hr to 10^{-2}/hr. Thus, the likelihood functions, unconditional on x, for each of the data source in the matrix A, are calculated as follows:

$$a := 1..4 \qquad fe(a,x) := dlnorm\left(x, ln\left(A_{a,1}\right), \frac{ln\left(A_{a,2}\right)}{1.645}\right) \qquad \text{(Eq. C-3)}$$

$$LA(a, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fe(a,x) \cdot dlnorm(x, \nu, \tau)\, dx \qquad \text{(Eq. C-4)}$$

(In the above formulas, a is an index used to particularize a likelihood function to a data source in the matrix A.)

For a data source providing exposure data (given in the form of a number n of recorded failures over an exposure time t), the likelihood function is a Poisson distribution, expressing the probability that n failures are observed when the expected number of failures is x times t. Here also, the likelihood needs to be expressed as a function unconditional on the failure rate x, which is done by integrating x out, in a similar manner as above:

$$b := 1..8 \qquad fd(b,x) := dpois\left(B_{b,1}, B_{b,2} \cdot x\right) \qquad \text{(Eq. C-5)}$$

$$LB(b, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fd(b,x) \cdot dlnorm(x, \nu, \tau)\, dx \qquad \text{(Eq. C-6)}$$

(In the above formulas, b is an index used to particularize a likelihood function to a data source in the matrix B.)

The maximum likelihood method is used to calculate ν and τ. This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source (this is because the data sources are independent from each other). It is equivalent and computationally convenient to find the maximum likelihood estimators for ν and τ by using the sum of the log-likelihood (logarithm of the likelihood) of each data source.

Therefore, the log-likelihood function to be maximized is:

$$L(\nu, \tau) := \sum_{a}^{4} ln(LA(a, \nu, \tau)) + \sum_{b}^{8} ln(LB(b, \nu, \tau)) \qquad \text{(Eq. C-7)}$$

To maximize a function, Mathcad requires guess values and a range over which to search for maxima. The quantity ν represents the logarithm of a failure rate, which is expected to be in the 10^{-6}/hr range. Therefore, a guess value for ν is:

$$\nu := ln\left(10^{-6}\right) \qquad \nu \quad -13.8$$

Based on a typical error factor value of 10, a guess value for τ is:

$$\tau := \frac{ln(10)}{1.645} \qquad \tau \quad 1.4$$

A reasonable range over which to perform the likelihood maximization is as follows:

$$Given \qquad \nu > -20 \qquad \nu < -1$$

$$\tau > 0.01 \qquad \tau < 5$$

The maximum likelihood estimators for ν and τ are:

$$L := Maximize(L, \nu, \tau) \qquad \nu := L_1 \qquad \nu \quad -11.478$$

$$\tau := L_2 \qquad \tau \quad 1.874$$

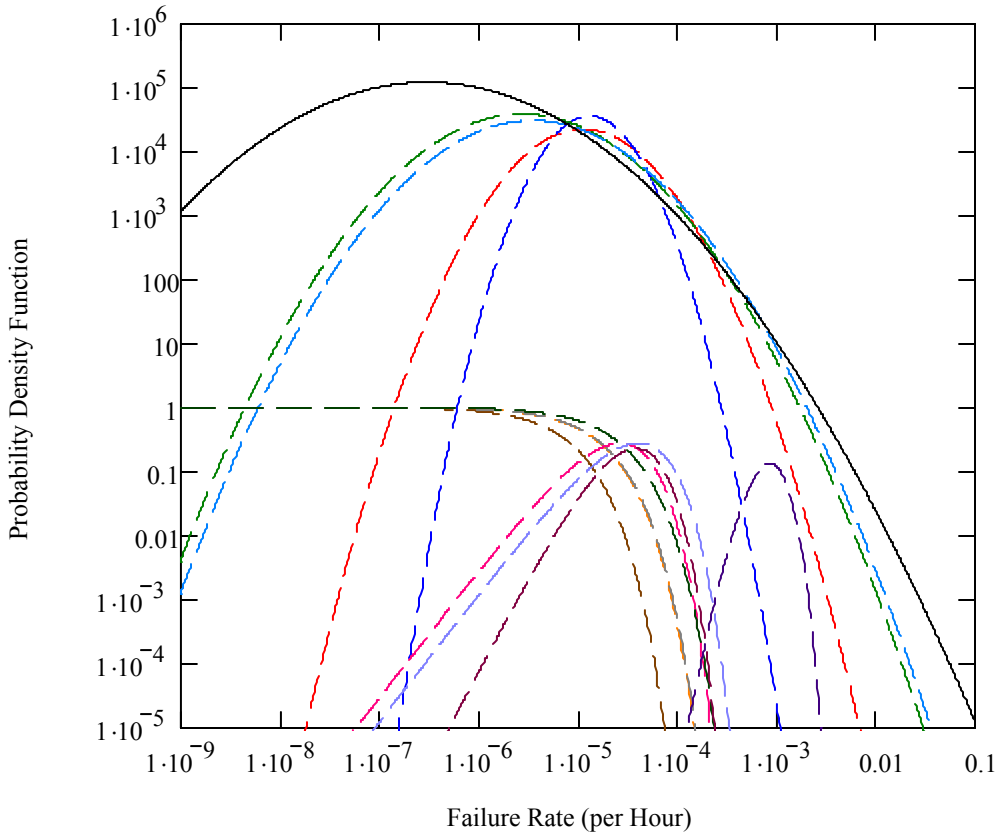
Therefore, the mean and error factors of the population-variability distribution for the failure rate are (based on the formula in NUREG/CR-6823 (Ref. C5.4, Section A.7.3)):

$$m := exp\left(\nu + \frac{\tau^2}{2}\right) \qquad m \quad 6.00 \times 10^{-5} \text{ per hour}$$

$$EF := exp(1.645 \cdot \tau) \qquad EF \quad 21.8$$

Notable percentiles of the population-variability distribution are as follows (expressed as hourly failure rates) and shown in Figure C2.1-1:

1st percentile:	$qlnorm(0.01, \nu, \tau)$	1.32×10^{-7}
5th percentile:	$qlnorm(0.05, \nu, \tau)$	4.75×10^{-7}
10th percentile:	$qlnorm(0.10, \nu, \tau)$	9.38×10^{-7}
50th percentile:	$qlnorm(0.50, \nu, \tau)$	1.04×10^{-5}
90th percentile:	$qlnorm(0.90, \nu, \tau)$	1.14×10^{-4}
95th percentile:	$qlnorm(0.95, \nu, \tau)$	2.26×10^{-4}
99th percentile:	$qlnorm(0.99, \nu, \tau)$	8.10×10^{-4}



Source: Original

Figure C2.1-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

C2.2 PARAMETER ESTIMATION IN CASE ONLY ONE DATA SOURCE IS AVAILABLE

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data (i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities) the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffrey's noninformative prior distribution. As indicated in NUREG/CR-6823 (Ref. C5.4, Section 6.2.2.5.2), this noninformative prior conveys little prior belief or information, thus allowing the data to speak for themselves.

As mentioned in "Bayesian Parameter Estimation in Probabilistic Risk Assessment," (Ref. C5.44, Section 4.2), the likelihood function associated with exposure data is either a Poisson distribution (in the case of failure rates), or a binomial distribution (in the case of failure probabilities).

Applying Bayes' theorem with Jeffrey's noninformative prior in conjunction with a Poisson likelihood function characterized by r recorded failures over an exposure time t results in a closed-form posterior distribution, namely a gamma distribution, characterized by a shape parameter equal to $0.5 + r$, and a scale parameter equal to t; the mean of this distribution is $(0.5 + r)/t$ (Ref. C5.4, Sections 6.2.2.5.2 and A7.6). In SAPHIRE, this distribution is characterized by its mean and by its shape parameter (i.e., $0.5 + r$).

Applying Bayes' theorem with Jeffrey's noninformative prior in conjunction with a binomial likelihood function characterized by r recorded failures out of n demands results in a closed-form posterior distribution, namely a beta distribution, characterized by a parameter "a" equal to $0.5 + r$, and a parameter "b" equal to $n - r + 0.5$; the mean of this distribution is $(0.5 + r)/(n + 1)$ (Ref. C5.4, Sections 6.3.2.3.2 and A7.8). In SAPHIRE, this distribution is characterized by its mean and by the parameter "b" (i.e., $n - r + 0.5$).

C3 COMMON CAUSE FAILURE DATA

Dependent failures are modeled in event tree and fault tree logic models, with potential dependent failures modeled explicitly via the logic models, whenever possible. For example, failure of the HVAC system is explicitly dependent upon failures in the electrical supply systems that are modeled in the fault trees. Similarly, the effects of erroneous calibration or other human failure events can be explicitly included in the system fault tree models and the basic event probabilities considered during the human reliability analysis. Otherwise, potential dependencies known as common-cause failures are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate common cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. C5.18), the Multiple Greek Letter method (Ref. C5.29) and (Ref. C5.30), and the Alpha Factor method (Ref. C5.31). These methods do not require an explicit knowledge of the dependence failure mode. For the YMP PCSA, common-cause failure rates or probabilities were estimated using the alpha factor method described in NUREG/CR-5485 (Ref. C5.31).

The vast majority of the equipment types for which common cause failure basic events were modeled in the YMP PCSA are not covered by the detailed component-specific alpha factor sources based on commercial nuclear plant equipment. Therefore, it was necessary to use alpha factors to address the common cause failure estimates for crane hoist wire ropes, gear boxes, over-torque sensors and the like.

The alpha factor method provides a model to treat common cause failure (CCF) probabilities of k-of-m components. In addition, industry-wide alpha factors have been developed for the US Nuclear Regulatory Commission from experience data collected at nuclear power plants. The data analysis reported in NUREG/CR-5485 (Ref. C5.31) consisted of:

1. Identifying the number of redundant components in each subsystem being reported (e.g., two, three, or four (this is termed the CCF group size, CCCG of size m)).

2. Partitioning the total number of reported failure events for a given component into the number of components that failed together (i.e., $k = 1$ for one component at a time, $k = 2$ for two components at a time, $k = 3$ for three components at a time, up to m for failure of all components in a given CCF group).

3. Estimating the alpha factor for a given component type based on its definition as the fraction of total failure events that involve k component failures due to common cause, for a system of m redundant components, using the alpha factor equation from NUREG/CR-5485 (Ref, C5.31, Table 5-10), as shown in Figure C3-1.

$$\alpha_k^m \quad \frac{n_k}{\sum_{j\ 1}^{m} n_j} \qquad k \quad 1, ..., m$$

Source: NUREG/CR-5485, p. 70 (Ref. C5.31)

Figure C3-1. Alpha Factor

4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produced industry-wide prior distributions for the alpha factors for each CCCG size, based on all CCF events in their database. Events were mapped to a given CCCG size, the maximum likelihood estimator obtained and fit to a constrained noninformative prior distribution. The parameter A_T of a Dirichlet distribution was then calculated for each alpha and the results combined using the geometric mean. The results are the industry-wide mean alpha factors and uncertainty bounds reported in of NUREG/CR-5485 (Ref. C5.31, Table 5-11) shown in Table C3-1:

Table C3-1. Alpha Factor Table

Table 5-11. Generic prior distributions for various system sizes.

CCCG Size m	α-Factor	Distributions Parameters		Percentiles			Mean
		a	b	P_{05}	P_{50}	P_{95}	
2	α_1	9.5300	0.470	8.20E-01	9.78E-01	1.00E-00	0.95300
	α_2	0.4700	9.530	1.42E-04	2.16E-02	1.81E-01	0.04700
3	α_1	15.2000	0.800	8.42E-01	9.67E-01	9.99E-01	0.95000
	α_2	0.3872	15.613	2.10E-05	8.79E-03	1.01E-01	0.02420
	α_3	0.4128	15.587	3.45E-05	1.01E-02	1.05E-01	0.02580
4	α_1	24.7000	1.300	8.67E-01	9.61E-01	9.95E-01	0.95000
	α_2	0.5538	25.446	1.44E-04	1.08E-02	7.81E-02	0.02130
	α_3	0.2626	25.737	2.98E-07	1.99E-03	4.82E-02	0.01010
	α_4	0.4836	25.516	6.29E-05	8.42E-03	7.17E-02	0.01860
5	α_1	38.042	1.958	8.86E-01	9.58E-01	9.91E-01	0.95106
	α_2	0.7280	39.272	3.72E-04	1.10E-02	6.05E-02	0.01820
	α_3	0.4120	39.588	1.32E-05	3.93E-03	4.22E-02	0.01030
	α_4	0.2336	39.766	4.57E-08	8.97E-04	2.89E-02	0.00584
	α_5	0.5840	39.416	1.24E-04	7.66E-03	5.27E-02	0.01460
6	α_1	50.4724	2.528	8.97E-01	9.58E-01	9.89E-01	0.95231
	α_2	0.7791	52.221	3.76E-04	9.20E-03	4.78E-02	0.01470
	α_3	0.5406	52.459	6.04E-05	5.02E-03	3.79E-02	0.01020
	α_4	0.3127	52.687	9.28E-07	1.56E-03	2.66E-02	0.00590
	α_5	0.2433	52.757	5.77E-08	7.67E-04	2.24E-02	0.00459
	α_6	0.6519	52.348	1.66E-04	6.93E-03	4.27E-02	0.01230
7	α_1	74.5360	3.464	9.12E-01	9.59E-01	9.86E-01	0.95559
	α_2	0.9906	77.009	6.44E-04	8.84E-03	3.79E-02	0.01270
	α_3	0.6817	77.318	1.39E-04	5.05E-03	2.99E-02	0.00874
	α_4	0.4891	77.511	2.21E-05	2.82E-03	2.42E-02	0.00627
	α_5	0.2941	77.706	3.39E-07	8.97E-04	1.74E-02	0.00377
	α_6	0.2051	77.795	3.84E-09	2.94E-04	1.35E-02	0.00263
	α_7	0.8034	77.197	2.89E-04	6.52E-03	3.32E-02	0.01030
8	α_1	97.6507	4.349	9.20E-01	9.60E-01	9.84E-01	0.95736
	α_2	1.1118	100.888	7.25E-04	7.91E-03	3.13E-02	0.01090
	α_3	0.7915	101.209	2.07E-04	4.87E-03	2.52E-02	0.00776
	α_4	0.6253	101.375	6.92E-05	3.34E-03	2.17E-02	0.00613
	α_5	0.4417	101.558	8.51E-06	1.76E-03	1.74E-02	0.00433
	α_6	0.2581	101.742	6.09E-08	4.74E-04	1.21E-02	0.00253
	α_7	0.1969	101.803	1.59E-09	1.93E-04	1.00E-02	0.00193
	α_8	0.9241	101.076	3.82E-04	6.12E-03	2.78E-02	0.00906

Source: NUREG/CR-5485 (Ref. C5.31)

These values were used in the YMP PCSA by multiplying the mean failure rate for the TYP-FM data by the appropriate alpha factor for k-of-n components for failure-on-demand events (e.g., pump failure to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run) as per the guidance in NUREG/CR-5485 (Ref. C5.31). For example, for a 2-out-of-2 failure on demand event, the mean alpha factor of 0.047 shown in the far right column of Table C3-1 associated with α_2 was multiplied by the mean failure probability for the appropriate component type and failure mode (from Table C4-1) to yield the common cause failure probability.

This approach was considered to provide conservative CCF data for all the component types for which common causes were modeled. This was considered particularly important since the

YMP has never operated and therefore the applicability of conventional nuclear plant alpha factors could not be justified.

The conservatism of this approach can be demonstrated by comparing the alpha factors used for the PCSA diesel generator CCF events to those posted on the U.S. Nuclear Regulatory Commission website for use in Probabilistic Risk Assessment studies of commercial nuclear power plants in the U.S.

The alpha factor used for the PCSA for 2 of 2 diesel generators failing to start was the 0.047 value cited earlier, while the mean alpha factor for a CCCG=2 cited by the NRC (Ref. C5.36) is 0.0136.

Diesel generators are the only component types for which such a comparison can be made since the other YMP component types for which common cause failures were modeled were not covered by the NRC equipment-specific alpha factors.

C4 ACTIVE COMPONENT RELIABILITY ESTIMATES INPUT TO SAPHIRE

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data had to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

- .BEA – attributes to assign information to the proper SAPHIRE fields
- .BED – descriptions of the component type name and failure mode
- .BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement such that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the YMP PCSA case was the TYP-FM coding). Examples of descriptions used for the PCSA template data were Clutch Failed to Operate, Relay Spurious Operation, Position Sensor Fails on Demand, and Wire Rope Breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the Lognormal Error Factor, or the shape parameter of the Beta or Gamma distributions.

Geometric means of the input parameters from the industry-wide data sources were initially used as screening values for each TYP-FM and were entered into the .BEI file, along with a default Error Factor of 10. Once the Bayesian combination process was completed for all 275 TYP-FM combinations, mean and uncertainty parameter information was entered into the .BEA files, and tested in SAPHIRE before being distributed to the systems analysts.

Failure probability per demand information was entered as SAPHIRE Calculation Type 1 for a simple probability and failure rate per hour information was entered as SAPHIRE Calculation Type 3 as a mean failure rate in the lambda field. Calc Type 3 uses the formula $P = 1 – \exp(- \lambda T_m)$, where λ is the mean failure rate (or lambda) and T_m is the mission time. Mission time is defined in the SAPHIRE Basics manual as "…the period of time that a component is required to operate in order to characterize the component operation as successful." Since the template data was to be used for all YMP facilities while the mission times would be system-specific, the mission time field in the three template data files was left blank and these times were instead input individually by the systems analysts.

The correlation class field was also used for the YMP template data files "to account for data dependencies among like events in the database" during the uncertainty analysis, as stated in the SAPHIRE Basics manual. This meant that all components in the same correlation class would be treated the same during the uncertainty analysis. This feature of SAPHIRE is based upon the observations documented (Ref. C5.2) that in the risk models, all components of the same type are quantified with the same failure rate or probability, therefore it is appropriate to group together the experience of all the nominally identified components in the same facility. Therefore, all components of the same type and failure mode are aggregated into a single number, meaning that the dependency between components of the same class must somehow be addressed. For example, if multiple motor-operated valves needed to open for success and all are assigned the same failure probability, then these basic events needed to be correlated via being assigned the same correlation class in the .BEI file. However, if different probabilities were to be used for different motor-operated valves based on the data, then the basic events would not be correlated. In all cases, a correlation class identifier, using the TYP-FM acronyms, was input to the .BEI file to indicate that all equipment with in the same TYP-FM should be correlated by the SAPHIRE model. SAPHIRE then would sample from one distribution and then use this sampled probability for all other basic events with the same correlation class.

The template data was also identified by TYP-FM combination and was utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the code, then by using the Modify Event feature to link the template data to each basic event in the fault tree. This permitted each active component of the same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the industry-wide data investigation and Bayesian combination process.

Table C4-1 shows the active component reliability estimates that were input to SAPHIRE as template data for fault tree model quantification.

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
AHU-FTR	Air Handling Unit Failure to Run	G	5.00E-01[b]		3.80E-06[b]	1 source; N/D	NUREG/CR-6928 (Ref. C5. 16)
ALM-SPO	Alarm/Annunciator Spurious Operation	L	1.30E+01		4.74E-07	5 sources N/D; 1 source mean	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40)
AT-FOH	Actuator (Electrical) Failure	L	1.24E+01		7.54E-05	3 sources; N/D	NPRD-95 (Ref. C5.40)
ATH-FOH	Actuator (Hydraulic) Failure	L	3.81E+01		8.91E-04	4 sources; N/D	NPRD-95 (Ref. C5.40)
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation	L	5.00E+00		1.34E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
AXL-FOH	Axle Failure	G	5.00E-01[b]		1.60E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
B38-FOH	Bearing Failure	L	1.13E+01		2.50E-06	8 sources; N/D	NPRD-95 (Ref. C5.40)
BEA-BRK	Lifting Beam/Boom Breaks	G	1.50E+00		2.40E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
BLD-RUP	Air Bag Ruptures	B	1.10E+04	1.36E-04		1 source; N/D	BSC 2007 (Ref. C5.7)
BLK-FOD	Block or Sheaves Failure on Demand	B	1.30E+06	1.15E-06		1 source; N/D	NPRD-95 (Ref. C5.40)
BRH-FOD	Brake (Hydraulic) Failure on Demand	L	5.50E+01	8.96E-06		3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
BRK-FOD	Brake Failure on Demand	L	6.30E+00	1.46E-06		3 sources; mean + EF	EPRI PRA (Ref. C5.8)
BRK-FOH	Brake (Electric) Failure	G	2.50E+00		4.40E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
BRP-FOD	Brake (Pneumatic) Failure on Demand	L	2.55E+00	5.02E-05		4 sources; N/D	NPRD-95 (Ref. C5.40)
BRP-FOH	Brake (Pneumatic) Failure	L	2.55E+00		8.38E-06	4 sources; N/D	NPRD-95 (Ref. C5.40)
BTR-FOD	Battery No Output Given Challenge	B	6.05E+01	8.20E-03		1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
BTR-FOH	Battery Failure	L	4.30E+00		4.29E-06	12 sources N/D; 8 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5. 16), SAIC Umatilla (Ref. C5.41)
BUA-FOH	AC Bus Failure	L	3.08E+00		6.10E-07	3 sources; N/D	IEEE 493 (Ref. C5. 22), NUREG/CR-6928 (Ref. C5. 16)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
BUD-FOH	DC Bus Failure	L	8.70E+01		2.40E-07	1 source mean + EF	IEEE-500 (Ref. C5.23)
BYC-FOH	Battery Charger Failure	L	1.00E+01		7.60E-06	1 source mean + EF	CCPS (Ref. C5.1)
C52-FOD	Circuit Breaker (AC) Fails on Demand	L	9.80E+00	2.24E-03		19 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
C52-SPO	Circuit Breaker (AC) Spurious Operation	L	2.29E+01		5.31E-06	12 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-6928 (Ref. C5.16), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
C72-SPO	Circuit Breaker (DC) Spurious Operation	L	1.20E+00		1.07E-06	3 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
CAM-FOH	Cam Lock Fails	L	8.30E+01		3.19E-06	4 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
CBP-OPC	Cables (Electrical Power) Open Circuit	G	5.00E-01		9.13E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CBP-SHC	Cables (Electrical Power) Short Circuit	G	5.00E-01		1.88E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CKV-FOD	Check Valve Fails on Demand	L	1.36E+01	6.62E-04		4 sources N/D; 7 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5. 16), SRS Reactors (Ref. C5.5)
CKV-FTX	Check Valve Fails to Check	L	1.50E+01	2.20E-03		1 source; mean + EF	CCPS (Ref. C5.1)
CON-FOH	Electrical Connector (Site Transporter) Failure	G	5.00E-01		7.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
CPL-FOH	Coupling (Automatic) Failure	L	5.00E+00		1.90E-06	1 source mean + EF	AIAA (Ref. C5.11)
CPO-FOH	Control System Onboard [TEV or Trolley] Failure	G	9.85E+01		2.10E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CRD-FOH	Card Reader Failure	L	5.00E+00		4.55E-05	1 source mean + EF	HID (Ref. C5.21)
CRJ-DRP	Jib Crane Drop	B	9.72E+04	2.60E-05		1 source; N/D	NUREG-1774 (Ref. C5.26)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
CRN-DRP	200 Ton Crane Drop	L	4.35E+01	3.21E-05		2 sources N/D; 4 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26), EPRI PRA (Ref. C5.8)
CRN-TBK	200 Ton Crane Two Block Drop	L	1.15E+01	4.41E-07		1 source N/D; 3 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26)
CRS-DRP	200 Ton Crane Sling Drop	B	2.06E+04	1.21E-04		1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-DRP	WP (Non-Single Failure Proof) Crane Drop	B	3.34E+04	1.05E-04		1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-TBK	WP (Non-Single Failure Proof) Crane Two Block Drop	B	3.34E+04	4.49E-05		1 source; N/D	NUREG-1774 (Ref. C5.26)
CSC-FOH	Cask Cradle Failure	G	1.50E+00		4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CT-FOD	Controller Mechanical Jamming	L	5.00E+00[b]	4.00E-06		1 source; mean + EF	EPRI PRA (Ref. C5.8)
CT-FOH	Controller Failure	L	1.00E+01		6.88E-05	1 source mean + EF	CCPS (Ref. C5.1)
CT-SPO	Controller Spurious Operation	L	1.00E+01		2.27E-05	1 source mean + EF	CCPS (Ref. C5.1)
CTL-FOD	Logic Controller Fails on Demand	L	1.10E+01	2.03E-03		3 sources; N/D	NUREG/CR-6928 (Ref. C5.16)
DER-FOM	Derailment Failure per Mile	G	3.97E+03		1.18E-05	1 source; N/D	Federal Railroad Administration (Ref. C5.17)
DG-FTR	Diesel Generator Fails to Run	L	1.51E+01		4.08E-03	8 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
DG-FTS	Diesel Generator Fails to Start	L	3.50E+00	8.38E-03		9 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days	G	5.05E+01		8.27E-04	1 source, N/D	NUREG/CR-6890 (Ref. C5.15)
DM-FOD	Drum Failure on Demand	L	1.00E+01	4.00E-08		2 sources mean + EF	EPRI PRA (Ref. C5.8)
DM-MSP	Drum Mis-spooling (Hourly)	G	5.00E-01		6.86E-07	1 source, N/D	NPRD-95 (Ref. C5.40)
DMP-FOH	Damper (Manual) Fails to Operate	L	4.30E+00		5.94E-06	3 sources mean + EF	IEEE-500 (Ref. C5.23), N-Reactor (Ref. C5.46), Moss (Ref. C5.32)
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)	L	3.20E+00		8.38E-08	2 sources N/D; 2 sources mean + EF	NUREG/CR-3154 (Ref. C5.6), NUREG/CR-1363 (Ref. C5.28), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
DMS-FOH	Demister (Moisture Separator) Failure	L	5.00E+00		9.12E-06	1 source mean + EF	EPRI AP-2071 (Ref. C5.10)
DRV-FOH	Drive (Adjustable Speed) Failure	G	5.0E-01		2.5E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
DRV-FSO	Drive (Adjustable Speed) Failure to Stop on Demand	B	2.5E+02		3.4E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
DTC-RUP	Duct Ruptures	L	2.6E+01		3.7E-06	9 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5), SAIC Umatilla (Ref. C5.41)
DTM-FOD	Damper (Tornado) Failure on Demand	L	5.0E+00	8.7E-04		1 source; mean + EF	IEEE-500 (Ref. C5.23)
DTM-FOH	Damper (Tornado) Failure	L	7.9E+00		2.3E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
ECP-FOH	Position Encoder Failure	G	5.0E-01		1.8E-06	2 sources; N/D	NPRD-95 (Ref. C5.40)
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)	L	5.0E+00	2.5E-04		1 source; mean + EF	EPRI PRA (Ref. C5.8)
FAN-FTR	Fan (Motor-Driven) Fails to Run	L	4.6E+01		7.21E-05	11 sources N/D; 6 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand	L	1.0E+01	2.0E-03		7 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
FRK-PUN	Forklift Puncture	L	1.06E+01		1.20E-05	1 source mean + EF	SAIC Umatilla (Ref. C5.41)
G65-FOH	Governor Failure	G	1.82E+02		1.16E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
GPL-FOD	Grapple Failure on Demand	B	1.30E+06	1.15E-06		1 source; N/D	NPRD-95 (Ref. C5.40)
GRB-FOH	Gear Box Failure	L	1.40E+01		2.21E-04	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
GRB-SHH	Gear box Shaft/Coupling Shears	L	5.00E+00		2.40E-06	1 source; mean + EF	EPRI PRA (Ref. C5.8)
GRB-STH	Gear Box Stripped	L	5.00E+00		7.86E-08	1 source; mean + EF	NPRD-95 (Ref. C5.40)
HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	L	8.39E+01	1.74E-03		1 source N/D; 3 sources mean + EF	EPRI PRA (Ref. C5.8), NPRD-95 (Ref. C5.40)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation	G	5.00E-01		5.23E-07	1 source N/D	NPRD-95 (Ref. C5.40)
HEP-LEK	Filter (HEPA) Leaks [Bypassed]	L	1.00E+01		3.00E-06	1 source; mean + EF	SRS Reactors (Ref. C5.5)
HEP-PLG	Filter (HEPA) Plugs	L	9.5E+00		4.3E-06	3 sources N/D; 2 sources mean + EF	IEEE-500 (Ref. C5.23), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
HOS-LEK	Hose Leaking	L	2.47E+01		1.48E-05	same as HOS-RUP with factor of 10	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
HOS-RUP	Hose Ruptures	L	2.47E+01		1.48E-06	2 sources N/D; 3 sources mean + EF	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
IEL-FOD	Interlock Failure on Demand	L	5.0E+00	2.8E-05		1 source; mean + EF	NPRD-95 (Ref. C5.40)
IEL-FOH	Interlock Failure	L	5.50E+01		3.43E-05	4 sources; N/D	NPRD-95 (Ref. C5.40)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
LC-FOD	Level Controller Failure on Demand	B	6.07E+03	6.25E-04		1 source; N/D	NUREG/CR-6928 (Ref. C5.16)
LRG-FOH	Lifting Rig or Hook Failure	G	4.65E+01		7.45E-07	1 source; N/D	NPRD-95 (Ref. C5.40)
LVR-FOH	Lever (two position; up-down) Failure	G	9.85E+01		2.10E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
MCC-FOH	Motor Control Centers (MCCs) Failure	L	1.00E+01		7.49E-06	composite of Relay (RLY-FTP) + Motor Starter (MST FOH) + Limit Switch (ZS-FOH)	
MOE-FOD	Motor (Electric) Fails on Demand	L	5.00E+00	6.00E-05		1 source; mean + EF	EPRI PRA (Ref. C5.8)
MOE-FSO	Motor (Electric) Fails to Shut Off	L	1.07E+01		1.35E-08	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MOE-FTR	Motor (Electric) Fails to Run	L	9.50E+00		6.50E-06	8 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), OREDA-2002 (Ref. C5.43)
MOE-FTS	Motor (Electric) Fails to Start (Hourly)	L	1.90E+01		7.14E-06	5 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40)
MOE-SPO	Motor (Electric) Spurious Operation	L	1.07E+01		6.74E-07	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MSC-FOH	Motor Speed Control Module Failure	G	5.00E-01		1.28E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
MST-FOH	Motor Starter Failure	L	1.33E+00		1.43E-07	2 sources; N/D	IEEE 493 (Ref. C5.22)
NZL-FOH	Nozzle Failure	L	7.50E+00		2.85E-06	5 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PIN-BRK	Pin (Locking or Stabilization) Breaks	L	1.46E+00		2.12E-09	4 sources; N/D	NPRD-95 (Ref. C5.40)
PLC-FOD	Programmable Logic Controller Fails on Demand	B	1.35E+03	3.69E-04		1 source; N/D	NPRD-95 (Ref. C5.40)
PLC-FOH	Programmable Logic Controller Fails to Operate	L	1.00E+01		3.26E-06	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
PLC-SPO	Programmable Logic Controller Spurious Operation	L	1.00E+01		3.65E-07	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PMD-FTR	Pump (Motor Driven) Fails to Run	L	9.9E+00		3.5E-05	6 sources N/D; 87 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand	L	3.80E+00	2.50E-03		7 sources N/D; 80 sources mean + EF	N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PPL-RUP	Piping (Lined) Catastrophic	L	1.50E+01		4.42E-07	1 source; mean + EF	CCPS (Ref. C5.1)
PPM-PLG	Piping (Water) Plugs	L	1.35E+01		7.26E-07	1 source N/D; 2 sources mean + EF	DuPont (Ref. C5.14), EPRI Pipe Failure Study (Ref. C5.10), SAIC Umatilla (Ref. C5.41)
PPM-RUP	Piping (Water) Ruptures	L	2.00E+01		8.75E-10	1 source; mean + EF	NUREG/CR-6928 (Ref. C5.16)
PR-FOH	Passive restraint (bumper) Failure	G	2.09E+02		4.45E-10	1 source; N/D	NPRD-95 (Ref. C5.40)
PRM-FOH	eProm (HVAC Speed Control) Failure	G	5.00E-01		5.38E-07	1 source; N/D	MIL-HDBK-217F (Ref. C5.12)
PRV-FOD	Pressure Relief Valve Fails on Demand	L	2.72E+01	6.54E-03		6 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
PV-SPO	Pneumatic Valve Spurious Operation	G	5.00E-01		2.92E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
QDV-FOH	Quick Disconnect Valve Failure	L	3.56E+00		4.26E-06	4 sources N/D	NPRD-95 (Ref. C5.40)
RCV-FOH	Air Receiver Fails to Supply Air	L	1.00E+01		6.00E-07	1 source; mean + EF	IEEE-500 (Ref. C5.23)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
RLY-FTP	Relay (Power) Fails to Close/Open	G	5.00E-01		8.77E-06	1 source N/D	NPRD-95 (Ref. C5.40)
SC-FOH	Speed Control Failure	G	5.00E-01		1.28E-04	1 source N/D	NPRD-95 (Ref. C5.40)
SC-SPO	Speed Control Spurious Operation	G	5.00E-01		3.20E-05	1 source N/D	NPRD-95 (Ref. C5.40)
SEL-FOH	Speed Selector Fails	L	5.34E+00		4.16E-06	3 sources N/D	NPRD-95 (Ref. C5.40)
SEQ-FOD	Sequencer Fails on Demand	B	7.49E+02	3.33E-03		1 source N/D	NUREG/CR-6928 (Ref. C5.16)
SFT-COL	Spent Fuel Transfer Machine (SFTM) Collision or Impact	L	4.00E+00	2.94E-06		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SFT-DRP	Spent Fuel Transfer Machine (SFTM) Drop	L	3.00E+00	5.15E-06		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5. 20)
SFT-RTH	Spent Fuel Transfer Machine (SFTM) Raised Fuel Too High	L	7.00E+00	7.36E-07		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SJK-FOH	Screw Jack [TEV] Failure	G	5.00E-01		8.14E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SRF-FOH	Flow Sensor Failure	G	5.00E-01		1.07E-06	1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
SRP-FOD	Pressure Sensor Fails on Demand	B	1.25E+02	4.00E-03		1 source; N/D	NPRD-95 (Ref. C5.40)
SRP-FOH	Pressure Sensor Fails	L	1.21E+01		2.95E-06	8 sources N/D	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16)
SRR-FOH	Radiation Sensor Fails	L	5.00E+00		2.00E-05	1 source; mean + EF	Laurus (Ref. C5.25)
SRS-FOH	Over Speed Sensor Fails	G	1.28E+02		2.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand	L	2.10E+00	7.33E-04		2 sources N/D	NUREG/CR-6928 (Ref. C5.16), OREDA-92 (Ref. C5.42)
SRT-FOH	Temperature Sensor/Transmitter Fails	L	1.41E+01		7.05E-07	4 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43)
SRT-SPO	Temperature Sensor Spurious Operation	L	2.80E+01		2.23E-06	1 source; mean + EF	OREDA-2002 (Ref. C5.43)
SRU-FOH	Ultrasonic Sensor Fails	G	5.00E-01		9.62E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
SRV-FOH	Vibration Sensor (Accelerometer) Fails	L	1.07E+01		9.40E-05	4 sources N/D	NPRD-95 (Ref. C5.40)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
SRX-FOD	Optical Position Sensor Fails on Demand	B	3.18E+03	1.10E-03		1 source; N/D	SAIC Umatilla (Ref. C5.41)
SRX-FOH	Optical Position Sensor Fails	L	5.00E+00		4.70E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
STU-FOH	Structure (truck or railcar) Failure	G	1.50E+00		4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
SV-FOD	Solenoid Valve Fails on Demand	L	1.17E+01	6.28E-04		4 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
SV-FOH	Solenoid Valve Fails	L	1.70E+01		4.87E-05	1 source; mean + EF	CCPS (Ref. C5.1)
SV-SPO	Solenoid Valve Spurious Operation	L	3.00E+00		4.09E-07	1 source; mean + EF	CCPS (Ref. C5.1)
SWA-FOH	Auto-Stop Switch (CTT hose travel) Fails	G	6.50E+00		3.12E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SWG-FOH	13.8kV Switchgear Fails	G	2.85E+01		1.31E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-FTX	Electric Power Switch Fails to Transfer	G	6.50E+00		3.59E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-SPO	Electric Power Switch Spurious Transfer	G	6.50E+00		1.55E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
TD-FOH	Transducer Failure	L	4.70E+00		9.84E-05	3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
TDA-FOH	Transducer (Air Flow) Failure	L	6.21E+00		1.65E-04	2 sources N/D	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDP-FOH	Transducer (Pressure) Fails	L	5.35E+01		2.20E-04	23 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDT-FOH	Transducer (Temperature) Fails	L	2.95E+01		1.04E-04	12 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
THR-BRK	Third Rail Breaks	L	1.00E+01		1.01E-08	1 source; mean + EF	NPRD-95 TRK-BRK adjusted with failure information from Federal Railroad Administration Safety Data website (Ref. C5.17)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
TKF-FOH	Fuel Tank Fails	L	1.11E+01		4.40E-07	15 sources; N/D	NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
TL-FOH	Torque Limiter Failure	G	8.05E+01		8.05E-05	1 source N/D	NPRD-95 (Ref. C5.40)
TRD-FOH	Tread (Site Transporter)	L	3.40E+00		5.89E-07	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), Rand (Ref. C5.38)
UDM-FOH	Damper (Backdraft) Failure	L	7.90E+00		2.26E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
UPS-FOH	Uninterruptible Power Supply (UPS) Failure	L	5.08E+00		2.02E-06	10 sources; N/D	NPRD-95 (Ref. C5.40)
WNE-BRK	Wire Rope Breaks	L	5.00E+00	2.00E-06		1 source; mean + EF	EPRI PRA (Ref. C5.8)
XMR-FOH	Transformer Failure	L	1.53E+01		2.91E-07	13 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
XV-FOD	Manual Valve Failure on Demand	L	1.00E+01	6.48E-04		3 sources N/D; 12 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
ZS-FOD	Limit Switch Failure on Demand	L	5.7E+00	2.9E-04		3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name and Failure Mode	Dist Type	Uncert Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
ZS-FOH	Limit Switch Fails	L	6.03E+00		7.23E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)
ZS-SPO	Limit Switch Spurious Operation	L	5.56E+00		1.28E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)

NOTE: [a] Refer to Section C1.2 for specific citation to data sources.
[b]There are minor differences between the specific values tagged by this footnote and those used to quantify the SAPHIRE model. Such differences are not meaningful in the context of this analysis because (a) the difference pertains only to the uncertainty of the component reliability or (b) the uncertainty in the reliability value is much greater than difference between the value given here and that used in the model.

B = Beta Distribution; EF = Lognormal Error Factor; G = Gamma Distribution; L = Lognormal Distribution; N/D = Numerator/Denominator

Source: Original

C5 REFERENCES; DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

C5.1 *AIChE (American Institute of Chemical Engineers) 1989. *Guidelines for Process Equipment Reliability Data with Data Tables.* G-07. New York, New York: American Institute of Chemical Engineers, Center for Chemical Process Safety. TIC: 259872. ISBN: 978-0-8169-0422-8.

C5.2 *Apostolakis, G. and Kaplan, S. 1981. "Pitfalls in Risk Calculations." *Reliability Engineering, 2,* 135-145. Barking, England: Applied Science Publishers. TIC: 253648.

C5.3 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.

C5.4 *Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment.* NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.

C5.5 *Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U).* WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.

C5.6 *Borkowski, R.J.; Kahl, W.K.; Hebble, T.L.; Fragola, J.R.; Johnson, J.W. 1983. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve - Component.* NUREG/CR-3154; ORNL/TM-8647. Oak Ridge, TN: Oak Ridge National Laboratory. ACC: MOL.20071129.0315.

C5.7 BSC 2007 (Bechtel SAIC Company). *Waste Form Throughputs for Preclosure Safety Analysis.* 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.

C5.8 *Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.* 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.

C5.9 *Crutchfield, D.M. 1996. "Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment." NRC Bulletin 96-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. Accessed February 12, 2008. ACC: MOL.20080213.0021. URL: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1996/bl96002.html

C5.10 *Derdiger, J.A.;Bhatt, K.M.;Siegfriedt, W.E. 1981. *Component Failure and Repair Data for Coal-Fired Power Units*. EPRI AP-2071. Palo Alto, CA: Electric Power Research Institute. TIC: 260070.

C5.11 *Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications.* AIAA Education Series. Washington, D.C.: American Institute of Aeronautics & Astronautics. TIC: 259878.

C5.12 *DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment.* MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.

C5.13 *Drago, J.P.; Borkowski, R.J.; Fragola, J.R.; and Johnson, J.W. 1982. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report — The Pump Component.* NUREG/CR-2886. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0222.

C5.14 *E.I. DuPont de Nemours & Company (Inc.) 1981. *Some Published and Estimated Failure Rates for Use in Fault Tree Analysis*. Washington, Delaware: E.I. DuPont de Nemours & Company (Inc). (DIRS 184415)

C5.15 *Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Station Blackout Risk.* Volume 2 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants.* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0165.

C5.16 *Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; Rasmuson, D.M.; and Atwood, C.T. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.* NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.

C5.17 *Federal Railroad Administration. 2004. "Train Accidents by Cause from Form FRA F 6180.54." Washington, D.C.: U.S. Department of Transportation, Federal Railroad Administration. Accessed 03/12/2004. ACC: MOL.20040311.0211. URL: http://safetydata.fra.dot.gov/OfficeofSafety/Query/Default.asp

C5.18 *Fleming, K.N. 1975. *A Reliability Model for Common Mode Failures in Redundant Safety Systems.* GA-A13284. San Diego, California: General Atomic Company. ACC: MOL.20071219.0221.

C5.19 *Fragola, J.R. and McFadden, R.H. 1995. "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom." *Reliability Engineering and System Safety, 47,* 255-273. New York, New York: Elsevier. TIC: 259675.

C5.20 *Framatome ANP (Advanced Nuclear Power) 2001. *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999.* Lynchburg, Virginia: Framatome Advanced Nuclear Power. ACC: MOL.20011018.0158.

C5.21 *HID Corporation [n.d.]. Ruggedized Card Reader/Ruggedized Keypad Card Reader. Dorado 740 and 780. Irvine, California: HID Corporation. TIC: 260007.

C5.22 *IEEE (Institute of Electrical and Electronics Engineers) Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205. ISBN 1-55937-969-3.

C5.23 *IEEE Std 500-1984 (Reaffirmed 1991). 1991. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.* New York, New York: Institute of Electrical and Electronics Engineers. TIC: 256281.

C5.24 *Kahl, W.K. and Borkowski, R.J. 1985. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report - Diesel Generators, Batteries, Chargers, and Inverters.* NUREG/CR-3831. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071212.0181.

C5.25 *Laurus Systems [n.d.]. Instruments and Software Solutions for Emergency Response and Health Physics. Ellicott City, Maryland: Laurus Systems. TIC: 259965.

C5.26 Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

C5.27 *Lopez Droguett, E.; Groen, F.; and Mosleh, A. 2004. "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety, 83,* 311-321. New York, New York : Elsevier. TIC: 259380.

C5.28 *Miller, C.F.; Hubble, W.H.; Trojovsky, M.; and Brown, S.R. 1982. *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980.* NUREG/CR-1363, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0223.

C5.29 *Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques.* Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

C5.30 *Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Procedural Framework and Examples.* Volume 1 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

C5.31 *Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.* NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106.

C5.32 *Moss, T.R. 2005. *The Reliability Data Handbook.* 1st Edition. New York, NY: ASME Press (American Society of Mechanical Engineers). ISBN: 0-7918-0233-7. TIC: 259912.

C5.33 Not Used.

C5.34 NRC (U.S. Nuclear Regulatory Commission) 1979. *Single-Failure-Proof Cranes for Nuclear Power Plants.* NUREG-0554. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 232978.

C5.35 NRC 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

C5.36 NRC 2005. *CCF Parameter Estimation 2005.* Washington, D.C.: Nuclear Regulatory Commission (NRC). ACC: MOL.20080213.0022.

C5.37 *NSWC (Naval Surface Warfare Center) 1998. *Handbook of Reliability Prediction Procedures for Mechanical Equipment*. NSWC-98/LE1. West Bethesda, Maryland: Naval Surface Warfare Center, Carderock Division. TIC: 245703.

C5.38 *Peltz, E.; Robbins, M.; Boren, P.; Wolff, M. 2002. "Using the EDA to Gain Insight into Failure Rates." *Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer.* Santa Monica, CA: RAND. TIC: 259917. ISBN: 0-8330-3115-5.

C5.39 *Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data*. NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.

C5.40 *Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995.* NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.

C5.41 *SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.* Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.

C5.42 *SINTEF Industrial Management 1992. *OREDA, Offshore Reliability Data Handbook.* 2nd Edition. Trondheim, Norway: OREDA. ISBN: 825150188.1.

C5.43 *SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook.* 4th Edition. Trondheim, Norway: OREDA. ISBN: 8214027055. TIC: 257402.

C5.44 *Siu, N.O. and Kelly, D.L. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment." *Reliability Engineering and System Safety, 62,* 89-116. New York, New York: Elsevier. TIC: 258633.

C5.45 *Trojovsky, M. 1982. *Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1980.* NUREG/CR-1205, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20080207.0024.

C5.46 *Zentner, M.D.; Atkinson, J.K.; Carlson, P.A.; Coles, G.A.; Leitz, E.E.; Lindberg, S.E.; Powers, T.B.; and Kelly, J.E. 1988. *N Reactor Level 1 Probabilistic Risk Assessment: Final Report.* WHC-SP-0087. Richland, Washington: Westinghouse Hanford Company. ACC: MOL.20080207.0021.

ATTACHMENT D
PASSIVE EQUIPMENT FAILURE ANALYSIS

CONTENTS

Page

FIGURES

Page

TABLES

Page

ACRONYMS AND ABBREVIATIONS

Acronyms

ASME	American Society of Mechanical Engineers
CDF	cumulative distribution function
COV	coefficient of variation
CTM	canister transfer machine
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EPS	equivalent (or effective) plastic strain
ETF	expended toughness fraction
FEA	finite element analysis
HLW	high-level radioactive waste
INL	Idaho National Laboratory
LLNL	Lawrence Livermore National Laboratory
MCO	multicanister overpack
PCSA	preclosure safety analysis
PDF	probability density function
PWR	pressurized water reactor
SAR	Safety Analysis Report
SFC	spent fuel canister
SLS	steel-lead-steel
SNF	spent nuclear fuel
TAD	transportation, aging, and disposal
TEV	transport and emplacement vehicle
WPTT	waste package transfer trolley

ACRONYMS AND ABBREVIATIONS (Continued)

Abbreviations

C	Celsius
cm	centimeter
F	Fahrenheit
ft	foot, feet
hr, hrs	hour, hours
J	joule
K	Kelvin
kg	kilogram
kV	kilovolt
kW	kilowatt
LOS	loss of shielding
m	meter
min	minute, minutes
m/s	meters/second
mrem	millirem
MPa	megapascal
mph	miles per hour
psig	pounds per square inch gauge
rem	roentgen equivalent man
W/m K	watt per meter Kelvin
W/m^2K	watt per square meter Kelvin

ATTACHMENT D
PASSIVE EQUIPMENT FAILURE ANALYSIS

Many event sequences described in Section 6.1 include pivotal events that arise from loss of integrity of a passive component, namely one of the aging overpacks, casks, or canisters that contain a radioactive waste form. Such pivotal events involve (1) loss of containment of radioactive material that may result in airborne releases, or (2) loss of shielding effectiveness. Both types of pivotal events may be failure modes caused by either physical impact to the container or by thermal energy transferred to the container. This attachment presents the results of passive failure analyses that provide conditional probability of loss of containment or loss of shielding. Many scenarios were selected for analysis as representative or bounding for anticipated scenarios in the risk assessment. Results of some scenarios may not have been used in the final event sequence quantification.

D1 LOSS OF CONTAINMENT DUE TO DROPS AND IMPACTS

The category of passive equipment includes canisters and casks used during transport, aging, and disposal of spent nuclear fuel. The canisters and casks contain the spent fuel and provide containment of radioactive material. During transport and handling, the canisters and casks could be subjected to drops, impacts, or fires, which may result in loss of containment. The probabilities of loss of containment due to various physical or thermal challenges are evaluated primarily through structural and thermal analysis and drop test data.

Passive equipment (e.g., transportation casks, storage canisters, and waste packages) may fail from abnormal use such as defined by the event sequences. Studies were performed and passive equipment failure probabilities were determined using the methodologies summarized in Section 4.3.2.2. The probability of loss of containment (breach) was determined for several types of containers, including transportation casks (analyzed without impact limiters), shielded transfer casks, waste packages, TAD canisters, DPCs, DOE standardized canisters, MCOs, HLW canisters, and naval SNF canisters. The mechanical breach of TAD canisters, DPCs and naval SNF canisters were analyzed as representative canisters as described in Section D1.1. The structural analysis of DOE standardized canisters and MCOs for breaches is described in Section D1.2 and then the probabilistic methodology of Section D1.1 was applied. Transportation casks, site transfer casks (STCs) and horizontal STCs were analyzed as representative transportation casks as describe in Section D1.1. The probabilistic estimation of breach from mechanical loads of all other waste containers is described in Sections D1.3 through D1.6. The analysis of loss or degradation of shielding of casks and overpacks against mechanical loads is described in Section D3. The probabilistic analysis of fire severity and the associated effects on casks, canisters, and overpacks with respect to both containment breach and shielding degradation or loss is described in Section D2. The analysis of mechanical failures and thermal failures included the specific configuration defined by the event sequences. For example, if the event sequence occurred during a process in which the canister is within a transportation casks or aging overpack, the analysis is performed in that configuration.

D1.1 LAWRENCE LIVERMORE NATIONAL LABORATORY ANALYSIS OF CANISTERS AND CASKS

Lawrence Livermore National Laboratory (LLNL) performed the FEA using Livermore Software–Dynamic Finite Element Program (LS-DYNA) to model drops and impacts for casks and canisters with selected properties for use as representative containers expected to be delivered to Yucca Mountain (Ref. D4.1.27). LS-DYNA, which has been used in nuclear facility and non-nuclear industrial applications, is appropriate to model nonlinear, transient responses of a passive component to a structural challenge such as a drop or an impact. Existing commercial casks and canisters that would likely be used on the Yucca Mountain Project (YMP) were identified and characterized. The cases analyzed are listed in Table D1.2-1.

Appropriate finite element models were developed for the representative cask, selected container types, configurations, and drop types. The level of detail for each model was selected to understand deformation and damage patterns, possible failure mode(s) in each structural element, and failure-related response. Special attention was required to properly model the bottom-weld and closure regions to ensure that coarser mesh of the simplified model would capture failure-related response with acceptable accuracy. A consistent failure criterion for each case was identified as part of the detailed analyses. The effective plastic strain in each element, in combination with material ductility data, was used to predict failure measures.

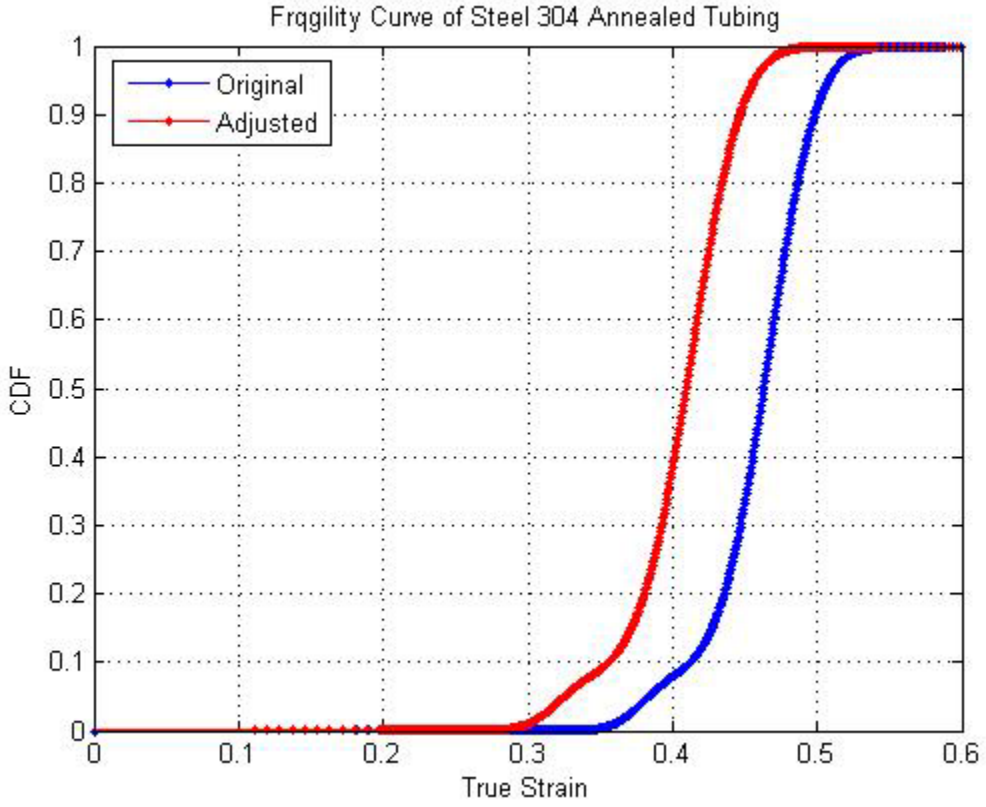
The maximum strain for each scenario was compared with the capacity distribution based on material properties to obtain containment failure probabilities using the methodology described in Section 4.3.2.2. For simplicity and consistency in interpreting results, the impact-surface conditions, including both the ground and the falling 10-ton load for the analyses, were considered infinitely stiff and unyielding, which is conservative.

The results of these cases are summarized in Tables D1.2-2 through D1.2-4. The bases for these results are summarized in the following paragraphs. If a probability for the event sequence is less than 1.0×10^{-8}, additional conservatism is incorporated in the PCSA by using a failure probability of 1.0×10^{-5}, which are termed "LLNL, adjusted". This additional conservatism is added to account for a) future evolutions of cask and canister designs, and b) uncertainties, such as undetected material defects, undetected manufacturing deviations, and undetected damage associated with handling before the container reaches the repository, which are not included in the tensile elongation data.

LLNL developed a fragility curve for the base metal by fitting a mixture of two normal probability density functions (PDFs) to the engineering (tensile) strain data (Ref. D4.1.4). Both the data and their corresponding log-transforms were found to be non-normally distributed ($p < 10^{-4}$) by the Shapiro-Wilk test (Ref. D4.1.62). These data collected at 100°F were determined to be reasonably well modeled as a sample from a weighted mixture of two normal distributions, one with a mean of 46% and a standard deviation of 2.24% (weight = 7.84%), and the other with a mean of 59.3% and a standard deviation of 4.22% (weight = 92.16%), with the goodness of fit ($p = 0.939$) assessed by the Kolmogorov-Smirnov 1 sample test (Ref. D4.1.33).

The stainless steel used in the LLNL (Ref. D4.1.27) analysis is alloy 304L. The un-annealed alloys have relatively shorter elongations at failure than annealed 304L. Therefore, the base

fragility cumulative distribution function (CDF) model was adjusted to different steels used in a typical design and to meet the code specification of the material model used in LS-DYNA. The adjustment consisted of shifting the distribution by -8.3% (Ref. D4.1.27, p. 93). Thus the initial fragility curve was shifted by 8.3% to a lower value of minimum elongation. The fragility curves before and after the shift are shown in Figure D1.1-1 and tabulated in Table D1.1-1. 316L stainless steel might be used for construction of some canisters and casks, but the stress-strain curves would be similar.



Source: (Ref. D4.1.27, Figure 6.3.7-3)

Figure D1.1-1. Original and Shifted Cumulative Distribution Functions (CDF) for Capacity (or Fragility) Plotted as a Function of True Strain

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1

True Strain (*TS*)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (*TS*)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.00	-1.70	0.0000E+00	1.6754E-15	0.36	0.05	1.0506E-02	1.0973E-01
0.01	-1.65	2.0924E-16	1.8688E-15	0.37	0.10	2.3978E-02	1.4282E-01
0.02	-1.60	4.1848E-16	2.0622E-15	0.38	0.15	4.3259E-02	1.9679E-01
0.03	-1.55	6.2772E-16	2.2555E-15	0.39	0.19	6.2863E-02	2.7687E-01

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1 (Continued)

True Strain (*TS*)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (*TS*)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.04	-1.50	8.3696E-16	2.4489E-15	0.40	0.24	7.9100E-02	3.8310E-01
0.05	-1.45	1.0462E-15	2.6422E-15	0.41	0.29	9.5539E-02	5.0814E-01
0.06	-1.41	1.2554E-15	2.8356E-15	0.42	0.34	1.2068E-01	6.3823E-01
0.07	-1.36	1.4647E-15	3.0290E-15	0.43	0.39	1.6410E-01	7.5736E-01
0.08	-1.31	1.6739E-15	3.2223E-15	0.44	0.44	2.3393E-01	8.5309E-01
0.09	-1.26	1.8832E-15	3.4157E-15	0.45	0.48	3.3371E-01	9.2036E-01
0.10	-1.21	2.0924E-15	3.6090E-15	0.46	0.53	4.5893E-01	9.6161E-01
0.11	-1.16	2.3016E-15	3.8024E-15	0.47	0.58	5.9615E-01	9.8363E-01
0.12	-1.11	2.5109E-15	2.8601E-14	0.48	0.63	7.2682E-01	9.9385E-01
0.13	-1.07	2.7201E-15	2.3645E-13	0.49	0.68	8.3454E-01	9.9797E-01
0.14	-1.02	2.9294E-15	1.6225E-12	0.50	0.73	9.1117E-01	9.9941E-01
0.15	-0.97	3.1386E-15	9.7686E-12	0.51	0.78	9.5806E-01	9.9985E-01
0.16	-0.92	3.3478E-15	5.2952E-11	0.52	0.82	9.8270E-01	9.9997E-01
0.17	-0.87	3.5571E-15	2.6233E-10	0.53	0.87	9.9379E-01	9.9999E-01
0.18	-0.82	3.7663E-15	1.2513E-09	0.54	0.92	9.9807E-01	1.0000E+00
0.19	-0.78	2.1733E-14	6.9107E-09	0.55	0.97	9.9948E-01	1.0000E+00
0.20	-0.73	2.1209E-13	2.6769E-08	0.56	1.02	9.9988E-01	1.0000E+00
0.21	-0.68	1.7358E-12	1.1600E-07	0.57	1.07	9.9998E-01	1.0000E+00
0.22	-0.63	1.1373E-11	4.8126E-07	0.58	1.11	1.0000E+00	1.0000E+00
0.23	-0.58	6.4625E-11	1.9316E-06	0.59	1.16	1.0000E+00	1.0000E+00
0.24	-0.53	4.1126E-10	7.5246E-06	0.60	1.21	1.0000E+00	1.0000E+00
0.25	-0.48	2.4773E-09	2.8566E-05	0.61	1.26	1.0000E+00	1.0000E+00
0.26	-0.44	1.2132E-08	1.0566E-04	0.62	1.31	1.0000E+00	1.0000E+00
0.27	-0.39	5.2343E-08	3.7635E-04	0.63	1.36	1.0000E+00	1.0000E+00
0.28	-0.34	2.4478E-07	1.2625E-03	0.64	1.41	1.0000E+00	1.0000E+00
0.29	-0.29	1.0945E-06	3.8474E-03	0.65	1.45	1.0000E+00	1.0000E+00
0.30	-0.24	4.7123E-06	1.0185E-02	0.66	1.50	1.0000E+00	1.0000E+00
0.31	-0.19	1.9709E-05	2.2466E-02	0.67	1.55	1.0000E+00	1.0000E+00
0.32	-0.15	7.9860E-05	4.0237E-02	0.68	1.60	1.0000E+00	1.0000E+00
0.33	-0.10	3.1104E-04	5.9110E-02	0.69	1.65	1.0000E+00	1.0000E+00
0.34	-0.05	1.1366E-03	7.5125E-02	0.70	1.70	1.0000E+00	1.0000E+00
0.35	**0.00**	**3.7379E-03**	**8.9858E-02**				

NOTE: The mean for true strain is 0.35, shown in bold. The standard deviation (std) of true strain is 0.21.

Source: Ref. D4.1.27, Table 6.3.7.3-1

The weldment at best can have the same mechanical properties as the hosting metal (native metal), but it is usually more brittle than the hosting metal. The failure likelihood of the

weldment substructure was considered, reflecting weighting factors of both 1.0 and 0.75 applied to estimated true strain at failure.

The capacity function is based on coupon tensile strength tests in uniaxial tension. However, cracking of a stainless steel may not be determined simply by comparing the calculated plastic strain to the true strain of failure, because the equivalent (or effective) plastic strain (EPS) is calculated from a complex 3-D state of stress, while the true strain at failure was based on data from a 1-D state of stress. A 3-D state of stress may constrain plastic flow in the material and lower the EPS at which failure occurs. This loss of ductility is accounted for by the use of a triaxiality factor, which is the ratio of normal stress to shear stress on the octahedral plane, normalized to unity for simple tension. For the purpose of determining the probability of structural failure, LLNL (Ref. D4.1.27) set the ductility ratio to 0.5. This is equivalent to a triaxiality factor of 2, which corresponds to a state of biaxial tension.

Failure of containment can occur when strain in a component is of sufficient magnitude that it results in breakage or puncture of the container. The probability of failure is calculated based on the maximum strain for a single finite element brick obtained from LS-DYNA simulations. Fracture propagation takes place on the milliseconds time-scale and thus propagates across the canister wall thickness very quickly, compared to the time-frame of the LS-DYNA simulations. Furthermore, the fragility curve is obtained on the basis of a maximum average strain over the thickness of the respective specimens, which are 2 in. long stainless steel 304L specimens. Although LS-DYNA results provide multiple values of the strain through the thickness of the canister wall (the wall thickness being represented by multiple finite element layers), it is more conservative to use the maximum strain value at a single finite element brick than the average of the multiple values across the thickness of the wall.

The probability of failure for each impact scenario is evaluated by finding the maximum strain at a location in which a through-wall crack would constitute a radionuclide release. A probability of failure is determined from the CDF of capacity or fragility curve (as discussed below) from the global maximum strain.

A conservative approach and aid to computational efficiency is achieved by performing calculations focusing on the regions of the container having high strain (and deformation) after a drop (“hot zones”). An importance sampling strategy was used which places greater-than-random emphasis on ranges of input-variable values, and/or on combinations of such value ranges, that are more likely to affect output. This approach is an alternative to Monte Carlo methods with the important advantage that possible combinations of upper-bound variable values are in fact incorporated into each probabilistic estimate of expected model output (which is not always guaranteed by uniform sampling).

Using the general probabilistic approach summarized here, LLNL (Ref. D4.1.27) calculated failure probabilities for representative canisters in an aging overpack, and in a transportation cask, and for the representative canister itself, as presented in Tables D1.2-2 through D1.2-5. For the drop of a 10-metric-ton load onto a cask, the falling mass is modeled as a rigid (unyielding) wall, oriented normal to longitudinal axis of the cask.

D1.2 IDAHO NATIONAL LABORATORY ANALYSIS OF SPENT NUCLEAR FUEL CANISTERS AND MULTICANISTER OVERPACKS

Drop tests of prototype canisters conducted by the Idaho National Laboratory (INL) confirmed that the stainless steel shell material can undergo significant strains without material failure leading to loss of containment. These drop tests also validated analytical models used to predict strains under various drop scenarios. Table D1.2-6 shows scenarios selected to address potential drop scenarios at YMP facilities and the predicted strains.

INL performed FEA (using ABAQUS/Explicit, which, like LS-DYNA, has been used in nuclear facility and non-nuclear industrial applications, and is appropriate to model nonlinear, transient responses of a passive component to a structural challenge such as a drop or an impact) of 23-foot drops, three degrees off vertical, to determine the extent of strain at various positions in the bottom head, cylindrical shell, and joining weld. The strain was evaluated and reported for the inside, outside, and middle layers (Ref. D4.1.64). The U.S. Department of Energy (DOE) standardized spent nuclear fuel (SNF) canisters were modeled at 300°F, the maximum skin temperature expected due to the heat evolved by the fuel (based on review of thermal analyses performed by transportation casks vendors), resulting in diminished casing material strength. It was found that greater strains would be expected in the multicanister overpacks (MCOs) at ambient temperatures than at elevated temperatures.

During a canister drop event, the majority of the kinetic energy at impact performs work on the material, which causes the worst locations to exhibit plastic strain. A good measure of this work is equivalent plastic strain, which is a cumulative strain measure that takes into account the deformation history starting at impact. From the peak equivalent plastic strain, LLNL (Ref. D4.1.27) developed failure probabilities using the method described in Section D1.1 for an 18 in. and 24 in. DOE standard canister and an MCO. Results are summarized in Table D1.2-7.

Table D1.2-1. Container Configurations and Loading Conditions

Container	Configuration	Drop Type/Impact Condition[a]	Drop Height
AO (aging overpack) cell with canister inside	Representative canister inside AO	A IC 1: End with vertical orientation	3-ft vertical
		A IC 2: Slapdown from a vertical orientation and 2.5 mph horizontal velocity	0-ft vertical
Transportation cask with spent nuclear fuel (SNF) canister inside	Representative canister inside representative cask	T IC 1a: End, with 4 degree off-vertical orientation	12-ft vertical
		T.IC 1b: Same as T.IC 1a	13.1-ft vertical
		T.IC 1c: Same as T.IC 1a	30-ft vertical
		T IC 2a: End, with 4 degree off-vertical orientation, and approximated slapdown	13.1-ft vertical
		T.IC 2b: Same as T.IC 2a, with no free fall	0-ft vertical
		T IC 3: Side, with 3 degree off-horizontal orientation	6-ft vertical
		T IC 4: Drop of 10-metric-ton load onto top of cask	10-ft vertical
DPC (Dual purpose canister) TAD (Transportation, aging, and disposal) canister	Representative canister	D IC 1a: End, with vertical orientation	32.5-ft vertical
		D IC 1b: Same as D.IC 1a	40-ft vertical
		D IC 2a: End, with 4 degree off-vertical orientation	23-ft vertical
		D IC 2b: Same as D.IC 2a	10-ft vertical
		D IC 2c: Same as D.IC 2a	5-ft vertical
		D IC 3: 40 ft/min horizontal collision inside the CTM bell	No drop
		D IC 4: Drop of 10-metric-ton load onto top of canister	10-ft vertical
		D.IC 2a: Hourglass-control study for end drop, with 4 degree off-vertical orientation	23-ft vertical
		D.IC 2a: Friction coefficient sensitivity study for end drop, with 4 degree off-vertical orientation	23-ft vertical
		D.IC 2a: Mesh density study for end drop, with 4 degree off-vertical orientation	23-ft vertical
		D.IC 2a: Shell- and bottom-lid-thickness sensitivity study for end drop, with 4 degree off-vertical orientation	23-ft vertical
DSNF (DOE spent nuclear fuel) canister	INL-analyzed case	O.IC 1: End, with 3-degree-off vertical orientation	23-ft vertical

NOTE: A = aging overpack; (AO) CTM = canister transfer machine; ft = foot; D = dual purpose canister; IC = impact condition; min = minute; mph = miles per hour; O = DOE SNF canister; SNF = spent nuclear fuel; T = transportation cask.

Source: [a] Ref. D4.1.27, Table 4.3.3-1a.

Table D1.2-2. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for Representative Canister within an Aging Overpack

Container Type/ Impact Condition[a]	Impact Condition Description	Max EPS[b]	Failure Probability[b]			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
A.IC 1	3-ft end drop, with vertical orientation	0.16%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
A.IC 2	Slapdown from a vertical orientation and 2.5-mph horizontal velocity	0.82%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$

NOTE: [a]"A" stands for aging overpack. "IC" stands for impact condition, which are defined in Table D1.2-1.
[b]Values of Max EPS and failure probability are applicable to the SNF canister.

Source: Ref. D4.1.27, Table 6.3.7.6-1.

Table D1.2-3. Failure Probabilities with and without Triaxiality Factor, with and without Fragility Curve Adjustment, for Representative Canister

Container Type/ Impact Condition[a]	Impact Condition Description	Max EPS[b]	Failure Probability[b]			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
D.IC 1a	32.5-ft end drop, with vertical orientation	2.13%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 1b	40-ft end drop, with vertical orientation	2.65%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 2a	23-ft end drop, with 4-degree off-vertical orientation	24.19%	$<1 \times 10^{-8}$	**7.71×10^{-1}**	**9.72×10^{-6}**	**9.96×10^{-1}**
D.IC 2b	10-ft end drop, with 4-degree off-vertical orientation	19.71%	$<1 \times 10^{-8}$	**7.01×10^{-2}**	**1.73×10^{-8}**	**3.19×10^{-1}**
D.IC 2c	5-ft end drop, with 4-degree off-vertical orientation	15.76%	$<1 \times 10^{-8}$	**4.10×10^{-5}**	$<1 \times 10^{-8}$	**3.12×10^{-2}**
D.IC 3	40-ft/min horizontal side collision	0.16%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 4	10-ft drop of 10-metric-ton load onto top of canister	0.75%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$

Table D1.2-3. Failure Probabilities with and without Triaxiality Factor, with and without Fragility Curve Adjustment, for Representative Canister (Continued)

Container Type/ Impact Condition[a]	Impact Condition Description	Max EPS[b]	Failure Probability[b]			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
D.IC 2a S1-L1	Same as D.IC 2a	24.19%	$<1 \times 10^{-8}$	**7.71×10^{-1}**	**9.72×10^{-6}**	**9.96×10^{-1}**
D.IC 2a S2-L1	Same as D.IC 2a	21.52%	$<1 \times 10^{-8}$	**1.66×10^{-1}**	**2.44×10^{-7}**	**7.62×10^{-1}**
D.IC 2a S3-L1	Same as D.IC 2a	16.53%	$<1 \times 10^{-8}$	**3.37×10^{-4}**	$<1 \times 10^{-8}$	**6.02×10^{-2}**
D.IC 2a S1-L2	Same as D.IC 2a	23.34%	$<1 \times 10^{-8}$	**5.52×10^{-1}**	**3.07×10^{-6}**	**9.78×10^{-1}**
D.IC 2a S1-L3	Same as D.IC 2a	25.15%	$<1 \times 10^{-8}$	**9.28×10^{-1}**	**3.48×10^{-5}**	**1.00**
D.IC 2a S2-L3	Same as D.IC 2a	22.57%	$<1 \times 10^{-8}$	**3.50×10^{-1}**	**1.07×10^{-6}**	**9.28×10^{-1}**
D.IC 2a S3-L3	Same as D.IC 2a	18.08%	$<1 \times 10^{-8}$	**1.22×10^{-2}**	$<1 \times 10^{-8}$	**1.14×10^{-1}**
D.IC 2a S2-L4	Same as D.IC 2a	24.07%	$<1 \times 10^{-8}$	**7.44×10^{-1}**	**8.27×10^{-6}**	**9.95×10^{-1}**
D.IC 2a S3-L4	Same as D.IC 2a	19.50%	$<1 \times 10^{-8}$	**6.29×10^{-2}**	**1.37×10^{-8}**	**2.77×10^{-1}**

NOTE: [a] "D" stands for dual purpose canister. "IC" stands for impact condition, which are defined in Table D1.2-1.
[b] Values of Max EPS and failure probability are applicable to the SNF canister. A range of canister shell and bottom plate thicknesses were evaluated. The values shown are for the configuration that yielded the highest strains (0.5-inch shell thickness and 2.313 inch bottom plate thickness).
See Table 6.3.3.5-1 of Ref. D4.1.27 for definitions of H1, F1, M1, etc. See Table 6.3.3.6-1 of Ref. D4.1.27 for definitions of S1, L1, etc.

Source: Seismic and Structural Container Analyses for the PCSA (Ref. D4.1.27, Table 6.3.7.6-3)

Table D1.2-4. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Representative Canister inside the Transportation Cask

Container Type/ Impact Condition[a]	Impact Condition Description	Max EPS[b]	Failure Probability[b]			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
T.IC 1a	12-ft end drop, with 4-degree off-vertical orientation	3.53%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1b	13.1-ft end drop, with 4-degree off-vertical orientation	4.06%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1c	30-ft end drop, with 4-degree off-vertical orientation	5.77%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 2a	13.1-ft end drop, with 4-degree off-vertical orientation, and approximated slapdown	4.35%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 2b	Approximated slapdown from vertical orientation	1.25%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 3	6-ft side drop, with 3-degree off-horizontal orientation	2.07%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 4	10-ft drop of 10-metric-ton load onto top of cask	0.96%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5a	30-ft end drop, with vertical orientation	3.55%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5b	30-ft end drop, with 4-degree off-vertical orientation	5.77%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5c	30-ft end drop, with 45-degree off-vertical orientation	6.41%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5d	30-ft end drop, with center of gravity over corner (i.e., point of impact)	6.63%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$

NOTE: [a]"T" stands for transportation cask. "IC" stands for impact condition, which are defined in Table D1.2-1.
[b]Values of Max EPS and failure probability are applicable to the SNF canister.

Source: Ref. D4.1.27, Table 6.3.7.6-2

Table D1.2-5. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Transportation Cask

Container Type/ Impact Condition[a]	Impact Condition Description	Max EPS[b]	Failure Probability	
			CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality
T.IC 1a	12-ft end drop, with 4-degree off-vertical orientation	9.20%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1b	13.1-ft end drop, with 4-degree off-vertical orientation	9.37%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1c	30-ft end drop, with 4-degree off-vertical orientation	11.25%	$<1 \times 10^{-8}$	9×10^{-7}
T.IC 2a	13.1-ft end drop, with 4-degree off-vertical orientation, and approximated slapdown	9.94%	$<1 \times 10^{-8}$	3×10^{-8}
T.IC 2b	Approximated slapdown from vertical orientation	5.30%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 3	6-ft side drop, with 3-degree off-horizontal orientation	7.42%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 4	10-ft drop of 10-metric-ton load onto top of cask	1.76%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5a	30-ft end drop, with vertical orientation	3.17%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5b	30-ft end drop, with 4-degree off-vertical orientation	11.25%	$<1 \times 10^{-8}$	9×10^{-7}
T.IC 5c	30-ft end drop, with 45-degree off-vertical orientation	70.56%	1	1
T.IC 5d	30-ft end drop, with center of gravity over corner (i.e., point of impact)	44.88%	0.9	1

NOTE: [a]"T" stands for transportation cask. "IC" stands for impact condition, which are defined in Table D1.2-1.
[b]Values of Max EPS and failure probability are applicable to the structural body of the transportation cask, which excludes the shield and shield shell.

Source: Probabilities calculated using Table D1.1-1 based on strains reported in *Seismic and Structural Container Analyses for the PCSA* (Ref. D4.1.27, Table 6.3.7.6-2)

Table D1.2-6. Strains at Various Canister Locations Due to Drops

Canister	Component	Maximum PEEQ Strains (%)			Load Case/ Conditions
		Outside Surface	Mid-Surface	Inside Surface	
18-inch DOE STD canister	Lower head	8	3	6	300°F, 23-foot drop, 3 degrees off-vertical Material: ASME Code minimum strengths
	Lower head-to-main shell weld	2	2	3	
	Main shell	2	2	3	
	Upper head-to-main shell weld	0	0	0	
	Upper head	1	0.2	2	
24-inch DOE STD canister	Lower head	2	0.7	1	300°F, 23-foot drop, 3 degrees off-vertical Material: ASME Code minimum strengths
	Lower head-to-main shell weld	0.2	0.3	0.5	
	Main shell	0.2	0.3	0.5	
	Upper head-to-main shell weld	0	0	0	
	Upper Head	0	0	0	
MCO	Lower head	35	16	14	70°F, 23-foot drop, 3 degrees off-vertical Material: Actual material properties (significantly higher than ASME Code minimums)
	Lower head-to-main shell weld	21	11	11	
	Main shell	13	15	29	
	Upper head-to-main shell weld	0	0	0	
	Upper head	0	0	0	

NOTE: ASME = The American Society of Mechanical Engineers; DOE STD = U.S. Department of Energy standard; MCO = multicanister overpack; PEEQ = peak equivalent.

Source: Ref. D4.1.64, Tables 13, 14, and 16

Table D1.2-7. Failure Probabilities for the DOE Spent Nuclear Fuel (DSNF) Canisters and Multicanister Overpack (MCO)

Component	Peak Equivalent Plastic Strain (%)			Probability of Failure					
				Original CDF			CDF adjusted to min elongation		
	Outside Surface	Middle	Inside Surface	Outside Surface	Middle	Inside Surface	Outside Surface	Middle	Inside Surface
18-inch standard canister containment PEEQ strains, 3 degrees off vertical drop, 300°F									
Lower Head	8	3	6	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Lower Head-to-Main Shell Weld	2	2	3	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Main Shell	2	2	3	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head-to-Main Shell Weld	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head	1	0.2	2	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
24-inch standard canister containment PEEQ strains, 3 degrees off vertical drop, 300°F									
Lower Head	2	0.7	1	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Lower Head-to-Main Shell Weld	0.2	0.3	0.5	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Main Shell	0.2	0.3	0.5	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head-to-Main Shell Weld	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
4 MCO containment PEEQ strains, 3 degrees off vertical drop, 70°F									
Bottom	35	16	14	3.74E-03	<1E-08	<1E-08	8.99E-02	<1E-08	<1E-08
Bottom-to-Main Shell	21	11	11	<1E-08	<1E-08	<1E-08	1.16E-07	<1E-08	<1E-08
Main Shell	13	15	29	<1E-08	<1E-08	1.09E-06	<1E-08	<1E-08	3.85E-03
Collar	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Cover	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08

NOTE: ASME = The American Society of Mechanical Engineers; CDF = cumulative distribution function; DOE STD = U.S. Department of Energy standard; MCO = multicanister overpack; PEEQ = peak equivalent.

Source: Ref. D4.1.27, Tables 6.3.7.6-4 and 6.3.7.6-5

D1.3 PROBABILITIES OF FAILURE OF HIGH LEVEL WASTE CANISTERS DUE TO DROPS

The probability of failure for drops of high-level radioactive waste (HLW) canisters was assessed by evaluating actual drop test data. Several series of tests were conducted including vertical, top, and corner drops of steel containers. The reports on these tests are summarized in *Leak Path Factors for Radionuclide Releases from Breached Confinement Barriers and Confinement Areas* (Ref. D4.1.17). No leaks were found after 27 tests, 14 of which were from

23 feet and 13 of which were from 30 feet. These tests can be interpreted as a series of Bernouilli trials, for which the outcome is the breach, or not, of the tested canister. The observation of zero failures in 13 tests was interpreted using a beta-binomial conjugate distribution Bayes analysis.

A uniform prior distribution, which indicates prior knowledge that the probability of failure is between 0 and 1, may be represented as a Beta(r,s) distribution in which both r and s equals 1. The conjugate pair likelihood function for a Beta(r,s) distribution is a Binomial(n, N) where n represents the number of failures within the tests and N represents the number of tests. The posterior distribution resulting from the conjugate pairing is also a Beta distribution with parameters r' and s', which are defined as follows:

$$r' = r + n \quad \text{and} \quad s' = s + N - n \qquad \text{(Eq. D-1)}$$

The mean, μ, and standard deviation, σ, of the posterior distribution are determined using the following equations:

$$\mu = r' / (r' + s') \quad \text{and} \quad \sigma = \{r's' / [(r' + s' + 1)(r' + s')^2]\}^{1/2} \qquad \text{(Eq. D-2)}$$

For n = 0 and N = 13, Equation D-2 results in $\mu = 0.067$ and $\sigma = 0.062$. For n = 0 and N = 27, $\mu = 0.034$ and $\sigma = 0.033$. These values are used for the failure probability of a dropped HLW canister, for example during its transfer by a canister transfer machine.

One element of the Nuclear Safety Design Basis (Section 6.9) requires that the transportation cask, which will deliver HLW and DOE standardized canisters, be designed to preclude contact between the canister and a transportation cask lid or other heavy object that might fall. Similarly, other large heavy objects are precluded from damaging these canisters, when residing within a co-disposal waste package by the design of the waste package, which includes separator plates that extend well above the canisters. These scenarios are not quantitatively analyzed herein.

The combined INL and LLNL analyses discussed previously conclude that a DOE SNF canister has a probability of breach less than 1E-08 for a 23 foot drop, 4 degrees off-normal (i.e., 4 degrees from vertical) onto an unyielding rigid surface. The LLNL results demonstrate that generally strains from impact and probability of failure is higher for off-normal drops than normal (i.e., vertical) drops for the same height. The LLNL results further show that a 10 ton load dropped from 10 feet onto a representative canister also results in a probability of breach of less than 1E-08. INL analysis EDR-NSNF-087 entitled Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository states that canister integrity was maintained for a 30 foot drop test onto a rigid, unyielding surface. The report discusses drop of a HLW canister on a DOE SNF canister and drop of a DOE SNF canister onto another one. Drops of these canisters onto canisters in the IHF or CRCF would occur with drop heights of less than 10 feet. Two main differences are noted between a drop of a DOE SNF and a drop of a HLW canister onto a DOE SNF. The first is that substantially lower kinetic energy of impact of the latter drop would result in significantly less skirt deformation. The non-flat bottom nature of the HLW/DOE SNF interaction would have a different skirt deformation pattern that the flat bottomed drop. INL concludes that the skirt would be expected

to absorb the bulk of the heaviest HLW canister (4.6 tons) drop energy and DOE SNF canister integrity would be maintained. A difference between a 10 ton drop of a load onto a representative canister and a drop onto a DOE SNF canister results from the difference diameters of the target as well as different materials and lid thicknesses. Nevertheless, INL concludes that the impact from 10 feet of a HLW canister onto a DOE SNF canister is less challenging than impact from a 30 foot drop. Since the probability from a 23 foot drop was calculated to be less than 1E-08, it is conservative to use a value of 1E-05 for the probability of failure of an HLW on DOE SNF impact. The increased value is assigned to account for uncertainties owing to the differences noted above.

D1.4 PROBABILITIES OF FAILURE OF WASTE PACKAGES DUE TO DROPS AND IMPACTS

The probabilities of containment failure are evaluated by comparing the challenge load with the capacity of the waste package to withstand that challenge in a manner similar to that described in *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis - Level of Information and Reliability Estimation.* HLWRS-ISG-02 (Ref. D4.1.56), and summarized in Section 4.3.2.2. Three scenarios are evaluated for the potential loss of containment by waste packages due to drops and impacts:

- Two-foot horizontal drop
- 3.4-mph end-to-end impact
- Rockfall on waste package in subsurface tunnels.

An additional scenario, drop of a waste package shield ring onto a waste package, is considered in Section D1.4.4.

For this assessment, the potential load has been determined by FEA in the calculations cited below as the sources of inputs. The load is expressed in terms of stress intensities and as expended toughness fraction (ETF), which is the ratio of the stress intensity to the true tensile strength. The ETF is used to obtain the failure probability by the following:

$$P \quad \int_{-\infty}^{x} N(t)\,dt \quad and \quad x \quad \frac{ETF - 1}{COV} \qquad \text{(Eq. D-3)}$$

Where:

P = probability of failure

$N(t)$ = standard normal distribution with mean of zero and standard deviation of one

t = variable of integration

ETF = expended toughness fraction

COV = coefficient of variation = ratio of standard deviation to mean for strain capacity distribution, applied here to stress capacity or true tensile strength

The capacity is the true tensile strength of the material, the stress the material can withstand before it separates. The minimum true tensile strength, σ_u, for the Alloy 22 typically used for the outer corrosion barrier (OCB) of the waste package is 971 MPa (Ref. D4.1.20, Section 7.7, p. 162). The variability in the capacity is expressed as the standard deviation of a normal distribution that includes strength variation data and variability of the toughness index, I_T, computed without triaxialty adjustments (uniaxial test data). The standard deviation as percent of the mean of σ_u is 25% (Ref. D4.1.20, Section 7.6, p. 162). The distribution of elongations used for defining the fragility curve in the LLNL analysis was expressed as two normal distributions, the larger of which was with a mean of 59.3% elongation and a standard distribution of 4.22% elongation, or a COV of 0.0712 (Ref. D4.1.27, Section 6.3.7.3). Thus the 0.073 reported for the OCB material is conservative compared with the LLNL data and is used for the COV in the expression above. The possibility of waste package weld defects is not explicitly considered in the analysis. However, as noted in Section D.1.4.5, weld defects are not expected to contribute significantly to the probability of waste package failure due to drops or other impacts.

D1.4.1 Waste Package Drop

A study investigating the structural response of the naval long waste package to a drop while it is being carried on the emplacement pallet, found the ETF for the outer corrosion barrier (OCB) to be 0.29 for a 10 m/s flat impact (Ref. D4.1.20, Table 7-15, pg. 117), equivalent to a 16.7-foot drop. This corresponds to a failure probability of less than 1×10^{-8}. The failure of the OCB is used to define the loss of containment, taking no credit for the inner vessel and the canister within. The description of the transport and emplacement vehicle (TEV) provided in *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (Ref. D4.1.12) mentions that the floor plate is lifted by four jacks and guided by a roller. The guide roller precludes tilted drops of the flat bed of the TEV. As was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of 1×10^{-5} is used for the probability that the waste package containment would fail due to a two-foot horizontal drop, which is much less severe than the modeled 16.7-foot drop.

D1.4.2 Rockfall onto a Waste Package

A seismic event during the preclosure period could cause rocks to fall from the ceiling of a drift onto the waste packages stored there prior to deployment of the drip shields. The extent of damage has been predicted for several levels of impact energy of falling rocks (Ref. D4.1.26). The maximum credible impact energy from a falling rock is about 1×10^6 joules (J) (Ref. D4.1.21, p. 57). The maximum ETF resulting from rockfall impacting with approximately 1×10^6 J is about 0.11 (Ref. D4.1.26, p. 54, Table 5), corresponding to a failure probability less than 1×10^{-8}. As was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of 1×10^{-5} should be used for the probability that the waste package containment would fail due to rockfall on the waste package.

D1.4.3 Results for the Three Assessed Scenarios

The failure probabilities for the three scenarios, derived from the results in the cited reports, are summarized in Table D1.4-1.

Table D1.4-1. Waste Package Probabilities of Failure for Various Drop and Impact Events

Event	Probability of Failure
2-Foot Horizontal Drop	$< 1 \times 10^{-5}$
3.4-mph end-to-end impact	$< 1 \times 10^{-5}$
20 metric ton Rockfall on Waste Package with and without Rock Bolt[a] Impacting the Waste Package	$< 1 \times 10^{-5}$

NOTE: [a]A rock bolt is a long anchor bolt, for stabilizing rock excavations, which may be tunnels or rock cuts.

Source: Original

D1.4.4 Drop of a Waste Package Shield Ring onto a Waste Package

After the co-disposal waste package has been welded closed in the Waste Package Positioning Room, the shield ring is lifted from it before the waste package transfer trolley is moved into the load out area. Grapple failures might cause the drop to occur at a variety of orientations relative to the top of the waste package. A frequency of canister breach from a potential drop as high as 10 feet is considered here. For a canister breach to occur, the shield ring must penetrate the 1-inch thick outer lid made of SB 575 (Alloy 22) and the 9 inch thick stainless steel inner lid (SA 240) before having an opportunity to impact the canister (Ref. D4.1.13). There are six inches separating the inner and outer lids. In the radial center area of that space, which would be directly above the DOE SNF canister, is a stainless steel lifting device attached to the inner lid. This adds another layer of energy absorption.

The shield ring weighs approximately 15 tons and is made of stainless steel with a lighter weight neutron absorber material. The impact energy of a 15-ton shield ring dropping 10 feet would be 0.4 MJ. The frequency of penetration of the sides of a waste package from a 20 metric ton rock impacting the side of the waste package with impact energy of 1 MJ is less than 1×10^{-8} (Table D1.4-1). The sides of a waste package are approximately three inches thick compared to a cumulative thickness (excluding lifting fixture) of 10 inches at the top. Although the impact energy could be more focused, the impact energy for the shield ring against the top of the waste package is less than the impact energy of the rockfall against the side and the top is much thicker than the side. The probability of failure due to shield ring impact against the top of the waste package is expected to be no worse than for the impact of a rock against the side. A conservative value of 1×10^{-5} is used in the analysis for this probability.

D1.4.5 Waste Package Weld Defects

Waste package closure involves engaging and welding the inner lid spread ring, inerting the waste package with helium, setting and welding the outer lid to the outer corrosion barrier, performing leak testing on the inner vessel closure, performing nondestructive examination of welds, and conducting postweld stress mitigation on the outer lid closure weld.

The weld process of the waste package closure subsystem is controlled as a special process by the Quality Assurance Program (Ref. D4.1.29, Section 9.0). The activities performed by the system are controlled by approved procedures.

The principal components of the system include welding equipment; nondestructive examination equipment for visual, eddy current, and ultrasonic inspections of the welds and leak detection; stress mitigation equipment for treatment of the outer lid weld; inerting equipment; and associated robotic arms. Other equipment includes the spread ring expander tool, leak detection tools, cameras, and the remote handling system. The system performs its functions through remote operation of the system components.

The capability of the waste package closure subsystem will be confirmed by demonstration testing of a full-scale prototype system. The prototype includes welding, nondestructive examinations, inerting, stress mitigation, material handling, and process controls subsystems. The objective of the waste package closure subsystem prototype program is to design, develop, and construct the complete system required to successfully close the waste package. An iterative process of revising and modifying the waste package closure subsystem prototype will be part of the design process. When prototype construction is finalized, a demonstration test of the closure operations will be performed on only the closure end of the waste package; thus, the mock-up will be full diameter but not full height as compared to the waste package. The purpose of the demonstration test is to verify that the individual subsystems and integrated system function in accordance with the design requirements and to establish closure operations procedures. This program is coordinated with the waste package prototype fabrication program.

The principal functions of the waste package closure subsystem are to:

- Perform a seal weld between the spread ring and the inner lid, the spread ring and the inner vessel, and the spread ring ends; perform a seal weld between the purge port cap and the inner lid; and perform a narrow groove weld between the outer lid and the outer corrosion barrier.

- Perform nondestructive examination of the welds to verify the integrity of the welds and repair any minor weld defects found.

- Purge and fill the waste package inner vessel with helium gas to inert the environment.

- Perform a leak detection test of the inner lid seals to ensure the integrity of the helium environment in the inner vessel.

- Perform stress mitigation of the outer lid groove closure weld to induce compressive residual stresses.

The gas tungsten arc welding process is used for waste package closure welds and weld repairs. Welding is performed in accordance with procedures qualified to the *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section IX), as noted below:

- The spread ring and purge port cap welds are two-pass seal welds.
- The outer lid weld is a multipass full-thickness groove weld.

Welding process procedures will be developed that identify the required welding parameters. The process procedures will:

- Identify the parameters necessary to consistently achieve acceptable welds.
- State the control method for each weld parameter and the acceptable range of values.

The welds are inspected in accordance with examination procedures developed using *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section V and Section III, Division 1, Subsection NC) as a guide, with modification as appropriate:

- Seal welds—visual inspection
- Groove welds—visual, eddy current, and ultrasonic inspection.

A weld dressing end effector is used for weld repairs. The defect is removed, resulting in an excavated cavity of a predetermined contour. The excavated cavity surface is inspected using the eddy current inspection end effectors. Then the cavity is welded and inspected in accordance with the welding and inspection procedures.

The stress mitigation process for the outer lid closure weld is controlled plasticity burnishing. Controlled plasticity burnishing is a patented method of controlled burnishing to develop specifically tailored compressive residual stress with associated controlled amounts of cold work at the outer surface of the waste package outer lid closure weld.

The inner vessel of the waste package is evacuated and backfilled with helium through a purge port on the inner lid. The inerting process is in accordance with the inerting process described in NUREG-1536 (Ref. D4.1.54, Sections 8.0 and V.1). After the waste package inner vessel is backfilled by helium, both the spread ring welds and the purge port plug are leak tested in accordance with *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section V, Article 10, Appendix IX) to verify that no leakage can be detected that exceeds the rate of 10^{-6} std cm^3/s.

Waste package closure welding, nondestructive examination, stress mitigation, and inerting are conducted in accordance with approved administrative controls. The processes for waste package closure welding, nondestructive examination, stress mitigation, and inerting will be developed in accordance with the codes and standards identified below. The processes are monitored by qualified operators, and resulting process data are checked and verified as acceptable by qualified individuals.

Waste package closure welding, nondestructive examination, stress mitigation, and inerting normal operating procedures will specify, for example, the welding procedure specification, nondestructive examination procedure, qualification and proficiency requirements for operators and inspectors, and acceptance and independent verification records for critical process steps.

The waste package closure subsystem–related welds, weld repairs, and inspections are performed in accordance with *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section II, Part C; Section III, Division I, Subsection NC; Section IX; Section V).

The inerting of the waste package is performed in accordance with the applicable sections of NUREG-1536 (Ref. D4.1.54).

PCSA event sequences involving waste packages include challenges ranging from low velocity collisions to a 20 metric ton rockfall to a spectrum of fires. Waste package failure probabilities are calculated to be very low. Furthermore, a significant conservatism in the analysis is that the containment associated with the canister is not included in the probability of containment breach. In other words, if the waste package breaches, radionuclide release is analyzed as if the canister has breached (if the event sequence is in Category 1 or 2). Analytically, the canister is not relied upon for event sequences involving waste packages. The analytical results from the LLNL analysis show a significant reduction in canister strains is achieved by transportation cask and aging overpack protection. Although not analyzed, a similar ameliorating effect on the canister would be expected to be provided by the waste package.

The weld, inspection and repair process ensures no significant defects to a high reliability. The event sequence analysis shows that all event sequences associated with waste package breach are Beyond Category 2. In the context of the event sequence analysis, a significant defect is one that would have increased the probability of breach of the canister within the waste package by orders of magnitude. Even for significant weld defects, the protection offered by the waste package to the canister containment function would remain. Therefore, the effect of waste package weld failure on loss of canister containment during event sequences is not further considered.

D1.4.6 Waste Package End-to-End Impact

An oblique impact of a long naval SNF waste package inside TEV) was modeled to assess the structural response (Ref. D4.1.19). Most of the runs were with initial impact velocity of 3.859 m/s corresponding to a drop height of 0.759 m (2.49 ft). The maximum ETF for the 3.859 m/s (12.66 ft/sec) oblique impact in the OCB is about 0.7 (Ref. D4.1.19, page 37, Table 7-3, runs 1, 2, and 3), corresponding to a failure probability of about 2×10^{-5}. The oblique impact should be bounding for a direct end impact Using equation D-4, an ETF of 0.11 is estimated for the hypothesized 3.4 mph end-to-end collision (two TEVs each traveling 1.7 mph), corresponding to a failure probability of less than 1×10^{-8}. The failure of the OCB is used to define the loss of containment, taking no credit for the inner vessel and the canister within. As was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of 1×10^{-5} is used for the probability that the waste package containment would fail due to a 3.4-mph end-to-end impact.

D1.5 PREDICTING OUTCOMES OF OTHER SITUATIONS BY EXTRAPOLATING STRAINS FOR MODELED SCENARIOS

Equation 17 in Section 6.3.2.2 demonstrates use of the probability of failure at a given drop height together with the COV to predict probabilities at other drop heights. A similar approach can be used to extrapolate from one strain to another to find the corresponding failure probability. The work done on damaging the container expressed in the form of strain should be roughly proportional to the energy input to the material due to the impact. The impact energy is proportional to the drop height or to the square of the impact velocity. Finite element modeling

demonstrated that the increase in strain is actually less than proportional to increase in drop height (Tables D1.2-3 and D1.2-4), so increasing the strain proportionally with drop height or the square of impact velocity is conservative. The strain is extrapolated by multiplying it by the square of the ratio of the velocity of interest to the reference velocity.

$$\tau_i \quad \tau_{ref}\left(\frac{v_i}{v_{ref}}\right)^2 \qquad \text{(Eq. D-4)}$$

Where:

τ_i = strain at velocity of interest (dimensionless)

τ_{ref} = strain at reference velocity (dimensionless)

v_i = velocity of interest (same units as v_{ref})

v_{ref} = reference velocity (same units as v_i)

In case D.IC.3, a 0.16% strain (τ_{ref}) was predicted for a side impact of 40 ft/min (v_{ref}). Using Equation D-4 to extrapolate for an impact velocity of 2.5 miles/hr gives an estimated strain of 4.84%.

The estimated strain is then compared with the fragility curve tabulated in D1.1-1. A failure rate of less than 1×10^{-8} is predicted for a strain of 4.84%. Probabilities of failure for a range of impact velocities are listed in Table D1.5-1.

Table D1.5-1. Calculated Strains and Failure Probabilities for Given Side Impact Velocities

Impact Velocity			
(ft/sec)	(ft/min)	% strain	Probability of failure
0.67	40	0.16	$< 1\times 10^{-8}$
1	60	0.36	$< 1\times 10^{-8}$
2	120	1.44	$< 1\times 10^{-8}$
4	240	5.76	$< 1\times 10^{-8}$
6	360	13	$< 1\times 10^{-8}$
8	480	23	$< 1\times 10^{-5}$

Source: Original

A similar approach is applied to estimate failure probabilities for vertical drops greater than 40 feet. The strains are extrapolated using the ratio of drop heights rather than the squared ratio of impact velocities in Equation D-4.

For the DPC, the maximum EPS is 2.65% for a 40-foot end drop (case D.IC.1b in Table D1.2-3). Strains of 2.98% and 3.31% are estimated for 45- and 50-foot drops, respectively. Doubling the strains to account for triaxiality and comparing these strains with Table D1.1-1 shows the

probabilities of failure are both < 1×10^{-8}. As before, conservative probabilities of 1×10^{-5} are used in the event sequence quantification.

For the DOE standard canister the maximum strain is 8% in the lower head of the 18-inch canister resulting from a 23-foot drop 3 degrees off vertical (Table D1.2-6). By the same approach as above, 10.4%, 15.7%, and 17.4% strains are estimated for 30-foot, 45-foot, and 50-foot drops. Doubling these strains and comparing with Table D1.1-1 yields the failure probabilities of 1×10^{-7}, 3×10^{-2}, and 9×10^{-2} for the 30-foot, 45-foot, and 50-foot drops, respectively. A conservative probability of 1×10^{-5} is used for the 30-foot drop of the DOE standardized canister.

D1.6 MISCELLANEOUS SCENARIOS

D1.6.1 Localized Side Impact on a Transportation Cask

One of the requirements specified for transportation casks is they be robust enough to survive a 40-inch horizontal drop onto an unyielding 6-inch diameter upright cylinder (Ref. D4.2.2, Paragraph 71.73). The impact energy for such a scenario involving a 250,000 pound cask (a typical weight for a loaded cask) – the NAC STC has a loaded weight of 260,000 pounds (Ref. D4.1.50, p. 1.1-1) is about 1.1 MJ. The maximum weight of a forklift is considerably less than 20,000 kg. At a maximum speed of 2.5 mph (1.12 m/s), the maximum impact energy would be 12.5 kJ, a factor of 90 less than the impact energy for the 40-inch drop of the cask. If the resultant strain is proportional to the impact energy and the drop event in the Safety Analysis Report (SAR) is just below the failure threshold (i.e. the median impact energy for failure), the impact energy due to the 2.5-mph impact would be a maximum of $1/90^{th}$ of the median failure impact energy, or 1 – 1/90 COVs less than a normalized median of 1. Equation D-3 is applicable substituting the ratio of impact energy to median failure impact energy for the factor ETF. Using 1/90 (=0.011) in place of the ETF in Equation D-3 gives a probability of failure of much less than 1×10^{-8} due to impact of a forklift against a transportation cask. If the impact speed were 9 mph instead of 2.5 mph, the impact energy would be about $1/7^{th}$ of the energy in the SAR drop event, 0.14 would be used in place of the ETF in Equation D-3, and the probability of failure would still be less than 1×10^{-8}.

D1.6.2 Screening Argument for TAD Weld Defects

TAD canister closure is the process that closes the loaded TAD canister by welding the shield plug and fully draining and drying the TAD canister interior, followed by backfilling the TAD canister with helium and fully welding the TAD canister lid around its circumference onto the body of the TAD canister.

The process control program for the closure welds produced by the TAD canister closure system is controlled as a special process by the Quality Assurance Program (Ref. D4.1.29, Section 9.0).

TAD canister closure is done at the TAD canister closure station in the cask preparation area. The shielded transfer cask containing a loaded TAD canister is transferred from the pool to the TAD canister closure station using the cask handling crane. The shielded transfer cask lid is unbolted and then removed using the TAD canister closure jib crane. The TAD canister is then partially drained via the siphon port in order to lower the water level below the shield plug in

preparation for welding. The TAD canister welding machine is positioned onto the TAD canister shield plug using the TAD canister closure jib crane, and the shield plug is welded in place. After a weld is completed, visual examination of the weld is performed in addition to the eddy current testing and ultrasonic testing that are performed by the TAD canister welding machine.

A draining, drying, and inerting system is connected to the siphon and vent ports in the shield plug and used to dry the interior of the TAD canister, followed by backfilling it with helium gas. Port covers are then placed over the siphon and vent ports and welded in place using the TAD canister welding machine. The TAD canister welding machine is removed, and the outer lid is placed onto the TAD canister using the TAD canister closure jib crane. The TAD canister welding machine is positioned onto the TAD canister outer lid, and the lid is welded in place. The TAD canister welding machine is removed, and the shielded transfer cask lid is placed onto the shielded transfer cask using the TAD canister closure jib crane and installed. Hoses are connected to the fill and drain ports on the shielded transfer cask, and the water is sampled for contamination. If the water is clean, the ports are opened to drain the annulus between the TAD canister and the shielded transfer cask. If the water is contaminated, then the annulus is flushed with treated borated water as needed. A drying system is then used to dry the annulus. The potential for contamination is kept to a minimum by the use of the inflatable seal.

The qualification of the TAD canister final closure welds is in accordance with ISG-18 (Ref. D4.1.55) as specified in *Basis of Design for the TAD Canister-Based Repository Design Concept* (Ref. D4.1.15, Section 33.2.2.36). Adherence to this guidance is deemed to provide reasonable assurance that weld defects occur at a low rate. However, TAD canister weld cracks are considered an initiating event after the TAD canister welding process in the Wet Handling Facility (WHF). If this occurs, the radionuclide release would be minimal because the incoming casks and canisters have already been opened. After TAD canisters are welded, they are placed in aging overpacks and moved by the site transporter to the Canister Receipt and Closure Facility (CRCF). The probability of TAD canister failure during removal from the aging overpack handling in the CRCF and placement into a waste package is considered in the CRCF event sequence analysis. The conditional probability of TAD canister failures during handling in the CRCF has been shown to be small. The low probability of weld defects and their size would not alter this result. After the TAD canister is placed in the waste package, the containment is considered to be the waste package and the TAD canister is no longer relied upon in event sequences involving mechanical impacts.

D2 PASSIVE FAILURE DUE TO FIRE

A risk assessment must consider a range of fires that can occur, as well as variations in the dynamics of the heat transfer and uncertainties in the failure temperature of the target. This section presents an analysis to determine the probability that a waste container will lose containment integrity or lose shielding in a fire. Section D2.1 addresses loss of containment and Section D2.2 addresses loss of shielding.

D2.1 ANALYSIS OF CANISTER FAILURE DUE TO FIRE

A common approach to safety analysis in regards to the effect of a fire is to postulate a specific fire (in terms of duration, combustible loading, heat rate, and other fire parameters) and then apply it to a specific configuration of a target. Then, a simple comparison is made between the temperature that the target reaches as a result of the fire, and the failure temperature of the target. Based on this comparison, a conclusion is made that either the target always fails, or never fails, or fails at some specific time. While such an approach may be appropriate for demonstrating that a specific design code has been met, it is not appropriate for a risk informed PCSA.

There are two parts to the assessment of the canister failure probability (sometimes referred to as the canister *fragility*): determining the thermal response of the canister to the fire and determining the temperature at which the canister will fail. In calculating the thermal response of the canister, variations in the intensity and duration of the fire are considered along with conditions that control the rate of heat transfer to the container (e.g., convective heat transfer coefficients, view factors, emissivities). In calculating the failure temperature of the canister, variations in the material properties of the canister material are considered along with variations in the loads that lead to failure.

D2.1.1 Uncertainty in Fire Severity

In the fragility analysis, fire severity is characterized by the fire temperature and duration, since these factors control the amount of energy that the fire could transfer to a target cask or canister. Uncertainty distributions were developed for the fire temperature and fire duration based on a review of generic and YMP-specific information.

D2.1.1.1 Uncertainty in Fire Duration

In the context of this study, this duration of the fire is from the perspective of the target (i.e., the cask or canister that could be compromised by the fire). Therefore, the fire duration used in the analysis is the amount of time a particular container is exposed to the fire, and not necessarily the amount of time a fire burns. As an example, a fire that propagates through a building over a four-hour period is not a four-hour hazard to a particular target. In calculating the exposure time for a specific target, it does not matter whether the fire started in the room where the target is, or it started in another room and ended where the target is, or the fire passed through the target room between its beginning and end. The exposure duration is how long the fire burns while consuming combustibles in the vicinity of the target. This allows a single probability distribution to be developed for the fire duration, regardless of how the fire arrived at the target, based on estimates of the duration of typical single-room fires.

In order to develop this curve, data on typical fire durations is required. A number of sources were used to derive insights regarding the range of expected durations of typical fires. The following sources were used:

- NUREG/CR-4679 (Ref. D4.1.53) reviewed the results of fire tests conducted by a number of organizations on a variety of types and amounts of combustible materials.

Although focused on nuclear power plants, the materials assessed are typical of those found at a variety of industrial facilities.

- NUREG/CR-4680 (Ref. D4.1.52) reports on the results of a series of tests conducted by Sandia National Laboratories using a series of fuel source packages representative of trash found around nuclear power plants. Once again, these packages are typical of what might be found around other types of industrial facilities.

The tests were not extensive, and represented only particular configurations. In general, the fire durations were found to depend upon the amount, type, and configuration of the available combustible material.

Based on a review of the available information, it was determined that two separate uncertainty distributions (i.e., probability distributions that represent uncertainty) would be needed: one for conditions without automatic suppression and one for conditions with automatic suppression. The derivation of these two distributions is discussed below.

D2.1.1.2 Fire Duration without Automatic Fire Suppression

The first uncertainty distribution was developed for fires in which automatic fire suppression is not available. The vast majority of the tests conducted were for this case. The following summarizes information presented in the three references listed above.

Sandia National Laboratories conducted two large-scale cable fire tests using an initial fire source of five gallons of heptane fuel, and an additional fuel loading of two vertical cable trays with a 12.5% fill consisting of 43-10-foot lengths of cable per tray (Ref. D4.1.53, Section 2.2.1). The only difference between the tests was that one test used unqualified cable and the other used IEEE-383 qualified cable. In the unqualified cable test, the cables reached peak heat release at approximately four minutes, and the rate decayed toward reaching zero at approximately 17 minutes. In the qualified cable test, the cables reached peak heat release at approximately seven minutes, and the rate decayed toward reaching zero at approximately 16 minutes.

Factory Mutual Research Corporation conducted tests for large-scale configurations of cable trays (Ref. D4.1.53, Section 2.2.3). One set of tests involved a configuration of 12 fully loaded horizontal trays in two stacked tiers. NUREG/CR-4679 (Ref. D4.1.53) provides detailed results for three of the "free-burn" tests (no automatic fire suppression). The first test reached and maintained the peak heat release rate at six minutes to 20 minutes, and reached zero at 25 minutes. The second test reached and maintained the peak heat release rate at seven minutes to 25 minutes, and reached zero at 34 minutes. The third test reached and maintained the peak heat release rate at 26 minutes to 40 minutes, and reached zero at 60 minutes.

Lawrence Berkeley Laboratory conducted tests on electrical cabinets (Ref. D4.1.53, Section 2.2.5). Two tests were conducted. The first was a single cabinet with only thermocouple wire and leads and no internal cabinet fuel loading. The fire that exposed the cabinet was two trash bags with loosely packed paper in a 32-gallon polyethylene trash receptacle, plus two cardboard boxes of packing "peanuts." This fire reached a peak heat release rate at seven minutes, and reached zero at 19 minutes. The second test involved two cabinets separated by a

steel barrier. The cabinets contained a total of 64 lengths of cable (48 and 16). The source fire in this test was similar in nature to the first test, but had a heavier container and loose paper instead of the "peanuts." This fire had two peaks, at six minutes and 18 minutes, with the second being much larger than the first. The fire decayed toward reaching zero between 25 minutes and 30 minutes.

The Department of Health and Human Services sponsored a series of tests on various types of furnishing materials (Ref. D4.1.53, Section 3). While the specific types of furnishings are unlikely to be found in a YMP preclosure facility, these results are instructive for combinations of combustible materials that could be found. The first test was on a molded fiberglass chair with a metal frame. The fire reached a peak heat release rate in two minutes, and reached zero at 10 minutes. The second test was for a wood frame chair with latex foam cushions. This fire reached a peak heat release rate in four minutes and reached zero at 40 minutes. The final test was on four stackable, metal frame chairs with cushions that appeared to consist of a wood base, foam core, and vinyl cover. The fire reached a relatively steady state peak heat release rate from four minutes to 23 minutes, and reached zero at 38 minutes.

Sandia National Laboratories performed a series of nine tests on representative transient fuel fires (Ref. D4.1.52). Five different fuel packages were used for the tests. The first two fuel packages used mixed wastes representative of cleaning materials that might be left by maintenance personnel during routine operations. The first package was about 1.8 kilograms, and the second about 2.2 kilograms. The other difference between the two packages was the first package had more cardboard, whereas the second had more plastic. In both tests on the first package, the fire reached a peak heat release rate at approximately four minutes. However, they reached zero at different times (greater than 30 minutes versus approximately 20 minutes). In the two tests on the second package, the time of peak heat release was different (a high peak at four minutes versus a relatively low peak at 10 to 20 minutes), but they both reached zero at approximately the same time (50 minutes).

The third fuel package was designed to represent normal combustibles that might be in control or computer rooms, and consisted primarily of cardboard and stacked paper, with some crumpled paper. Total mass was about 7.9 kilograms. In both tests, the fire reached a peak heat release rate in approximately two minutes, but reached zero at different times (16 minutes versus 20 minutes).

The fourth fuel package was designed to represent mixed waste that might be found in a control room, computer room, security room, or similar location. It consisted primarily of a plastic trash can filled with paper and rags. Total mass was about 1.6 kilograms. In both tests, the fire reached a peak heat release rate in approximately three minutes and remained relatively steady for most of the duration of the fire, but reached zero at different times (54 minutes versus 70 minutes).

The fifth fuel package was designed to represent larger industrial waste containers that might be found in a variety of places in an industrial facility. It consisted primarily of a large plastic receptacle filled with wood, cardboard, paper, and oily rags. Total mass was about 6.5 kilograms. Only one test was conducted with this fuel package, and the fire reached two

separate peak heat release rates (at 35 and 50 minutes) and decayed toward reaching zero at 80 minutes.

The preceding test data were reviewed and a probability distribution for the fire duration was developed based on engineering judgment. This distribution is characterized by 10% to 90% hazard levels of 10 minutes and 60 minutes, respectively (i.e., it was concluded that 10% of the fires would result in a target exposure duration of less than 10 minutes and 90% of the fires would result in a target exposure duration of less than 60 minutes). These values were fitted to a lognormal distribution with a mean and standard deviation of 3.192 and 0.6943, respectively. The mean of this distribution is approximately 31 min, the median (50^{th} percentile) is approximately 24 min, and the error factor (i.e., the ratio of the 95^{th} percentile over the median) is about 3.1. The resultant probability distribution is presented in Table D2.1-1 as the probability of target exposure durations over a set of discrete intervals. The 30-minute design basis fire duration mandated in 10 CFR 71.73 (Ref. D4.2.2) corresponds to the 62nd percentile value of this distribution.

Table D2.1-1. Probability Distribution for Fire Duration - Without Automatic Fire Suppression

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (minutes)	Interval Probability[a]
10	0.1	0 to 10	0.1
20	0.39	10 to 20	0.29
30	0.62	20 to 30	0.23
40	0.76	30 to 40	0.14
50	0.85	40 to 50	0.09
60	0.903	50 to 60	0.053
70	0.936	60 to 70	0.033
90	0.97	70 to 90	0.034
120	0.989	90 to 120	0.019
150	0.9956	120 to 150	0.0066
180	0.998	150 to 180	0.0024
210	0.999	180 to 210	0.001
270	0.99974	210 to 270	0.00074
360	0.99995	270 to 360	0.00021
∞	1	>360	5E-05

NOTE: [a] The interval probability is the difference between the cumulative probability at the top of the interval and the cumulative probability at the bottom of the interval.

Source: Original

D2.1.1.3 Fire Duration with Automatic Suppression

The second uncertainty distribution that was developed is for fires where automatic suppression is available. There were only a limited number of tests conducted for this case.

Factory Mutual Research Corporation conducted tests for large-scale configurations of cable trays, as discussed in the previous sections. In addition to the tests conducted without

suppression, a number of tests were conducted with suppression. NUREG/CR-4679 (Ref. D4.1.53, pp. 26-31) provides detailed results for six of these "extinguishment tests." All these tests involved a configuration of 12 fully loaded horizontal trays in two stacked tiers. Two of the six also involved the addition of two fully loaded vertical cable trays. The cables were polyvinyl chloride (PVC) - jacket with polyethylene insulation. The results of the first four tests were that the fires reached their peak heat release rates at 8, 9, 12, and 12 minutes. The associated times when the heat release rate dropped to zero were 10, 12, 16, and 29 minutes, respectively. The results of the final two tests were peak heat release rates at 9 and 16 minutes, with zero being reached at 24 and 36 minutes, respectively.

These were the only extinguishment tests reported in the references. Therefore, an analysis of a wooden box-type fire conducted by Parsons also was examined. This is not an actual test, but rather a calculation of a "typical" fire where credit was given for the actuation of fire suppression. The calculation gave a peak heat release rate occurring at 7 minutes and extending to 15 minutes. The calculation showed the fire decaying towards zero at approximately 20 minutes.

These test data were reviewed and a probability distribution for the fire duration was developed based on engineering judgment. Although the data are somewhat sparse, they were taken in the overall context of how the actuation of suppression affected the tests conducted and how that compared to the free-burn tests. This was extrapolated to the other free-burn tests. It was judged likely that the operation of automatic suppression would have little effect on the lower end of the distribution, as such fires would likely burn out without actuating suppression. However, there would be a significant effect for the longer fires. It was concluded that a reasonable estimate of the 10 to 90% hazard levels was 10 minutes and 30 minutes (i.e., it was concluded that it was a reasonable interpretation of the data to state that 10% of the fires would result in target exposure duration of less than 10 minutes and 90% of the fires would result in target exposure duration of less than 30 minutes). These values were fitted to a lognormal distribution with a mean and standard deviation of 2.849 and 0.4286, respectively. The resultant uncertainty distribution is presented in Table D2.1-2 as the probability of target exposure durations over a set of discrete intervals.

Table D2.1-2. Probability Distribution for Fire Duration - With Automatic Fire Suppression

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (min)	Interval Probability[a]
10	0.1	0 to 10	0.1
15	0.37	10 to 15	0.27
20	0.63	15 to 20	0.26
25	0.81	20 to 25	0.18
30	0.901	25 to 30	0.091
40	0.975	30 to 40	0.074
50	0.993	40 to 50	0.018
60	0.9982	50 to 60	0.0052
80	0.9998	60 to 80	0.0016
100	0.99998	80 to 100	0.00018
∞	1	>100	2E-05

NOTE: [a] The interval probability is the difference between the cumulative probability at the top of the interval and the cumulative probability at the bottom of the interval.

Source: Original

D2.1.2 Uncertainty in Fire Temperature

As used in the fire fragility analysis, the fire temperature is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. D4.1.61, p. 2-56). A review of the available fire temperature data for liquid and solid fuels is discussed below.

Experimental measurements of liquid hydrocarbon pool fires with radii from 0.25 to 40.0 m indicate effective blackbody radiation temperatures between 1,200°K and 1,600°K (927°C and 1,327°C) (Ref. D4.1.61, p. 2-56). Testing of rail tank cars engulfed in a liquid hydrocarbon pool fire indicates an effective blackbody temperature of 816°C to 927°C (1,089°K to 1,200°K) (Ref. D4.1.2).

Heat release data for combustible solid materials such as wood, paper, or plastic are plentiful, but fire temperature data have generally not been presented. However, *The SFPE Handbook of Fire Protection Engineering* (Ref. D4.1.61, pp. 3-82 to 3-87) discusses the hot gas temperatures associated with fully-developed compartment fires that do include combustion of solid materials. Fully-developed fires involve essentially all combustible material in a compartment, so the peak hot gas temperature should be reasonably indicative of the *effective* fire temperature. The data indicate typical peak temperatures between 400°C and 1,200°C (750°F and 2,190°F). (The 400°C value applies to small, short duration fires and is too low to represent a true fire temperature.)

Fires within one of the YMP facilities are likely to involve both combustible solid and liquid materials. Judgment suggests that most postulated fires should generally resemble the compartment fires discussed in *The SFPE Handbook of Fire Protection Engineering* (Ref. D4.1.61, Section 2, Chapter 7). This implies that the assigned temperature distribution

should be strongly influenced by the 400°C and 1,200°C range. However, combustible liquids (e.g., diesel fuel in a site transporter) may also contribute significantly to some fires, so the upper bound of the fire temperature distribution should include the higher temperatures indicated by the pool fire data. Based on this reasoning, the fire temperature distribution is normally distributed with a mean of 1,072°K (799°C) and a standard deviation of 172°K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C mandated in 10 CFR 71.73 (Ref. D4.2.2).

This fire temperature probability distribution has a value of 400°C for the 5th percentile and 1,327°C for the 99.9th percentile. The first value represents the lower end of the compartment fire temperature range while the second corresponds to the upper end of the liquid pool fire effective blackbody temperature range. Therefore, the distribution applies to fires involving both liquid and solid fuels.

It should be noted that data from fire testing indicate that the fire temperature is not constant over the duration of the fire. The fire temperature generally increases to a peak value and then decreases considerably as the combustible material is consumed. In the fire fragility analysis, herein, the fire temperature is treated as constant, which tends to increase the maximum target temperature.

D2.1.3 Correlation of Fire Temperature and Duration

Testing has shown that fire temperature and duration are negatively correlated. Intense fires with high fire temperatures tend to be short-lived because the high temperature results from very rapid burning of the combustible material. In contrast, long duration fires generally result from slower burning of the combustible material. In the probabilistic fire fragility analysis discussed below, the fire temperature and duration were correlated with a conservative correlation coefficient of -0.5. It is conservative because this correlation allows some fires that have both a high temperature and long duration.

D2.1.4 Uncertainty in the Thermal Response of the Canister

The probability distributions discussed in Section D2.1.1 characterize the uncertainty in the fire severity. In order to determine the probability that a canister fails due to a fire, models are needed to calculate the uncertainty in the thermal response of the container to a fire and the uncertainty in the failure temperature of the container.

The following sections describe the two simplified heat transfer models used to determine the thermal response of the canister to the fire. The heat transfer models have been simplified in order to allow a probabilistic analysis using Monte Carlo sampling. The two models discussed below apply to bare canisters or canisters inside a waste package, transportation cask, or a canister transfer machine (CTM) shielded bell. The simplified model was validated by comparison with a more complete model as discussed in Section D2.1.4.3.

D2.1.4.1 Heat Transfer to Bare Canisters

Bare canisters near or engulfed in a fire can be heated primarily by two heat transfer mechanisms: convection and radiation. Convection heating occurs when hot gases from the fire

circulate and come into contact with the canister surface. Due to gravitational effects, the hot gases from the fire are expected to rise and collect near the ceiling of the room. Thus, unless a canister is engulfed in the fire, the hot gases are unlikely to come into direct contact with the canister, and radiation should be the dominant mode of heating. Further, radiation from the flame (luminous portion of the fire gases) is expected to far exceed radiation from the hot gas layer near the ceiling. For that reason, radiative heating by the hot gas layer is not considered in the fragility analysis. The heat transfer model described in the following sections are believed to capture the important aspects of the heat transfer from the fire.

Due to substantial conduction within the metal wall of the canister, the canister wall is modeled as a single effective temperature (thin-wall approximation) during heatup. Using this approach, the canister temperature (T_c) was advanced in time using the following Euler finite-difference formulation:

$$T_c \quad \frac{q_{c,net}\Delta t}{m_c c_{p,c}} + T_{c,i} \qquad \text{(Eq. D-5)}$$

where

m_c = mass of the canister wall

$c_{p,c}$ = specific heat of the canister material

Δt = time step

$T_{c,i}$ = canister temperature at the beginning of the time step, and

$q_{c,net}$ = net rate of energy deposition into the canister.

The net rate of energy deposition into the canister during the fire is given by the following equation:

$$q_{c,net} \quad q_{r,fire} + q_{c,fire} - q_{r,f} \qquad \text{(Eq. D-6)}$$

where

$q_{r,fire}$ = radiative heat transfer to the canister from the fire

$q_{c,fire}$ = net convective heat transfer to the canister (positive if the canister is engulfed by the fire and negative if the canister is not engulfed by the fire)

$q_{r,f}$ = radiative heat transfer from the canister to material stored in the canister.

The terms on the right-hand-side of this equation are defined below.

An earlier formulation of Equation D-6 included convective heat transfer from the canister wall to the gas inside the canister and from this gas to the spent fuel inside the canister. The addition of this heat transfer term did not significantly affect the heating rate of either the canister or the fuel, but did significantly increase the calculation time for the analysis. For that reason,

convective heat transfer to the gas inside the canister was not included in the subsequent probabilistic analysis.

In this analysis, the important parameters are: (1) the fire temperature, size, and location relative to the canister, (2) treatment of the fire surface as a blackbody, and (3) treatment of the canister surface as diffuse and gray. Thus, the net rate of radiative heat transfer to the canister surface, $q_{r,fire}$, is given by:

$$q_{r,fire} \quad \varepsilon_c A_c F_{c\text{-}fire} F_s \sigma \left(T_{fire}^4 - T_c^4 \right) \qquad \text{(Eq. D-7)}$$

where

ε_c = emissivity of the canister surface

A_c = surface area of the canister

$F_{c\text{-}fire}$ = view factor between the canister and the fire, which is the related to the fraction of radiation leaving the fire that strikes the canister surface

F_s = suppression scale factor (discussed below)

σ = Stefan-Boltzmann constant

T_{fire} = effective blackbody temperature of the fire

T_c = canister temperature.

In Equation D-6, $q_{c,fire}$ is the energy input due to convective heating from the fire, which is given by:

$$q_{c,fire} \quad A_c F_s h_{conv} \left(T_{fire} - T_c \right) \qquad \text{(Eq. D-8)}$$

where h_{conv} is the convective heat transfer coefficient and all other terms are defined as above.

The final term in Equation D-6 is the rate of heat transfer from the canister to the spent fuel or high level waste. This term is given by the following equation:

$$q_{r,f} \quad \frac{A_c F_{c\text{-}f} \sigma \left(T_c^4 - T_f^4 \right)}{1/\varepsilon_c + 1/\varepsilon_f - 1} \qquad \text{(Eq. D-9)}$$

where $F_{c\text{-}f}$ is the view factor between the canister and the fuel, ε_f is the emissivity of the fuel, and T_f is the temperature of the fuel being heated by the canister (outer portion of the fuel).

As the canister becomes hotter and heat is transferred to the fuel, the fuel temperature will also increase according to the following equation:

$$T_f \quad \frac{(q_{r,f} + q_{DH})\Delta t}{m_f c_{p,f}} + T_{f,i} \qquad \text{(Eq. D-10)}$$

where q_{DH} is the decay heat generated in the fuel, m_f is the mass of fuel heated by the canister (outer portion of the fuel), $c_{p,f}$ is the specific heat of the fuel, and $T_{f,i}$ is the fuel temperature at the beginning of the time step.

Equation D-10 uses the mass of fuel being heated by the canister and the corresponding decay heat in this portion of the fuel. This equation ignores heat transfer from the heated fuel to unheated fuel. That is, there is no energy exchange between the outer fuel and the inner fuel.

The fuel mass to use in Equation D-10 can be estimated by calculating the thermal penetration depth within the fuel during the fire. In a number of previous studies (for example, (Ref. D4.1.25)), the fuel region inside the canister has been treated as a homogeneous material with effective thermal properties. The effective thermal properties used in these studies were determined for many different fuel configurations based on the results from detailed thermal analyses. Table D2.1-3 presents the effective thermal properties for 21-PWR fuel in the TAD canister (Ref. D4.1.25).

Table D2.1-3. Effective Thermal Properties for 21-PWR Fuel in a TAD

Property	Value
Density, ρ	3,655 kg/m^3
Specific Heat, c_p	438 J/kg K
Thermal Conductivity, k	4.29 W/m K
Thermal Diffusivity, α	2.6×10^{-6} m^2/s

NOTE: PWR = pressurized water reactor; TAD = transportation, aging, and disposal (canister)

Source: Ref. D4.1.25, Table 17, and Equation 2 of Section 6.2.2.

Based on the effective thermal properties listed in the table, estimation of the thermal penetration depth during a typical fire is given by the following equation:

$$\delta \quad \sqrt{\alpha t} \qquad \text{(Eq. D-11)}$$

where α is the effective thermal diffusivity and t is the time (3,600 seconds). Based on the effective thermal diffusivity shown in the table, a thermal penetration depth of approximately 9.5 cm is calculated. The fuel volume corresponding to this penetration depth is calculated by multiplying the canister interior surface area by the penetration depth. The effective fuel mass is then calculated by multiplying this volume by the effective density of the fuel. The resulting fuel mass is approximately 9,700 kg.

D2.1.4.2 Heat Transfer to a Canister inside a Cask, Waste Package, or Shielded Bell

The calculation of the heating of a canister inside another container or structure is slightly more complex than that for a canister directly exposed to fire. When inside another container, the canister is not directly heated by the fire. Rather, the container is first heated by the fire and then the interior surface of the heated container radiates heat to the canister and also convects heat to any air or other gas in the annular region between the outer container and canister. When there are multiple heat transfer barriers (e.g., the waste package, which has an outer barrier and an

inner barrier), heat transfer between the barriers must also be considered. The following discussion includes the presence of an inner and outer barrier, as is the case for a waste package.

The calculation of canister heating was accomplished by first calculating the temperature of the outer barrier when exposed to a fire. Then, the energy radiated from the outer barrier to the inner barriers was calculated. Next, the energy radiated from the inner barrier to the canister was calculated. Models that included convective heat transfer to and from the gas in the annular spaces between these regions demonstrated that convective heating and cooling had little effect on the heating of the canister, but caused calculation times to be significantly longer. As a result, the convective heat transfer was removed from the models and the temperature increase of the inner barrier and canister were calculated based on radiative heating only.

It should also be noted that many transportation casks have neutron or gamma shielding composed of a low melting point material such as borated polyethylene. This material is likely to melt very quickly so its effect on heat transfer was not considered in the model. In reality, this layer of material would have a substantial resistance to heat transfer, at least initially. Ignoring this thermal resistance is therefore conservative.

The heating of the outer barrier is calculated in the same general manner as that of a bare canister exposed directly to a fire. Due to the substantial conduction within the metal barrier, the thin-wall approximation was applied. Using this approach, the outer barrier temperature (T_{ob}) was advanced in time using the following Euler finite-difference formulation:

$$T_{ob} \quad \frac{(q_{ob} - q_{ib})\,\Delta t}{m_{ob} c_{p,\,ob}} + T_{ob,i} \qquad \text{(Eq. D-12)}$$

where

q_{ob} = radiation and convection to the outer barrier from the fire

q_{ib} = radiation to the inner barrier from the outer barrier

m_{ob} = mass of the outer barrier

$c_{p,ob}$ = specific heat of the outer barrier

Δt = time step

$T_{ob,i}$ = outer barrier temperature at the beginning of the time step.

Equation D-12 does not consider convective heat transfer to the air inside the container. Initial calculations showed that convective heat transfer to the air in the container would be small compared to the radiation heat loss term, so convective heat transfer was neglected.

If (1) the fire temperature, size, and location relative to a container are known, (2) the fire surface can be treated as a blackbody, and (3) the outer barrier surface can be considered diffuse and gray, then the net rate of radiative heat transfer to the outer barrier surface (q_{ob}) can be approximated as:

$$q_{ob} \quad \varepsilon_{ob} A_{ob} F_{fc} F_s \sigma\left(T_f^4 - T_{ob}^4\right) \qquad \text{(Eq. D-13)}$$

where

ε_{ob} = emissivity of the outer barrier surface

A_{ob} = surface area of the outer barrier

F_{fc} = view factor for radiative heat transfer, which is related to the fraction of radiation leaving the fire that strikes the outer barrier surface

F_s = suppression scale factor (discussed below)

σ = Stefan-Boltzmann constant

T_f = fire (flame) temperature

T_{ob} = temperature of the outer barrier.

Once the temperature of the outer barrier is known, the heating of the inner barrier can be found in the same manner. Instead of a fire temperature, the temperature of the heated outer barrier is used and the net rate of radiative heat transfer from the outer barrier interior surface to inner barrier (q_{ib}) can be approximated as:

$$q_{ib} \quad \frac{A_{ob} F_{oi} \sigma\left(T_{ob}^4 - T_{ib}^4\right)}{1/\varepsilon_{ib} + 1/\varepsilon_{ib} - 1} \qquad \text{(Eq. D-14)}$$

where

ε_{ib} = emissivity for of the inner barrier

F_{oi} = view factor for radiation between the outer and inner barriers (discussed below)

T_{ib} = inner barrier surface temperature.

The temperature of the inner barrier is calculated using an equation similar to Equation D-12; however, in this equation, the thermal radiation incident on the inner barrier comes from the outer barrier rather than the fire and the heat loss from the inner barrier is to the spent fuel or high level waste canister.

Finally, the temperature of the canister is calculated using the following equation, which has a form similar to Equation D-12:

$$T_c \quad \frac{(q_{ib} + q_{DH})\Delta t}{m_c c_{p,c}} + T_{c,i} \qquad \text{(Eq. D-15)}$$

where q_{DH} is the total decay heat generated by the contents of the canister and all other terms are defined as in preceding equations.

In Equation D-15, the heat capacity of the contents of the canister is conservatively neglected so that all decay heat is transmitted to the canister wall. In reality, some fraction of the decay heat would be transmitted to the contents of the canister (e.g., the spent fuel or high level waste), increasing the temperature of the contents. Neglecting this term is conservative since it increases the temperature increase of the canister itself.

Note also that, in order to simplify the model, heat transfer from the canister to its contents is ignored in Equation D-15. In reality, some heat would be transferred from the canister wall to the spent fuel or high level waste inside the canister. Neglecting this heat removal is conservative since it increases the temperature increase of the canister.

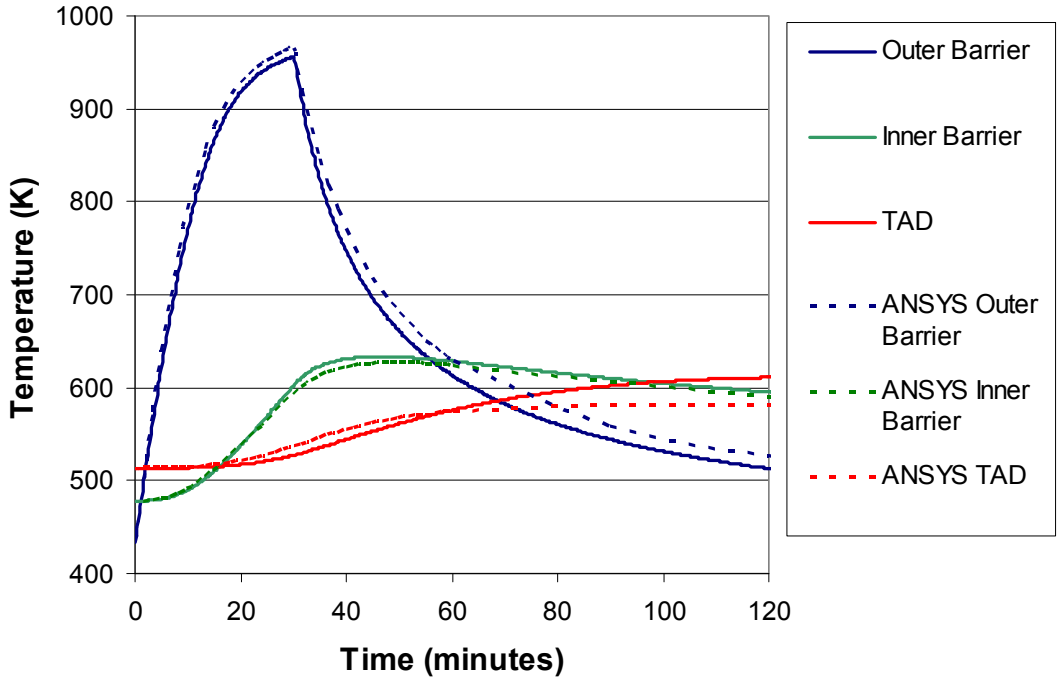
Unlike the bare canister case in which heating of the canister ends when the fire ends, heating of a canister that is inside other containers will increase after the fire ends as heat is transmitted from the heated outer and inner barrier. After the fire has been extinguished, heat will be lost by the outer barrier due to a combination of radiation to cooler surfaces and convection to the air in the room. A temperature of 400°K was used as the surface and air boundary condition. The surfaces were modeled as blackbodies in the radiation heat transfer calculation. Convective heat transfer was calculated based on a heat transfer coefficient of 2.0 W/m^2 K. The fragility analysis showed that the predicted canister failure probability was not sensitive to either the boundary condition temperature or the convective heat transfer coefficient.

D2.1.4.3 Validation of the Simplified Heat Transfer Models

In order to validate the simplified heat transfer models discussed above, results were compared to results calculated using more detailed models. In one such comparison, results calculated using the model for heating of a canister in a waste package were compared to the results from a similar ANSYS calculation (Ref. D4.1.25, Attachment V). ANSYS is a finite-element analysis software application use in nuclear facility and non-nuclear industrial applications to model temperature evolutions of complex systems. The simplified model was set up to match the inputs to the ANSYS calculation as closely as possible. The only differences between the two included:

- The ANSYS run was made with temperature-dependent specific heats whereas average specific heats were used in the simplified model.
- The ANSYS run treated the TAD canister and its contents as a homogeneous material with average properties, whereas the simplified model treated the TAD canister but ignored heat transfer to its contents.

Figure D2.1-1 shows a comparison of the calculated time-dependent temperatures from these two calculations. The figure shows that the simplified model accurately predicts the results from the more detailed analysis. Because heat transfer from the TAD canister to its contents is ignored in the simplified model, the canister reaches slightly higher temperatures with the simplified model compared to the more detailed model.



NOTE: TAD = transportation, aging, and disposal canister.
Source: Original

Figure D2.1-1. Comparison Between Results Calculated Using the Simplified Heat Transfer Model and ANSYS – Fire Engulfing a TAD Canister in a Waste Package

A similar comparison was made between the results reported in the HI-STAR safety analysis report (SAR) (Ref. D4.1.38, Table 3.5.4) and results calculated using the simplified model. These calculations simulated a design basis 30-minute fire. The maximum canister temperature reported in the HI-STAR SAR was 419°F (215°C). This temperature was predicted to occur approximately 3 hours after the start of the fire. The simplified model predicted a peak canister temperature of 213.5°C at approximately 4 hours after the start of the fire. This comparison again demonstrates the accuracy of the simplified model in predicting the maximum canister temperature due to the fire.

Detailed ANSYS calculations were not performed for the bare canister configuration. However, it is possible to infer the accuracy of the simplified bare canister model based on the accuracy of the simplified model in predicting the thermal response of the outer barrier in the waste package configuration. As shown in Figure D2.1-1, the simplified heat transfer accurately predicted the thermal response of the outer barrier both during the 30-minute fire and after.

D2.1.4.4 Heat Transfer Model Inputs and Uncertainties

The heat transfer models discussed in Sections D2.1.4.1 and D2.1.4.2 include a large number of input parameters. Some of these parameters are known to a high degree of confidence whereas

others are considered to be uncertain. This uncertainty was explicitly considered in the probabilistic analysis discussed in Section D2.1.1. The following sections discuss the major inputs to the models and the treatment of the uncertainty in these inputs.

D2.1.4.4.1 View Factor

The radiation view factor from the container (e.g., cask or waste package) to the fire can be calculated if the size of the fire and distance between the fire and the container can be determined. The size (height and width) of the fire can be approximated using published correlations in the SFPE handbook (Ref. D4.1.61, Section 1, Chapter 6). The distance between the fire and the container depends on the location of combustible materials and ignition sources relative to the container.

Since the location of combustible materials and ignition sources relative to the container is difficult to predict and would vary from one room to another, a conservative approach in which the container was engulfed by the fire is followed. For a container completely engulfed by the fire the view factor is essentially 1.0. This is conservative for the long vertically-oriented containers because even an engulfing fire may engulf only the lower portion of the container.

A view factor of 1.0 was applied only to the cask, waste package, or a shielded bell that encase a canister. Bare canisters are treated differently. Since a canister is only bare as it is being withdrawn from a cask or inserted into a waste package, only a portion of the canister could be exposed to the fire at any given time. In this case, the view factor is given by fraction of the canister actually exposed to the fire. This fraction depends on the space between the top of the cask or waste package and the ceiling of the loading or unloading room. Generally, this fraction would be considerably less than 50%.

The radiation view factor between concentric cylinders (e.g., the inner and outer barrier of a waste package) can be estimated very easily if the cylinders are very long compared to their diameters. Under this condition, which is true of most configurations of interest in the current study, the view factor can be approximated by D_i/D_o where D_i and D_o are the inner and outer diameters of the two cylinders (Ref. D4.1.63, Configuration C-63).

D2.1.4.4.2 Consideration of Fire Suppression on Canister Heating

The effect of fire suppression on canister heating is treated using a suppression scale factor. The suppression scale factor is included in the heat transfer equations as an adjustment to the rate of heat transfer to the canister from the fire. The value of the suppression scale factor used in the model is based on testing at the Building and Fire Research Laboratory, which is part of the National Institute of Standards and Technology (Ref. D4.1.31).

The Building and Fire Research Laboratory tests considered a range of fires and a range of sprinkler system spray densities. Results were presented for the net heat release rate from the fire both before and after actuation of the fire suppression system. The fire suppression scale factor implicitly includes consideration of the time delay before actuation of the fire suppression system and the effectiveness of the system. Rooms with early actuation and effective fire suppression would have a very small suppression scale factor, whereas rooms with delayed

actuation and/or ineffective fire suppression would have a large suppression scale factor (upper bound of 1.0 when no suppression is present).

Because no credit is taken for fire suppression in this analysis, the fire suppression scale factor was set equal to 1.0 in all of the analyses discussed in this document.

D2.1.4.4.3 Convective Heat Transfer Coefficient during the Fire

In testing of containers engulfed in a fire, considerable variations in the convective heat transfer coefficient have been measured. Values as high as 30 W/m^2 K have been measured in vigorously burning pool fires (Ref. D4.1.51, pp. 19-21), although values on the order of 20 W/m^2K or less are considered more typical (Ref. D4.1.57, Table 3-2). For fire conditions in which the combustible material is burning more slowly, values on the order of 5 W/m^2 K or lower have been measured (Ref. D4.1.51, p. 19). To capture the potential variability in the convective heat transfer coefficient, a probability distribution for the convective heat transfer coefficient was included in the model. A normal distribution applies with a mean and standard deviation of 17.5 W/m^2 K and 4.2 W/m^2 K, respectively. This distribution yields practical upper and lower bound values (0.1 and 99.9th percentiles) of approximately 5 and 30 W/m^2K.

D2.1.4.4.4 Decay Heat

The canisters processed through the preclosure facilities will contain spent fuel with varying decay heat levels. Based on information provided in the safety analysis reports for transportation casks, a probability distribution was developed for the decay heat level in the canister. A normal distribution applies with a mean and standard deviation of 17kW and 3kW, respectively. This distribution yields practical upper and lower bound values (0.1 and 99.9th percentiles) of approximately 8kW and 26kW.

D2.1.4.4.5 Other Model Inputs

Other inputs required by the heat transfer model include (1) the thermal and physical properties of all materials, (2) the dimensions of the canister, cask, waste package, or shielded bell, (3) the initial temperatures of each layer, (4) decay heat generated within the canister, and (5) the post-fire convective heat transfer coefficient and temperature. The values for these input parameters are provided in Tables D2.1-4 through D2.1-7. The tables also provide a brief rationale or a reference for the values used in the analysis.

As shown in the tables, calculations were performed for two spent fuel canister wall thicknesses: 0.5 inches (0.0127 m) and 1.0 inch (0.0254 m). This was done for two reasons. First, initial calculations showed that the wall thickness greatly influences both the heating and failure of the canister. Second, a review of the available canister information indicated a range of canister thicknesses from 0.5 inches to 1 inch. A substantial fraction of the older transport cask designs have spent fuel canisters with wall thicknesses of 0.5 or 0.625 inches, whereas newer designs (e.g., the naval spent fuel canister or TAD canister) are expected to have a wall thickness of 1.0 inch.

Table D2.1-4. Model Inputs – Bare Canister

Model Parameter	Value	Basis/Rationale
Canister Properties		
Outer Diameter (m)	1.68	Minimum outer diameter listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Density (kg/m^3)	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400C (Ref. D4.1.25, Table 8)
Emissivity	0.8	Estimated value for stainless steel that has undergone some oxidation
Initial Temperature (K)	513	Initial temperature upon removal from the cask. Estimated from *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Fuel Properties		
Heated Mass (kg)		Calculated based on thermal penetration depth (see text)
Specific Heat (J/kg K)	438	Average for fuel region taken from *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Table 15)
Effective Surface Area (m^2)	28.18	Projected area for radiation heat transfer. Calculated based on outer diameter of fuel region (1.67 m)
Emissivity	0.8	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Table 17)
Initial Temperature (K)	543	Estimated from *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Post-Fire Conditions		
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)
Heat Transfer Coefficient (W/m^2 K)	2.0	Approximate value based on correlations in (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-5. Model Inputs – Canister in a Waste Package

Model Parameter	Value	Basis/Rationale
Canister Properties		
Outer Diameter (m)	1.68	Minimum diameter listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Density (kg/m^3)	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Outer Barrier of Waste Package		
Outer Diameter (m)	1.8816	Listed in *TAD Waste Package Configuration* (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0254	Listed in *TAD Waste Package Configuration* (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Length (m)	5.4	Heated length adjacent to the TAD canister – same as TAD canister length
Density (kg/m^3)	8690	Value for Alloy 22 (Ref. D4.1.5, Section II, Part B, SB-575, Section 7.1)
Specific Heat (J/kg K)	476	Value for Alloy 22 at 400°C (Ref. D4.1.36, p. 13)
Emissivity	0.87	Value for Alloy 22 (Ref. D4.1.45, p. 10-297)
Initial Temperature (K)	433	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Inner Barrier of Waste Package		
Outer Diameter (m)	1.8212	Listed in *TAD Waste Package Configuration* (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0508	Listed in *TAD Waste Package Configuration* (Ref. D4.1.22), (Ref. D4.1.23.), and (Ref. D4.1.24)
Length (m)	5.4	Heated length adjacent to the TAD canister – same as TAD canister length
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)

Table D2.1-5. Model Inputs – Canister in a Waste Package (Continued)

Model Parameter	Value	Basis/Rationale
Initial Temperature (K)	478	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Post-Fire Conditions		
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)
Heat Transfer Coefficient (W/m^2 K)	2.0	Approximate value based on correlations in *Introduction to Heat Transfer* (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-6. Model Inputs – Canister in Transportation Cask

Model Parameter	Value	Basis/Rationale
Canister Properties		
Outer Diameter (m)	1.68	Minimum diameter listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Density (kg/m^3)	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Transportation Cask Outer Shell		
Outer Diameter (m)	2.438	From HI-STAR Transportation Cask SAR (Ref. D4.1.38, p. 1.2-3)
Wall Thickness (m)	0.0127	Minimum outer shell thickness listed in cask SARs
Length (m)	5.4	Length adjacent to the TAD canister
Density (kg/m^3)	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)

Table D2.1-6. Model Inputs – Canister in Transportation Cask (Continued)

Model Parameter	Value	Basis/Rationale
Emissivity	0.8	Average value for carbon steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	381	Initial temperature in HI-STAR SAR (Ref. D4.1.38, Figure 3.5.3)
Transportation Cask Gamma Shield		
Outer Diameter (m)	2.148	From HI-STAR Transportation Cask SAR (Ref. D4.1.38, Drawing No.3913)
Wall Thickness (m)	0.19	A lower value for the combined thickness of gamma shield and inner containment listed in cask SARs
Length (m)	5.4	Length adjacent to the TAD canister
Density (kg/m^3)	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)
Emissivity	0.8	Average value for carbon steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	405	Approximate average initial temperature in HI-STAR SAR (Ref. D4.1.38, Figure 3.5.3)
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)
Heat Transfer Coefficient (W/m^2 K)	2.0	Approximate value based on correlations in *Introduction to Heat Transfer* (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SAR = Safety Analysis Report; SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-7. Model Inputs – Canister in a Shielded Bell

Model Parameter	Value	Basis/Rationale
Canister Properties		
Outer Diameter (m)	1.68	Minimum diameter listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in *Transportation, Aging and Disposal Canister System Performance Specification* (Ref. D4.1.28, Section 3.1.1)
Density (kg/m^3)	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)

Table D2.1-7. Model Inputs – Canister in a Shielded Bell (Continued)

Model Parameter	Value	Basis/Rationale
Emissivity	0.62	Average value for Type 316 stainless steel in *Mark's Standard Handbook for Mechanical Engineers* (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Figure 1)
Shielded Bell		
Outer Diameter (m)	2.388	From *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. D4.1.11)
Wall Thickness (m)	0.273	From *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. D4.1.11)
Length (m)	7.62	From *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. D4.1.11)
Density (kg/m^3)	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.67	Approximate value at elevated temperature (corresponds to little oxidation of the surface)
Initial Temperature (K)	306	Maximum interior facility temperature of 90°F (Ref. D4.1.16, Section 3.2)
Post-Fire Conditions		
Ambient Temperature (K)	367	Post-fire temperature of 190°F - a value 100°F higher than the maximum operating temperature listed above
Heat Transfer Coefficient (W/m^2 K)	2.0	Approximate value based on correlations in *Introduction to Heat Transfer* (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

D2.1.4.5 Uncertainty in Canister Failure Temperature

Using the models discussed in Sections D2.1.4.1 and D2.1.4.2, the temperature increase of a canister due to a fire can be calculated. In order to determine whether the temperature is sufficient to cause the canister to fail, it is necessary to determine the canister temperature at which failure would occur. Two failure modes were considered:

1. *Creep-Induced Failure.* Creep is the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load. This mode of failure is possible for long duration fires.

2. *Limit Load Failure.* This failure mode occurs when the load exerted on a material exceeds its structural strength. As the temperature of the canister increases in temperature, its strength decreases. Failure is generally predicted at some fraction (usually around 70 percent) of the ultimate strength.

The modeling associated with these failure modes is described in the following subsections.

D2.1.4.5.1 Modeling Creep-Induced Failure

Creep failure could occur if the canister is maintained at a high temperature for a lengthy period of time. One way to predict creep failure is to calculate a creep damage index, which defines the ratio of the creep damage to the cumulative creep required for failure. Such a model has been used by researchers at Argonne National Laboratory to predict failure of steam generator tubes under accident conditions (Ref. D4.1.46). In the Argonne National Laboratory model, failure occurs when the creep damage index reaches a value of 1. Written in the form of an equation, this condition is given by:

$$\int_0^{t_f} \frac{dt}{t_R(T,\sigma)} \quad 1 \qquad \text{(Eq. D-16)}$$

where

- T = the temperature experienced by the canister (a function of time)
- σ = the tensile stress exerted on the canister wall, and
- t_f = the canister failure time (the time at which the equality is satisfied).

The function in the denominator of Equation D-16 is

$$t_R \quad 10^{\frac{P_{LM}}{T} - 20} \qquad \text{(Eq. D-17)}$$

where P_{LM} is the Larson-Miller parameter (Ref. D4.1.44), which is a material property of the canister material and is a function of the applied stress.

Since the canisters are pressurized to varying degrees with a combination of helium or air used to backfill the canister and gases released when the fuel fails, the pressure inside the canister will increase as the canister gets hotter. The internal pressure exerts a hoop stress in the radial direction that puts the canister wall under tension. It is this stress that controls failure of the canister wall. The hoop stress, σ, is calculated using the following equation:

$$\sigma \quad \frac{P r_c}{h} \qquad \text{(Eq. D-18)}$$

where

- h = the thickness of the canister wall
- r_c = the mean radius of the canister
- P = the pressure difference across the canister wall.

D2.1.4.5.2 Modeling Limit Load Failure

Limit load failure occurs when the load on a structure exceeds its ability to withstand that load. As with the creep failure mode, the load on the canister wall is a hoop stress and is calculated using Equation D-18.

The capability of the canister to withstand a load is given by a flow stress, which is defined by (Ref. D4.1.46, p. 3):

$$\bar{\sigma} \quad k(\sigma_y + \sigma_u) \qquad \text{(Eq. D-19)}$$

where

k = a multiplication factor (0.5 in the current analysis)

σ_y = the yield strength (temperature dependent)

σ_u = the ultimate strength (temperature dependent).

The yield and ultimate strength are both temperature-dependent properties, so the flow stress is also a temperature-dependent property. For a typical 316 stainless steel, a value of 0.5 for k yields a flow stress that is approximately 0.7 times the ultimate strength. Failure is predicted if the hoop stress exceeds the flow stress.

This failure condition is consistent with the failure condition outlined in *2004 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.6, Appendix F, paragraph F-1331). The ASME code specifies that for ferritic steels, the primary membrane stress intensity shall not exceed $0.7\,\sigma_u$. For austenitic steels, the primary membrane stress intensity shall not exceed the greater of $0.7\,\sigma_u$ or $\sigma_y + (\sigma_u + \sigma_y)/3$. As is noted below, for type 316 stainless steels, $0.7\,\sigma_u$ is always the controlling condition.

D2.1.4.5.3 Inputs to the Canister Failure Models

The canister failure models require the following inputs:

- the value for the Larson-Miller parameter (a function of temperature and stress)
- the value for the flow stress (a function of temperature)
- the time-dependent internal pressure and temperature experienced by the canister.

The following discussion outlines how these values were determined.

D2.1.4.5.3.1 Larson-Miller Parameter

The value for the Larson-Miller parameter can be determined based on creep data provided by material suppliers. In the absence of data specific to the steels used for the spent fuel and high level waste canisters to arrive at Yucca Mountain, a literature review was performed to obtain representative creep rupture data for steels of the type expected to be used.

The primary focus of this data search was type 316 stainless steel since that is the steel most likely to be used for the spent fuel or high level waste canisters. Data were collected from the following sources:

- "Properties and Selection of Metals." Volume 1 of *Metals Handbook* (Ref. D4.1.3).
- Reliability and Longevity of Furnace Components as Influenced by Alloy of Construction. H-3124 (Ref. D4.1.35).
- *Creep of the Austenitic Steel AISI 316L(N) -Experiments and Models* (Ref. D4.1.58).
- Assessment of Creep Behaviour of Austenitic Stainless Steel Welds (Ref. D4.1.59).
- *Materials Selection for High Temperature Applications* (Ref. D4.1.60).

The creep data provides the time required for creep rupture given a specified constant temperature and applied tensile stress.

Using this data, the value for the Larson-Miller parameter (Ref. D4.1.44) can be determined from the following equation:

$$P_{LM} \quad T[C + \log(t_f)] \qquad \text{(Eq. D-20)}$$

where

T = temperature (K)

t_f = failure time (hours) determined in testing

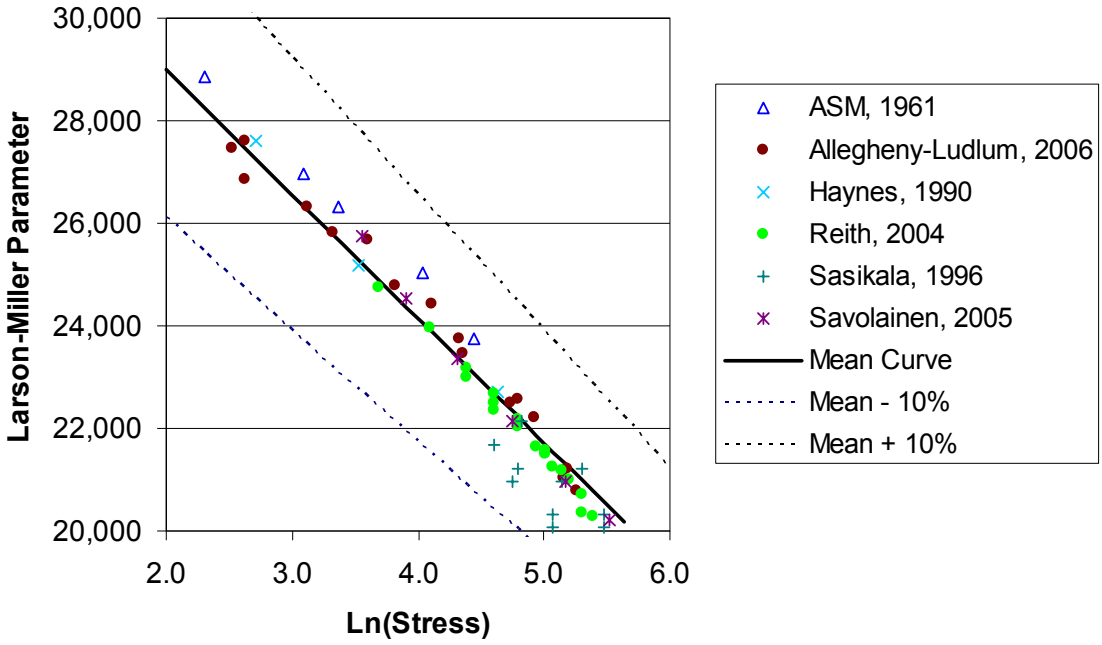
C = a constant that is approximately 20 for most stainless steels

Using this equation and the data collected in the literature review, values for the Larson-Miller parameter were calculated. The calculated values for the Larson-Miller parameter are shown in Figure D2.1-2. As shown in the figure, the Larson-Miller parameter decreases as the applied stress increases.

In order to apply the results shown in the table outside the range of stresses considered in the table, it is necessary to determine a correlation that best fits the data. The best-fit curve, which is also plotted in Figure D2.1-2, is given by the following equation:

$$P_{LM} \quad 33{,}845 - 2{,}423\ln(\sigma) \qquad \text{(Eq. D-21)}$$

As shown in Figure D2.1-2, the value for the Larson-Miller parameter varies from one metal specimen to the next and from one vendor to the next. This variability is illustrated, in part, by the variability in the data shown in the figure. In addition, the research by Sasikala, et al. (Ref. D4.1.59) showed that stainless steel weld material is generally less creep-resistant than the base metal (this is illustrated by the five outlier points on the figure which were determined for the weld material rather than the base metal). The variability in the Larson-Miller parameter must be reflected in the uncertainty analysis for the canister failure temperature.



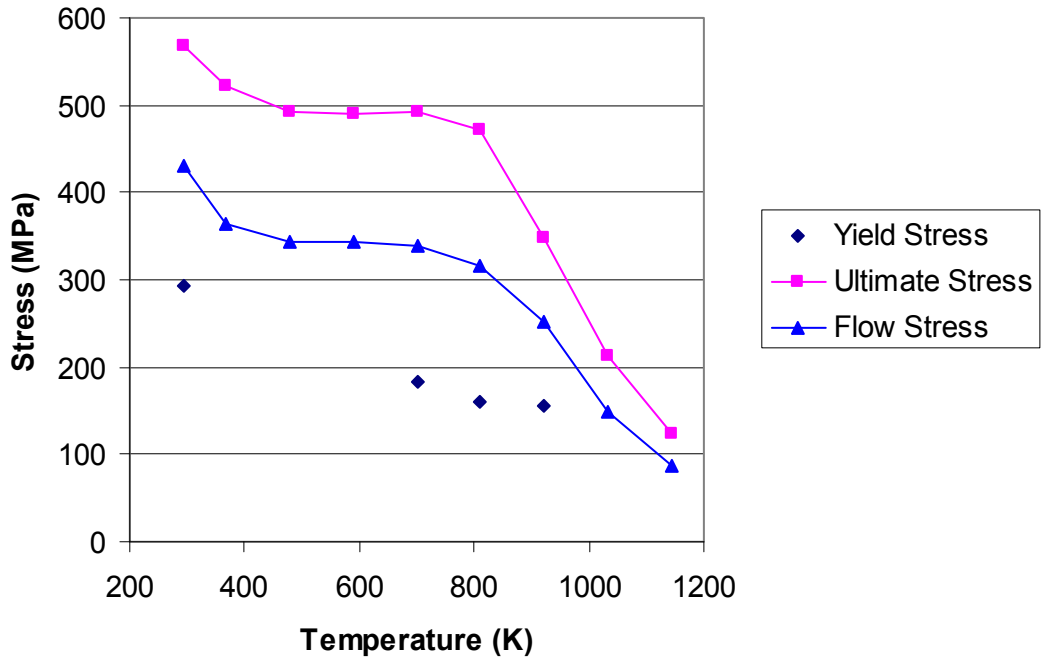
Source: Excel Spreadsheet *Creep rupture - Fast Heatup 1 inch.xls* found in Attachment H.

Figure D2.1-2. Plot of Larson-Miller Parameter for Type 316 Stainless Steel

The uncertainty in the Larson-Miller parameter is treated within the canister failure analysis by multiplying the calculated value for P_{LM} by a factor (1+a), where the value for *a* is normally distributed with a mean of 0.0 and a standard deviation of 0.038. Using this formulation, 99% of all canister steels would have P_{LM} values within approximately 10% of the calculated value. This uncertainty is believed to reflect the variability between different canister steels as well as the variability between the base metal and the weld material.

D2.1.4.5.3.2 Flow Stress

In the canister failure analysis, the flow stress is the average of the yield and ultimate strength. Both the yield and ultimate strength are temperature-dependent and decrease rapidly above a temperature of about 800°K. Figure D2.1-3 presents typical curves for the yield and ultimate strength of Type 316 stainless steel as a function of temperature (Ref. D4.1.1). The figure also presents the calculated flow stress curve. For temperatures with no yield strength data, the flow stress equals 0.7 times the ultimate strength.



NOTE: MPa = megapascals.

Source: Original

Figure D2.1-3. Yield, Ultimate, and Flow Stress for Type 316 Stainless Steel

For the temperature range of interest, the flow stress curve can be fit to two straight lines: one line for temperatures between 350°K and 800°K and another for temperatures above 800°K. The equations for these two lines are provided below:

$$\bar{\sigma} \quad 395.9 - 0.0925\,T \quad \text{for } T < 800\ \text{K} \quad (R^2 \quad 0.889) \qquad \text{(Eq. D-22a)}$$

$$\bar{\sigma} \quad 899.1 - 0.7139\,T \quad \text{for } T \geq 800\ \text{K} \quad (R^2 \quad 0.989) \qquad \text{(Eq. D-22b)}$$

Note that the fit is particularly good for the upper temperature range, which is of greatest interest in the current analysis.

As with the value for the Larson-Miller parameter, the value for the flow stress is uncertain. The uncertainty in the flow stress was treated in the same manner at the uncertainty in the Larson-Miller parameter. Specifically, the mean value described by the equations provided above was multiplied by a factor (1 + a) where the value for *a* is normally distributed with a standard deviation of 0.038. This distribution results in 99% of all canister steels having a flow stress within 10% of the mean value given by the equations. This adequately reflects the variability in the material properties of Type 316 steels, the variability between the properties of the base metal and weld material, and the potential for other types of steel with lower or higher tensile strength to be used in manufacture of the canisters.

D2.1.4.5.3.3 Pressure Difference and Temperature Histories

Creep failure and limit load failure depend on the time-dependent internal pressure and canister temperature. The canister temperature depends on the fire severity and also on whether the canister is bare or enclosed in a waste package or cask. The canister temperature is calculated using a separate analysis, as discussed above. Rather than attempting to couple the canister failure and canister heatup analyses into a single calculation, a separate canister failure analysis was completed. This analysis required the following inputs: the rate of temperature increase of the canister wall and the relationship between the internal canister pressure and the temperature of the canister wall.

Based on a series of runs with the canister heat transfer models discussed above, it was determined that the rate of temperature increase for a bare canister was likely to range from a low of around 25°K/min to a high of around 175°K/min. This range was input as a normal distribution with a mean of 100°K/min and a standard deviation of 25°K/min. Similar runs for the non-bare canister cases indicated a much slower heatup rate. For these cases, the canister heatup rate was input as a normal distribution with a mean of 10°K/min and a standard deviation of 2.5°K/min.

Analyses with a special version of the bare canister heat transfer model were also used to characterize the rate at which the temperature of the gas inside the canister would increase as a result of heating of the canister wall. This version of the model included convective heat transfer from the canister wall to the gas, from the canister wall to fuel assemblies inside the canister, and from the fuel assemblies to the gas inside the canister. These analyses showed a substantial lag in temperature between the canister wall and the gas.

The following equation was used to calculate the internal pressure of the canister based on the canister temperature:

$$P \quad P_0\left[1 + C\left(\frac{T_{can} - T_{can,0}}{T_{can,0}}\right)\right] \qquad \text{(Eq. D-23)}$$

where

P_0 = initial pressure inside the canister (including potential fuel failures)

$T_{can,0}$ = initial temperature of the canister wall

T_{can} = canister temperature at the current timestep

C = a constant that depends on the canister heating rate.

Note that if the value for C is set equal to 1.0 in this equation, the proportional change in pressure is equal to the proportional change in temperature. This would be true if the gas and canister temperatures increased at the same rate. Because the gas temperature lags behind the canister temperature, the value for C is always less than 1. Rather than attempting to model the variability in the value for C, the analysis used a bounding value of 0.5 for all analyses. This value bounded the range of values calculated in the separate heat transfer analysis.

The initial pressure, P_0, in Equation D-23 varies over a wide range depending on the amount of overpressure supplied when the canister is sealed, the extent of fuel rod failures, and the type of fuel stored in the canister. Since the canister failure analysis considers only the increase in gas temperature due to the fire, the initial pressure must reflect potential fuel failures during the fire.

The SARs prepared by transportation cask vendors were consulted for information on internal pressure under normal and accident conditions (see for example, Section 3.6.6 of *GA-9 Legal Weight Truck From-Reactor Spent Fuel Shipping Cask, Final Design Report* (Ref. D4.1.34)). The SARs provide information on the initial overpressure in the canister and the pressure increase associated with fuel rod failures. Based on this information, an uncertainty distribution for the initial pressure in the canister was developed. The uncertainty is characterized by a Weibull distribution with a minimum of 5 psig, a scale factor of 45 psig, and a shape factor of 2.4. This distribution is applied to all canisters considered in the preclosure safety analysis (PCSA).

D2.1.5 Probabilistic Fragility Analysis

The mechanistic models described above produce results that are deterministic. That is, for a given set of input values, they yield a single answer. However, as has been shown, the inputs to the models are uncertain. Uncertainty in the input parameters could lead to a substantial variation in the predicted canister thermal response and failure temperature. Therefore, it is necessary to treat the analysis in a probabilistic manner. It is in the fragility analysis that all the parameters that affect the failure of the spent fuel or high level waste canister are addressed in a probabilistic fashion.

The fragility analysis consists of two separate probabilistic analyses: (1) an analysis to determine the probability distribution for the canister failure temperature, and (2) an analysis to determine the maximum temperature reached by the canister due to the fire. These two analyses are combined to determine the probability that the canister fails as a result of the fire.

Calculations were performed for canisters inside a waste package, a cask, or a shielded bell. As discussed earlier, two canister wall thicknesses were evaluated: 0.5 inches (hereafter referred to as *thin-walled* canisters) and 1.0 inch (hereafter referred to as *thick-walled* canisters). The following sections describe how these analyses are performed and present the calculated failure probabilities for the various canister configurations of interest.

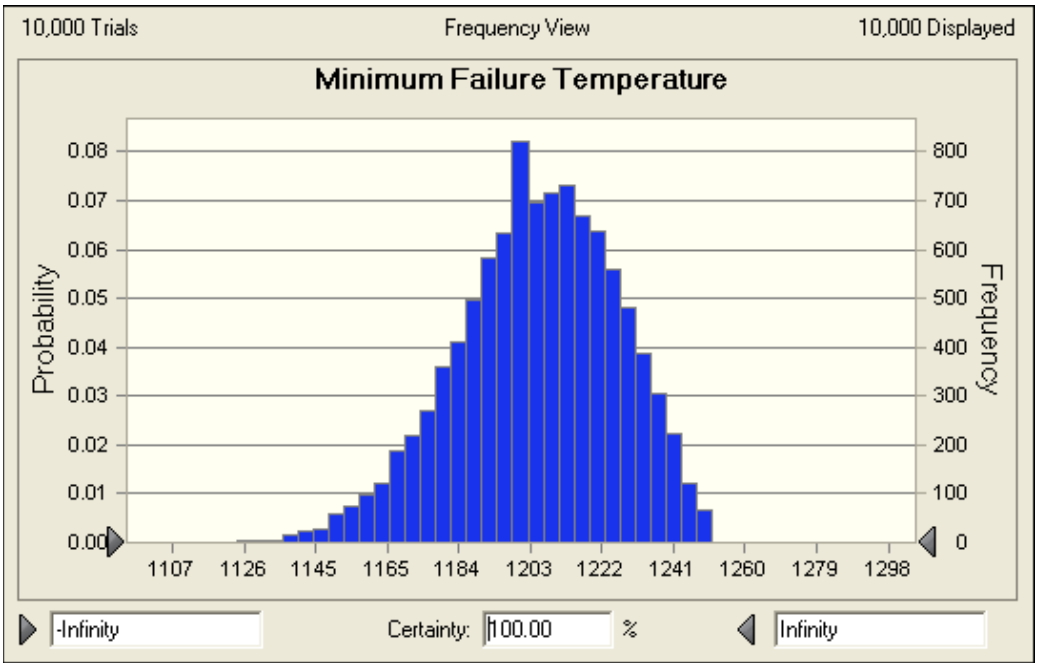
D2.1.5.1 Probabilistic Analysis of Canister Failure Temperature

The first step in the fragility analysis was to determine the probability distribution for the canister failure temperature. The probability distribution was determined using a Monte Carlo analysis in which the failure models outlined in Section D2.1.4 were repeatedly solved with parameter values sampled from the uncertainty distributions discussed in that section. The failure temperature for each sample was the lower of the two temperatures calculated based on creep rupture or limit load failure.

A Microsoft Excel add-in product, Crystal Ball, was used to perform Monte Carlo simulation. Latin hypercube sampling was used to ensure that parameter samples represented the assigned distributions adequately.

Figure D2.1-4 shows the calculated canister failure temperature distribution for canisters inside a waste package, transportation cask, or shielded bell. This calculation used the lower heating rate discussed in Section D2.1.4.5.3.3. The probability distribution shown in Figure D2.1-4 is well-characterized by a normal distribution with a mean of 1,203°K and a standard deviation of 22.85°K. This normal distribution provides a particularly good fit to the lower failure temperature portion of the distribution which is the most important for the canister failure analysis.

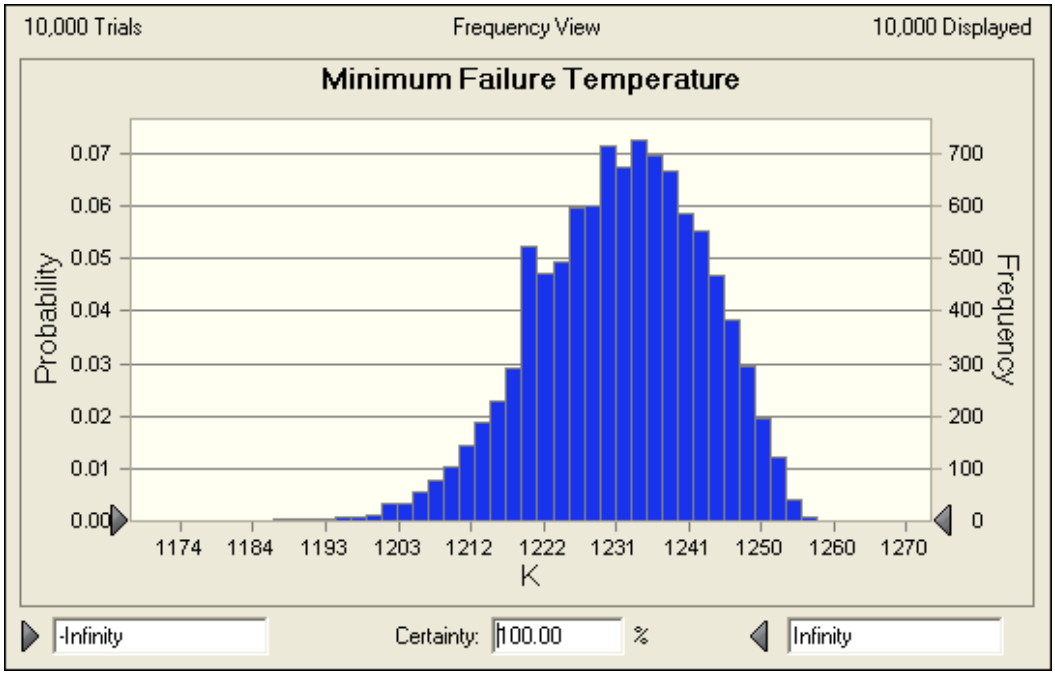
A similar analysis was performed for bare canisters. This calculation used the higher heating rate discussed in Section D2.1.4.5.3.3. The resulting probability distribution was nearly identical to the one shown in Figure D2.1-4. The reason for this is that canister failure was nearly always due to limit load failure rather than creep failure, so the difference in heating rates for the two configurations was not important.



Source: Original

Figure D2.1-4. Probability Distribution for the Failure Temperature of Thin-Walled Canisters

A similar analysis was performed for thick-walled canisters. As with the thin-walled canisters, the probability distribution for the canister failure temperature was found to be nearly independent of the canister heating rate. Figure D2.1-5 shows the calculated probability distribution. This probability distribution is well-characterized by a normal distribution with a mean of 1,232°K and a standard deviation of 12.3°K. This normal distribution provides a particularly good fit to the lower failure temperature portion of the distribution which is the most important for the canister failure analysis.



Source: Original

Figure D2.1-5. Probability Distribution for the Failure Temperature of Thick-Walled Canisters

D2.1.5.2 Probabilistic Analysis to Determine the Maximum Canister Temperature and Canister Failure Probability

The next step in the fragility analysis was to determine the maximum temperature of the canister as a result of the fire. In this analysis, Monte Carlo techniques were used to repeatedly sample from the uncertainty distributions discussed in Section D2.1.4 while applying the canister heating models to determine the maximum temperature of the canister due to the fire. As with the failure temperature analysis, Crystal Ball was used to perform the Monte Carlo simulation.

For each Monte Carlo sample, the calculated maximum canister temperature was then compared to a canister failure temperature sampled from the probability distribution discussed in Section D2.1.5.1. The canister is considered failed if the maximum temperature of the canister exceeded the sampled failure temperature for that Monte Carlo sample. The failure probability was determined as the fraction of the samples for which failure was calculated.

This process was repeated for a sufficient number of samples to provide a good statistical basis for the failure probability. The rule of thumb used in determining the required number of samples was that at least 10 failures had to be calculated. Thus, if the failure probability was on the order of 10^{-4}, 100 thousand (10^5) samples were needed. The maximum number of samples for any run was set at 1 million. If no failures were calculated for one million samples, the failure probability was recorded as being less than 10^{-6}.

Since each Monte Carlo sample has two possible outcomes (failure or no failure), each sample represents a Bernoulli trial. Since the probability of failure or no failure is the same for each trial, the outcome from the sampling process can be represented by a binomial distribution. The

binomial distribution is closely approximated by a normal distribution if the number of failures is greater than about five. The mean of the normal distribution is simply the number of failures divided by the total number of samples. The standard deviation of the normal distribution is given by the following equation:

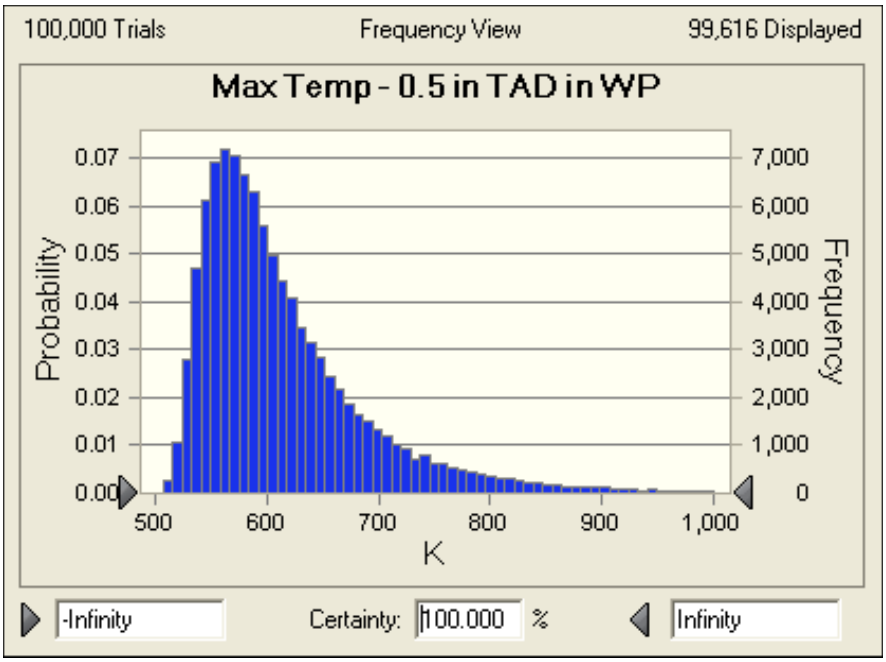
$$\sigma \quad \sqrt{\frac{\frac{n_{fail}}{N}\left(\frac{N - n_{fail}}{N}\right)}{N}} \qquad \text{(Eq. D-24)}$$

where n_{fail} is the number of failures, N is the total number of Monte Carlo samples, and p_{fail} is the calculated mean failure probability (n_{fail}/N).

Figure D2.1-6 shows the calculated distribution for the maximum temperature reached by a thin-walled canister inside a waste package. The figure shows that the vast majority of the Monte Carlo samples had maximum temperatures well below 950°K. Only under extreme combinations of fire temperature and duration did the calculated maximum temperature approach the failure temperatures shown in Figure D2.1-4. Consequently there were only 32 calculated canister failures out of a total of 100,000 Monte Carlo samples. The resulting mean value for the canister failure probability is therefore 32/100,000 or 3.2×10^{-4}. The standard deviation calculated using Equation D-24 is 5.7×10^{-5}. The mean and standard deviation of the failure probability are shown in Table D2.1-8.

A similar analysis was performed for a thick-walled canister inside a waste package. Because of the thicker wall, the failure temperature of the canister is higher than for the thin-walled canister. In addition, the thick-walled canister heats up more slowly than the thin-walled canister because of its greater mass. These two factors combine to substantially lower the probability of failure for these canisters. In the Monte Carlo analysis, 20 failures were calculated for 200,000 samples, which results in a mean failure probability of 1×10^{-4} and a standard deviation of 2.2×10^{-5}.

Similar calculations have been performed for a canister inside a transportation cask and a canister inside the shielded bell of the CTM. The resulting mean and standard deviation for the canister failure probability are provided in Table D2.1-8.



Source: Original

Figure D2.1-6. Probability Distribution for Maximum Canister Temperature – Thin-Walled Canister in a Waste Package

Table D2.1-8. Summary of Canister Failure Probabilities in Fire

Configuration[b]	Monte Carlo Results		Failure Probability	
	Total Failures	Total Trials	Mean	Standard Deviation
Thin-Walled Canister in a Waste Package[a]	32	100,000	3.2×10^{-4}	5.7×10^{-5}
Thick-Walled Canister in a Waste Package[a]	20	200,000	1.0×10^{-4}	2.2×10^{-5}
Thin-Walled Canister in a Transport Cask	2	1,000,000	2.0×10^{-6}	1.4×10^{-6}
Thick-Walled Canister in a Transport Cask	1	1,000,000	1.0×10^{-6}	1.0×10^{-6}
Thin-Walled Canister in a Shielded Bell	27	200,000	1.4×10^{-4}	2.6×10^{-5}
Thick-Walled Canister in a Shielded Bell	27	300,000	9.0×10^{-5}	1.7×10^{-5}

NOTE: [a] For the 5-DHLW/DOE SNF waste package, this probability applies only to the DOE HLW canisters located on the periphery of the waste package. The DOE SNF canister in center of the waste package would not be heated appreciably by the fire.

[b] Configurations not addressed in this table include, any canister in a waste package that is inside the transfer trolley or any canister inside an aging overpack. In these configurations, the canister is protected from the fire by the massive steel transfer trolley or by the massive concrete overpack. Calculations have shown that the temperatures experienced by the canister in these configurations are well below the canister failure temperature. Although failures for these configurations could be screened on this basis, a conservative screening probability of 1×10^{-6} is used in the PCSA.

Source: Original

Note that Table D2.1-8 contains no failure probability for a bare canister configuration. The reason for this is that the canister is outside of a waste package or cask for only a short time. During that time, the canister is usually inside the shielded bell of the CTM. The preceding

analysis addressed a fire outside the shielded bell. When in that configuration, the canister is shielded from the direct effects of the fire. A fire inside the shielded bell, which could directly heat the canister, was not considered to be physically realizable for two reasons. First, the hydraulic fluid used in the CTM equipment is non-flammable (Ref. D4.1.48, p 30) and no other combustible material could be present inside the bell to cause a fire. Second, the annular gap between the canister and the bell only 3 inches wide, but is approximately 27 feet long. Given this configuration, it is unlikely that there would be sufficient inflow of air to sustain a large fire. There may be sufficient inflow to sustain a localized fire, but such a fire would not be adequate to heat the canister to failure.

The canister is also outside of a cask, waste package, or shielded bell as it is being moved from a cask into the shielded bell or from the shielded bell into a waste package. The time during which the canister would be in this configuration is extremely short (a matter of minutes) so a fire that occurs during this time is extremely unlikely. In addition, because the gap between the top of the waste package or cask and ceiling of the transfer cell is generally much shorter than the height of the canister, only a small portion of the canister surface would be exposed to the fire. Furthermore, this exposure would only be for the short time that the canister was in motion.

For these reasons, failure of a bare canister was not considered a physically realizable threat to breach of a canister and was not treated further.

The notes to Table D2.1-8 mention two other configurations for which fire-induced canister failure is not credible: a fire outside a waste package inside a waste package transfer trolley (WPTT) and a fire outside an aging overpack. These two special cases are discussed below.

The failure probability for a waste package in the WPTT was determined using the probabilistic methodology discussed above. For this calculation, the waste package calculation discussed earlier was modified by simply adding a thermal barrier outside the waste package to represent the WPTT. The fire heats the WPTT which then transfers heat by radiation to the outer barrier of the waste package. The WPTT was modeled as having an equivalent external diameter of 3.05 meters, a thickness of 20.3 cm (steel thickness only[1]), and a mass of 89,000 kg. The transfer trolley was considered to be made of a stainless steel with an average specific heat of 476 J/kg K. The probabilistic analysis was run for 1 million Monte Carlo samples and no failures were calculated. Though the maximum temperature calculated in this analysis was well below the failure temperatures shown in Figures D2.1-4 and D2.1-5, a conservative failure probability of 1×10^{-6} is used in the PCSA.

The probabilistic methodology discussed above could not be used for analysis of canister failure for a fire outside an aging overpack. The reason for this is that the concrete that comprises the majority of the aging overpack has a very low thermal conductivity. Therefore, the underlying premise of a relatively uniform temperature in each cylindrical region would be incorrect. Instead, a simple heat conduction calculation was performed to determine how far into the concrete heat could be conducted during a fire. The thermal penetration depth (from Equation D-11) was estimated based on a bounding 2-hour fire and concrete with the following

[1] There is also a 7.5-inch layer of borated polyethylene. Because this layer is likely to melt early in the fire transient, it is ignored in the analysis.

average properties: thermal conductivity = 1.2 W/m K; density = 2,200 kg/m^3; and specific heat = 1,000 J/kg K. The thermal penetration depth calculated for these conditions was 6.3 cm. Since the aging overpack is expected to be at least 24 inches (61 cm) thick, the canister inside the aging overpack will not be heated significantly by the fire. A conservative failure probability of 1×10^{-6} is used in the PCSA.

Note that, in this calculation, the fire was modeled as being only on the outside of the aging overpack. Though the overpack has ventilation openings for natural circulation, this flow path is expected to provide sufficient resistance to airflow that (1) combustion could not be sustained inside the overpack even if fuel entered through the openings, and (2) hot gases would likely flow over the outer surface of the overpack rather than enter the ventilation openings and flow up through the annulus inside the overpack. In fact, because oxygen would be consumed by the fire near the bottom of the overpack, air may actually flow downward through the ventilation openings to supply air to the fire.

D2.1.5.3 Analysis To Determine Failure Probabilities For Bare Fuel in Casks Exposed To Fire

Another fire-induced failure mode is of interest in the PCSA; namely, failure of a transport cask containing bare spent fuel assemblies. The analysis uses GA-4/GA-9 transportation casks to represent casks of this type. Should a transportation cask containing uncanistered spent nuclear fuel fail in a fire, it is of interest for determining the source term to know if the fuel cladding is heated above its failure temperature (approximately 700°C to 800°C).

A modified version of the model for failure of a canister in a transportation cask was used to determine the probability that fuel will exceed this failure temperature. In the modified spreadsheet, the canister was replaced by the mass of fuel that would be heated during the fire. As in the bare canister analysis discussed in Section D2.1.4.1, this mass was estimated based on the calculated thermal penetration depth. Based on the information provided in the GA-9 SAR report (Ref. D4.1.34, p. 3.6-3), the following average spent fuel properties were determined: thermal conductivity = 1.5 W/m K, density × specific heat = 9.9×10^5 J/m^3 K. For a 1-hour fire, the calculated thermal penetration depth is 7.4 cm and the effective fuel mass is 1,910 kg. Since the severe fires of greatest concern have durations of 1 hour or longer, this fuel mass represents a reasonable, but probably conservative, estimate.

Other modifications to the model included changes to model the geometry and materials used in the GA-4/GA-9 casks. The inputs to the model are presented in Table D2.1-9. As in the previous analyses, the model does not rely on neutron shield because it is liable to melt early in the transient.

The model was run for three different fuel failure temperatures: 700°C, 750°C, and 800°C. This range of failure temperatures represents the lower end of the values reported in the literature (Ref. D4.1.65, pp. 7-20 to 7-21). As shown in Table D2.1-10, the calculated fuel failure probabilities were less than 0.001.

Table D2.1-9. Model Inputs – Bare Fuel Cask

Model Parameter	Value	Basis/Rationale
Fuel Properties		
Heated Mass (kg)	1,910	Calculated based on thermal penetration depth (see text)
Specific Heat (J/kg K)	438	Average for fuel region taken from *Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Table 15)
Effective Surface Area (m^2)	10.0	Projected area for radiation heat transfer. Calculated based on equivalent outer diameter of fuel region (0.66 m)
Emissivity	0.8	From *Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident* (Ref. D4.1.25, Table 17)
Initial Temperature (K)	400	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)
Transportation Cask Outer Shell		
Outer Diameter (m)	1.12	Equivalent diameter estimated based on GA-9 SAR (Ref. D4.1.34, Figure 1.2-9)
Wall Thickness (m)	0.0032	Minimum outer shell thickness listed in cask SAR (Ref. D4.1.34)
Length (m)	4.25	Length adjacent to the fuel region
Density (kg/m^3)	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)
Emissivity	0.8	Average value for carbon steel in Avallone and Baumeister, (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	344	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)
Transportation Cask Gamma Shield[a]		
Outer Diameter (m)	0.902	Equivalent diameter estimated based on GA-9 SAR (Ref. D4.1.34, Figure 1.2-9)
Wall Thickness (m)	0.107	Combined thickness of stainless steel and depleted uranium shields (steel: 0.0445 m; DU: 0.0622 m)(Ref. D4.1.34)
Length (m)	4.25	Length adjacent to the fuel region
Mass × Specific Heat (J/K)	3.45×10^6	Based on calculated masses of steel and DU and specific heats listed in GA-9 SAR (Ref. D4.1.34, Tables 2.2-1 and 3.2-2)
Emissivity	0.8	Average value for carbon steel in Avallone and Baumeister, (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	360	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)

Table D2.1-9. Model Inputs – Bare Fuel Cask (Continued)

Model Parameter	Value	Basis/Rationale
Post-Fire Conditions		
Ambient Temperature (K)	361	Post-fire temperature of 190°F from *Discipline Design Guide and Standards for Surface Facilities HVAC Systems* Ref. D4.1.16, Section 3.2). This value is 100 °F higher than the maximum interior facility temperature
Heat Transfer Coefficient (W/m^2 K)	2.0	Natural convection based on anticipated post-fire surface temperature and standard convective heat transfer correlations (Results not sensitive to this value)

NOTE: [a] Composite properties representing both the stainless steel cask wall and depleted uranium gamma shield. DU = depleted uranium

Source: Original

Table D2.1-10. Summary of Fuel Failure Probabilities

Fuel Failure Temperature	Monte Carlo Results		Failure Probability	
	Total Failures	Total Trials	Mean	Standard Deviation
700°C	54	100,000	5.4×10^{-4}	7.4×10^{-5}
750°C	27	100,000	2.7×10^{-4}	5.2×10^{-5}
800°C	13	100,000	1.3×10^{-4}	3.6×10^{-6}

Source: Original

D2.1.5.4 Analysis To Determine Failure Probabilities For Casks Exposed To Fire

NUREG/CR-6672 (Ref. D4.1.65, Section 6) provides an analysis of seal failure in bare fuel transportation casks. The analysis uses a simple 1-D axisymmetric heat transfer model that is similar to the simple model used in the fire fragility analysis presented in Section D2. The simple model is used to determine the length of time the cask could be exposed to an 800°C or 1,000°C fire before seal failure would be predicted.

The report notes that the elastomer seals used in many transportation casks degrade completely at 500°C, but that the degradation rate increases significantly at 350°C (Ref. D4.1.65, p. 2-9). Other seal degradation information provided by cask vendors indicates that the maximum design temperature for the metallic o-ring seals in the TN-68 casks is 536°F (280°C) (Ref. D4.1.66, p. 3-2). This is the maximum safe temperature for continuous operation. The actual failure temperature for these seals would be much higher. Based on this information, seal failure is anticipated at temperatures of around 350°C to 450°C.

NUREG/CR-6672 indicates that the seals in a steel/depleted uranium (DU) truck cask would reach 350°C if exposed to a 1,000°C fire for 0.59 hours (Ref. D4.1.65, Table 6.5). In a steel/lead/steel (SLS) truck cask, this temperature would be reached in 1.04 hours. The times for rail casks were longer at 1.06 hours for an SLS rail cask and 1.37 hours for a monolithic steel rail cask.

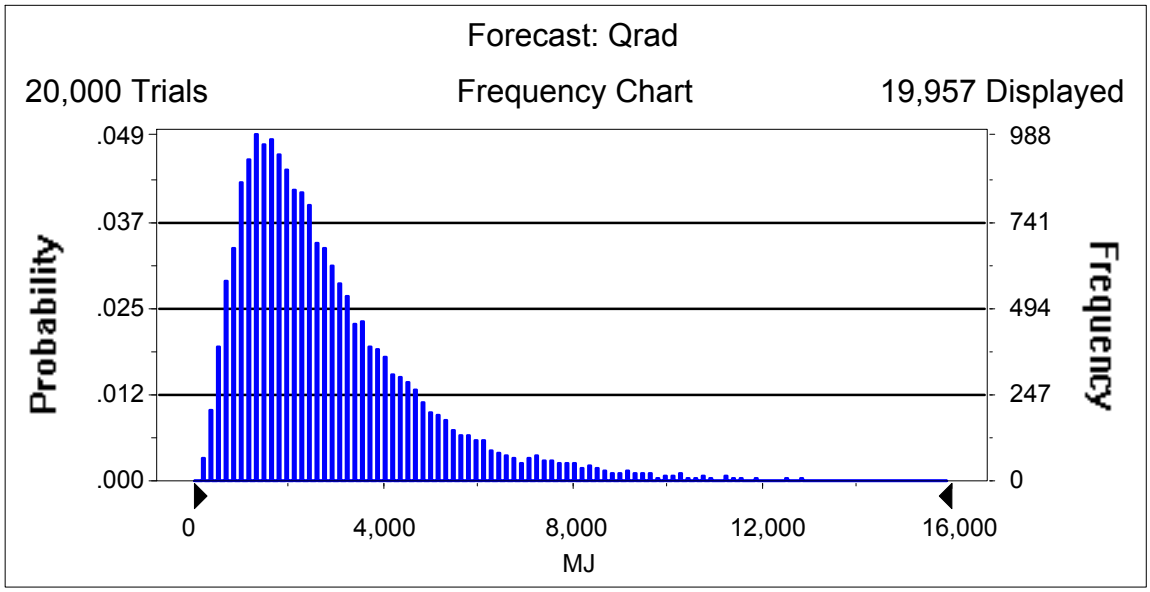
The probability distributions for fire temperature and fire duration discussed in section D2.1.1 can be used to determine the probability that the fire conditions listed in the preceding paragraph would be exceeded. This is accomplished by first determining the probability distribution (using Crystal Ball) for the maximum thermal radiation energy from the fire using the following equation:

$$Q_{rad} \quad \sigma A T_{fire}^{4} t_{fire} \qquad \text{(Eq. D-25)}$$

where:

σ = the Stefan-Boltzmann constant (5.668×10^{-8} W/m^2 K^4)
A = cask surface area exposed to the fire
T_{fire} = fire temperature (sampled from the probability distribution)
t_{fire} = fire duration (sampled from the probability distribution)

The probability distribution for Q_{rad} is shown in the figure below:



Source: Original

Figure D2.1-7. Distribution of Radiation Energy from Fire

Next, the value for Q_{rad} corresponding to the NUREG/CR-6672 fire temperature and duration for seal failure is calculated. The probability distribution for Q_{rad} can then be used to determine the probability that the fire will be severe enough to cause seal failure (i.e., will exceed the value for Q_{rad} calculated based on the NUREG/CR-6672 conditions).

The values for Q_{rad} corresponding to a 1,000°C fire and the fire durations reported in NUREG/CR-6672 are listed below along with the probability of exceedance determined from the probability distribution. The exceedance probabilities can be used as an estimate of the seal

failure probability for seals that fail at the temperature, T_{fail}, listed in Table D2.1-11. For example, for a SLS truck cask that has seals that fail at 350°C, the probability that the seals fail due to a fire is 6.9×10^{-3}.

By multiplying the highest seal failure probability in Table D2.1-11 (0.05) by the highest probability of fire-induced cladding failure in Table D2.1-11 (5.4×10^{-4}), it is shown that the joint conditional probability of a fire that causes additional cladding failure in a truck cask, given a fire, is less than 3×10^{-5}. Because the fire initiating event frequency over the preclosure period of such truck cask fires is less than 1 (see Attachment F for the facilities that contain these, i.e. WHF and Intra-Site operations), such fires are beyond Category 2 and not analyzed further.

Table D2.1-11. Probabilities that Radiation Input Exceeds Failure Energy for Cask

Cask Type	T_{fail} (°C)	Temperature (°C)	Duration (hrs)	Q_{rad} (MJ)	P_{exceed}
Steel/DU Truck Cask	350	1,000	0.59	7,208	5.0×10^{-2}
Steel/Lead/Steel Truck Cask	350	1,000	1.04	12,405	6.9×10^{-3}
Steel/Lead/Steel Rail Cask	350	1,000	1.06	12,950	5.6×10^{-3}
Monolithic Steel Rail Cask	350	1,000	1.37	16,737	1.7×10^{-3}
Steel/DU Truck Cask	500	1,000	≈ 1.0[a]	≈ 12,200	7.1×10^{-3}
Steel/Lead/Steel Truck Cask	500	1,000	≈ 1.3[a]	≈ 15,900	2.2×10^{-3}

NOTE: [a] Estimated from Figure 6.6 in NUREG/CR-6672 (Ref. D4.1.65).

Source: Original

D2.2 SHIELDING DEGRADATION IN A FIRE

The NUREG/CR-6672 (Ref. D4.1.65) transportation study performed analyses on the internal temperatures of cask for long duration fires of 1,000°C. The transportation study included scenarios for fire-only and fire-plus-impact in the calculation of the probability of loss of shielding (LOS).

D2.2.1 Analysis of Loss of Shielding for Transportation Casks

All transportation casks contain separate gamma and neutron shields. The neutron shields are generally composed of a low melting point polymer material that would melt and offgas very quickly when exposed to a fire. For that reason, it is given that the neutron shield is always lost in fire scenarios. The composition of the gamma shield varies between cask designs, with some designs having layers of steel and depleted uranium, others having layers of steel and lead, or and others with layers of steel. Only casks containing lead could lose their gamma shielding in a fire.

As previously discussed, the thermal analyses for the transportation casks (Ref. D4.1.65, Table 6.5) shows that the internal regions of the cask reach the 350°C range in the range of 0.59 to 1.37 hours for the long duration 1,000°C fire. The least time represents the steel- depleted uranium casks and the longest the monolithic steel. The time to reach 350°C for steel-lead-steel (SLS) casks is about one hour. The time to reach the lead melting temperature (327.5°C) should be somewhat less than one hour but is not specified. However, NUREG/CR-6672 (Ref. D4.1.65)

indicates that lead melting in itself does not result in significant LOS but the melting must be accompanied by outer shell puncture that permits the lead to flow out of the shield configuration.

NUREG/CR-6672 states that there are four characteristic fires of interest in the transportation risk analysis: 10 minutes as the duration of a typical automobile fire; 30 minutes for a regulatory fires; 60 minutes for an experimental pool fire for fuel from one tanker truck; and 400 minutes for an experimental pool fire from one rail tank car. These typical durations suggest that a real fire is unlikely to last long enough to result in a LOS condition for transportation scenarios.

D2.2.2 Probability of LOS in Fire Scenarios

Melting of the lead shielding and loss of containment of the molten lead results in loss of shielding for SLS casks. Two mechanisms for escape of the molten lead are considered:

- Puncture of the outer shell
- Rupture lead containment due to internal pressure

Puncture of the 2-inch thick (or more) outer shell, in addition to exposure to fire, would allow molten lead to escape, resulting in LOS. The shell puncture would be an independent failure with a probability of 10^{-8} for the low speeds at which the cask would be moving (Table 6.3-4). With the additional failure of exposure to fire, the LOS probability would be even less.

Containment of the molten lead could be lost due to thermal expansion of the lead coincident with the thermal weakening of the steel. Molten lead is cast into the cavity bounded by the inner and outer shells and the bottom plate ((Ref. D4.1.50, p. 1.1-4); (Ref. D4.1.49, p. 1.2-2); (Ref. D4.1.9, p. 1.2-5); and (Ref. D4.1.47, p. 1-5)). The lead contracts as it cools and solidifies. When the cask is exposed to a fire and the lead melts, it expands to reoccupy the volume when originally cast. When heated beyond the melting point, the liquid lead could continue to expend, exerting hoop stresses upon the inner and outer shells. The shells are thick and strong, e.g. the inner and outer shell thicknesses for the MP197 are 1.25 and 2.5 inches, respectively (Ref. D4.1.47, Drawing 1093-71-4, rev. 1), and the bottom plate thickness is 6.5 inches (Ref. D4.1.47, Drawing 1093-71-2, rev. 1). Consequently, failure of the steel is considered very unlikely.

As part of the PCSA, an attempt was made to analyze hydraulic failure of the molten lead containment due to a fire. Unfortunately, the thermal and physical properties of lead necessary for this analysis could not be found. Thus, hydraulic failure cannot be conclusively disproved. For that reason, a probability of 1.0 is used for LOS by transportation casks due to fire.

D2.2.3 Bases for Screening of Loss of Shielding Pivotal Events for Aging Overpacks in Fire Scenarios

This section summarizes the rationale for screening loss of shielding pivotal events associated with heating of aging overpacks in a fire. Loss of shielding could occur if the concrete that comprises the majority of the aging overpack spalled as a result of the fire. Spalling would reduce the thickness of the concrete and, if sufficient spalling occurs, the thickness could be reduced below the level required for adequate shielding.

D2.2.3.1 Thickness of Concrete Required for Adequate Shielding

The concrete thickness needed for adequate shielding can be estimated by determining the dose outside the overpack for different concrete thicknesses and comparing that dose to the exposure limits for radiation workers. For this calculation, the exposure rate on the surface of the aging overpack prior to the fire is 40 mrem/hr (Ref. D4.1.15, Section 33.2.4.17).

The dose outside the aging overpack is primarily due to Co-60 gamma radiation, the gamma attenuation due to concrete can be estimated based on data available from the National Institute of Standards and Technology (NIST) (Ref. D4.1.40). This reference lists a value for the mass attenuation coefficient of the concrete divided by the concrete density (μ/ρ) of 0.058 cm^2/g for the gammas produced by Co-60. Multiplying this value by an approximate concrete density of 2.3 g/cm^3 (Ref. D4.1.39, Table 4.2.5) yields a value for the mass attenuation coefficient of 0.133 cm^{-1}. Based on this value, there is approximately a factor of 10 reduction in the gamma dose for each 17.2 cm (6.8 inches) of concrete.

If the outer 6.8 inches of concrete were to spall as a result of the fire, the dose at the surface of the aging overpack would increase to 400 mrem/hr. If an additional 6.8 inches of concrete were to spall, the dose on the surface would be 4 rem/hr. The original concrete thickness is 34 inches based on existing aging overpack drawings (Ref. D4.1.14). There is 27.2 inches of concrete remaining after the first 6.8 inches of spallation and 20.4 inches of concrete remaining after the second 6.8 inches of spallation.

The dose outside the aging overpack can be estimated by noting that the dose decreases as the square of the distance from the source. After 13.6 inches of concrete has spalled, the dose 20.4 inches from the surface of the aging overpack would be 1 rem/hr, and the dose 61.2 inches from the surface would be 250 mrem/hr. Therefore, even in the case of extensive concrete spalling, workers involved in fire fighting or post-fire activities could be in close proximity to the degraded aging overpack for a lengthy period of time without exceeding either the annual exposure limit of 5 rem or special exposure limits outlined in 10 CFR Part 20 (Ref. D4.2.1, Paragraph 20.1206).

D2.2.3.2 Extent of Concrete Spalling in a Fire

The current aging overpack design has a steel liner outside the concrete shielding. Consequently, spalling and removal of concrete from the surface cannot occur unless the steel liner is removed or fails catastrophically. However, because alternative aging overpack designs have been considered without a steel outer liner, the potential for substantial spallation with a bare concrete shield was assessed.

Extensive spalling of structural concrete has been observed under some conditions when the structural concrete is exposed to intense fires. The most extensive spalling has been observed in tunnel fires, such as the Channel Tunnel fire in 1996. In such cases, a significant fraction of the concrete spalled when exposed to the intense heat from the long-duration fires.

Due to the potential significance of spalling in reducing the strength of concrete support structures, spallation of concrete has been the subject of considerable study. "Limits of Spalling

of Fire-Exposed Concrete." (Ref. D4.1.37) provides a good overview of the factors that control concrete spalling due to fire. Hertz indicates that that there are three types of spalling that can occur: (1) aggregate spalling, (2) explosive spalling, and (3) corner spalling. Aggregate spalling occurs with some aggregates (such as flint or sandstone) and results in superficial craters on the surface of the concrete. Corner spalling occurs only on the convex corners of beams or other structures and is caused by a localized weakening and cracking of the concrete such that the corner breaks off under its own weight. This mode of spalling is not relevant for the aging overpacks. Explosive spalling occurs when sufficient pressure builds up inside the concrete to cause pieces of concrete to be ejected from the surface. Explosive spalling is believed to account for the extensive concrete loss observed in the Channel Tunnel fire. Of the three modes of spalling, only explosive spalling could produce the loss of concrete necessary to significantly reduce the shielding capability of the aging overpack.

"Predicting the fire resistance behaviour of high strength concrete columns," (Ref. D4.1.43) notes that explosive spalling occurs when sufficient pressure builds up in the pores of the concrete to cause ejection of concrete from the surface. Buildup of such a high pressure requires three things: (1) low concrete permeability, (2) high moisture content in the concrete, and (3) rapid heating and resulting large thermal gradients. In addition, "Limits of Spalling of Fire-Exposed Concrete." (Ref. D4.1.37) notes that spallation is more pronounced in concrete structures undergoing high compressive stress, such as support columns.

Low permeability prevents gas migration and allows pressure to build. High structural strength concretes, such as those used in tunnel construction, are known to have very low permeability and are therefore more prone to spalling. In contrast, normal strength concretes do not have low permeability and spallation is not observed (Ref. D4.1.43). Because the concrete used for shielding in the aging overpacks is not counted on for structural strength and is therefore classified as normal strength concrete[2], spallation is unlikely to occur.

Moisture content is a major factor in pressure buildup because water vapor is the gas primarily responsible for high pore pressures in the concrete. The concrete in the aging overpacks is unlikely to have a high moisture content because it is heated both internally by decay heat and externally by solar heat. In addition, it is likely to have been sitting in the Nevada desert for a lengthy period of time.

Thus, although the fire will produce large thermal gradients in the concrete, these gradients are unlikely to result in pressure buildup sufficient to cause extensive spallation due to the expected high permeability and low moisture content of the aging overpack concrete. This would be true regardless of whether the outer steel liner is present or not.

D2.2.3.3 Conclusion

The preceding discussion has shown that a substantial amount of concrete would have to spall during a fire to produce a hazard to workers involved in either fire fighting or post-fire activities. In addition, it was shown that spallation is very unlikely given the type of concrete to be used in

[2] For example, the compressive strength of the concrete used in the HI-STORM storage overpack (Ref. D4.1.39, Table 1.D.1) is listed as 3,300 psi or 22.75 MPa, which is well below the strength of 55 MPa usually defined as necessary for high strength concrete (Ref. D4.1.43).

the aging overpacks and the likelihood that the aging overpacks will have an outer steel liner. For these reasons, loss of aging overpack shielding in a fire is considered Beyond Category 2 and need not be analyzed further.

D3 SHIELDING DEGRADATION DUE TO IMPACTS

Neutrons emitted from transportation casks are shielded by a resin surrounded by a steel layer. The neutron shielding is present in the top lid, bottom and shell. Neutron shields designed to 10 CFR Part 71 (Ref. D4.2.2) are robust against 10 CFR Part 71 hypothetical accident conditions related to impacts or drops, exhibiting factors of safety greater than 1 for Service Level D allowables. Meeting *2004 ASME Boiler and Pressure Vessel Code* Service Level D (Subsection NF) (Ref. D4.1.6) provides for twice the allowable stress intensity as normal operation but still results in an extremely low failure probability. In addition, neutron dose typically attenuates quickly with distance from the transportation cask so it is only a small fraction of the gamma dose to personnel more than two meters away. Evacuation to that distance is the way to reduce personnel dose from neutrons. For these reasons, the analysis below focuses on the principle threat to workers on the site, which is degradation of gamma shielding.

This section summarizes information on loss of shielding mechanisms that could occur in event sequences for repository waste handling operations. The information is derived from transportation cask accident risk analyses. This information provides insights and bases for estimating probabilities of passive failures that result in LOS for casks and overpacks in waste handling event sequences.

The repository facilities process three categories of waste containers that provide shielding: transportation casks (truck and rail) and aging overpacks. The event sequence diagrams for operations involving processing of transportation casks and aging overpacks include the pivotal event “loss of shielding” for event sequences that are initiated by physical impact or fire. LOS due to fire was addressed previously in section D2.2 of this attachment. The following discussion focuses specifically on LOS due to drops and impacts.

The information in this section is based in large part on results of finite-element analysis (FEA) performed for four generic transportation cask types for transportation accidents as reported in NUREG/CR-6672 (Ref. D4.1.65) and NUREG/CR-4829 (Ref. D4.1.32). The results of the FEA were used to estimate threshold drop heights and thermal conditions at which LOS may occur in repository event sequences, using damage severity levels keyed to the FEA results to determine the challenge needed to cause LOS. The four cask types included one steel monolith rail cask, one steel/depleted uranium truck cask, one SLS truck cask and one SLS rail cask. NUREG/CR-6672 states that the steel in any of the cask is thick enough to provide some shielding, but the depleted uranium and lead provide the primary gamma shielding for the multi-shell cask types. The referenced study performed structural and thermal analyses for both failure of containment boundaries and loss of shielding for accident scenarios involving rail cask and truck cask impacting unyielding targets at impact speeds of 30-60, 60-90, 90-120, and greater than120 mph. The impact orientations included side (0–20 degrees), corner (20 degrees–85 degrees), and end (85 degrees–90 degrees). The referenced study also correlated the damage from impacts on real targets including soil and concrete.

The event sequences used in the transportation accident analyses included impact-only, impact plus-fire, and fire-only conditions. The results of the FEA indicate that LOS could occur in the impact-only at speeds as low as 30 mph with an unyielding target and in fire scenarios of sufficient intensity and duration. The structural analyses did not credit the energy absorption capability of impact limiters. Therefore, the results are deemed applicable to approximate the structural response of transportation and similar casks in drop scenarios.

The primary reference NUREG/CR-6672 (Ref. D4.1.65), however, does not provide a threshold below which no LOS could be assured. Therefore, information quoted in an evaluation by the Association of American Railroads (AAR) (Ref. D4.1.30) was used to establish thresholds for LOS conditions based on damage categories that are correlated to plastic strain in the inner shell of a cask. That information is based on a prior transportation accident analysis known as the Modal Study (Ref. D4.1.32). For potential PCSA applications, FEA results for inner shell strain versus impact speed were extended to estimate the lower bound of impact speed or drop heights to establish conditions at which LOS may occur in cask-drop scenarios in repository operations.

NUREG/CR-6672 (Ref. D4.1.65) addresses two modes of LOS in accident scenarios: deformations of lid and closure geometry that permit direct streaming of radiation; and/or reductions in cask wall thickness or relocation of the depleted uranium or lead shielding. The LOS due to lid/closure distortion can be accompanied by air-borne releases if the inner shell of the cask is also breached.

The results of the FEA reported in NUREG/CR-6672 (Ref. D4.1.65) provides some definitive results that are deemed to be directly applicable to the repository event sequence analyses:

- Monolithic steel rail casks do not exhibit any LOS, but there may be some radiation streaming through gaps in closure in any of the impact scenarios. This result can be applied to both transportation casks.

- Steel/depleted uranium/steel truck cask exhibited no LOS, explained by modeling that included no gaps between forged depleted uranium segments so that no displacement of depleted uranium could occur.

- The SLS rail and truck casks exhibit LOS due to lead slumping. Lead slump occurs mostly on end-on impact with a lesser amount in corner orientation. For side-on orientation, there is no significant reduction in shielding.

Therefore, this analysis focuses on LOS for SLS casks to estimate the drop or collision conditions that could result in LOS from lead slumping. Figure D3.2-1 illustrates the effect of cask deformation and lead slumping for a SLS rail cask following an end-on impact at 120 mph onto an unyielding target from the result of the FEA reported in NUREG/CR-6672 (Ref. D4.1.65).

D3.1 DAMAGE THRESHOLDS FOR LOS

The AAR study (Ref. D4.1.30) is used as a reference for this report. The information cited, however, was derived from an earlier transportation cask study known as the "Modal Study,"

(Ref. D4.1.32). The Modal Study assigned three levels of cask response characterized by the maximum effective plastic strain within the inner shell of a transport cask. The severity levels are defined as:

- S1–implies strain levels < 0.2%
- S2–implies strains between 0.2 and 2.0%
- S3–implies strain levels between 2.0 and 30%.

The amount of damage to a cask for the respective severity levels is summarized in the following:

S1:

- No permanent dimensional change
- Seal and bolts remain functional
- Little if any radiation release
- Less than 40 g axial force on lead for all orientations
- No lead slump
- Fuel basket functional; up to 3% of fuel rods may release into cask cavity
- Loads/releases within regulatory criteria.

S2:

- Small permanent dimensional changes
- Closure and seal damage; may result in release
- Limited lead slump
- Up to 10% of fuel rods release to cask cavity.

S3:

- Large distortions
- Seal leakage likely
- Lead slump likely
- 100% fuel rods release to cask cavity.

As stated above, limited lead slumping may occur at damage level S2, but is likely to occur at damage level S3. The respective strain levels associated with damage levels S2 and S3 were applied to the results from NUREG/CR-6672 (Ref. D4.1.65) to establish a threshold impact speed for the onset of LOS.

D3.2 SEVERITY OF DAMAGE VERSUS IMPACT VELOCITY

The FEA results given in Table 5.3 of NUREG/CR-6672 (Ref. D4.1.65) are summarized in Table D3.2-1. The strain in the inner shell of the SLS casks are shown in Table D3.2-1 and illustrated in Figure D3.2-1. These data were plotted (Figures D3.2-2 and D3.2-3). The data points start at the lowest speed range of 30 to 60 mph. The data were plotted as points using the

lower boundary of each of the four speed ranges on the abscissa. The strain plots were extended to the origin by including the point (0, 0) with the Table D3.2-1 data.

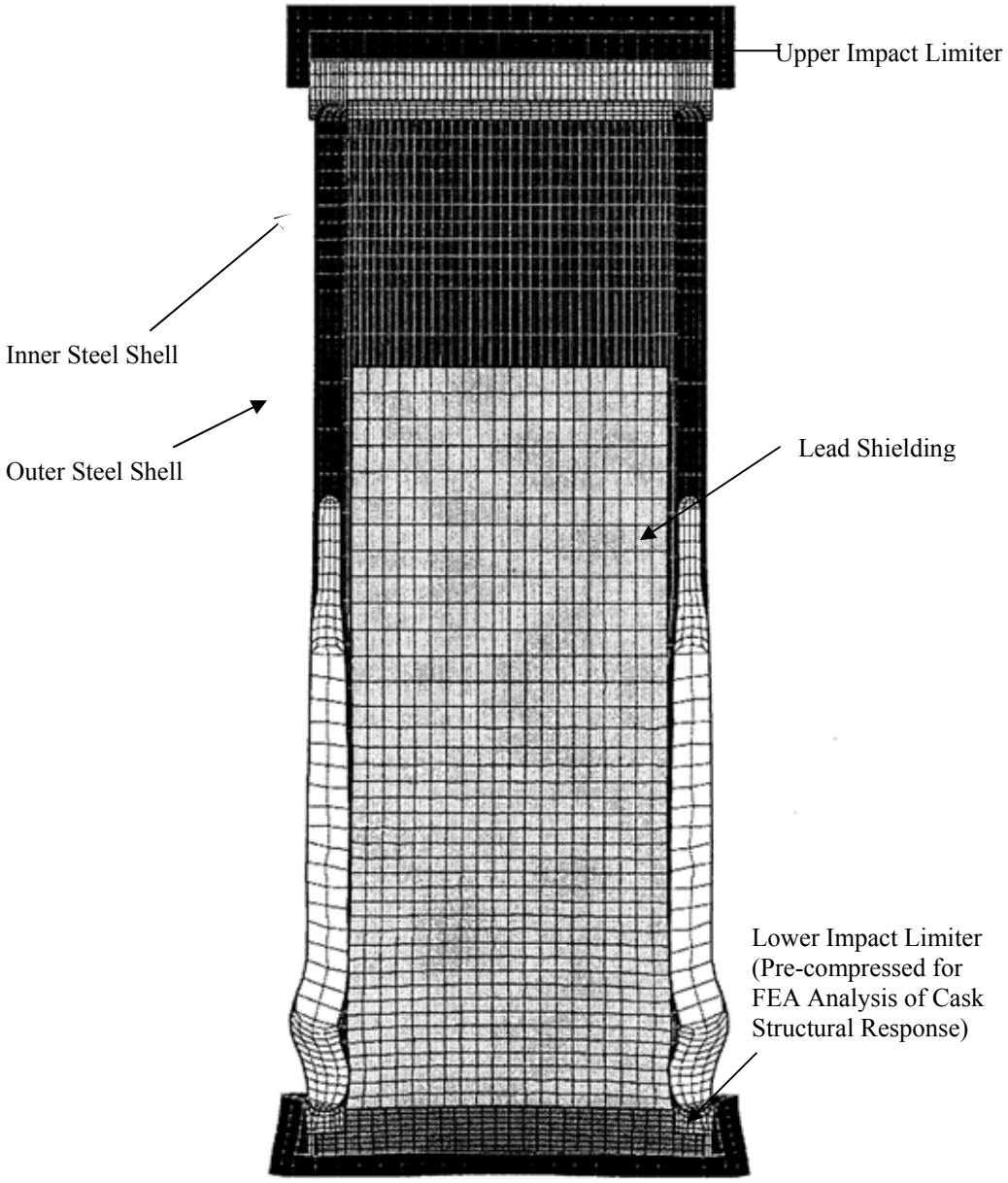
Two horizontal lines were superimposed on Figures D3.2-2 and D3.2-3 to plot the 0.2% and 2.0% strain to represent the respective S2 and S3 thresholds for inner shell strain. The intersections of the strain curves with the respective threshold values indicate the minimum impact speed at which the respective S2 and S3 strain thresholds appear to be exceeded.

Table D3.2-1. Maximum Plastic Strain in Inner Shell of Sandwich Wall Casks

Cask Type	Orientation: Speed, mph	Corner Impact Strain, %	End Impact Strain, %	Side Impact Strain, %
SLS Truck	30	12	3.9	N/A
	60	29	12	16
	90	33	18	24
	120	47	27	27
SDUS Truck	30	11	1.8	6
	60	27	4.8	13
	90	43	8.3	21
	120	55	13	30
SLS Rail	30	21	1.9	5.9
	60	34	5.5	11
	90	58	13	15
	120	70	28	N/A

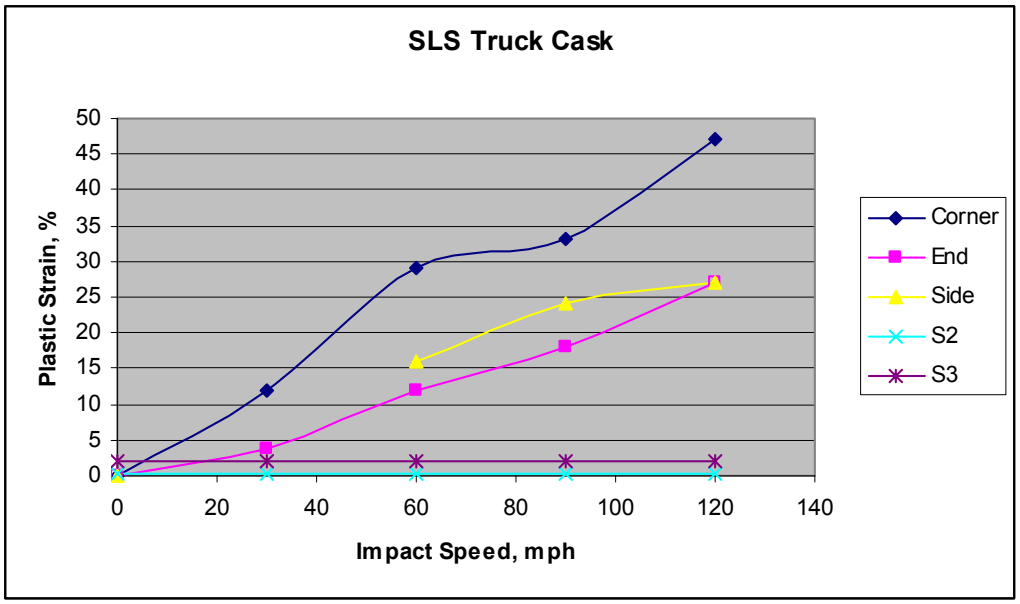
NOTE: SDUS = steel-depleted uranium-steel; SLS = steel-lead-steel.

Source: From Ref. D4.1.65, Table 5.3.



Source: From Ref. D4.1.65, Figure 5.9

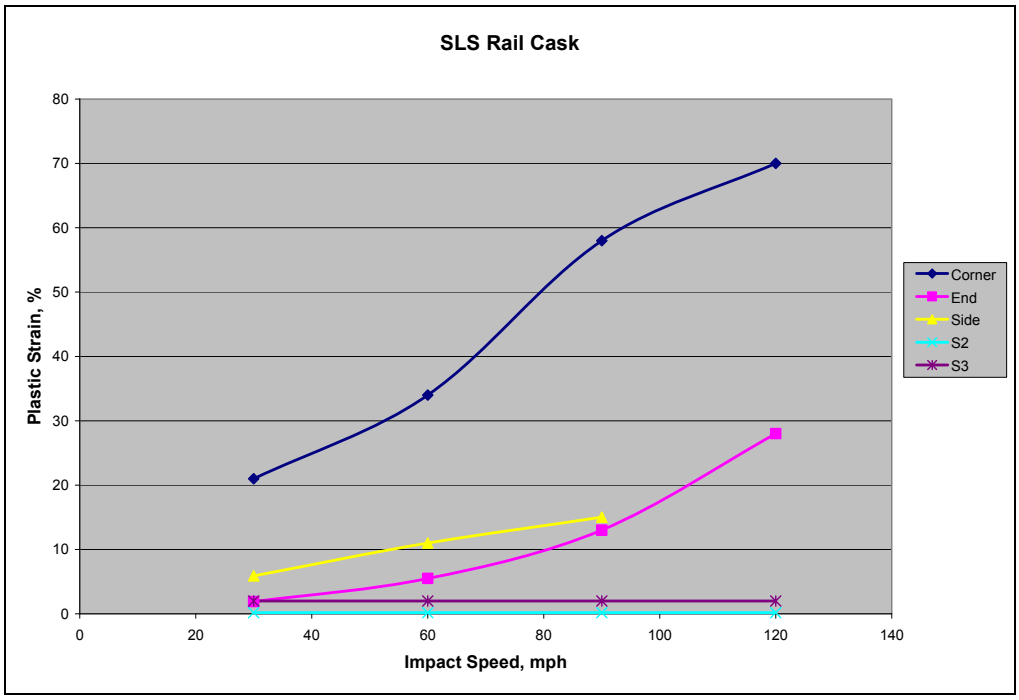
Figure D3.2-1. Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph



NOTE: [1] Data points for strain versus speeds greater than 30 mph taken directly from NUREG/CR-6672, Table 5.3: plots extended to origin (0,0) to determine crossover for S2 and S3 threshold strains.
[2] S2 and S3 threshold strains based on information in *A Railroad Industry Critique of the Model Study* (Ref. D4.1.30). mph = miles per hour; SLS = steel-lead-steel.

Source: Original

Figure D3.2-2. Truck Steel/Lead/Steel Inner Shell Strain versus Impact Speed



NOTE: [1] Data points for strain versus speeds greater than 30 mph taken directly from NUREG/CR-6672 (Ref. D4.1.65, Table 5.3): plots extended to origin (0,0) to determine crossover for S2 and S3 threshold strains. [2] S2 and S3 threshold strains based on information in *A Railroad Industry Critique of the Model Study* (Ref. D4.1.30). mph = miles per hour; SLS = steel-lead-steel.

Source: Original

Figure D3.2-3. Rail Steel/Lead/Steel Strain versus Impact Speed

D3.3 ESTIMATE OF THRESHOLD SPEEDS FOR LOSS OF SHIELDING DUE TO IMPACTS

The plots in Figures D3.2-2 and D3.2-3, and Table D3.2-1 illustrate that the S2 threshold is exceeded for both the truck and rail SLS casks for all four speed ranges and all orientations. Since NUREG/CR-6672 (Ref. D4.1.65) does not report LOS conditions for low impact speeds, it is concluded that the S2 criterion is not a valid threshold for LOS in SLS casks. Therefore, the remainder of this analysis applies the S3 criterion (2% shell strain) as a basis for estimating LOS threshold impact speeds.

Figures D3.2-2 and D3.2-3, and Table D3.2-1 indicate that the S3 threshold is exceeded for both truck and rail SLS casks for all orientations. The intersections of the strain curves and the 2% strain line in Figures D3.2-2 and D3.2-3 illustrate the impact speed at where the S3 threshold is reached for each case. A small exception being the end drop of a SLS rail cask in the 30-60 mph range for which the shell strain of 1.9% is just below the lower bound for S3 damage. However, this margin is too small to exclude that case. Although the strains for the side drop cases exceed the threshold for lead slumping, NUREG/CR-6672 (Ref. D4.1.65) states that lead slumping does not occur in side drops. Therefore, LOS for side drops is excluded from the remainder of this report.

Using the 2% shell strain condition as the threshold for LOS in SLS casks, the following is observed:

- LOS for the truck SLS cask would occur at impact speeds of about 5 mph for corner impact and about 18 mph for end impact
- LOS for the rail SLS cask would occur at about 3 mph for corner impact and about 30 mph for end impact.

It is observed that the corner drop cases give the largest shell strain at a given impact speed but the finite element analyses indicate that the extent of lead slumping is less in corner drops than for end impacts.

Table D3.3-1 shows the drop height equivalents for impact speed onto a horizontal unyielding surface. Thus, to exceed 5 mph, for example, a drop height greater than 0.8 ft is required; to exceed 30 mph impact, a drop height greater than 30 ft is required. Using the results cited above:

- LOS for the truck SLS cask would occur at impact speeds of about 0.8 ft (5 mph) for corner impact and about 10 ft (18 mph) for end impact
- LOS for the rail SLS cask would occur at about 0.5 ft (3 mph) for corner impact and about 30 ft (30 mph) for end impact.

Such drop heights could occur in some GROA handling operations.

However, when the effect of the energy absorption by real targets is considered, much greater impact speeds are required to impose the damage equivalent to impacts on unyielding targets. NUREG/CR-6672 (Ref. D4.1.65) provides a correlation of impact speeds for real versus unyielding target, but provides only bounding values for a large number of cases as presented in Table D3.3-2. Therefore, if LOS occurs at 30 mph for an end drop of a SLS train cask on unyielding surface, a speed of greater than 150 mph is required for an impact on concrete. This impact speed would require a drop of over 500 ft. Such drop heights cannot be achieved in repository handling.

Some of the LOS cases, including corner drops of truck and rail SLS casks, appear to result in LOS for impact speeds less than 10 mph. If the corner drops are onto concrete, a speed of 2 to 3 times the threshold speed for LOS for impact on an unyielding target. This implies a threshold impact speed of 20 to 30 mph for a corner drop onto concrete. The corresponding drop height is 13 feet to 30 feet. Such drops could occur in event sequences for repository handling.

Table D3.3-1. Drop Height to Reach a Given Impact Speed

Impact Speed, mph	Equivalent Drop Height, ft
2	0.1
5	0.8
10	3.3
20	13.4
30	30.1
40	53.4
50	83.5
60	120.2
70	163.7
80	213.8
90	270.6
100	334.0
110	404.2
120	481.0

Source: Original

Table D3.3-2. Impact Speeds on Real Target for Equivalent Damage for Unyielding Targets

Cask Type	Real Target type	Impact Type\Orientation w/o Impact Limiters	Impact Speed , mph			
			30	60	90	120
Rail SLS	Soil	End	>>150	>>150	>>150	>>150
		Side	72	>150	>>150	>>150
		Corner	68	133	>150	>150
	Concrete slab	End	>150	>>150	>>150	>>150
		Side	85	>150	>>150	>>150
		Corner	>>150	>>150	>>150	>>150
Truck SLS	Soil	End	>150	>>150	>>150	>>150
		Side	70	>150	>>150	>>150
		Corner	61	>150	>>150	>>150
	Concrete slab	End	123	180	>>150	>>150
		Side	35	86	135	>150
		Corner	56	123	>150	>>150

NOTE: mph = miles per hour; SLS = steel-lead-steel.

Source: Based on NUREG/CR-6672 (Ref. D4.1.65, Tables 5.10 and 5.12)

D3.4 PROBABILITY OF LOSS OF SHIELDING

NUREG/CR-6672 (Ref. D4.1.65) develops probabilities for LOS in transportation accidents. The probability of LOS uses event tree analysis with split fractions for various types of transportation accidents and frequencies based on accident rates per mile of travel for cask-bearing truck trailers or rail cars. The results of probability analyses of LOS as derived in

NUREG/CR-6672 (Ref. D4.1.65) do not have any direct relevance to event sequences for waste handling operations. However, the basic approach that breaks down the overall probability of an event sequence involving LOS into conditional probabilities for occurrence of various physical conditions that lead to LOS can be adapted for PCSA.

The vulnerability to LOS for repository event sequences varies with the container type:

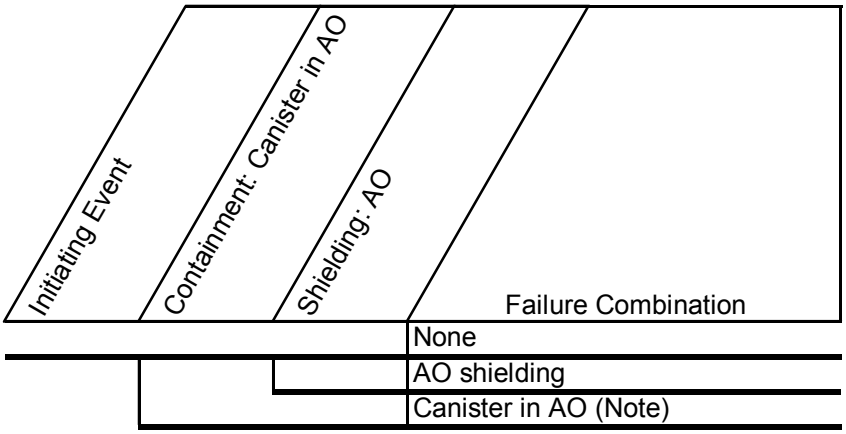
1. Concrete overpack with no containment boundary (aging overpack)

2. Sandwich type with steel containment boundary and lead in the annulus between the steel shells (transportation cask).

3. All other casks including monolithic steel casks or casks with layers of steel or steel and depleted uranium (transportation cask, shielded transfer cask (STC)).

Concrete Overpacks

Aging overpacks provide shielding but not containment. They are used within the GROA to transport DPCs and TAD canisters between buildings and to and from the aging pads. The event sequences that involve both are of the form shown in Figure D3.4-1 below.



NOTE: AO = aging overpack
Source: Original

Figure D3.4-1. Summary Event Tree Showing Model Logic for Canisters and Aging Overpacks

A site transporter transports aging overpacks with canisters within the GROA. The transporter is designed for a maximum speed of 2.5 mph (Ref. D4.1.18, Sections 3.2.1 and 3.2.4) and will elevate the aging overpack no more than 3 feet from the ground (equipment limit is 12 inches (Ref. D4.1.18, Section 2.2, item 9)), additional two feet is allowed for potential drop off edge of aging pad). Expanding the probability of success (no breach) of a canister within an aging overpack yields:

$$p_{AO}(C) \quad p_{AO}(C \mid O)p_{AO}(O) + p_{AO}(C \mid \overline{O})p_{AO}(\overline{O}), \qquad \text{(Eq. D-26)}$$

where

$p_{AO}(C)$ probability of canister success within an AO.

$p_{AO}(C \mid O)$ probability of canister success given AO shielding does not fail.

$p_{AO}(O)$ probability that AO shielding does not fail.

$p_{AO}(C \mid \overline{O})$ probability of canister success given AO shielding fails.

$p_{AO}(\overline{O})$ probability that AO shielding fails.

The inner and outer steel lined 3 foot concrete aging overpack is much more robust against impact loads than a DPC. Therefore, if the overpack fails, it is much more likely that the canister will breach. This yields: $p_{AO}(C \mid O) >> p_{AO}(C \mid \overline{O})$. Furthermore, the probability of aging overpack breach is much less than probability of aging overpack success at the above drop and speed conditions. Therefore: $p_{AO}(O) >> p_{AO}(\overline{O})$. The second term on the right hand side of Equation D-26 is much less than the first term and need not be considered further in this analysis.

This leaves

$$p_{AO}(C) \cong p_{AO}(C \mid O) p_{AO}(O) \qquad \text{(Eq. D-27)}$$

Note that

$p_{AO}(C) \quad 1 - p_{AO}(\overline{C})$ and $\qquad p_{AO}(O) \quad 1 - p_{AO}(\overline{O})$ and

$$p_{AO}(C \mid O) \quad 1 - p_{AO}(\overline{C} \mid O) \qquad \text{(Eq. D-28)}$$

Substituting Equations D-28 into D-27 and rearranging yields:

$$p_{AO}(\overline{O}) \cong 1 - \frac{1 - p_{AO}(\overline{C})}{1 - p_{AO}(\overline{C} \mid O)} \qquad \text{(Eq. D-29)}$$

LLNL has developed a mean probability of failure for a canister within an aging overpack, $p_{AO}(\overline{C})$, for a 3-foot drop onto a rigid surface with an initial velocity of 2.5 mph (Ref. D4.1.27).

This analysis uses a conservative value of 1E-05 relative to the 1E-08 value in the referenced LLNL report. The probability of canister failure given the aging overpack does not fail, $p_{AO}(\overline{C} \mid O)$, must be less than the overall probability of canister failure within an aging overpack, $p_{AO}(\overline{C})$. It is, therefore, reasonable to use a range of values of 1E-06 to 1E-05 for this, both of which are conservative relative to the value in the reference. The LLNL (Ref. D4.1.27) value, itself, has a conservative element in that it analyzes impact onto a rigid surface. The more realistic concrete surface would have a lower canister failure probability. Using the average between 1E-06 and 1E-05 of 5E-06 for $p_{AO}(\overline{C} \mid O)$ and also substituting the aforementioned value for $p_{AO}(\overline{C})$ into Equation D-29, there obtains:

$$\mathrm{p_{AO}}(\overline{\mathrm{O}}) \cong 1 - \frac{1 - \mathrm{p_{AO}}(\overline{\mathrm{C}})}{1 - \mathrm{p_{AO}}(\overline{\mathrm{C}} \mid \mathrm{O})} \quad 1 - \frac{1 - 10^{-5}}{1 - 5 \times 10^{-6}} \quad 5 \times 10^{-6} \qquad \text{(Eq. D-30)}$$

Steel/Lead/Steel Sandwich-Type Casks

For these sandwich-type casks, the probability of LOS due to lead slumping can be estimated from results of transportation cask studies that can be coupled to event sequence probability analysis and insights from the passive failure analyses. Since the speed of transport of transportation casks to, and within, the processing facilities is limited to a few mph, it is judged that LOS of SLS casks (and the other types) may be screened out from collision scenarios. However, LOS for SLS casks due to drops cannot be ruled out, if SLS casks are processed in the repository.

For SLS casks, the probability of LOS is derived from the probability that the drop height or impact speed exceeds the threshold at which lead shielding may slump. For all cask types, the probability of LOS is derived from the probability that the drop height or impact speed exceeds the threshold at which cask closure and/or seals fail in such a way to permit to permit direct streaming. A simplified conservative approach to estimating the probability of LOS due to lead slumping resulting from a drop of an SLS cask is summarized in the next section.

The PCSA considers drop and collision event sequences of transportation casks. Should a canister rupture occur, the analysis conservatively models the shielding as also lost. In such event sequences the probability of loss of shielding is taken to be 1.0 given canister rupture. This applies to all types of casks.

Event sequences also include LOS without canister rupture. That is, the drop or collision was not severe enough to cause a rupture but a LOS is possible in some casks. Such an event sequence can not occur in the steel/depleted uranium truck casks. The loss of shielding associated with streaming through the head of steel monolith rail casks is due to structural failure of the casks. The probability of this is estimated by taking the breach/rupture probability of a steel monolith transportation cask at the weakest location and applying it as a head rupture probability.

Collisions of casks will occur at less than 5 mph. Drops can occur as high as 30 feet. Drops may be at any orientation: side, bottom, and end. A conservative approach to estimation of the probability of SLS LOS is to use the information associated with end drops, which can cause bulging of the steel containment that allows the lead to collect towards one end. Although the corner impact can cause greater strain in the steel containment, it does not cause the spreading that increases collection of the lead at one end. All surfaces in the repository upon which a transportation cask can be dropped (concrete or soil) are concrete or softer. Therefore, the concrete related drop height vs. LOS information may be accurately used.

An impact of at least 123 mph against a real surface such as concrete or soil is required in order to cause the same damage as an impact of 30 mph against an unyielding surface (Table D3.3-2). The vast majority of casks are to be delivered to the repository by rail. The maximum strain due to an end impact of 30 mph against an unyielding surface, or 123 mph against a real surface, is about 3.9% for a truck cask (greater than the 1.9% strain for a rail cask) (Table D3.2-1). Noting in Figure D3.2-3 that the amount of strain is roughly linear with the impact velocity, a velocity of 63 mph is estimated to correspond to the strain of 2% indicative of S3 damage and lead slumping. A 63 mph collision, equivalent to a 133-foot drop, is the threshold for causing enough damage to indicate potential loss of shielding due to lead slumping.

In order to develop fragility over height, the available information described herein indicates that an estimate of a median threshold for a failure drop height is 133 feet. This would yield 2% strain. A coefficient variation (the ratio of standard deviation to the median) is 0.1. This is an estimate derived from the distribution of capacity associated with the tensile strength elongation data described in Section D1.1. The probability of LOS due to lead slumping resulting from a 15-foot vertical drop would be less than 1×10^{-8}, given the drop event. For a 30-foot drop resulting from a 2-blocking event, the computed failure probability based on the 133-foot median drop height is also less than 1×10^{-8}. LOS due to lead slumping applies only to those casks using lead for shielding but the PCSA applied this analysis to all casks. A conservative value of 1×10^{-5} is used to be consistent with the probabilities based on the LLNL (Ref. D4.1.27) results.

Results are shown in Tables D3.4-1.

Table D3.4-1. Probabilities of Degradation or Loss of Shielding

	Probability	Note
Sealed transportation cask and shielded transfer casks shielding degradation after structural challenge	1×10^{-5}	Section D3.4
Aging overpack shielding loss after structural challenge	5×10^{-6}	Section D3.4
CTM shielding loss after structural challenge	0	Structural challenge sufficiently mild to leave the shielding function intact[a]
WPTT shielding loss after structural challenge	0	Structural challenge sufficiently mild to leave the shielding function intact[a]
TEV shielding loss (shield end)	0	Structural challenge sufficiently mild to leave the shielding function intact[a]
Shielding loss by fire for waste forms in transportation casks or shielded transfer casks	1	Lead shielding could potentially expand and degrade. This probability is conservatively applied to transportation casks and STCs that do not use lead for shielding
Shielding loss by fire of aging overpacks, CTM shield bell, and WPTT shielding	0	Type of concrete used for aging overpacks is not sensitive to spallation; Uranium used in CTM shield bell and WPTT shielding does not lose its shielding function as a result of fire

NOTE: [a]In the event sequence diagrams of the PCSA, the shielding function for the CTM, WPTT and TEV is queried for the challenges that do not lead to a radioactive release. Such challenges, which were not sufficiently severe to cause a breach of containment of the waste form container, are also deemed mild enough to leave the shielding function of the CTM, WPTT and TEV intact.

CTM = canister transfer machine; STC = shielded transfer cask; TEV=transport and emplacement vehicle; WPTT = waste package transfer trolley.

Source: Original

All Other Cask Types

For all other cask types, the results of the transportation cask study indicate that the only mechanism for LOS is streaming via closure failures and closure geometry changes. Therefore, the probability of LOS can be equated to the probability of rupture/breach of such casks.

D4 REFERENCES

D4.1 DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that

implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

D4.1.1* Allegheny Ludlum 2006. "Technical Data Blue Sheet, Stainless Steels Chromium-Nickel-Molybdenum, Types 316 (S31600), 316L (S31603), 317 (S31700), 317L (S31703)." Technical Data Blue Sheet. [Brackenridge, Pennsylvania]: Allegheny Ludlum. TIC: 259471. LC Call Number: TA 486 .A4 2006.

D4.1.2* A.M. Birk Engineering 2005. *Tank Car Thermal Protection Defect Assessment: Updated Thermal Modelling with Results of Fire Testing*. TP 14367E. Ontario, Canada: Transportation Development Centre of Transport Canada. ACC: MOL.20071113.0095.

D4.1.3* ASM (American Society for Metals) 1961. "Properties and Selection of Metals." Volume 1 of *Metals Handbook.* 8th Edition. Lyman, T.; ed. Metals Park, Ohio: American Society for Metals. TIC: 257281. LC Call Number: TA459 .M43 1961 Vol.1.

D4.1.4* ASM 1976. *Source Book on Stainless Steels*. Metals Park, Ohio: American Society for Metals. TIC: 259927. LC Call Number: TA479 .S7 S64 1976.

D4.1.5* ASME (American Society of Mechanical Engineers) 2001. *2001 ASME Boiler and Pressure Vessel Code (includes 2002 addenda).* New York, New York: American Society of Mechanical Engineers. TIC: 251425.

D4.1.6* ASME 2004. *2004 ASME Boiler and Pressure Vessel Code.* 2004 Edition. New York, New York: American Society of Mechanical Engineers. TIC: 256479.

D4.1.7* ASTM (American Society for Testing and Materials) G 1-03. 2003. *Standard Practice for Preparing, Cleaning, and Evaluating Corrosion Test Specimens.* West Conshohocken, Pennsylvania: American Society for Testing and Materials. TIC: 259413.

D4.1.8* Avallone, E.A. and Baumeister, T., III, eds. 1987. *Marks' Standard Handbook for Mechanical Engineers*. 9th Edition. New York, New York: McGraw-Hill. TIC: 206891. ISBN: 0-07-004127-X.

D4.1.9* BNFL Fuel Solutions 2003. *FuelSolutions™ TS125 Transportation Cask Safety Analysis Report, Revision 5.* Document No. WSNF-120. Docket No. 71-9276. Campbell, California: BNFL Fuel Solutions. TIC: 257634.

D4.1.10 Not Used.

D4.1.11 BSC 2006. *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope.* 000-MJ0-HTC0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061120.0011.

D4.1.12 BSC 2007. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle.* 000-30R-HE00-00200-000 REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0002.

D4.1.13 BSC 2007. *5-DHLW/DOE SNF - Long Co-Disposal Waste Package Configuration.* 000-MW0-DS00-00203-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070719.0007.

D4.1.14 BSC 2007. *Aging Facility Vertical DPC Aging Overpack Mechanical Equipment Envelope Sheet 1 of 2.* 170-MJ0-HAC0-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070928.0032.

D4.1.15 BSC 2007. *Basis of Design for the TAD Canister-Based Repository Design Concept.* 000-3DR-MGR0-00300-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0042.

D4.1.16* BSC 2007. *Discipline Design Guide and Standards for Surface Facilities HVAC Systems.* 000-3DG-GEHV-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070514.0007.

D4.1.17 BSC 2007. *Leak Path Factors for Radionuclide Releases from Breached Confinement Barriers and Confinement Areas.* 000-00C-MGR0-01500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0002.

D4.1.18 BSC 2007. *Mechanical Handling Design Report - Site Transporter.* 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.

D4.1.19 BSC 2007. *Naval Long Oblique Impact Inside TEV.* 000-00C-DNF0-01200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070806.0016.

D4.1.20 BSC 2007. *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert.* 000-00C-DNF0-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071017.0001.

D4.1.21 BSC 2007. *Probabilistic Characterization of Preclosure Rockfalls in Emplacement Drifts.* 800-00C-MGR0-00300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070329.0009.

D4.1.22 BSC 2007. *TAD Waste Package Configuration.* 000-MW0-DSC0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0010.

D4.1.23 BSC 2007. *TAD Waste Package Configuration.* 000-MW0-DSC0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0011.

D4.1.24 BSC 2007. *TAD Waste Package Configuration.* 000-MW0-DSC0-00103-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0012.

D4.1.25 BSC 2007. *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident.* 000-00C-WIS0-02900-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070220.0008.

D4.1.26 BSC 2007. *Waste Package Capability Analysis for Nonlithophysal Rock Impacts.* 000-00C-MGR0-04500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071113.0017.

D4.1.27 BSC 2008. *Seismic and Structural Container Analyses for the PCSA*. 000-PSA-MGR0-02100-000. Rev. 00A. Las Vegas, NV: Bechtel SAIC Company. ACC: ENG.20080220.0003.

D4.1.28 DOE (U.S. Department of Energy) 2007. *Transportation, Aging and Disposal Canister System Performance Specification.* WMO-TADCS-000001, Rev. 0. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070614.0007. (DIRS 181403)

D4.1.29 DOE 2007. *Quality Assurance Requirements and Description.* DOE/RW-0333P, Rev. 19. Washington, D. C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070717.0006. (DIRS 182051)

D4.1.30* English, G.W.; Moynihan, T.W.; Worswick, M.J.; Birk, A.M. 1999. *A Railroad Industry Critique of the Model Study.* 96-025-TSD. Kingston, Ontario, Canada: Association of American Railroads Safety & Operations. TIC: 260032. LC Call Number: TK9152.17 .T73 1999.

D4.1.31* Evans, D.D. 1993. "Sprinkler Fire Suppression Algorithm for HAZARD." *Fire Research and Safety, 12th Joint Panel Meeting, October 27-November 2, 1992, Tsukuba, Japan.* Pages 114-120. Tsukuba, Japan: Building Research Institute and Fire Research Institute. ACC: MOL.20071114.0163.

D4.1.32* Fischer, L.E.; Chou, C.K.; Gerhard, M.A.; Kimura, C.Y.; Martin, R.W.; Mensing, R.W.; Mount, M.E.; and Witte, M.C. 1987. *Shipping Container Response to Severe Highway and Railway Accident Conditions.* NUREG/CR-4829. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: NNA.19900827.0230; NNA.19900827.0231.

D4.1.33* Friedrich, T. and Schellhaas, H. 1998. *Computation of the percentage points and the power for the two-sided Kolmogorov-Smirnov one sample test*. Statistical Papers 39:361-75. TIC: 260013.

D4.1.34* General Atomics. 1995. *GA-9 Legal Weight Truck From-Reactor Spent Fuel Shipping Cask, Final Design Report (FDR).* 910354 N/C. San Diego, California: General Atomic. ACC: MOV.20000106.0003.

D4.1.35* Haynes International 1990. Reliability and Longevity of Furnace Components as Influenced by Alloy of Construction. H-3124. Kokomo, Indiana: Haynes International. TIC: 256362.

D4.1.36* Haynes International 1997. Hastelloy C-22 Alloy. Kokomo, Indiana: Haynes International. TIC: 238121.

D4.1.37* Hertz, K.D. 2003. "Limits of Spalling of Fire-Exposed Concrete." *Fire Safety Journal, 38,* 103-116. [New York, New York]: Elsevier. TIC: 259993.

D4.1.38* Holtec International 2003. *Storage, Transport, and Repository Cask Systems, (Hi-Star Cask System) Safety Analysis Report, 10 CFR 71, Docket 71-9261.* HI-951251, Rev. 10. [Marlton, New Jersey]: Holtec International. ACC: MOL.20050119.0271.

D4.1.39* Holtec International 2005. *Final Safety Analysis Report for the HI-STORM 100 Cask System.* USNRC Docket No.: 72-1014. Holtec Report No.: HI-2002444. Marlton, New Jersey: Holtec International. TIC: 258829.

D4.1.40* Hubbell, J.H. and Seltzer, S.M., *Tables of X-Ray Mass Attenuation Coefficients and Mass Energy-Absorption Coefficients* (version 1.4). National Institute of Standards and Technology, Gaithersburg, MD, 2004. (Originally published as NISTIR 5632, National Institute of Standards and Technology, Gaithersburg, MD, 1995) (Available online at: http://physics.nist.gov/PhysRefData/XrayMassCoef/tab4.html) ACC: MOL.20080303.0046.

D4.1.41* Incropera, F.P. and DeWitt, D.P. 1996. *Introduction to Heat Transfer*. 3rd Edition. New York, New York: John Wiley and Sons. TIC: 241057. ISBN: 0-471-30458-1.

D4.1.42 Not used.

D4.1.43* Kodur, V.K.R.; Wang, T.C.; and Cheng, F.P. 2004. "Predicting the Fire Resistance Behaviour of High Strength Concrete Columns." *Cement & Concrete Composites, 26,* 141-153. [New York, New York]: Elsevier. TIC: 259996.

D4.1.44* Larson, F.R. and Miller, J. 1952. "A Time-Temperature Relationship for Rupture and Creep Stresses." *Transactions of the American Society of Mechanical Engineers, 74,* 765-775. New York, New York: American Society of Mechanical Engineers. TIC: 259911.

D4.1.45 Lide, D.R., ed. 1995. *CRC Handbook of Chemistry and Physics.* 76th Edition. Boca Raton, Florida: CRC Press. TIC: 216194. ISBN: 0-84930476-8.

D4.1.46* Majumdar, S.; Shack, W.J.; Diercks, D.R.; Mruk, K.; Franklin, J.; and Knoblich, L. 1998. *Failure Behavior of Internally Pressurized Flawed and Unflawed Steam Generator Tubing at High Temperatures – Experiments and Comparisons with Model Predictions.* NUREG/CR-6575. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071106.0053.

D4.1.47* Mason, M. 2001. "NUHOMS-MP197 Transport Packaging Safety Analysis Report." Letter from M. Mason (Transnuclear) to E.W. Brach (NRC), May 2, 2001, E-21135, with enclosures. TIC: 255258.

D4.1.48* Morris Material Handling 2008. *Mechanical Handling Design Report - Canister Transfer Machine*. Morris Material Handling. V0-CY05-QHC4-00459-00018-001-004; ACC: ENG.20080121.0010.

D4.1.49* NAC (Nuclear Assurance Corporation) 2000. *Safety Analysis Report for the NAC Legal Weight Truck Cask.* Revision 29. Docket No. 71-9225. T-88004. [Norcross, Georgia]: Nuclear Assurance Corporation International. ACC: MOL.20070927.0003.

D4.1.50* NAC (Nuclear Assurance Corporation) 2004. "NAC-STC NAC Storage Transport Cask, Revision 15." Volume 1 of *Safety Analysis Report.* Docket No. 71-9235. Norcross, Georgia: NAC International. TIC: 257644.

D4.1.51* Nakos, J.T. 2005. *Uncertainty Analysis of Steady State Incident Heat Flux Measurements in Hydrocarbon Fuel Fires*. SAND2005-7144. Albuquerque, New Mexico: Sandia National Laboratories. ACC: MOL.20071106.0054.

D4.1.52* Nowlen, S.P. 1986. *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report.* NUREG/CR-4680. SAND86-0312. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0099.

D4.1.53* Nowlen, S.P. 1987. *Quantitative Data on the Fire Behavior of Combustible Materials Found in Nuclear Power Plants: A Literature Review.* NUREG/CR-4679. SAND86-0311. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0100.

D4.1.54* NRC (U.S. Nuclear Regulatory Commission) 1997. *Standard Review Plan for Dry Cask Storage Systems.* NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.

D4.1.55* NRC 2003. *Interim Staff Guidance - 18. The Design/Qualification of Final Closure Welds on Austenitic Stainless Steel Canisters as Confinement Boundary for Spent Fuel Storage and Containment Boundary for Spent Fuel Transportation.* ISG-18. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 254660.

D4.1.56* NRC 2007. *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis - Level of Information and Reliability Estimation.* HLWRS-ISG-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.

D4.1.57* Quintiere, J.G. 1998. *Principles of Fire Behavior.* Albany, New York: Delmar Publishers. TIC: 251255. ISBN: 0-8273-7732-0.

D4.1.58* Rieth, M.; Falkenstein, A.; Graf, P.; Heger, S.; Jäntsch, U.; Klimiankou, M.; Materna-Morris, E.; and Zimmermann, H. 2004. *Creep of the Austenitic Steel AISI 316L(N), Experiments and Models.* FZKA 7065. Karlsruhe, Germany: Forschungszentrum Karlsruhe GmbH. TIC: 259943.

D4.1.59* Sasikala, G.; Mathew, M.D.; Bhanu Sankara Rao, K.; and Mannan, S.L. 1997. "Assessment of Creep Behaviour of Austenitic Stainless Steel Welds." *Creep-Fatigue Damage Rules for Advanced Fast Reactor Design, Proceedings of a Technical Committee Meeting, Manchester, United Kingdom, 11-13 June 1996.* IAEA-TECDOC-993. Pages 219-227. Vienna, Austria: International Atomic Energy Agency. TIC: 259880.

D4.1.60* Savolainen, K.;Mononen, J.; Ilola, R.; Hanninen, H. 2005. *Materials Selection for High Temperature Applications [TKK-MTR-4/05].* TKK-MTR-4/05. Helsinki, Finland, Espoo, Finland: Helsinki University of Technology, Laboratory of Engineering Materials; Otamedia Oy. TIC: 259896. ISBN: 951-22-7892-8.

D4.1.61* Society of Fire Protection Engineering (SFPE) 1988. *The SFPE Handbook of Fire Protection Engineering, Society of Fire Protection Engineers.* Edition 1. Boston, MA: Society of Fire Protection Engineering (SFPE). TIC: 101351. ISBN: 0-87765-353-4.

D4.1.62* Shapiro, S. S. and Wilk, M. B. 1965. "An analysis of variance test for normality (complete samples)", *Biometrika*, 52 (3 - 4), pages 591-611. TIC: 259992.

D4.1.63* Siegel, R. and Howell, J.R. 1992. *Thermal Radiation Heat Transfer.* 3rd Edition. Washington, D.C.: Taylor & Francis. TIC: 236759. ISBN: 0-89116-271-2. (Radiation view factors also available online at: http://www.me.utexas.edu/~howell/index.html.

D4.1.64* Snow, S.D. 2007, *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-Foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations*, EDF-NSNF-085, Rev. 0. [Idaho Falls, Idaho: Idaho National Laboratory]. ACC: MOL.20080206.0062.

D4.1.65* Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; and Yoshimura, H.R. 2000. *Reexamination of Spent Fuel Shipment Risk Estimates.* NUREG/CR-6672. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20001010.0217.

D4.1.66* Transnuclear 2001. *TN-68 Transport Packaging Safety Analysis Report, Revision 4.* Hawthorne, New York: Transnuclear. TIC: 254025.

D4.2 DESIGN CONSTRAINTS

D4.2.1 10 CFR 20. 2007. Energy: Standards for Protection Against Radiation. Internet Accessible.

D4.2.2 10 CFR 71. 2007. Energy: Packaging and Transportation of Radioactive Material. ACC: MOL.20070829.0114.

ATTACHMENT E
HUMAN RELIABILITY ANALYSIS

CONTENTS

Page

CONTENTS (Continued)

Page

CONTENTS (Continued)

Page

CONTENTS (Continued)

Page

CONTENTS (Continued)

Page

CONTENTS (Continued)

Page

FIGURES

Page

TABLES

Page

TABLES (Continued)

Page

TABLES (Continued)

Page

ACRONYMS AND ABBREVIATIONS

Acronyms

APOA	assessed proportion of affect
ASD	adjustable speed drive
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event Analysis
BWR	boiling water reactor
CBDT	Cause-Based Decision Tree
CFF	cognitive function failure
CPC	common performance condition
CREAM	Cognitive Reliability and Error Analysis Method
CTM	canister transfer machine
CTT	cask transfer trolley
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EFC	error forcing context
EOC	error of commission
EOO	error of omission
EPC	error-producing condition
EPRI	Electric Power Research Institute
ESD	event sequence diagram
FLIM	Failure Likelihood Index Method
GTT	generic task type
HAZOP	hazard and operability
HCR	Human Cognitive Reliability
HCTT	cask tractor and cask transfer trailer
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HEPA	high-efficiency particulate air (filter)
HFE	human failure event
HRA	human reliability analysis
HSTC	horizontal shielded transfer cask
HVAC	heating, ventilation, and air-conditioning
INPO	Institute of Nuclear Power Operations
ISFSI	independent spent fuel storage installation

ACRONYMS AND ABBREVIATIONS (Continued)

LLW	low-level radioactive waste
MAP	mobile access platform
MAUD	Multi-Attribute Utility Decomposition
MERMOS	Methode d'Evaluation de la Relisation des Missions Operateur pour la Surete
MLD	master logic diagram
NARA	Nuclear Action Reliability Assessment
NASA	National Aeronautics and Space Administration
NDE	nondestructive examination
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
PCSA	preclosure safety analysis
PIC	person in charge
PLC	programmable logic controller
PPE	personal protective equipment
PRA	probabilistic risk assessment
PSF	performance-shaping factor
PWR	pressurized water reactor
SHARP	Systematic Human Action Reliability Procedure
SLIM	Success Likelihood Index Method
SNF	spent nuclear fuel
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SPM	site prime mover
SSCs	structures, systems, and components
STC	shielded transportation cask
TAD	transportation, aging, and disposal (canister)
THERP	Technique for Human Error Rate Prediction
TRC	Time-Reliability Correlation
TTC	a transportation cask that is upended using a tilt frame
VTC	a transportation cask that is upended on a railcar
WHF	Wet Handling Facility
YMP	Yucca Mountain Project

Abbreviations

in.	inch

E1 INTRODUCTION

This document describes the work scope, definitions, terms, methods, and analysis for the human reliability analysis (HRA) task of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA) reliability assessment.

The HRA task identifies, models, and quantifies human failure events (HFEs) postulated in the PCSA to assess the impact of human actions on event sequences modeled in the PCSA. The HFEs evaluated and quantified by this task are identified during the following activities:

- Initiating event identification and grouping
- Event sequence development and categorization
- System analysis
- Sequence quantification and uncertainty analysis.

The HRA task ensures that the HFEs identified by the other tasks (e.g., hazard and operability (HAZOP) evaluation, event sequence diagram (ESD) development, event tree analysis, fault tree analysis) are quantified with HRA techniques. The ESD finding is that the human-induced initiating events dominate the HRA. No post-initiator human actions have been credited in this analysis. The HRA task also ensures that modeled HFEs are appropriately incorporated into the PCSA and provides appropriate human error probabilities (HEPs) for all modeled HFEs. It is important to note that YMP operations differ from those of traditional nuclear power plants (NPPs), and the HRA analysis reflects these differences; Appendix E.IV of this analysis provides further discussion on these differences and how they influenced the choice of methodology.

E1.1 SUMMARY

The HRA was carried out using a nine-step process that is derived from A Technique for Human Event Analysis (ATHEANA) (Ref. E8.1.22):

1. Define the scope of the analysis.

2. Describe the base case progression of actions and responses that constitute successful completion of the operations being evaluated (base case scenarios).

3. Identify and define HFEs of concern.

4. Perform preliminary (screening) analysis and identify HFEs requiring detailed analysis.

5. Identify potential vulnerabilities for the HFEs requiring detailed analysis.

6. Search for HFE scenarios (i.e., scenarios of concern).

7. Quantify probabilities of HFEs.

8. Incorporate HFEs into the PCSA.

9. Evaluate HRA/PCSA results and iterate with design.

After the scope was defined, the facility operations were split into logical groups that relate to the various phases of the Wet Handling Facility (WHF) operations. For each of these operational phase groups, a base case scenario was defined that describes in detail the normal operations for that group. Once the operations were defined and the base cases were documented, HFEs were identified through an iterative process whereby the human reliability analysts, in conjunction other PCSA analysts and Engineering and Operations personnel, met and discussed the design and operations in order to appropriately model the human interface. This process consisted of the HAZOP evaluation, master logic diagram (MLD) and event sequence development, fault tree and event tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the model. The iteration with the event sequence and system reliability analysis also identified HFEs of potential concern. HFEs identified include both errors of omission (EOOs) and errors of commission (EOCs).

Included in this process was an extensive information collection process where the human reliability analysts reviewed industry data and interviewed subject matter experts to identify potential vulnerabilities and HFE scenarios.

The result of this identification process was a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then became the error forcing context (EFC) for a specific HFE. Additions and refinements to these initial EFCs were made during the preliminary and detailed analyses.

A preliminary, or screening-type, analysis was then performed to preserve HRA resources so that detailed analyses can be focused on only the most risk-significant HFEs. The preliminary analysis included verification of the validity of HFEs included in the initial PCSA model, assignment of a conservative screening value to each HFE, and verification of preliminary values. The actual quantification of preliminary values was a six-step process that is described in detail in Appendix E.III of this analysis. Once the preliminary values were assigned, the PCSA model was quantified (initial quantification), and HFEs were identified for detailed analysis if: (1) the HFE was a risk-driver for a dominant sequence, and (2) using the preliminary values, that event sequence was above Category 1 or 2 according to the 10 CFR Part 63 (Ref. E8.2.1) performance objectives. The remaining HFEs retained their preliminary values. The remaining HFEs retained their preliminary values. While most of the activities associated with preliminary analysis were time-consuming, extra care was taken to perform these tasks conscientiously since the results of the initial quantification were used to identify which HFEs require detailed analysis.

Although many of the HFEs are modeled in a simplified form in the event trees and fault trees for the preliminary analysis, each action is separated as much as possible for the detailed analysis. This separation is done to ensure that the detailed analysis is thorough and that the relationship between the system functionality and operations crew is transparent. First an HFE is broken down into the various scenarios that lead to the failure. Then, each scenario is further broken down into specific required actions and their applicable procedures, along with the systems and components that must be operated during performance of each action. Each action

in each scenario has its own unique context, dependencies, and set of PSFs, and each was thus quantified independently. The failure probabilities for these unsafe actions were quantified by the HRA method appropriate to the HFE, its classification (e.g., EOC, EOO, observation error, execution error), and the context. The HRA methods used in this analysis include the Technique for Human Error Prediction (THERP) (Ref. E8.1.26), Human Error Assessment and Reduction Technique (HEART) (Ref. E8.1.28), Nuclear Action Reliability Assessment (NARA) (Ref. E8.1.11), Cognitive Reliability and Error Analysis Method (CREAM) (Ref. E8.1.18), and the expert elicitation process from ATHEANA (Ref. E8.1.22).

As described in Appendix E.IV of this analysis, no single HEP quantification method is suitable for all HFEs identified in the event sequence quantification. For example, there are unsafe actions within the YMP HFEs that would best fit the HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11) approach and others that would best fit the CREAM (Ref. E8.1.18) approach. The documentation of each HFE subjected to a detailed analysis defines the method used and the basis for its use.

After estimates for HFE probabilities were generated, these results were reviewed by the HRA team and, in some cases, by knowledgeable operations personnel as a "sanity check." Principally, such checks were used, for example, to compare the probabilities of different HFEs and determine whether or not these probabilities were reasonable. A review of this type was particularly important for HFE probabilities that were generated using data from the THERP method (Ref. E8.1.26) because THERP does not account for PSFs in a standard formulaic way. In addition, the HFE probability estimates were reviewed to ensure that they did not exceed the lower limit of credible human performance as defined by NARA (Ref. E8.1.11).

For the preliminary analysis, HFEs were modeled at a high level in order to reduce dependencies that arise from modeling detailed actions. For a detailed assessment, where the various actions that constitute an HFE were explicitly quantified, dependencies were also explicitly addressed using the method described in THERP (Ref. E8.1.26), which is adopted by NARA (Ref. E8.1.11)

HFE probabilities produced in this analysis are mean values with associated error factors. Uncertainties in both the preliminary and detailed HEP quantification were accounted for by assigning a lognormal distribution and applying an error factor of 3, 5, or 10 to the distribution, depending on the mean value of the final HEP.

Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to the analysis. This iteration was particularly necessary when an event sequence proved to be noncompliant with the performance objectives of 10 CFR Part 63 (Ref. E8.2.1) because the probability of a given HFE dominated the probability of that event sequence. In those cases, a design feature or procedural control was added to reduce the probability or completely eliminate the HFE, and the scenario was reanalyzed for human failures.

To guide the reader through the analysis, Section E6.0.1 explains how the HRA write-up is structured and how it interfaces with other parts of the PCSA, including a simplified diagram of the facility operations (which defines analysis sections) and a map that links this analysis back to the MLD, the ESD, and the HAZOP evaluation.

E2 SCOPE AND BOUNDARY CONDITIONS

E2.1 SCOPE

The scope of the HRA is established in order to focus the analysis on the issues pertinent to the goals of the overall PCSA. Thus, the scope is as follows:

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers.

2. Pursuant to the above, the following types of HFEs are excluded:

   A. HFEs resulting in standard industrial injuries (e.g., falls)

   B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount

   C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.

3. The identification of HFEs is restricted to those areas of the facility that handle waste forms and only during the times that waste forms are being handled (e.g., HFEs are not identified for the Cask Preparation Area during the export of empty transportation casks).

4. The exception to #3 is that system-level HFEs are considered for support systems when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.

5. Recovery post-initiator actions (as defined in Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.

6. In accordance with Section 4.3.10.1 (boundary conditions of the PCSA), initiating events associated with conditions introduced in structures, systems, and components (SSCs) before they reach the site are not, by definition of 10 CFR 63.2 (Ref. E8.2.1), within the scope of the PCSA nor, by extension, within the scope of the HRA.

E2.2 BOUNDARY CONDITIONS

Unless specifically stated otherwise, the following general conditions and limitations are applied throughout the HRA task. The first two conditions always apply. The remaining conditions apply unless the HRA analyst determines that they are inappropriate. This judgment is made for each individual action considered:

- Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior (i.e., deliberate acts of sabotage and the like) are not considered in this task.

- All facility personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard operating procedures is made because employees believe their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.

- Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include spent nuclear fuel (SNF) handling at reactor sites having independent spent fuel storage installations (ISFSIs), chemical munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the geologic repository operations area facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.

- The facility is initially operating under normal conditions and is designed to the highest quality human factors specifications. The level of operator stress is optimal unless otherwise noted in the analysis.

- In performing the operations, the operator does not need to wear protective clothing unless the operation is similar to those performed in other comparable facilities where protective clothing is required.

- The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are experienced and have functioned in their present positions for a sufficient amount of time to be proficient.

- The environment in the facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment.

- Personnel involved with the facility operations are expected to have the proper training commensurate with nuclear industry standards. As appropriate, this training is followed by a period of observation until the operator is proficient.

- While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill-of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

E3 METHODOLOGY

E3.1 METHODOLOGY BASES

The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in the American Society of Mechanical Engineers (ASME RA-S-2002 *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. E8.1.4) and incorporates the guidance provided by the U.S. Nuclear Regulatory Commission (NRC) in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. E8.1.23).

E3.2 GENERAL APPROACH

The HRA consists of several steps, that follow the intent of ASME RA-S-2002 (Ref. E8.1.4) and the process guidance provided in *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.22). Detailed descriptions of each HRA step are provided in the following subsections to summarize the processes used by the analysts. The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt the material based on NPPs to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. E8.1.22). Further discussion on information collection and use of expert judgment in this process can be found in Section E4.

HFE probabilities produced in this analysis are mean values. The HEPs are modeled as a lognormal distribution, where the error factors are defined based on the method presented in Section E3.4.

E3.2.1 Step 1: Define the Scope of the Analysis

The objective of the YMP HRA is to provide a comprehensive quantitative assessment of the HFEs that can contribute to the facility's event sequences resulting in radiological release, criticality, or direct exposure. Any aspects of the work that provide a basis for bounding the analysis are identified in this step. In the case of the YMP, the scope is bounded by the design state of the facilities and equipment.

E3.2.2 Step 2: Describe Base Case Scenarios

In this step, the base case scenarios are defined and characterized for the operations being evaluated. In general, there is one base case scenario for each operation included in the model. The base case scenario:

- Represents the most realistic description of expected facility, equipment, and operator behavior for the selected operation.
- Provides a basis from which to identify and define deviations from such expectations (Step 6).

In the ideal situation (which is seldom achieved), the base case scenario:

- Has a consensus operator model[1]
- Is well-defined operationally
- Has well-defined physics
- Is well-documented in public or proprietary references
- Is realistic.

Since operators and "as built, as operated" information are not currently available for YMP, this information is sought from comparable facilities with comparable operations. Documented reference analyses (e.g., engineering analyses) can assist in defining the scenario from the standpoint of physics and operations. The reference analyses may need to be modified to be more realistic. Expert judgment, engineering documents and applicable industry experience are the keys to defining realistic base case scenarios for YMP operations; Section E4 provides greater detail on how information was collected and the role of subject matter experts in this process.

E3.2.3 Step 3: Identify and Define HFEs of Concern

Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken, or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The classification process is described further in Section E5.1.1. The analyses performed in later steps (i.e., Steps 4 through 7) may identify the need to define an HFE or unsafe action not previously identified in Step 3.

Human errors were identified based upon the three temporal parts generally analyzed by probabilistic risk assessment (PRA) and are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs
- Post-initiator HFEs[2]:
  - Non-recovery
  - Recovery.

Each of these types of HFEs is defined in Section E5.1.1.1; identification of the HFEs for each temporal phase is described in the following sections.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns

[1]ATHEANA (Ref. E8.1.22), Section 9.3.1defines a consensus operator model in the following manner: "Operators develop mental models of plant responses to various PRA initiating events through training and experience. If a scenario is well defined and consistently understood among all operators (i.e., there is a consensus among the operators), then there is a consensus operator model."

[2]Terminology common to NPPs refer to non-recovery post-initiator events as Type C events and recovery events as Type CR events.

(e.g., PSFs). This combination of conditions and human factor concerns then becomes the EFC for a specific HFE. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses.

E3.2.3.1 Identifying Pre-initiator HFEs

Pre-initiators are identified by the system analysts when modeling fault trees, while performing the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human common-cause failure.

E3.2.3.2 Identifying Human-Induced Initiator HFEs

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the facility and SSCs in order to appropriately model the human interface. This iterative process begins with the HAZOP evaluation and MLD development, described and documented in *Wet Handling Facility Event Sequence Development Analysis* (Ref. E8.1.10), followed by a second iteration during the initial fault tree and event tree modeling, and ending with a third iteration through the preliminary analysis and incorporation of HFEs into the model. Included in this process is an extensive information collection process where industry data was reviewed (Section E4.1) and subject matter experts were interviewed (Section E4.2) to identify potential vulnerabilities and HFE scenarios. HFEs identified include both EOOs and EOCs.

E3.2.3.3 Identifying Non-recovery Post-initiator HFEs

Non-recovery post-initiator HFEs are identified by examining the human contribution to pivotal events in the event tree analysis. The event sequence analysts, with support from the human reliability analysts, identify HFEs that represent the operator's failure to perform the proper action to mitigate the initiating event and/or the unavailability of automatic mitigation functions as called for in the emergency operating procedures or in accordance with their emergency response training. This identification includes all actions required, whether in a control room or locally. Post-initiator EOCs and EOOs are also considered. It should be emphasized that this section presents the methodology that is used to identify non-recovery post-initiator events. However, as shown in Section E6, none of these types of errors have been identified for the WHF event sequence and categorization analysis. During the qualitative evaluation, non-recovery post-initiator events were considered and ruled out because it was unnecessary to credit non-recovery actions to demonstrate compliance with the performance objectives stated in 10 CFR 63.111 (Ref. E8.2.1).

E3.2.3.4 Identifying Recovery Post-initiator HFEs

Recovery actions are of limited relevance to YMP operations and, for conservatism, were not credited in this analysis. Recovery post-initiator HFEs are outside the scope of this analysis (Section E2.1).

E3.2.4 Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis

The preliminary analysis is a type of screening analysis used to identify HFEs of concern. A screening analysis is commonly performed in HRA to conserve resources and focus the effort on the subsequent detailed analysis of those HFEs that are involved in the important event sequences. Preliminary values are assigned for the probabilities of HFEs based upon predetermined characteristics of each HFE. This analysis involves the following steps:

- Verification of the validity of HFEs included in the initial PCSA model
- Assignment of conservative preliminary values to all HFEs included in the initial PCSA model
- Verification of assigned preliminary probabilities to all HFEs in the PCSA
- Quantification of the initial PCSA model using preliminary values (i.e., the "initial quantification")
- Identification of HFEs for detailed analysis.

The human reliability analyst performs the first three of these steps with the assistance of the PCSA quantification task leader, who also performs the last two steps. While most of the activities associated with this preliminary analysis are time-consuming, it is important to perform these tasks conscientiously since the results of the initial quantification are used to identify those HFEs requiring detailed analysis.

Analysts must strike a balance between conservatism and too much conservatism. Using too conservative a value for an HEP can overemphasize the importance of an HFE in the sequence quantification, perhaps masking a significant component failure event. By contrast, using a less conservative preliminary HEP may lead to inappropriately screening out a potentially significant event sequence. Instead of the usual screening process used in PRA, where relatively high screening values of 1.0 or 0.1 for an HEP are often inserted in initial fault tree and event sequence quantification, the PCSA applies an intermediate process where conservative preliminary values are assigned based on the context and failure modes of the HFE. Appendix E.III of this analysis provides specific details on guidelines for preliminary quantification.

Depending on the results obtained with the preliminary quantification, the event sequence and human reliability analysts may conclude that the preliminary results are sufficient for event sequence quantification and that a detailed analysis would not provide a better basis for event sequence categorization or more insights into the human factors issue for a particular waste handling operation. The preliminary quantification process is based on a characterization of each human action with respect to complexity and operational context using a judgment-based approach consisting of the following subtasks:

1. Complete the initial conditions required for quantification.
2. Identify the key or driving factors of the scenario context.

3. Generalize the context by matching it with generic, contextually anchored rankings or ratings.

4. Discuss and justify the judgments made in subtask 3.

5. Refine HFEs, associated contexts, and assigned HEPs.

6. Determine final preliminary HEPs for each HFE and associated context. These HEPs are then entered into the PRA logic structure to see which HFEs call for more detailed evaluation. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a given sequence, and (2) using the preliminary values, that sequence falls in a category (i.e., a Category 1 or Category 2) such that it does not meet 10 CFR 63.111 performance objectives (Ref. E8.2.1).

Appendix E.III of this analysis defines and provides technical bases for the HEP preliminary values recommended to be used in the YMP PRA for different categories of HFEs, depending on the general HFE characteristics. Section E4.2 provides a list of experts used in this process.

E3.2.5 Step 5: Identify Potential Vulnerabilities

This information collection step defines the context for Step 6 in which scenarios that deviate from the base case are identified. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in the HFEs and/or unsafe actions identified in Step 4. Potential traps[3] inherent in the ways operators may respond to the initiating event or base case scenario are identified through the following:

- Investigation of potential vulnerabilities in operator expectations for the scenario
- Understanding of the base case scenario time line and any inherent difficulties associated with the required response
- Identification of operator action tendencies and informal rules
- Evaluation of formal rules and operating procedures expected to be used in the scenario.

The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). Section E4 provides a description of the information types that comprise this knowledge base.

[3] A "trap" is a human failure that is encouraged or enabled by the existence of a specific vulnerability. That is, vulnerabilities influence operators to fall into particular traps.

E3.2.6 Step 6: Search for HFE Scenarios

In this step, the analyst must identify deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These deviations are referred to as HFE scenarios. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions (which form the EFC).

The principal method for identifying HFE scenarios is a HAZOP evaluation-like search scheme, coupled with a means for relating scenario characteristics with error mechanisms for each stage in the information processing model (Ref. E8.1.1). The result of such a search is a description of the HFE scenarios, including system and equipment conditions, along with any resident or triggered human factor concerns (e.g., PSFs). Again, this combination of conditions and human factor concerns then becomes the EFC for a specific HFE. As defined by the ATHEANA document (Ref. E8.1.22), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. (Additions and refinements to this initial EFC are likely in later steps of the process).

E3.2.7 Step 7: Quantify Probabilities of HFEs

Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with 10 CFR 63.111 performance objectives (Ref. E8.2.1) after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9, Section E3.2.9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CFR 63.111 (Ref. E8.2.1) performance objectives. The qualitative analysis in steps 3, 5, and 6 sets the stage for the detailed quantification by providing the accident progression(s) for a given HFE and its context. Specifically, the qualitative analysis provides a list of unsafe actions, along with their context, characteristics, and classification (i.e., EOO or EOC). For each unsafe action, the following steps are performed:

1. Qualitative analysis (e.g., identification of PSFs, definitions of important characteristics of the given unsafe action, assessment of dependencies)

2. Selection of a quantification model

3. Quantification

4. Verification that HFE probabilities are appropriately updated in the PCSA database.

The detailed quantification process relies on expert judgment to choose the most applicable HRA method or failure mode and identify the relevant PSFs. Section E4.2 provides detail on the experts used in this process and their qualifications.

E3.2.7.1 Qualitative Analysis

Before a given HFE can be quantified, a qualitative HRA analysis must be performed to fully describe each unsafe action for an HFE and to capture the dependencies between the unsafe actions. Much of this information was gathered in steps 3, 5, and 6 and is applied here. Qualitative analyses are also used to validate HRA approximations and required procedural controls, if any, for each HFE and associated event sequence to:

- Ensure that the general flow of the operator's response to dominant sequences is clearly understood from other information sources
- Confirm that the HFEs identified in the PRA models make sense relative to the actual experience and operating practice
- Identify potential influences or difficulties in implementing the procedures and making the decisions required in each event sequence
- Confirm that the cues for operator action are as identified in the HRA
- Qualitatively assess performance-influencing factors (PSFs) and other influences that might affect the reliability of responses.

E3.2.7.2 Selection of Quantification Model

Based on the characteristics and context of the unsafe action, expert judgment is used to pick the most applicable failure mode from the appropriate HRA method. There are four HRA methods that have been selected for this quantification:

1. CREAM (Basic and Extended)—*Cognitive Reliability and Error Analysis Method, CREAM* (Ref. E8.1.18)[4]
2. HEART/NARA—"HEART - A Proposed Method for Assessing and Reducing Human Error" (Ref. E8.1.28)/*A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.11)
3. THERP (with some modifications)—*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Ref. E8.1.26).

When an applicable failure mode cannot be reasonably found in one of the above methods, then the following HRA method is used:

4. ATHEANA's expert elicitation approach—*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.22).

[4]Extended CREAM (Ref. E8.1.18) creates a link between CREAM and HEART (Ref. E8.1.28), and enhances the ability of CREAM to quantify skill-based HFEs.

The selection of a specific quantification method for the failure probability of an unsafe action(s) is based upon the characteristics of the HFE quantified. The characteristics considered in the selection of the quantification method for each HFE include those discussed in Section E5.1.1.

Appendix E.IV of this analysis provides a discussion why these specific methods were selected for quantification, as well as a discussion of why some methods, deemed appropriate for HRA of NPPs, are not suitable for application in the PCSA. This discussion summarizes the main differences between NPPs and repository operations with respect to contexts and failure modes that affect potential HFEs. It also gives some background about when a given method is applicable based on the focus and characteristic of the method.

E3.2.7.3 Quantification

When the information collected is sufficient to allow the human reliability analyst to estimate the input parameters (i.e., failure mode and PSFs), these parameters are used in the selected quantification model to estimate the HEP for each unsafe action. The mean occurrence probability of the HFE is then obtained by combining the unsafe action HEPs with mechanical failure rates (as applicable) in a Boolean expression that expresses the logic of the HFE scenario. Dependencies are accounted for in this quantification process according to the method presented in Section E3.3, and uncertainties are accounted for by applying an error factor to the mean value of the overall HFE according to the guidelines presented in Section E3.4.

It should be noted, that when using NARA to calculate the HEP of a given unsafe action, the NARA HEP equation is used from *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.11), p. 14).

In addition, it should also be noted that in CREAM there is a discrepancy in the values quoted for observation errors O2 and O3 (*Cognitive Reliability and Error Analysis Method, CREAM* , Table 9, Chapter 9, p. 252 (Ref. E8.1.18)). The National Aeronautics and Space Administration (NASA) shuttle PRA study (Ref. E8.1.16) cites a mean value of 3E−03 for these failure modes, which is consistent with the value found in the CREAM example (*Cognitive Reliability and Error Analysis Method, CREAM*, Table 16, Chapter 9, p. 258 (Ref. E8.1.18)) for O3. The changes to the original CREAM values for observation errors O2 and O3 made in the NASA shuttle PRA study reflect the correction of a typographical error in the original CREAM value. These changes were made based on a conversation with the CREAM author (Ref. E8.1.27). The HRA team in the current analysis therefore judged that the correct mean value for these failure modes to be 3E−03, as cited in the shuttle PRA.

E3.2.7.4 Verification of Human Error Probabilities

After estimates for HFE probabilities are generated, these results are reviewed by the HRA analyst and operations personnel (whenever available) for a "sanity check." Such checks can be used, for example, to compare the probabilities of different HFEs and to determine whether or not these probabilities are reasonable with respect to the associated operator actions. A review of this type is particularly important for HFE probabilities that are generated using data from the THERP (Ref. E8.1.26) method since it is difficult to identify all important PSFs.

In addition, the HFE probability estimates are reviewed to ensure that the combinations of unsafe actions within an HFE do not exceed the lower limit of credible human performance. In this regard, the human performance limiting values from NARA (Ref. E8.1.11) were applied. Table E3.2-1 is adapted from the NARA documentation (Ref. E8.1.11).

Table E3.2-1. Human Performance Limiting Values

Actions	HPLV
Actions taken by a single team.	1E−5/d
Actions taken by more than one team either when the significance of the goal is well understood and the time is adequate or when extended time is available.	1E−6/d
Actions taken by more than one team when the significance of the goal is well understood and a fundamental part of training. Extended time must also be available so that inaction would have to persist for several hours if no further attempts were made to achieve the desired goal.	1E−7/d

NOTE: d = demand; HPLV = human performance limiting values.

Source: Modified from *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.11) p.17.

Overall HFE values can be lower than these values when there are other nonhuman events and/or failures that must occur in addition to operator unsafe actions in order for an HFE to occur. These events can include interlock failures, other mechanical failure, or physical phenomena that are independent of the unsafe actions. However, an absolute floor of 1E−8/d is applied regardless of these additional failures.

E3.2.8 Step 8: Incorporate HFEs into PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. E8.1.22) provides an overview of the state-of-the-art method for performing this step in PRAs. This process is done in conjunction with the PCSA analysts. Appendix E.I of this analysis provides the recommended approach for incorporation of human errors in the YMP PCSA, and Appendix E.V of this analysis provides the recommended naming conventions for HFEs incorporated in the fault tree models.

HFEs are incorporated, in the form of basic events, into the fault trees that support the initiating event and pivotal events of event trees. The HEP that is entered in a basic event is modeled as a lognormal distribution, whose mean value is the nominal value of the HEP, to which an error factor is assigned (Section E3.4) to reflect the uncertainty in the probability estimate. In many cases, the equipment failures and the associated HFEs are calculated as part of an integrated HRA. The resulting probability of both equipment and human failures is then placed in the fault tree as a single basic event.

E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design

This last step in HRA is performed each time the PCSA is quantified. The primary results are the HFEs in dominant cut sets and the associated qualitative inputs to such HFEs. Potential "fixes" to the design or operational environment can be supported by these results.

Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is noncompliant with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1) because the probability of a given HFE dominates the probability of the event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or to completely eliminate the HFE. In such cases, the modification is analyzed for potential new HFEs, and the applicable HFEs are requantified, along with the event sequences.

E3.3 DEPENDENCY

Dependency between human actions is defined to exist when the outcome of a particular human action is related to the outcome of a prior human action or actions. According to THERP (Ref. E8.1.26), the joint probability of human error for a set of dependent human actions is higher than if they were independent.

The possibility of dependencies between human actions and defined HFEs is recognized throughout the HRA task. The concern with respect to dependencies is that the joint probabilities separately assigned to a set of dependent HFEs treated as independent actions can result in a lower event sequence frequency than would result if dependencies among the HFEs were appropriately recognized and treated. This situation is especially important in the HRA activities leading up to and including preliminary analysis where an inappropriately low HEP might lead to an inappropriate screening out of a potentially significant cut set or event sequence. If dependence were properly identified and treated, the resulting HEP might then appear in dominant cut sets and, therefore, be identified for detailed analysis.

E3.3.1 Capturing Dependency

Dependencies between defined HFEs can exist for two reasons:

- Due to the characteristics of the event sequence in which the HFEs are modeled
- Due to the modeling style, especially the degree of decomposition, in HFE definition.

In the first case, dependencies are unavoidable due to the inherent characteristics of the initiator type or event sequence. In the second case, dependencies can be avoided by redefining dependent HFEs into a single HFE. In either case, dependencies can be treated by using a structured method for adjusting probabilities to account for dependencies. However, some HRA quantification methods (e.g., ATHEANA (Ref. E8.1.22)) account for certain types of dependencies within their formulation by combining dependent events as part of the normal process of addressing the accident scenario as a whole. These methods do not require additional treatment.

All event sequences that contain multiple HFEs are examined for possible dependencies. If practical, HFEs that are completely dependent may be redefined and modeled as a single event.

For the preliminary analysis, HFEs are modeled at a high level where several subtasks are combined into a single task so that explicit consideration of dependencies between subtasks is eliminated. For a detailed assessment, where the various actions that constitute an HFE are

explicitly quantified, dependencies are explicitly addressed using the formulae in Table E3.3-1 from THERP (Ref. E8.1.26), where N is the independently derived HEP. The THERP dependency model was selected for its formalism and reproducibility. The model itself is not dependent on what the source of the baseline (i.e., independent) HEP is; it can be obtained from any existing model or from expert elicitation. None of the other "objective" quantification approaches used (i.e., HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11) or CREAM (Ref. E8.1.18) has its own dependency model, and NARA (Ref. E8.1.11) specifically endorses the use of the THERP (Ref. E8.1.26) approach.

Table E3.3-1. Formulae for Addressing HFE Dependencies

Level of Dependence	Zero	Low	Medium	High	Complete
Conditional Probability	N	$\frac{1 + 19N}{20}$	$\frac{1 + 6N}{7}$	$\frac{1 + N}{2}$	1.0

Source: Modified from *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278 (Ref. E8.1.26), Table 20-17, p. 20-33.

E3.3.2 Sources of Dependency

The determination of the level of dependence between HFEs is left to the judgment of the HRA analyst. Certain factors typically are recognized as indicators of dependency. Examples of such factors are:

- Common time constraints for task performance
- Common cues or indicators for task performance
- Common diagnosis of situation
- Common facility function or system operation involved in task performance
- Common procedure steps for task performance
- Common personnel and location for task performance
- Common PSFs.

In addition, any human-induced failures of equipment that can directly or indirectly cause other equipment to fail through equipment dependencies are also identified as human dependencies.

E3.4 UNCERTAINTY

As with the values of failure probabilities used for active and passive components used in other parts of the PCSA, it is important that HFE quantification accounts for uncertainty. The HRA quantification, therefore, provides a mean HEP and an expression of the uncertainty. There are a number of ways to approach this task, as each of the HRA methods discussed in Section E3.2.7.2 provides recommendations on uncertainty parameters or bounds for HEPs. These recommendations run from the specific to the general and are often inconsistent. After a review of various recommendations, the HRA team has determined that to use any of them in their specific applications is both impractical and questionable. Rather, it was decided to develop a simple set of generic error factors developed through the use of the judgment by the HRA team, based on a holistic overview of the various recommendations presented in the following sources:

- Section 6 of NARA (Ref. E8.1.11)
- HEART (Ref. E8.1.28)
- Chapter 9 of CREAM (Ref. E8.1.18)
- Chapter 20 of THERP (Ref. E8.1.26).

Although ATHEANA (Ref. E8.1.22) does not provide specific recommendations regarding uncertainty estimation, it stresses that it is important to consider uncertainty in HRAs and that one way to approach it is through the use of expert judgment. To this extent, it can be said that the approach follows the guidance established in ATHEANA.

After review and due consideration of the uncertainty recommendations, the HRA team determined that for the purposes of this study it would be both reasonable and acceptable to establish a generic set of uncertainty parameters based on the calculated (total) HEP for any given HFE. The HRA team reached a consensus on the following error factor values to be applied to a lognormal distribution based on the mean HEP, as shown in Table E3.4-1. For each HEP range, the error factor reflects the HRA team's degree of confidence in the probability estimate.

Table E3.4-1. Lognormal Error Factor Values

Calculated Mean HEP	Lognormal Error Factor
≥ 0.05	3
>0.0005–<0.05	5
≤0.0005	10

NOTE: HEP = human error probability.

Source: Original

The same error factors are applied to both preliminary values and results of detailed HRAs. Therefore, after the HRA team has decided on an appropriate mean value, the corresponding generic error factor is assigned unless there is a basis from the detailed analysis to do otherwise.

E3.5 DOCUMENTATION OF RESULTS

The following information is included in the documentation of the results for the YMP PCSA HRA:

- General discussion of the overall set of PSFs (e.g., error-producing conditions (EPCs), common performance condition (CPCs)) on human performance that are applicable to or especially important for the YMP PCSA and how they apply to the operations of the facility in question
- A list of all HFEs (by basic event name and category, along with a brief description of the HFE) included in the PCSA model, with their final assigned HFE probabilities
- Identification of preliminary values used for these HFEs
- Identification of the HFEs analyzed in detail
- A more detailed description of each HFE analyzed in detail
- Identification of all expected pertinent procedures or, if no procedures are expected to exist, alternative evidence that supports the identification and quantification of HFEs and recoveries or substantiates the likelihood of human actions (e.g., normal operating practices, formal training)
- For each HFE analyzed in detail, identification of the quantification method, associated input parameters (e.g., PSFs), and any approximations or required procedural controls used to determine probabilities for that HFE
- References to sources of input information (e.g., thermal-hydraulic calculations) used in detailed quantification
- Results of qualitative and preliminary analysis
- Results of detailed quantitative analysis.

E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT

This section addresses how and what information was collected to support the HRA analysis and how expert judgment was used in the identification and quantification of HFEs.

E4.1 FACILITY FAMILIARIZATION AND INFORMATION COLLECTION

E4.1.1 General Information Sources

As with all of the tasks in the PCSA, facility information is required to support the HRA. In addition to the information that is gathered to support the other modeling tasks (e.g., initiating events, systems), the analysts obtain specific additional information that is needed to support the HRA task.

Since the YMP is in the design phase, there are limits on facility-specific information available to support the HRA. Sources utilized in this analysis include the following:

- Design drawings and design studies
- Concept of operations documents
- Engineering calculations
- Discussions of event sequences with knowledgeable individuals
- Event trees and supporting documentation
- Fault trees and supporting documentation.

Information from similar facilities is used, including NPPs (particularly those with ISFSIs), chemical agent disposal facilities, and any other facilities whose primary function includes handling and disposal of very large containers of hazardous material. This was conducted primarily for ISFSI activities at NPPs. The use of this information in place of YMP plant-specific information is pursuant to the third analytical boundary condition specified in Section E2.2. Following are sources of information from ISFSI that are applied to support the YMP PCSA:

- Interviews with plant operators, operations personnel, and/or other ISFSI knowledgeable personnel

- Pertinent ISFSI procedures (e.g., operating procedures, test and maintenance procedures)

- Plant walk-downs (e.g., at locations where operations similar to those at repository may be performed) and operations reviews

- Studies, including PRAs and HRAs, conducted at these facilities that would substitute for the previously mentioned sources.

This information was acquired from two sources. First, information was obtained by the HRA team from outside sources specifically for use on the YMP, such as from NPPs, industry organizations, and governmental sources. Some of this information may have been obtained directly by the HRA team or may have been provided to the HRA team by members of the Licensing and Nuclear Safety, Engineering, or Operations departments who had obtained the information as a part of their regular duties on the YMP (Section E4.2.2). Second, information was obtained by the HRA team directly from internal sources, including members of the aforementioned departments who had past experience and information on ISFSIs from prior employment and projects before joining the YMP (Section E4.2.1).

Initially, information is gathered to support the identification of pre-initiator, human-induced initiator, and non-recovery post-initiator HFEs. This information is needed to:

- Identify test and maintenance activities performed for equipment included in the PCSA model

- Determine the frequency of test and maintenance activities

- Identify the procedures used to perform test and maintenance activities
- Determine what equipment is impacted by test and maintenance activities.

For human-induced initiator and post-initiator HFEs, such information is needed to:

- Identify important operator tasks
- Identify the specific actions required for each operator task
- Identify the procedures (e.g., normal operating and emergency operating procedures) and procedure steps associated with each operator task
- Identify the cues (e.g., procedure steps, alarms) for operator tasks
- Assess the procedures that support operator tasks as PSFs
- Assess the training that supports operator tasks as PSFs.

E4.1.2 Industry Data Reviewed by the HRA Team

The following sources of industry data were reviewed by the HRA team for potential vulnerabilities and HFE scenarios applicable to the YMP:

- *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*, NUREG-1774 (Ref. E8.1.19)
- *Control of Heavy Loads at Nuclear Power Plants*, NUREG-0612 (Ref. E8.1.20)
- Navy Crane Center, Naval Facilities Engineering Command Internet Web Site. The database includes the following information:
  - Navy Crane Center Quarterly Reports (“Crane Corner”) 2001 through 2007
  - Fiscal Year 06 Crane Safety Report (covers fiscal years 2001 through 2006)
  - Fiscal Year 06 Audit Report
- U.S. Department of Energy (DOE) Operational Experience Summary (2002 through 2007) (http://www.hss.energy.gov/CSA/analysis/orps/orps.html).
- Institute of Nuclear Power Operations (INPO) database (https://www.inpo.org). The INPO database contains the following information:
  - Licensee Event Reports
  - Equipment Performance and Information Exchange System
  - Nuclear Plant Reliability Data System.
- *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)* (Ref. E8.1.5)

- All Scientech/Licensing Information Service data on ISFSI events (1994 through 2007) Scientech Licensing Information Service Database and Dry Storage Information Forum (New Orleans, LA, May 2-3, 2001). This database includes the following information:

  – Inspection reports
  – Trip reports
  – Letters, etc.

E4.2 USE OF EXPERTS AND ENGINEERING JUDGMENT IN THE HRA

Subject matter experts were employed in the identification, verification, preliminary analysis, and detailed analysis of HFEs. Identification of HFEs, of which a HAZOP evaluation was a part, was performed as a combined effort by experts from a wide range of areas. This identification was not specifically a part of the HRA task, but it was used by the HRA team in the process of identifying HFEs. A description of the HAZOP evaluation process and a list of experts who specifically participated in the HAZOP evaluation is provided in the *Wet Handling Facility Event Sequence Development Analysis* (Ref. E8.1.10).

E4.2.1 Role of HRA Team Judgment

Preliminary and detailed analyses were primarily performed by the HRA team in a consensus-based process. For the preliminary analysis, the judgment process can be summarized in the following fashion:

- Each HFE that was identified during the HAZOP evaluation and the operational experience review was characterized with input from the Engineering and Operations departments, including the context under which the HFE would occur.

- Once the individual members of the HRA team were confident that they understood the HFE and the context, they each independently assigned an HEP to the HFE and briefly documented the rationale relative to a set of anchor points established for the HRA (the basic anchor points can be found in Appendix E.III of this analysis).

- The values and rationales were combined into a single spreadsheet, and the team then met to discuss their values.

- The HRA team used their knowledge of the preclosure process and design to develop a consensus on the factors affecting the HFE and a resulting conservative estimate of the HEP. In most cases, the team ultimately reached a consensus on a value and a rationale. In a few cases a consensus could not be reached, and the most conservative value and rationale from that team member was used. The value and rationale applied was then documented.

This process is explained in much greater detail in Appendix E.III of this analysis.

The detailed analyses were performed by individual members of the HRA team and were reviewed by the rest of the HRA team. Judgment was used to identify the details of the scenarios

that could lead to the HFE, the appropriate quantification methodology to apply to each unsafe action, the actual quantification of the unsafe action, and any probabilities for other key failures within the HFE for which probabilities were not available in the active or passive failure database. However, in no instance was expert judgment used to quantify an entire HFE, so in the context of the ATHEANA concept of an expert elicitation approach to quantification, it was not necessary to utilize the strict formalism. Each HFE was broken down into various combinations of unsafe actions and mechanical failures. In all but one case, every unsafe action was quantified using one of the "structured" HRA quantification techniques (i.e., HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11), CREAM (Ref. E8.1.18), or THERP (Ref. E8.1.26), and so expert elicitation was not required. In the one exception, the process that was followed is that the team member who performed the detailed quantification of the HFE provided a detailed rationale for the selection of a value based on judgment. The entire HFE quantification, including the judgment value, was provided to the other team members for review and concurrence, and the resultant value and rationale were included in the final HFE quantification. In addition, there were cases where some of the mechanical failures within the HFE also required the use of judgment in selecting a probability of occurrence. These values were selected in accordance with the engineering judgment approach used throughout the PCSA for selection of such values. This approach anchors the selection of failure probability based on the level of understanding of the physical phenomena involved, rather than the use of anchors based on the context of the HFE. This approach is documented in Section 4.3.10.2.

The members of the HRA team are listed in the following section.

E4.2.1.1 HRA Team

Paul J. Amico—Mr. Amico is a nuclear engineer with 30 years of experience in risk, safety, regulation, and operation of NPPs, nuclear material production reactors, nuclear weapons research, production and storage facilities, nuclear fuel cycle facilities, chemical demilitarization facilities, and industrial chemical plants. He has been involved in the conduct and review of HRA since 1979. His experience includes the use of THERP, Time-Reliability Correlation (TRC), Systematic Human Action Reliability Procedure (SHARP), Human Cognitive Reliability (HCR), HEART, ATHEANA, CREAM and NARA, and he has been involved in projects related to methodology enhancements to some of these techniques. Prior to joining the YMP, he was involved in HRA for a number of NPP PRAs in the United States and overseas; for chemical process plants; and for SNF handling and storage at NPPs, including the development of project procedures for HRA. He developed a phased approach to the use of HRA during the design process of advanced NPPs and supported a project to expand HRA techniques for SNF handling operations.

Erin P. Collins—Ms. Collins is a risk analyst with over 20 years of experience in safety, reliability, and risk analysis for the U.S. Army chemical weapons destruction program, NASA, the Federal Aviation Administration, NPPs, and the chemical process industry. Her specialties are equipment reliability database development and HRA. Ms. Collins was a prime participant in a safety hazard analysis of an acrylic fiber spinning facility in northeastern Italy. This analysis evaluated worker risk in various areas of the facility through the use of hazard analysis techniques, including a HAZOP evaluation, and resulted in the recommendation of economical risk reduction measures. Her project experience in Spain includes technical review and support

of the HRAs for the Ascó and the Santa Maria de Garoña nuclear plant PRAs. She also supported the review of the Kola and Novovoronesh Russian nuclear reactor HRAs for the DOE. In the United States, Ms. Collins has participated in PRA-related HRAs of the Hanford N Reactor and the Robinson (using simulator exercises), Crystal River 3, and Catawba NPPs. Throughout these efforts, she has applied the HEART, CREAM, THERP, and TRC methods of quantification.

Douglas D. Orvis, Ph.D.—Dr. Orvis is a registered professional engineer (California, Nuclear No. 0925) with over 35 years of experience in nuclear engineering, regulation, and risk analysis of NPPs, alternative concepts for interim storage of SNF, and aerospace applications. Dr. Orvis has participated in the development of HRA techniques (e.g., SHARP for Electric Power Research Institute (EPRI), effects of organizational factors for the NRC) and has measured and analyzed data for evaluating the reliability of NPP control room operators during simulated accidents. These data-based analyses included the EPRI-sponsored Operator Reliability Experiments (ORE) (e.g., measurements performed at the Diablo Canyon, Kewaunee, and LaSalle simulators) and the follow-on programs performed at the Maanshan (Taiwan) simulator. Data collection and analysis included observing operator behavior, variability between crews, developing time-response correlations for key operator actions, and evaluating the numbers and kinds of errors and deviations committed. Postsimulation interviews with crew members and trainers were conducted to elicit information on conditions and factors that contributed to crew performance. The data analysis included comparisons of data to the HCR model and a statistical evaluation of the types and causes of errors and deviations. A similar data collection evaluated the efficacy of an expert system called the Emergency Operating Procedures Tracking System.

Dr. Orvis participated in a comprehensive review of HRA methods for a Swiss agency and was a consultant to the International Atomic Energy Agency to incorporate concepts of HRA and organizational factors into (Assessment of the Safety Culture in Organizations Team) guidelines for plant self-assessment of safety culture. Dr. Orvis has performed event tree and fault tree analyses of hazardous systems for both internal events and seismic initiators that included consideration of HRA. Dr. Orvis has participated in HAZOP evaluation sessions for repository operations.

Mary R. Presley—Ms. Presley is an engineer with 3 years of experience in risk analysis for NPPs, specializing in human reliability. Ms. Presley graduated in 2006 from the Massachusetts Institute of Technology with her M.S. in nuclear engineering, where she wrote her thesis *On the Assessment of Human Error Probabilities for Post Initiating Events*, which included an extensive review of current HRA methods. While her work focused on the EPRI HRA calculator and the NRC ATHEANA framework, she is also familiar with other HRA methods, including THERP, Accident Sequence Evaluation Program (ASEP), HEART, NARA, Failure Likelihood Index Methodology (FLIM), Success Likelihood Index Method/Multi-Attribute Utility Decomposition (SLIM/MAUD), Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H), CREAM, Methode d'Evaluation de la Relisation des Missions Operateur pour la Surete (MERMOS), Cause-Based Decision Tree (CBDT), and HCR/ORE.

E4.2.2 Role of Subject Matter Expert Judgment

Subject matter experts were also consulted during the compilation of the base case scenarios. The outline of the base case scenarios came from the mechanical handling block flow diagram. The details of human interaction with the mechanical systems were derived from expected operations inferred directly from the design by the subject matter experts. Where a detailed design was not available, the experts extrapolated these details from common industry practice for similar operations. These experts come from the YMP Engineering, Operations, and PCSA groups, as well as from outside the YMP project.

In addition to the development of base case scenarios, subject matter experts were regularly consulted during the analysis to provide clarification of design, clarification of expected operations, and insight into expected operating conditions and failure modes. These experts provided details about the design of systems that were relevant to human performance, such as the presence of job aids and interlocks and the intended design of control system interfaces. They also provided details regarding the concept of operations for the processes, such as the role of the humans versus the use of automatic systems, the operational controls, and the use of procedures. These experts would also review specific parts of the analysis for technical accuracy.

Below is a list of some areas where subject matter experts were consulted during the HRA for their expertise:

- PCSA models (i.e., facility or system fault trees)
- Site prime mover (SPM), railcar, truck trailer, cask transfer trolley (CTT), cask tractor and cask transfer trailer (HCTT), and site transporter design and operation
- Crane operations (critical lifts)
- Crane design – Single-failure proof cranes (i.e., gantry cranes designed to NOG-1 level 1 standards (Ref. E8.1.2) or jib cranes designed to NUM-1 Type 1A (Ref. E8.1.3))
- Crane design – Non-single failure proof cranes (i.e., gantry cranes designed to NOG-1 level 2 standards (Ref. E8.1.2) or jib cranes designed to NUM-1 Type 1B (Ref. E8.1.3))
- Platform operations (shield plate and non-shield plate)
- Gas sampling process
- Canister transfer machine (CTM) design and operations
  - Adjustable speed drive (ASD) features and operations
  - Grapple interfaces
  - Interlocks

- Radiation protection (e.g., cask shielding/shield rings; locks, interlocks, and procedural controls for entering high radiation areas; PPE (personal protective equipment))
- General facility layout and time line of operations
- Interlocks (general)
- Dual-purpose canister (DPC) cutting equipment and process
- Pressure relief system for DPC filling/cooling
- Pool maintenance (i.e., maintaining boration)
- SNF handling operations (i.e., pool operations, spent fuel transfer machine)
- Transportation, aging, and disposal (TAD) welding equipment and process
- TAD drying system
- Aging overpack, horizontal shielded transfer cask (HSTC), shielded transportation cask (STC), TTC, and a transportation cask that is upended on a railcar (VTC) design and handling
- Other systems

E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES

Over the history of performance of HRAs, certain terminology has become commonplace and different classification schemes for human error has been developed. This section provides a background of this terminology and associates it to the YMP PCSA HRA. In addition, the description of operations includes references to different types of personnel. The functions of each classification of personnel are described in this section. Finally, a discussion is provided of the specific issues that relate to human performance at the YMP.

E5.1 TERMINOLOGY

E5.1.1 Classification of HFEs

As noted in the methodology (Section E3.2), HFEs are classified to support the HRA preliminary analysis, selection of HRA quantification methods, and detailed quantification. A combination of four classification schemes is used in the YMP HRA. The first three schemes are familiar standards in HRA. The fourth scheme has its basis in behavioral science and has been used in some second-generation HRA methods.[5]

[5]There is another classification not included here that has been often used in nuclear power plant PRAs: the behavior type taxonomy. This category classifies HFEs into skill-, rule-, or knowledge-type behavior. While this taxonomy has limited usefulness in addressing HFEs that take place in an NPP control room under time constraints, this distinction is not particularly useful for other types of actions. As a result, it is generally not used for HRAs in

The four classification schemes are based on the following:

1. The three temporal phases used in PRA modeling:

   A. Pre-initiator
   B. Human-induced initiator
   C. Post-initiator

2. Error modes:

   A. EOOs
   B. EOCs

3. Human failure types:

   A. Slips/lapses
   B. Mistakes

4. Informational processing failures:

   A. Monitoring and detection
   B. Situation awareness
   C. Response planning
   D. Response implementation.

The following sections define these classification methods.

E5.1.1.1 Temporal Phases of HFEs

There are three temporal phases of HFEs:

- Pre-initiator HFE—An HFE that represents actions taken before the initiating event that causes systems or equipment to be unavailable. Examples of such HFEs are miscalibration of equipment or failure to restore equipment to an operable state after testing or maintenance activities.

- Human-Induced Initiator—An HFE that represents actions that cause or lead to an initiating event.

- Post-initiator HFE[6]—A post-initiator HFE represents those operator failures to manually actuate or manipulate systems or equipment, as required for accident response. Post-initiator HFEs can be further divided into recovery and non-recovery events.

such applications as chemical process facilities, chemical demilitarization facilities, or NASA manned-mission risk assessments. Given the type of human actions and HFEs that are important at the YMP, use of this approach for the YMP PCSA HRA is not recommended.

[6] The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

– A non-recovery post-initiator HFE (i.e., failure during response to an initiator) is when an operator does not operate frontline equipment in accordance with required procedural actions due to errors in diagnosis or implementation. For quantification purposes, these HFEs are usually decomposed into cognitive and implementation parts, as shown in Appendix E.II of this analysis. In general, post-initiator HFEs associated with such actions are incorporated directly in the model prior to initial PRA quantification using preliminary values. The results of the initial event sequence quantification are used to determine if detailed modeling of these HFEs is needed.

– A recovery post-initiator HFE represents operator failure to manually actuate or manipulate frontline equipment (or alternatives to frontline equipment[7]) that has failed to automatically actuate as required. In general, post-initiator HFEs associated with correction or recovery of failed frontline systems from either equipment or human failures are not modeled until after initial PRA quantification. The results of initial event sequence quantification are used to determine if modeling of such recovery HFEs is needed.

E5.1.1.2 Error Modes

HFEs can be classified by error mode as either an EOO or EOC. EOOs and EOCs can occur in any temporal phase (i.e., pre-initiator, initiator, or post-initiator). This classification is highly dependent upon the specific event tree or fault tree model. In other words, the same operator action could be modeled as either an EOO (e.g., failed to actuate system x) or an EOC (e.g., actuated system y instead of x). The error mode model is chosen based on consistency with the PCSA model and at the discretion of the HRA analyst. In early PRAs, EOCs were often excluded. Current PRAs, however, address both EOOs and EOCs, although there are still few methods for identifying and quantifying EOCs. In the current analysis, EOO and EOC are defined as follows:

- EOO—An HFE that represents the failure to perform one or more actions that should have been taken and that then leads to an unchanged or inappropriately changed configuration with the consequences of a degraded state. Examples include the failure of a radiation protection worker to perform the radiologic survey before a cask is released from the facility.

- EOC—An HFE that represents one or more actions that are performed incorrectly or some other action(s) that is performed instead. It results from an overt, unsafe action that, when taken, leads to a change in configuration with the consequence of a degraded state. Examples include commanding a crane to lift when it should be lowered.

E5.1.1.3 Human Failure Type

Human failure types include the following:

[7]Alternatives to frontline equipment, include equipment that operators can use for performing the functions of frontline equipment in case of an impossibility to recover the failed frontline equipment in a timely manner.

- Slip/lapses—An action performed where the outcome of the action was not as intended due to some failure in execution. Slips are errors that result from attention failures, while lapses are errors that result from failures in memory recall.

- Mistake—An action performed as intended, but the intention is wrong. Mistakes are typically failures associated with monitoring (especially deciding what to monitor and how frequently to monitor), situation awareness, and response planning. Section E5.1.1.4 provides definitions of these terms.

E5.1.1.4 Informational Processing Failures

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is recommended for the YMP HRA is based on the discussion in Chapter 4 of ATHEANA (Ref. E8.1.22) and consists of the following elements:

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.

- Situation awareness—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents operators' understanding of the present situation and their expectations for future conditions and consequences.

- Response planning—This term is defined as the process operators use to decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.

- Response implementation—This term is defined as the activities involved with physically carrying out the actions identified in response planning.

When there are short time frames for response and the possibility of severely challenging operating conditions (e.g., environmental conditions) exists, then failures in all information processing stages must be considered. Also, slips/lapses and mistakes are considered for each information processing stage. Response implementation failures are expected to dominate the pre-initiator failures that are modeled. Post-initiator failures and failures that initiate event sequences can occur for all information processing stages, although detection failures are likely to be important only for events requiring response in very short time frames.

E5.1.2 Personnel Involved in WHF Operations

A list of personnel involved in WHF operations with a brief description of their duties is provided below:

Crane operator—The person who is designated to operate the crane for a given operation (i.e., the cask handling crane, the auxiliary crane, or the jib cranes).

Crew member—A generic term for personnel (not including crane operators, radiation protection workers, or supervisors) involved in the facility operations.

CTM operator—The person who is designated to operate the CTM for canister transfer activities. This person is located in the WHF Control Room and controls the CTM remotely.

DPC cutter—The person who is designated to operate the DPC cutting machine to cut open the DPC.

Engineer—The person from Nuclear Engineering who is in charge of performing the nuclear engineering calculations, including developing and/or checking the TAD loading plan.

Gas sampling operator—The person who is designated to perform gas sampling of the cask and gas sampling and venting of the canister.

HCTT operator—The person who is designated to operate the cask tractor to move a HCTT unit into or out of the facility.

Level 2 and 3 NDE personnel—The person(s) who is certified to inspect the TAD canister welds and sign off on the process. This person(s) must have a level 2 and level 3 nondestructive examination (NDE) certification.

Person in charge (PIC)—The certified crew member who is in charge of coordinating and overseeing the facility operation. This is the person who is notified when a waste form is coming to the facility and who coordinates, according to this information, the appropriate personnel, procedures, and equipment to be used to process this cask type. This person is in charge of communicating this information to all the crew members involved in the processing of this cask and ensuring that the relevant equipment is properly staged and in proper operational condition.

Quality control—The certified crew member in charge of quality control. This person is involved in supervising critical operations and tracking the appropriate documentation (i.e., checking off on the fuel assembly serial numbers and TAD loading plan).

Radiation protection worker—The certified health physics technician, whose job is to monitor radiation during cask-related activities. This person is responsible for stopping operations if high radiation levels are detected.

Signaling crew member—The person who is designated to provide signals to the crane operator. This person is predesignated and is distinguished from the verification crew member (most likely through an orange hard hat, orange gloves, or an orange vest as per the high-level radioactive waste *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)* (Ref. E8.1.12)).

Spent fuel transfer machine operator—The person who is designated to operate the spent fuel transfer machine to move fuel assemblies. This person has special training on how to read and track TAD loading plans.

SPM operator—The person who is designated to operate the SPM to bring a railcar or truck trailer into the facility.

Site transporter operator—The person who is designated to operate the site transporter to move an aging overpack into and around the facility.

Supervisor—The person who is in charge of the given operation and who supervises and checks off critical operations in a given step. For steps requiring independent verification, this analysis uses the term supervisor as the person who provides the independent check. This analysis does not rely upon the fact that this check is performed by the actual supervisor, only that an independent check is done by someone with the appropriate training and qualifications (i.e., the supervisor).

Verification crew member—The person who is designated to assist with crane operations that require a second spotter. This person can only give the stop signal to the crane operator.

Welding operator—The person who is designated to operate the welding machine to weld close the TAD.

E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES

This section discusses the general human performance issues that characterize the human interaction with the YMP facilities.

Limited Automation (Significant Human Interaction)—The types of operations being performed in the WHF are not always conducive to automation. In particular, crane and transport operations are generally performed both manually and locally. Even those that are performed remotely require significant interaction by the operators. The dependence on human performance is quite high, and that dependence provides many opportunities for unsafe actions.

Limited Nature of Procedures—Other than those operations that are performed remotely from a control room, YMP operations are not highly proceduralized, but rather they depend primarily on skills learned and training. That is, while written procedures exist for all activities and training of all personnel is thorough, the actual use of procedures and checklists during operation (i.e., the step-by-step following of written procedures) generally occurs only during operations in a control room. The vast majority of local operations (e.g., skill-of-craft activities performed outside the control room) does not use written procedures at all during the actual performance of the tasks and does not have formal checklists or verbal confirmation requirements spelled out in

procedures physically in the possession of the crew performing the operation. This circumstance is consistent with observations of activities at NPPs during ISFSI operations.

Communication Difficulties—There are significant challenges in communication between the team members performing WHF operations. The environment contains a not insignificant amount of background noise, predominantly machine noise. Although headsets may be used by key participants for communication, they do not eliminate the potential for misunderstanding. Garbled communication (due to system interference or background noise) is clearly possible, and in some cases it may not even be possible to clearly determine who is speaking. A belief that a particular individual is speaking, even if they are not, can bias the listeners into hearing what they expect to hear.

Visual Challenges–For most of the remote operations, successful completion of the operation requires a certain amount of visual acuity both for the performance of the operation and the confirmation of the status. Safety concerns require that visual observation be performed using cameras that provide images to screens in the control room. Even local crane operations create visual challenges. The crane operator can only be at one given distance and orientation with relation to the operation, and therefore cannot be viewed on all three axes. In addition, views may be obstructed, such as by the yoke, the load being moved, or some other structure or equipment. Thus, the operator is often put in the position of being the hands for someone else's eyes, which make the operations vulnerable to the communication vulnerabilities discussed previously.

Unchallenging Activities—The activities involved in WHF operations are, in general, quite simple in nature. In addition, the speed of the movements is quite slow, so each action takes a long time to complete. Basically, this is mostly boring work, with a significant amount of downtime between actions for some individuals. There is ample opportunity for diversion and distraction, and an air of informality and complacency can easily exist within and amongst the crew members. From a psychological perspective, there is insufficient dynamic activity to generate an optimum stress level for performance.

E6 ANALYSIS

E6.0 BACKGROUND

E6.0.1 Reader's Guide to the HRA Analysis

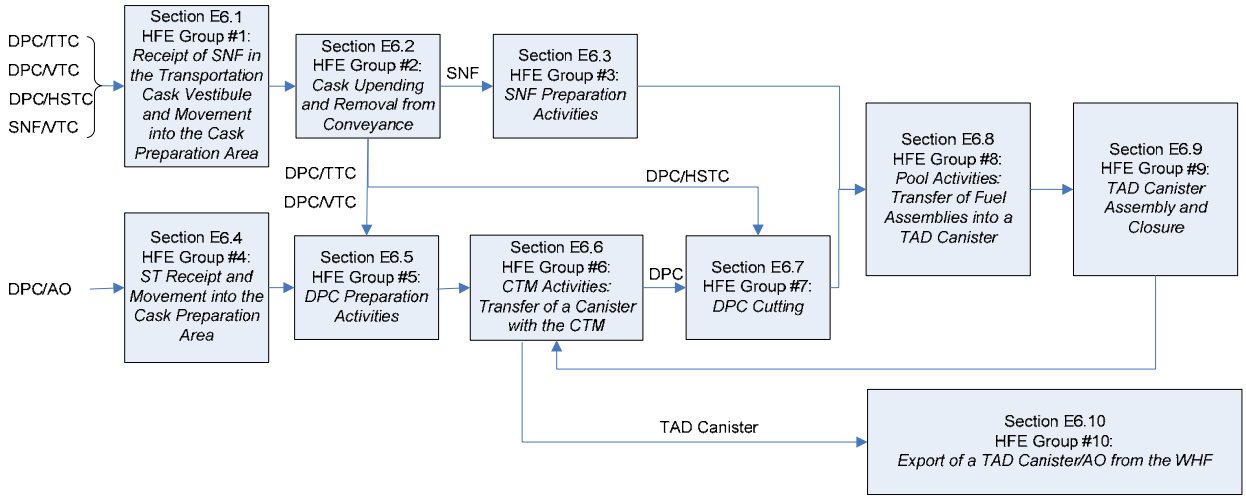
Section E3.2 describes nine steps that comprise the HRA process. This section describes the implementation of Steps 2 through 8.

The HFEs were analyzed in logical groups that relate to the various phases of WHF operations. For each group of operations, the following is presented:

- A base case scenario describing the normal operations for that group of operations (Step 2)
- Descriptions of the HFEs of concern identified for the group (Step 3)

- Preliminary values for each HFE identified (Steps 4 and preliminary Step 8)
- Detailed analysis for significant HFEs (Steps 5 through 7 and final Step 8).

Figure E6.0-1 is an overview of how the facility operations were grouped. For the WHF, there are ten HFE groups analyzed, with each presented in a separate subsection of Section E6.



NOTE: AO = aging overpack; CTM = canister transfer machine; DPC = dual-purpose canister; HFE = human failure event; HSTC = cask tractor and cask transfer trailer; SNF = spent nuclear fuel; ST = site transporter; TAD canister = transportation, aging, and disposal canister; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar; WHF = Wet Handling Facility.

Source: Original

Figure E6.0-1. HFE Groups Associated with Facility Operations

The HRA is conducted to link the HFEs to the event sequence analysis for the operations in a given HFE group of the facility. When added to the generic information contained in the topics common to multiple HFEs (Section E6.0.2), each major section shown in Figure E6.0-1 (e.g., E6.1, E6.2) treats one set of operations in its entirety and is designed to stand alone and be complete with respect to the actions in that HFE group.

The ordering of the major sections follows the high-level flow diagram in Figure E6.0-1, and it is essential to note that, because this facility handles several types of waste forms, there may be multiple variations of the facility operations (i.e., multiple paths such as in Figure E6.2-1). At various points in this attachment, therefore, it may be necessary for the reader to "loop back" to evaluate an alternative path through the process. In these cases, an HFE group (Section E6.x, where x denotes a particular subsection) does not follow logically from the previous HFE group (Section E6.x-1, where x-1 denotes the subsection prior to x). This can happen multiple times in the course of analyzing the facility operations. It is intended that the reader begin by reviewing the material contained in this introductory section (as it applies to all groups) and then read each individual major section to understand the event sequence assessment of its associated operations.

Operations within a given HFE group may also have multiple variations. The reader is cautioned that an HFE group may also not flow cleanly in sequential order from beginning to end. A flow diagram is provided in the introduction to each major section to assist the reader in navigating through the operations of an HFE group.

Each HFE group begins with the flow diagram and a description of the base case scenario for that group. The flow diagram allows the reader to understand how any given part of the base case scenario relates to the rest of the base case scenario. A table is then provided that summarizes the HFE descriptions and the preliminary values assigned. Detailed analyses, where appropriate, are then explained in terms of the HFE scenarios (identified by a basic event name) and the unsafe actions within these scenarios. For these detailed analyses, an explanation of how each action was quantified is provided, indicating the specific quantification method and task type identifier used for the quantification. Each HFE group subsection concludes with a table summarizing the final HEP values for the relevant HFE scenarios. Where no detailed analyses were performed, the HFE description and preliminary value table provides this information. By associating each scenario with a basic event name, the link between the HRA results and the PCSA models is clearly established because the HFE can be traced directly to its position(s) in the fault tree(s).

The HFEs listed in each HFE group were identified through an iterative process involving the HAZOP evaluation, development of the MLD, ESDs and initial event trees/fault tree models, and extensive conversations between subject matter experts (Section E4.2.2) and the HRA team (Section E4.2.1). Because the HRA was performed as part of an integrated process with the rest of the PCSA, to put this analysis in context, the reader must have an understanding of the other components of the PCSA, including:

- The process flow diagram
- HAZOP evaluation
- MLD
- Event trees
- Faults trees (including the pivotal event fault trees)
- ESDs.

To provide traceability between the HRA and the rest of the PCSA, Table E6.0-1, provides a cross-reference between the HFE groups and the ESD and HAZOP evaluation node(s)[8] applicable to a given group.

Each HFE group represented in Figure E6.0-1 corresponds to a HAZOP evaluation node(s) addressing that group and the ESDs and event trees that represent the event sequences covering that group. In this way, a reader looking to understand how human failures affect the results of the event sequence quantification for the event tree in any specific event tree group need not move back and forth between the major sections of E6, but can find everything related to all HFEs within each set of operations for an HFE group in a single major section. There is some necessary repetition of similar information used in more than one major section when the

[8] HAZOP nodes are defined by the PFD in Volume 1 of the PCSA *Wet Handling Facility Event Sequence Development Analysis* (Ref. E8.1.10).

operations performed in their respective groups are similar (or identical). Material on HRA methodology that is common to all HFE analyses is not repeated; however, cross-references to applicable sections and appendices are provided, as appropriate.

Table E6.0-1. Correlation of HFE Groups to ESDs and HAZOP Evaluation (PFD) Nodes

Activity	HAZOP Evaluation (PFD) Node	ESD
HFE Group #1: RC, TT and HCTT Receipt and Movement into Cask Preparation Area		
Move RC/Truck into Cask Preparation Area	1	1,2
Move HCTT into Cask Preparation Area		4
HFE Group #2: Cask Upending and Removal from Conveyance		
Cask upending (VTC and HSTC)	2-4	5, 6
Cask upending (TTC)	3, 4, 6-9	
Move Cask to CTT (VTC or TTC with DPC)	10	
Move Cask to SNF Preparation Station (TTC with SNF)	5	
Move Cask to DPC Cutting Station (HSTC with DPC)	5	
HFE Group #3: SNF Preparation Activities		
Preparation activities – all (gas sampling and cask lid lift fixture installation)	21	8, 16
HFE Group #4: ST Receipt and Movement into ST Vestibule		
Move ST with AO to ST Vestibule	1	3
HFE Group #5: DPC Preparation Activities		
Preparation activities – Lid on (gas sampling and cask lid lift fixture installation)	1, 10	7
Preparation activities– Lid off (cask lid removal and DPC lift fixture installation)	10	9
Move CTT to Cask Unloading Room	11	10
Move ST to Cask Loading Room	15	11
HFE Group #6: CTM Activities		
CTM activities (i.e., canister transfer and lid removal/emplacement)	12-14	13
HFE Group #7: DPC Cutting		
DPC cutting activities	5, 16-19	14, 15, 17, 18
HFE Group #8: Pool Activities		
Move cask to pool ledge	20	19, 20, 30
Move cask to/from pool bottom and transfer of fuel assemblies	22	21, 22, 30
Move cask from pool ledge to TAD closure station		24, 30
HFE Group #9: TAD Assembly and Closure		
TAD closure (e.g., welding, drying, etc.)	23	25-27
Move STC/TAD to Preparation Station with Crane	5	28
Move STC/TAD to Unloading Room with CTT	11	10

Table E6.0-1. Correlation of HFE Groups to ESDs and HAZOP Evaluation (PFD) Nodes (Continued)

Activity	HAZOP Evaluation (PFD) Node	ESD
HFE Group #10: Export of TAD/AO from WHF		
Closure and Export of AO	15	11

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HAZOP = hazard and operability; HCTT = cask tractor and cask transfer trailer; HFE = human failure event; HSTC = horizontal shielded transfer cask; PFD = process flow diagram; RC = railcar; SNF = spent nuclear fuel; ST = site transporter; TAD = transportation, aging, and disposal; TT = truck trailer; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar; WHF = Wet Handling Facility.

Source: Original

The following ESDs refer to actions that fall under several HFE groups and process flow diagram nodes:

- ESD 12: Event Sequences Associated with Aging Overpack (DPC or TAD) on Site Transporter or STC/TAD on CTT Colliding with Cask Loading Shield Door (HFE groups 5, 7, 9 and 10).
- ESD 23: Event Sequences for Activities Associated with Low-Level Liquid Waste (No HFEs associated with this ESD, see Section E6.0.2.3.6).
- ESD 29: Direct Exposure Event Sequences for Activities Associated with Cask Preparation or CTM Movement (HFE groups 2, 5, 6, 7, 9, and 10).
- ESD 31: Event Sequences for Fires Occurring in the WHF (Fire analysis is treated separately in Attachment F).

HFEs that are generic to several HFE groups can be found in Section E6.0.2; otherwise the HFEs that correspond to these ESDs are located in the appropriate HFE group. Section E7 provides a cross-reference linking these ESDs to their corresponding HFEs.

E6.0.2 Topics Common to Multiple HFE Groups

There are a number of cross-group generic issues and HFEs that were evaluated at the facility level and determined to be conducive to establishing ground rules (i.e., how the combination of interlocks and unsafe actions are modeled in the facility) for use throughout the analysis.

E6.0.2.1 Interlocks

For the HRA, interlocks were generally modeled explicitly in the fault tree instead of being embedded in the HRA for the preliminary analysis. The approach chose by the team to assign preliminary HEPs when interlocks were present was simplified. Since the interlock would prevent the operator from completing an unsafe action (even if the operator tried to) it was conservatively analyzed as if the operator would always take the unsafe action (i.e., the HEP for the HFE containing the unsafe action was conservatively set to 1.0 as a first approximation of the HEP). Unless otherwise specified, this was done for all cases where the human cannot easily

defeat the interlock that protects against the associated unsafe action and HFE. Therefore, the analysis is relying entirely upon the interlock to prevent the failure. The interlock failure probability is taken from the active component failure database (Attachment C), which gives a value of 2.7E−5 per demand (approximately 3E−5/demand). It is recognized in using this approach that, despite the interlock not being easy to defeat, there is always a possibility that it could be defeated (either by the operator or by the maintenance crew and then not restored). However, if this were the case then it would still be necessary for the operator to erroneously conduct the unsafe action. The team considered that it was very unlikely that the screening combination of the bypass error and the unsafe action would approach or exceed the 3E−5 value for the random failure of the interlock. The team judged that this preliminary value would implicitly account for the failure to restore an interlock after maintenance if that interlock is difficult to bypass and is not bypassed during normal maintenance. If this conservative approach was not adequate to demonstrate compliance with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1), a more realistic preliminary value was applied and justified. That is, the team went back and took a further look at the unsafe action and its associated interlock, and determined whether a lower preliminary HEP for the unsafe action could be justified. If so, this is clearly discussed and documented in the preliminary analysis. Interlocks that humans can reasonably defeat were generally not explicitly modeled in the fault tree, but rather included in the HEP for the HFE since they are not independent of operator actions. Regardless of this approach, in any case where the preliminary HEP was not sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1) and a detailed analysis was needed, all interlocks and other mechanical failures or physical phenomena that contribute to the overall HFE were integrated into the HRA along with the contributing unsafe actions and evaluated within the overall HFE quantification as part of the context of the HFE and fully discussed and documented in the detailed analysis. In all cases, interlocks that rely on programmable logic controller (PLCs) were not credited in this analysis since they won't be declared important to safety.

E6.0.2.2 Crane Drops—Drop of Cask or Drop of Object onto Cask

There are several lifts in the WHF operations, including lifts with the cask handling crane, the auxiliary hook, the CTM, and several jib cranes. These lifts of canisters, casks and heavy objects can potentially result in a drop. Crane-drop-related HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane/rigging types. Documentation for this failure can be found in Attachment C (active component failure data). The only exception to this is drops from the CTM; these were explicitly modeled because the CTM is sufficiently different from standard industry cranes to warrant a separate analysis.

E6.0.2.3 Preliminary Analysis of Cross-Cutting HFEs

E6.0.2.3.1 Operator Introduces Moderator Source in to Moderator-Controlled Areas of the WHF

The analysts have not found any way for operators to introduce significant quantities of moderator in the moderator-controlled areas of the WHF; therefore, this failure was omitted from analysis.

E6.0.2.3.2 Load Lifted too Heavy for Crane

There are several lifts in the WHF operations that may potentially result in the operator attempting to lift a load which is too heavy for the crane. Some of these opportunities include:

- Attempting to remove the cask lid with the CTM or auxiliary hook of the cask handling crane when all the lid bolts have not been removed
- Attempting to remove the impact limiters with the auxiliary hook of the cask handling crane when all the bolts have not been removed
- Attempting to lift the cask from the conveyance with the cask handling crane when the tie downs have not been removed
- Attempting to lift the cask from the tilting frame before disengaging the cask from the frame.

Of this set of HFEs, only the failure involving cask lid removal with the CTM was modeled explicitly in the fault trees because it is different than a typical crane. All other drops due to attempting to lift a load that is too heavy for the crane have been omitted from analysis because they would require a combination of multiple human errors and mechanical errors. All cranes that handle casks are designed to a single-failure proof standard; in this case, there are at least two interlocks which prevent an overload (i.e., load cell and temperature interlock). In addition to the failure of the crane, the crew would have to fail to disconnect the cask/lid from what it is attached to, and then fail to notice that what is being lifted is not correct (i.e., that the railcar is being lifted with the cask); there are at least three crew members involved in all these operations that should be actively observing the lift.

E6.0.2.3.3 Operator Causes Collision between Shield Door and Waste Conveyance

There are several instances where a conveyance, containing a waste form, travels through a shield door. Shield doors are involved in the following transfers:

- The CTT carrying a transportation cask moves from the Cask Preparation Area into the Canister Unloading Room
- The CTT carrying a STC cask moves between the Cask Preparation Area and the Canister Unloading Room
- The site transporter carrying an aging overpack moves between the Cask Loading Room and the Site Transporter Vestibule.

Each time a conveyance moves through a set of shield doors, two HFEs are possible: an operator can cause the conveyance to collide into the shield door or an operator can close the shield door on the conveyance. These collisions were considered separately from collision of the conveyance into other SSCs because if a conveyance impacts a shield door, the shield door itself can fall back onto the conveyance; these failures are encompassed in ESD 12. Collision into a shield door, as dictated by the nuclear safety design basis, does not result in the shield door

falling onto the conveyance; therefore, the only failure considered for ESD 12 is operator closes shield door on conveyance. The collision into a shield door is accounted for in the generic collision value for a given conveyance. Each transfer was assessed separately for these failures, but the operations were considered sufficiently similar to allow for one common preliminary value to be applied to all transfers. This preliminary value is described below:

050-OpSDClose001-HFI-NOD: Operator Closes Shield Door on Conveyance

Preliminary Value: 1.0

Justification: The operator can inadvertently close the shield door on the conveyance as it travels through the door. In order to accomplish this, the anti-collision interlock on the shield door must fail. To be conservative, a preliminary HEP value of 1.0 has been assigned to all unsafe actions that require an equipment failure in addition to one or more unsafe actions to cause an initiating event.

E6.0.2.3.4 HVAC System

The heating, ventilation, and air-conditioning (HVAC) system is a universal part of WHF operations, and HFEs contributing to failure of the HVAC system are thus applicable to all WHF operational groups. The following pre-initiating HFEs were identified and assigned preliminary values:

050-VCSO-DR00001-HFI-NOD: Operators Open Two or More Vestibule Doors in WHF

Preliminary Value: 1E−02

Justification: Failure to properly restore an operating system to service when the degraded state is not easily detectable.

050-VCSO-HFIA000-HFI-NOM: Human Error Exhaust Fan Switch Wrong Position

Preliminary Value: 1E−01

Justification: Failure to properly restore a standby system to service.

050-VCSO-HEPALK-HFI-NOD: Operator Fails to Notice HEPA Filter Leak in Train B

Preliminary Value: 1.0

Justification: To be conservative, credit was not given for the operator noticing HEPA (high-efficiency particulate air filter) filter leaks.

E6.0.2.3.5 Electrical System

The electrical system is a universal part of WHF operations, and HFEs contributing to failure of the electrical system are thus applicable to all WHF operational groups. The following pre- and post-initiating HFEs were identified and assigned preliminary values:

050-#EEE-LDCNTRA-BUA-ROE and 050-#EEE-LDCNTRB-BUA-ROE: Operator Fails to restore ITS Load Center (Trains A and B) Post Maintenance

CTT 26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS: Operator Fails to Restore Diesel Generator to Service

Preliminary Values and Justification: For electrical systems, the HFE assigned to operator failure to restore a system (i.e., load center or diesel generator) to service was assigned a conservative value of 0.1. The overall failure probability for load centers (050-#EEE-LDCNTRA-BUA-ROE and 050-#EEE-LDCNTRB-BUA-ROE) is 1.03E−05 and for diesel generators (26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS) is 1.95E−04. These failure probabilities reflect the probability that the load center or diesel generator require service, and are further discussed in Attachment B (Sections B8.4.1.5 and B8.4.2.5).

E6.0.2.3.6 Contamination Events

There are several possible contamination events associated with handling low-level radioactive waste (LLW) which were screened out by the WHF analysts because they are part of normal operations. Therefore, these events are not part of this HRA. Section 6.0 of the main PCSA report provides the screening justification. These events include:

050-LLW-Cleanup: Operator Exposed during LLW cleanup

050-LLW-Collision: Operator Causes Collision with LLW Container

050-LLW-Decon-Fail: Operator Improperly Performs Decontamination Procedures

050-Op-Filter-Expose: Operator Exposed During Filter Change out

050-OpExpose-Decon: Operator Exposed During Decontamination

E6.0.2.3.7 Summary of Preliminary Values for Cross-Cutting HFEs

Table E6.0-2 summarizes the preliminary values for the cross-group generic HFEs.

Table E6.0-2. Summarizing Preliminary Values for the Cross-group Generic HFEs

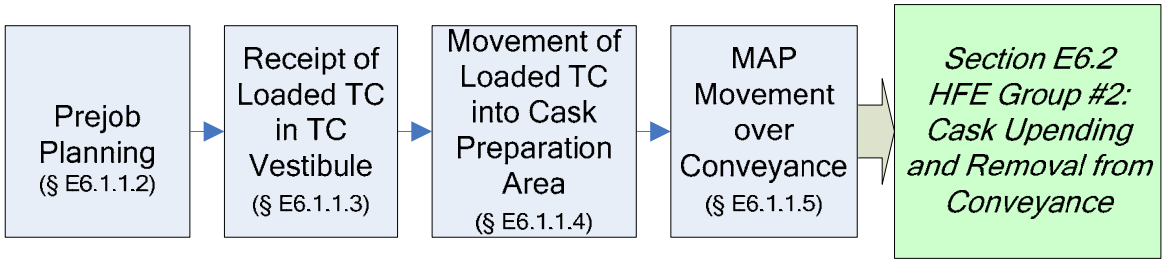
HFE ID	HFE Brief Description	Preliminary Value
Moderator	Operator Introduces Moderator Source in to Moderator-Controlled Areas of the WHF	N/A
Load too Heavy	Operator attempts to lift load which is greater than crane rating	N/A
050-OpSDClose001-HFI-NOD	Operator Closes Shield Door on Conveyance	1.0
050-VCSO-DR00001-HFI-NOD	Operators Open 2 or More Vestibule Doors in WHF	1E−02
050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1E−01
050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0
050-#EEE-LDCNTRA-BUA-ROE 050-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore Load Center Post Maintenance	1.03E−05
26D-#EEY-ITSDG-A-#DG-RSS 26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator to Service	1.95−04
050-LLW-Cleanup	Operator Exposed during LLW cleanup	N/A
050-LLW-Collision	Operator Causes Collision with LLW Container	N/A
050-LLW-Decon-Fail	Operator Improperly Performs Decontamination Procedures	N/A
050-Op-Filter-Expose	Operator Exposed During Filter Change out	N/A
050-OpExpose-Decon	Operator Exposed During Decontamination	N/A

NOTE: HEPA = high-efficiency particulate air filter; HFE = human failure event; ID = identification; LLW = low-level radioactive waste; N/A = not applicable; WHF = Wet Handling Facility.

Source: Original

E6.1 ANALYSIS OF HUMAN FAILURE EVENT GROUP #1: RECEIPT OF SPENT NUCLEAR FUEL IN THE TRANSPORTATION CASK VESTIBULE AND MOVEMENT INTO THE CASK PREPARATION AREA

HFE group #1 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering receipt of a conveyance and movement into the Cask Preparation Area. The operations covered in this HFE group are shown in Figure E6.1-1. The activities covered in HFE group #1 begin where the conveyance (i.e., railcar, truck trailer or HCTT) containing the transportation cask is just outside the door to the Transportation Cask Vestibule, just before the vestibule door is opened. It continues through the movement of the conveyance to its staging position in the Cask Preparation Area and ends when the mobile access platform (MAP) is in place around the conveyance.



NOTE: § = section; HFE = human failure event; MAP = mobile access platform; TC = transportation cask.

Source: Original

Figure E6.1-1. Activities Associated with HFE Group #1

E6.1.1 Group #1 Base Case Scenario

E6.1.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #1 activities:

1. The conveyance is located at the door of the Transportation Cask Vestibule loaded as follows:

   A. SNF in a transportation cask on a truck trailer.
   B. DPC in a VTC or TTC on a railcar.
   C. DPC in a HSTC on a HCTT.

2. The transportation cask is secured to the conveyance by tie-downs. For the truck trailer and railcar, impact limiters surround the cask and a personnel barrier is in place.

3. There are no speed governors or interlocks on the railcar or truck trailer; there are, however, wheel blocks at the end of the rail and a speed governor on the SPM.

4. Interlocks ensure that the inner Transportation Cask Vestibule door is closed if the outer door is open, and vice versa.

The following personnel are involved in this set of operations:

- Crew member (two)
- PIC
- SPM operator
- HCTT operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.1.1.2 Prejob Plan

Before the transportation cask and conveyance reach the WHF, a PIC is notified of the type of cask/conveyance to expect and how to process it. According to this information, the PIC determines the appropriate procedures and equipment to be used to handle this cask type, and communicates this information to all the crew members involved in the handling of this cask. The PIC also fills out a pre-lift safety checklist (Ref. E8.1.12) verifying that the equipment is properly staged and in proper operational condition. All crane operators are properly trained and abide by the procedures of the facility.

The prejob plan includes "campaign" information and a TAD canister loading plan as described here. Configuration and placement of the fuel assemblies (i.e., pressurized water reactor (PWR) assemblies or boiling water reactor (BWR) assemblies) into a TAD canister is predetermined by Engineering. The TAD canister loading plan includes a map of the TAD canister grid, with the serial numbers of the fuel assemblies appropriately mapped on the grid. The TAD canister fits 21 PWR assemblies or 44 BWR assemblies. All the assemblies needed to fill a TAD canister must be in the pool before the TAD canister loading begins. Truck casks hold 4 PWR assemblies or 9 BWR assemblies, so a "campaign" would include prestaging six truck casks worth of PWR fuel assemblies or 5 of BWR fuel assemblies in the staging racks before bringing the TAD canister into the pool.

DPCs can fit more than 21 PWR fuel assemblies or more than 44 BWR fuel assemblies (in comparison to a TAD canister). After filling a TAD canister with PWR or BWR fuel from a DPC, there are left over assemblies. The extra assemblies are staged in the staging rack. In this case, a "campaign" likely includes filling several TAD canisters until there are no PWR assemblies left in the pool. However, there is some likelihood that PWR and BWR fuel assemblies to be in the pool at the same time. It should be noted that the BWR assemblies are significantly shorter than the PWR assemblies (and, thus, the BWR staging rack is significantly shorter than the PWR staging rack), and therefore are not easily confused.

E6.1.1.3 Receipt of a Loaded Transportation Cask in the Transportation Cask Vestibule

Two crew members are in attendance at the Transportation Cask Vestibule to deal with the reception of loaded casks. The loaded railcar or truck trailer is pushed by a SPM (a diesel/electric vehicle with on board controls), and is driven by the SPM operator who is located in the cab of the SPM. The cask transfer trailer is pulled by the cask tractor (together they make

up a HCTT unit). When the conveyance approaches the WHF, it is visually inspected and one crew member opens the outside overhead door and the other crew member uses hand signals to direct the conveyance into the Transportation Cask Vestibule after ensuring there are no vehicles or obstructions in the path. The crew members follow all relevant restrictions and procedures regarding conveyance speed and direction of travel. Once the railcar or truck trailer has cleared the door, the first crew member closes the outside door.

E6.1.1.4 Movement of Loaded Cask into Cask Preparation Area

Once the conveyance is in the Transportation Cask Vestibule, the inside overhead door is opened and the conveyance proceeds to the Cask Preparation Area and stops. A crew member sets the conveyance brakes and chocks the wheels. The cask tractor engine is turned off at this time. For a railcar or truck trailer, the SPM detaches from the railcar/truck trailer and proceeds back to the Transportation Cask Entrance Vestibule. The inside overhead door is closed by a crew member. A checklist is signed to indicate that the inside door has been closed and the brakes set.

The inner and outer doors have an interlock that normally prevents both doors from being opened simultaneously; however, this interlock can be bypassed.

E6.1.1.5 Move Mobile Access Platform over Conveyance

A crew member raises the MAP and moves it over the conveyance, positioning it for conveyance unloading activities.

E6.1.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during receipt of the railcar, truck trailer or HCTT are summarized in Table E6.1-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.1-1. HFE Group #1 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpRCCollide1-HFI-NOD	*Operator Causes Low-speed Collision between a RC, TT, or HCTT and facility SSCs*: Operator causes collision of a RC, TT or HCTT with a facility structure or piece of equipment while moving through the Transportation Cask Vestibule to the Cask Preparation Area or, operator of an auxiliary vehicle causes a collision with the conveyance while the conveyance is parked in the Cask Preparation Area.	2	3E−3	In this step, the railcar, truck trailer or HCTT moves into the Cask Preparation Area. The railcar, truck trailer and HCTT have very similar failure modes and conditions for this step and therefore have the same preliminary values. There are three observers with clear visibility, the operation is simple, the travel distance is short, the conveyance (railcar, truck trailer or HCTT) speed is low, and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a railcar, truck trailer, or HCTT are limited, and include: • Improper motion (i.e., backward or lateral motion beyond the limit) could result in collision with the end stops, wall, or vestibule doors. • An improperly attached railcar/truck trailer could continue moving when the SPM stops, resulting in collision with the end stops, wall, or vestibule doors. • An improperly attached cask transfer trailer could continue moving when the cask tractor stops, resulting in collision with the end stops, wall, or vestibule doors. • A forklift or other auxiliary vehicle could collide into the conveyance. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted because there are several ways for a collision to occur, and there are potentially multiple other vehicles (forklifts) that can collide into the conveyance (×3). Also, in general, collisions were considered relatively more likely than drop events. The dominant contributor to this failure was determined to be collision of forklift into the conveyance.
050-OpTTCollide1-HFI-NOD		1		
050-OpHTCollide1-HFI-NOD		4		
050-OpRCIntCol01-HFI-NOD	*Operator Causes High-speed Collision between a RC, TT or HCTT and facility SSCs*: Operator causes a collision of the RC, TT or HCTT at a speed higher than design requirements. If the speed governor of the SPM or cask tractor fails, the operator could collide the RC, TT, or HCTT into an SSC.	2	1.0	The SPM or cask tractor can overspeed, resulting in a collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
050- OpTTIntCol01-HFI-NOD		1		
050- OpHTIntCol01-HFI-NOD		4		
050-OpRCIntCol02-HFI-NOD	*Operator Causes the Mobile Access Platform to Collide into a RC, TT or HCTT*: When a RC, TT or HCTT is parked in the Cask Preparation Area, the operator normally moves the MAP over the conveyance. In this HFE, the operator fails to sufficiently raise the MAP and runs into the conveyance. The MAP has an anti-collision interlock that prevents movement of the platform if there is an obstruction in its path.	2	1.0	The operator can cause the MAP to collide into the railcar/truck trailer/HCTT while moving it into position over the conveyance. In order to accomplish this, the MAP must be lowered, and the platform’s anti-collision interlock must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
050-OpTTIntCol02-HFI-NOD		1		
050-OpTTRollover-HFI-NOD	*Operator Causes a TT or HCTT to Rollover as the Conveyance Moves into the Cask Preparation Area*: The operator drives over a significantly uneven surface or jackknifes while moving the TT or HCTT into the Cask Preparation Area, causing the TT or HCTT to rollover.	1, 4	N/A	For a truck trailer or HCTT to rollover, the center of mass has to shift laterally. This can be done by traversing a significantly uneven surface or running over a very large object. There are no significantly uneven surfaces in the WHF Transportation Cask Vestibule/Cask Preparation Area; it is incredible for the operator to run over an object large enough necessary to shift the truck’s center of mass significantly. The other mode of failure considered here is jackknifing the truck. This failure mode was also seen as incredible because there is not enough room in the Transportation Cask Vestibule/Cask Preparation Area to physically cause the truck to jackknife. The truck moves slowly and there are three observers, and if the truck and trailer were significantly out of alignment, the trailer might impact the building, but it would not jackknife and roll over. Therefore, this HFE was omitted from analysis.
RC Derailment	*Operator Causes RC to Derail as the RC travels into the Cask Preparation Area*.	1	N/A[a]	In this step, the railcar moves from outside the facility, through the Transportation Cask Vestibule and into the Cask Preparation Area. During this travel, there is a probability that the railcar can derail, leading to a tipover of the railcar. This HFE was not explicitly quantified because the probability of derailment due to human failure is incorporated in the historical data used to provide a general failure probability for derailment. Documentation for this failure can be found in Attachment C.
050-OpSDClose001-HFI-NOD	*Operator Closes Shield Door on Conveyance*: The RC, TT, and HCTT passes through shield doors as it enters the Preparation Area. During this transfer, the operator can close the shield door on the RC, TT, or HCTT.	12	1.0	The railcar, truck trailer and HCTT pass through shield doors as they enter the Cask Preparation Area. During this transfer, the operator can cause the railcar, truck trailer or HCTT to collide into the shield door or a crew member can cause the shield door to close on the railcar, truck trailer, or HCTT. Section E6.0.2.3.3 (Operator Causes Collision between Shield Door and Waste Conveyance) provides a justification of this preliminary value.

NOTE: [a] HRA preliminary value replaced by use of historic data.
ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; HCTT = cask tractor and cask transfer trailer; MAP = mobile access platform; N/A = not applicable; RC = railcar; SPM = site prime mover; SPM = site prime mover; SSC = structure, system, or component; SSCs = structures, systems, and components; TT = truck trailer.

Source: Original

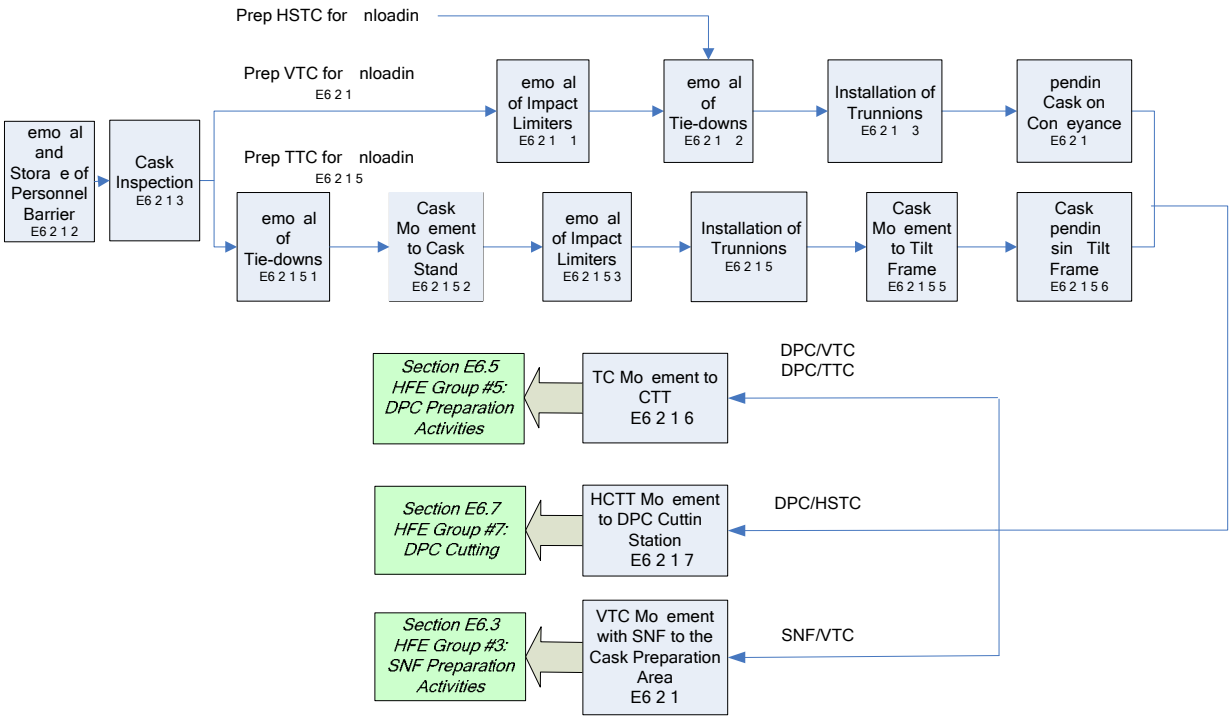
E6.1.3 Detailed Analysis

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E6.2 ANALYSIS OF HUMAN FAILURE EVENT GROUP #2: CASK UPENDING AND REMOVAL FROM CONVEYANCE

HFE group #2 corresponds to the operations and initiating events associated with the ESD and HAZOP nodes listed in Table E6-0.1, covering upending and transfer of the cask to the CTT. This process is shown in Figure E6.2-1. This operation starts with the conveyance (i.e., the railcar or truck trailer) and the MAP in place in the Cask Preparation Area. The transportation cask is removed from the conveyance and secured on the CTT, ready for preparation activities. This activity ends prior to the lowering of the cask preparation platform and movement of the shield plate over the cask. There are four variations of this step:

1. HSTCs are upended on the HCTT and moved to the DPC cutting station.
2. SNF in a VTC is upended on the railcar or truck trailer and moved to the SNF preparation station.
3. DPCs in a VTC are upended on the railcar and moved to the CTT.
4. TTCs are moved to a cask stand. The TTC and cask stand are moved to a tilting frame where the TTC is upended. The TTC is then moved to the CTT.



NOTE: § = section; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure event; HSTC = horizontal shielded transfer cask; SNF = spent nuclear fuel; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar.

Source: Original

Figure E6.2-1. Activities Associated with HFE Group #2

E6.2.1 Group #2 Base Case Scenario

E6.2.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #2 activities:

1. The railcar, truck trailer, or HCTT is parked in the Cask Preparation Area with its brakes set and the transportation cask secure in the conveyance.
2. For DOE (short) casks, a cask pedestal is pre-staged in the CTT.
3. The MAP has an anti-collision interlock.
4. The cask handling crane (200-ton crane with 20-ton auxiliary hook) has the following safety features:

    A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.

    B. There are end-of-travel interlocks on the trolley and bridge.

    C. There are speed limiters built into the motors.

    D. There is a weight interlock that cuts off power to the crane when the crane capacity is exceeded.

    E. There is a temperature interlock that cuts off power to the hoist when the temperature is too high; an indicator comes on before this temperature is reached.

    F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

Crane operations in this activity are not part of a specific procedure outlined in the YMP documentation, but rather reflect critical lift crane operations that are standard in the nuclear industry.

The following equipment is available for upending and transferring the cask:

1. Crane:

    A. 200-ton cask handling crane
    B. 20-ton auxiliary crane.

2. Lift fixtures:

    a. Impact limiter lifting device (uneven slings)
    b. Personnel barrier lifting device (sling)

C. Cask sling (for TTCs)
D. Yoke (adjustable, for all casks).

3. Common tools and platform.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Radiation protection worker[9]
- Supervisor.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.2.1.2 Removal and Storage of Personnel Barrier (if required)

Most personnel barriers are removed at the geologic repository operations entrance; however, this facility retains the capacity to remove personnel barriers if necessary. HSTCs do not have a personnel barrier. In order to remove the personnel barrier from the transportation cask, the crew members must first unbolt the barrier from the cask. The crane operator retrieves the crane and removes the personnel barriers as follows:

Alignment of Crane to Personnel Barrier—The crane operator lowers the 20-ton auxiliary crane into position over the personnel barrier. The operator is positioned on the floor in view of the crew members on either side of the personnel barrier. A signaling crew member next to the personnel barrier uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). A verification crew member on the opposite side of the personnel barrier checks the alignment of the crane. The verification crew member can only signal to stop the crane. Once positioned, a crew member connects the crane to the personnel barrier using the personnel barrier lifting device, which is expected to be a sling. In order to use a sling, a crew member must secure the sling around the personnel barrier, attach the sling to the crane, and ensure that, when lifted, the load is level. If the sling is not positioned and the load is not level, the signaling crew member signals the crane operator to stop and lower the personnel barrier so that the sling can be repositioned.

Vertical Lifting of the Personnel Barrier—Upon signal from the signaling crew member that all is well, the crane operator begins to raise the personnel barrier. Once the personnel barrier has been raised (i.e., is hanging free) to the proper height (based on visual inspection), the crane operator stops raising the personnel barrier. The crane operator clears the railcar, truck trailer, or HCTT and then lowers the personnel barrier to the movement height. This action is confirmed by hand signals from the signaling crew member. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

[9]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

Movement of Personnel Barrier to Staging Location—The crane operator moves the 20-ton auxiliary crane to locate the personnel barrier over the position where it is lowered in the staging area, following the indicated safe load path marked on the floor. The crane operator performs this task visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lowering of Personnel Barrier and Disengagement of the Sling—When properly positioned in the staging area and the placement area is clear, the signaling crew member signals the crane operator to lower the personnel barrier. The crane operator then proceeds to lower the personnel barrier at or below the maximum allowable speed. Once the personnel barrier is stable on the floor of staging area, a crew member disengages the sling and the crane operator lifts the crane in preparation for the next operation.

E6.2.1.3 Cask Inspection

Once the conveyance is parked in the facility and the personnel barriers have been removed, the crew visually inspects and conducts radiological surveys of the exterior of the cask.

E6.2.1.4 Preparation of VTC and HSTC for Unloading

As illustrated in Figure E6.2-1, the upending processes for the three cask types are very similar, but not identical. At this point the processes for preparing the three types of casks for upending diverge. The VTC and HSTC are discussed first, followed by a similar discussion for the TTC in Section E6.2.1.5.

E6.2.1.4.1 Removal and Storage of Impact Limiters (VTC only)

This section describes the removal and staging of impact limiters using the 20-ton auxiliary crane with standard rigging, common tools, and the MAP. This step is performed twice, as each cask has two impact limiters.

Crew members, working with the crane operator, attach the impact limiter lifting device (uneven slings) to the 20-ton auxiliary crane.

After the personnel barrier is removed and the cask is inspected, the crew removes and stores the impact limiters. HSTCs do not have impact limiters, so this step is only applicable to VTCs. This operation is performed on the conveyance with training and procedures. The first step is to remove the restraining bolts on the impact limiters. Depending on the cask type, there can be anywhere from 24 to 36 bolts to remove, with several crew members removing the bolts simultaneously. Once removed, the bolts are counted, and the crew supervisor uses a checklist to verify and document bolt removal. Once bolt removal is verified, the crane operator removes and stores the impact limiters using the 20-ton auxiliary crane as follows:

Movement of Crane to Impact Limiter Position—The crane operator positions the crane over the impact limiter, following the indicated safe load path marked on the floor. The crane operator performs this task visually and also receives confirmatory hand signals from the

signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Alignment of Crane to Impact Limiter—The crane operator lowers the crane into position over the impact limiter. The crane operator is positioned on the floor in view of the crew members on either side of the impact limiter. A signaling crew member, next to the impact limiter, uses hand signals to guide the movement of the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the impact limiter, checking alignment of the crane. The verification crew member can only signal the crane operator to stop. Once positioned, a crew member connects the crane to the impact limiter using the uneven sling and integral lift points.

Vertical Lifting of the Impact Limiter—Upon signal from the signaling crew member, the crane operator ensures the impact limiter is free of the transportation cask (this may include moving the impact limiters horizontally to free them) and then begins to raise the impact limiter. Once the impact limiter has been raised (i.e., is hanging free) such that it has cleared the conveyance, the crane operator stops raising the impact limiters. The crane operator bases this on a visual inspection and is confirmed by hand signals from the signaling crew member. Once past the conveyance, the crane operator lowers the impact limiter to the proper height for movement. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. The crane operator bases this height estimation on a visual inspection, confirmed by hand signals from the signaling crew member.

Movement of Impact Limiter to Staging Area—The crane operator moves the crane so as to locate the impact limiter over the position where it should be lowered in the staging area, following the indicated safe load path marked on the floor. The crane operator performs this task visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lowering of Impact Limiter and Disengagement of the Sling—When properly positioned and the placement area is clear, the signaling crew member signals the crane operator to lower the impact limiter to the ground or staging rack. The crane operator then proceeds to lower the impact limiter at or below the maximum allowable speed. Once the impact limiter is lowered, a crew member disengages the sling, and the crane operator lifts the crane to the maximum height in preparation for the next operation

E6.2.1.4.2 Removal of Tie -downs

Tie-downs that secure the transportation cask to the conveyance are removed using the MAP for access. Once the impact limiters are removed, the crew removes the cask tie-downs in preparation to lift the transportation cask off the conveyance. This operation is done on the conveyance according to written procedures. The crew removes all the bolts of the tie-down, with four crew members removing the bolts simultaneously. Once removed, the bolts are counted, and the crew supervisor checks off bolt removal. Once bolt removal is verified, the crane operator (using a 200-ton crane with yoke) can proceed to lift the cask if there are trunnions on the cask; if not, then the crew must install trunnions on the cask.

E6.2.1.4.3 Installation of Trunnions (if required)

Trunnions are installed onto the cask by using common tools, standard rigging, cask handling crane (auxiliary hook), and the MAP.

Crew members retrieve the trunnions to be installed. Trunnions are located in a package on the conveyance. If required, the 20-ton auxiliary crane is used to place the trunnions in the proper position. Crew members secure the trunnions according to training.

E6.2.1.4.4 Upending Transportation Cask on the Conveyance

The transportation is upended cask using the 200-ton cask handling crane with yoke.

Prior to attempting to upend the transportation cask on the conveyance, the crew members must properly attach the yoke to the 200-ton cask handling crane. Once that is done, the crew can proceed to initiate upending of the cask.

Movement of Crane to Transportation Cask—The operator positions the crane over the transportation cask. The crane movement follows the indicated safe load path marked on the floor. The operator performs a visual check, and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Alignment of Crane to Cask—The crane operator lowers the yoke into position so that the yoke arms are lined up with the trunnion. The crane operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask using hand signals to guide the operator's movement (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask, checking alignment of the second trunnion. This worker can only signal the crane operator to stop.

Yoke Arms Engaged on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. The crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). If the arms are sufficiently engaged on both sides, the crane operator knows by an indicator on the controller, and the signaling crew member signals the operator to raise the yoke a slight amount to put pressure on the arms. The crane operator sees on the controller that the crane is bearing weight. Both crew members verify that the yoke remains level. If the arms do not engage on the initial attempt, either crew member signals to the operator to stop, and the crane operator sets the cask down and opens the yoke arms to disengage. The signaling crew member then directs movement of the crane (again with hand signals) to compensate and then signals the operator to close the yoke arms.

Vertical Positioning of Cask—Upon receiving a signal from the signaling crew member, the crane operator begins to raise the cask. Since the bottom of the cask remains stationary because of the cask restraints, the operator moves the crane to remain directly above the upper trunnions (i.e., to keep the cables straight). The operator performs this task visually. The operator also gets hand signals from the signaling crew member to ensure that the cask is "upending" properly.

Once the cask is fully upright, the crane operator stops raising the cask. The crane operator bases this on a visual inspection, confirmed by hand signals from the signaling crew member.

Cask Unbolting from Pivot Point—Without detaching the crane from the cask, the crew uses common tools and the MAP to unbolt the constraints on the bottom half of the cask so the cask can be lifted. This step is verified.

This ends the discussion of upending a VTC or HSTC. Section E6.2.1.5 discusses the process of upending a TTC, which includes an intermediate transfer to a cask preparation stand. Once the VTC is upright, it is then moved to the CTT (Section E6.2.1.6); once the HSTC is upright, it is then moved to the DPC cutting station (Section E6.2.1.7).

E6.2.1.5 Preparation of a TTC for Transfer to the CTT

As illustrated in Figure E6.2-1, the upending process for a VTC/HSTC and TTC are very similar, but not identical. The upending process for a TTC requires that the cask be removed from the conveyance and upended using a tilting frame with an intermediate transfer to a cask stand. This process is described in this section.

E6.2.1.5.1 Removal of Tie-downs

Crew members remove transportation cask tie-downs using common tools and handling equipment and the MAP. This step is identical to Section E6.2.1.4.2.

Once the impact limiters are removed, the crew removes the cask tie-downs in preparation to lift the transportation cask off the conveyance. Crew members remove transportation cask tie-downs using common tools and handling equipment and the MAP. This step is identical to Section E6.2.1.4.2. This operation is done on the conveyance. The crew is trained to execute this task. The crew removes all the bolts of the tie-down, with several crew members removing the bolts simultaneously. Once removed, the bolts are counted, and the crew supervisor checks off bolt removal. Once bolt removal is verified, the crane operator (using the 200-ton cask handling crane with cask sling) proceeds to lift the cask.

E6.2.1.5.2 Movement of Transportation Cask with Impact Limiters to Cask Stand

In this step the crane operator moves the transportation cask with impact limiters attached to the cask stand using the 200-ton cask handling crane with standard rigging. Prior to this step the cask stand is pre-staged in the appropriate place, the slings used to move the personnel barrier are removed from the crane, and the cask sling is attached to the crane.

Crane Movement to Transportation Cask—The crane operator moves the 200-ton cask handling crane so as to locate the crane over the transportation cask, following the indicated safe load path marked on the floor. The operator does this visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Crane Alignment to Cask and Engagement of Sling—The crane operator lowers the crane into position so that the crew members can place the sling (which is connected to an I-beam)

around the cask. Once in position, the crew members place the sling around the cask. The supervisor verifies, via checklist, that the sling is properly attached. The crane operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask who uses hand signals to guide the operator's movement (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask, checking the placement of the sling. The verification crew member can only signal the crane operator to stop. Once the sling is secured around the cask, the crane operator initiates the lift, and the crew members ensure that, when lifted, the load is level. If the sling is not positioned properly and the load is not level, either crew member signals the crane operator to stop and lower the cask so that the sling can be repositioned.

Vertical Lifting of Cask—The signaling crew member signals the crane operator to lift the cask. The crane operator lifts the cask vertically until it clears the conveyance. The crane operator bases this on a visual inspection, confirmed by hand signals from the signaling crew member. Once the transportation cask is past the conveyance, the crane operator lowers the cask to the proper height for movement. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path. The crane operator determines the proper height based on visual inspection, confirmed by hand signals from the signaling crew member.

Cask Positioning over the Cask Stand—The operator moves the 200-ton cask handling crane so as to locate the cask over the cask stand, following the indicated safe load path marked on the floor. The operator determines the path visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member. Once aligned, the signaling crew member signals the crane operator to lower the cask. The crane operator lowers the cask, and then the crew members, ensuring stable placement, detach the slings from the crane. The crane operator then lifts the crane to the appropriate height for movement, confirmed by the signaling crew member. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path. The crane operator, guided by the signaling crew member, moves the crane to the cask sling stand, where the crew member removes the cask sling.

E6.2.1.5.3 Removal of Impact Limiters from Cask while on Cask Stand

The removal of impact limiters is identical to the operations discussed in Section E6.2.1.4.1, other than that the impact limiter removal occurs while the cask is on the cask pedestal.

Impact limiters are removed using the 20-ton auxiliary crane with standard rigging, common tools, and the cask access platform. This step is performed twice because each cask has two impact limiters.

In preparation for this step, the crew members and crane operator attach the impact limiter lifting device (uneven slings) to the 20-ton auxiliary crane.

Once the cask is positioned on the cask stand, the crew removes and stores the impact limiters. This operation is done on the cask stand according to training. The first step is to remove the restraining bolts on the impact limiters. Depending on the cask type, there can be anywhere from 24 to 36 bolts to remove, with several crew members removing the bolts simultaneously. Once

removed, the bolts are counted, and the crew supervisor checks off bolt removal from the checklist. Once bolt removal is verified, the crane operator (using a 20-ton crane with auxiliary hook) removes and stores the impact limiters.

Positioning Crane over Impact Limiter—The crane operator positions the crane over the impact limiter, following the indicated safe load path marked on the floor. The crane operator performs this task visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Crane Alignment with Impact Limiter—The crane operator lowers the crane into position over the impact limiter. The crane operator is positioned on the floor in view of the crew members on either side of the impact limiter. There is a signaling crew member next to the impact limiter who uses hand signals to guide the crane operator's movements (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the impact limiter, checking alignment of the crane. The verification crew member can only signal the crane operator to stop. Once positioned, one of the crew members connects the crane to the impact limiter using the uneven sling and integral lift points.

Vertical Lifting of Impact Limiter—Upon signal from the signaling crew member, the crane operator ensures that the impact limiter is free of the transportation cask (this may include moving the impact limiters horizontally to free them) and then begins to raise the impact limiter. Once the impact limiter has been raised (i.e., is hanging free) such that it has cleared the cask stand, the crane operator stops raising the impact limiters. The crane operator bases this on a visual inspection, and this is confirmed by hand signals from the signaling crew member. Once past the cask stand, the crane operator lowers the crane to the proper height for movement. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. The crane operator determines the proper height based on a visual inspection, confirmed by hand signals from the signaling crew member.

Impact Limiter Positioning for Lowering—The crane operator moves the crane to locate the impact limiter over the position where it should be lowered in the staging area, following the indicated safe load path marked on the floor. The crew member does this visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Impact Limiter Lowering and Disengagement—When properly positioned and the placement area is clear, the signaling crew member signals the crane operator to lower the impact limiter. The crane operator lowers the impact limiter at or below the maximum allowable speed. Once the impact limiter is lowered, a crew member disengages the sling, and the crane is lifted to the maximum height in preparation for the next operation.

E6.2.1.5.4 Installation of Trunnions (if required)

Trunnions are installed onto the cask by using common tools, standard rigging, the cask handling crane (auxiliary hook), and the MAP. This step is identical to Section E6.2.1.4.3.

Crew members retrieve the trunnions to be installed. Trunnions are located in a package on the conveyance. If required, the 20-ton auxiliary crane is used to place the trunnions in the proper position. Crew members secure the trunnions according to training.

E6.2.1.5.5 Transportation Cask Movement to Cask Tilting Frame

In preparation for this step, the cask tilting frame is pre-staged in the preparation area. It is possible the cask stand is an integral component with the tilting frame, however, for this analysis they are considered separate entities, and the extra sling lift is required.

Transportation Cask Movement and Placement onto Tilting Frame—Once the tilting frame is in place and the impact limiters removed, the crane operator and crew members retrieve and attach the cask sling to the 200-ton cask handling crane.

Crane Alignment to Cask—The crane operator lowers the 200-ton cask handling crane into position so that the slings can be attached to the crane. The crane operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask who uses hand signals to guide the operator's movements (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask, checking alignment of the second trunnion. The crew member signals the crane operator to stop. Once in position, the other crew members attach the sling to the crane and ensure that, when lifted, the load is level. If the sling is not positioned and the load is not level, the signaling crew member signals the crane operator to stop and lower the object so that the sling can be repositioned.

Vertical Lifting of the Cask—Upon signal from the signaling crew member, the crane operator begins to raise the cask. Once the cask is raised to roughly 6 in. above the cask stand, the crane operator stops raising the cask, based on a visual inspection and confirmation by hand signals from the signaling crew member. The crane operator clears the cask stand and lowers the crane to the proper height for movement. The crane operator bases this on a visual inspection and a confirmatory hand signals from the signaling crew member. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path.

Cask Positioning for Lowering—The crane operator moves the crane to position the cask over the tilting frame, following the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Cask Lowering and Disengagement of Sling—When properly positioned and the placement area is clear, the signaling crew member signals the crane operator to lower the cask onto the tilting frame. The crane operator proceeds to lower the cask at or below the maximum allowable speed. Once the cask is lowered and stable, a crew member disengages the sling, and the crane operator lifts the crane in preparation for the next operation.

Once the cask is on the tilting frame, the crew secures the transportation cask to the tilting frame using common tools and the cask handling platform. This step is guided by a procedure and is verified by a supervisor signature on a checklist before the cask is upended.

E6.2.1.5.6 Upending Transportation Cask Using Cask Tilting Frame

The transportation cask is upended using the tilting frame and 200-ton cask handling crane with yoke.

Once the cask is placed on the tilting frame, the crane operator and crew members place the cask sling on its stand and retrieve and attach the yoke. Once that is done, the crew proceeds to initiate the upending.

Crane Positioning over the Transportation Cask—The operator positions the crane over the transportation cask, following the indicated safe load path marked on the floor. The crane operator performs this task visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Crane Alignment with Cask—The crane operator lowers the crane into position so that the yoke arms are lined up with the trunnions. The crane operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask using hand signals to guide the operator's movement (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask, checking alignment of the second trunnion. The verification crew member can only signal the crane operator to stop.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. Crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). The crane operator knows if the arms are sufficiently engaged on both sides by an indicator on the controller, and the signaling crew member signals the operator to raise the crane a slight amount to put pressure on the arms. The crane operator can see on the controller that the crane is bearing weight. Crew members verify that the yoke remains level. If the arms do not engage on the initial attempt, either crew member signals the operator to stop, and the crane operator sets the cask down and opens the yoke arms to disengage. The signaling crew member then directs movement of the crane (again with hand signals) to compensate, and then signals the operator to close the yoke arms.

Vertical Positioning of Cask—Upon signal from the signaling crew member, the crane operator begins to raise the cask. Since the bottom of the cask remains stationary, the operator moves the crane to remain directly above the upper trunnions (i.e., to keep the cables straight). The crane operator visually performs this task and gets hand signals from the signaling crew member that the cask is "upending" properly. Once the cask is fully upended, the crane operator stops raising the cask, basing this on a visual inspection, confirmed by hand signals from the signaling crew member.

Cask Unbolting from Pivot Point—Without detaching the crane from the cask, the crew uses common tools and the MAP to remove the constraints from the tilting frame so the cask can be lifted. This step is verified.

This ends the discussion of preparing a TTC for transfer to the CTT (Section E6.2.1.6).

E6.2.1.6 Transportation Cask Movement to CTT (DPCs in VTCs and TTCs only)

Vertical Lifting of Cask—Once the cask is upended and unconstrained, the signaling crew member signals the crane operator to lift the cask vertically. The crane operator lifts the cask vertically until it reaches the proper height for movement, basing this on a visual inspection, confirmed by hand signals from the signaling crew member. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path. This requires the crane operator to clear the cask from the conveyance/tilting frame before lowering the cask to movement height.

Cask Positioning over CTT—The crane operator moves the crane to position the cask over the CTT, following the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member since the operator's view of the alignment "ring" on the CTT is obstructed. Once properly positioned, the signaling crew member signals the crane operator to lower the cask onto the CTT. The crane operator lowers the cask and, with the confirmation of the signaling crew member, disengages the yoke and lifts the crane to proper moving height.

Securing the Transportation Cask to the CTT—Once the cask is properly loaded, the crew member(s) secures the transportation cask to the CTT, which is like a cage that locks into position. There may be bumpers installed prior to closing the CTT door. This step is defined in training and must be signed off via a checklist prior to movement of the CTT.

E6.2.1.7 Movement of the HSTC to the DPC Cutting Station

This step is a continuation of Section E6.2.1.4 (upending the HSTC).

Once the HSTC is upended, without detaching the cask handling crane from the cask, the crane operator lifts the cask over the HCTT and aligns the cask at the DPC cutting station, following the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. A crew member opens the DPC cutting platform doors for the crane operator. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member since the operator's view of the platform alignment may be obstructed. Once properly positioned, the signaling crew member signals the crane operator to lower the cask. The crane operator lowers the cask and, with the confirmation of the signaling crew member, disengages the yoke and lifts the crane to proper moving height.

E6.2.1.8 Movement of the VTC with SNF to the Cask Preparation Station

This step is a continuation of Section E6.2.1.4 (upending the VTC).

Once the VTC is upended, without detaching the cask handling crane with cask handling yoke from the cask, the crane operator moves the cask to preparation station #1, #2 or #3.

Movement of the VTC to the Cask Preparation Area – The operator raises the cask to clear the railcar or truck trailer and then lowers the cask to the proper height for movement. The

proper height for movement is roughly 6 in. above the highest obstacle in the movement path. The crane operator confirms the height visually and gets confirmation from the signaling crew member, before beginning movement to the Cask Preparation Area. The crane operator follows the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member that is on the opposite side of the cask of the signaling crew member. The verification crew member can only give the crane operator a signal to stop. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member since the operator's view of the alignment in the pit is obstructed. Once properly positioned, the crew member signals the crane operator to lower the cask. Because truck casks are smaller than other casks, the cask is placed into a transportation cask handling frame and the crew secures the cask to the frame by closing the frame door and ensuring it is locked into position.

E6.2.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during cask upending and removal are summarized in Table E6.2-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III; Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.2-1. HFE Group #2 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
Crane Drops	*Operator Drops Cask during Upending and Removal*: To upend a cask and move it into the CTT, the operator must lift the cask using the cask handling crane. TTCs must be lifted three times: once to the cask stand using a sling, once to the tilting frame using a sling, and once to upend the cask and move it to the CTT using the yoke. VTCs and TTCs only require one lift using the cask handling yoke to upend the cask and move it to the CTT or cutting platform. During these lifts, the operator can cause the cask to drop by improperly engaging the sling or yoke, two-blocking the cask, or other such failures.	5, 6	N/A [a]	In this step the operator uses the cask handling crane and auxiliary hook to move the cask and other heavy objects. All casks have one cask lift using the cask handling crane with cask handling yoke. TTCs have two additional cask lifts using the cask handling crane with sling. There are three heavy-object lifts (a personnel barrier and two impact limiters) using the auxiliary hook and slings. Each of these lifts can potentially result in a drop. These HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane/rigging types. Documentation for this failure can be found in Attachment C.
	Operator Drops Object on Cask during Upending and Removal: To upend a cask and move it into the CTT, the operator must lift several heavy objects over the cask using the cask handling crane auxiliary hook and standard rigging. These objects include the personnel barrier and the impact limiters (2). During these lifts, the operator can drop the object onto the cask by improperly connecting the object to the crane, two-blocking the object, or other such failures.	5, 6	N/A [a]	
050-OpTCImpact01-HFI-NOD	*Operator Causes an Impact Between Cask and SSC during Upending and Removal*: While performing crane operations, the operator can impact the cask in the following ways: 1. Impact to the cask while moving an object with the crane. 2. Impact to the cask with the crane hook. 3. Collide the cask into an SSC while moving the cask with the crane. 4. MAP lowers into the cask. 5. Bridge or trolley impacts end stop.	5, 6	3E−03	In this step the cask is moved from the conveyance ultimately to the CTT, DPC cutting station or SNF preparation station. For crane operations in this step there are three observers with clear visibility. The operations are simple, the travel distances are short, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. There are no interlocks to prevent this error. The dominant contributors to the impact of a cask include: • Crane is moved outside its safe load path (i.e., operators cut corners). • Crane is moved in the wrong direction. • Failure to maintain proper vertical and horizontal distance between cask and SSCs during crane operations. • MAP lowers into cask. • Bridge or trolley impacts end stop. The operator must manually maintain movement within the safe load path. It is not unlikely for the operator to stray slightly from that path, or that an object may be slightly within that path. However, these crane operations are very slow and within clear direct view of three observers. For the whole operation, the likelihood of impacting a cask was assessed to be comparable to the railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) and was accordingly assigned the same preliminary value with the same rationale. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted because there are several ways for an impact to occur (×3).
050-OpSpurMove01-HFI-NOD	*Operator Causes Spurious Movement of the CTT while Cask is Loaded into the CTT*: The CTT is supposed to be deflated, with the control pendant stored during this operation. However, if the CTT is not in the proper configuration for loading, the operator can inadvertently cause the CTT to move. If this spurious movement occurs while the cask is being lowered into the CTT, the result is an impact to the cask.	6	1E−04	In this step the CTT is sitting in the Cask Preparation Area ready to be loaded with a cask. The CTT is deflated, with the control pendant stored. For operations in this step there are three observers with clear visibility, the operations are simple, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. This error was considered to be extremely unlikely (0.0001) because it requires multiple human errors. It would require the CTT to be left inflated, the observers (the crane operator, two crew members, or the radiation protection worker) would have to fail to notice or fail to stop operations and deflate the CTT, and an operator would have to access the pendent and signal the CTT to move. This failure mode is only applicable to DPCs in a VTC or TTC.

Table E6.2-1. HFE Group #2 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpTipover001-HFI-NOD	*Operator Causes Cask to Tip Over*: If the crane rigging is attached to the cask, RC, TT, HCTT or CTT (either accidentally or purposefully) and the crane or conveyance moves, the cask/conveyance can potentially be tipped over. The following are contributors to this HFE: 1. Crane hook, grapple or rigging catches conveyance/cask. 2. Horizontal movement with the hook lowered and attached to the cask. 3. Crane travels in the wrong direction. 4. Cask not lifted high enough to clear the conveyance.	5, 6	1E−04	In this step there are several crane operations using both the cask handling crane and the auxiliary crane. For crane operations there are three observers with clear visibility, the operations are simple, the travel distances are short, the time the cask is vertical is small, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. There are no interlocks to prevent this error. The contributors to cask tipover include: • Crane hook, grapple, or rigging catches conveyance/cask. • Horizontal movement with hook lowered and attached to cask. • Crane travels in wrong direction. • Cask not lifted high enough to clear conveyance. The dominant contributor is the crane hook catching the cask. While it may be unlikely (0.01) that a stray hook or grapple might be hanging from the crane, it would still need to catch on the cask securely enough to pull it over (infrequently, 0.1) and then the cask tipping would have to go unnoticed by all three observers. This is done in an open area with direct observation, and tipover is a slow process; therefore the value was adjusted by a further 0.1.
050-OpCollide001-HFI-NOD	*Operator Causes Low-speed Collision with RC, TT, HCTT, CTT or TTC*: Operator can cause an auxiliary vehicle to collide into a loaded RC, TT, HCTT or CTT while the conveyance is parked in the Cask Preparation Area. The operator can also cause the auxiliary vehicle to collide directly into a TTC while it is on the cask stand or in the tilting frame. If the speed governor of the auxiliary vehicle is properly functioning, then it is a low-speed collision.	5, 6	3E−03	In this step the cask is in several positions that are vulnerable to impact via collision: • A railcar, truck trailer, or HCTT is parked in the Cask Preparation Area, loaded with a cask. • CTT is parked in the Preparation Area, loaded with a cask. • TTC is on the cask stand or tilting frame on the floor of the Cask Preparation Area. Throughout this scenario there are three observers with clear visibility, the speed of auxiliary vehicles is low, the conveyance or cask is stationary, and the conveyance or cask is very visible. Procedural controls are expected to limit the number of other vehicles in the Cask Preparation Area during cask operations. The railcar, truck trailer, and HCTT have their brakes set, and the CTT is deflated so that they cannot move to collide into something; however, if the operators failed to set the brakes of the railcar/truck trailer/HCTT or failed to deflate the CTT, it is unlikely these conveyances, while loaded with a cask, would move significantly. As a result, the most likely possibility for a collision involving a cask is limited to collisions with forklifts or other auxiliary vehicles. This HEP was assigned the same preliminary probability as railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) because the dominant mechanism of both failures is collision with an auxiliary vehicle. In this case, the preliminary value is conservative because the railcar collision HFE has additional failure modes associated with movement of the SPM which are not applicable here.
050-OpFLCollide1-HFI-NOD	*Operator Causes High-speed Collision of Loaded Conveyance or Cask with Auxiliary Vehicle*: Operator can cause an auxiliary vehicle to collide into a loaded RC, TT, HCTT or CTT while the conveyance is parked in the Cask Preparation Area. The operator can also cause the auxiliary vehicle to collide directly into a TTC while it is on the cask stand or in the tilting frame. If the collision is due to the auxiliary vehicle speed governor malfunctioning, then it is a high-speed collision.	5, 6	1.0	An auxiliary vehicle (i.e., forklift) over speeds, resulting in a collision with the railcar, truck trailer, HCTT, CTT or TTC. In order for this to occur, the speed governor of the colliding vehicle must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.

NOTE: [a] HRA preliminary value replaced by use of historic data (Attachment C).

CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HCTT = cask tractor and cask transfer trailer; HEP = human error probability; HFE = human failure event; HRA = human reliability analysis; ID = identification; MAP = mobile access platform; N/A = not applicable; RC = railcar; SNF = spent nuclear fuel; SPM = site prime mover; SSC = structure, system, or component; SSCs = structures, systems, and components; TT = truck trailer; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar.

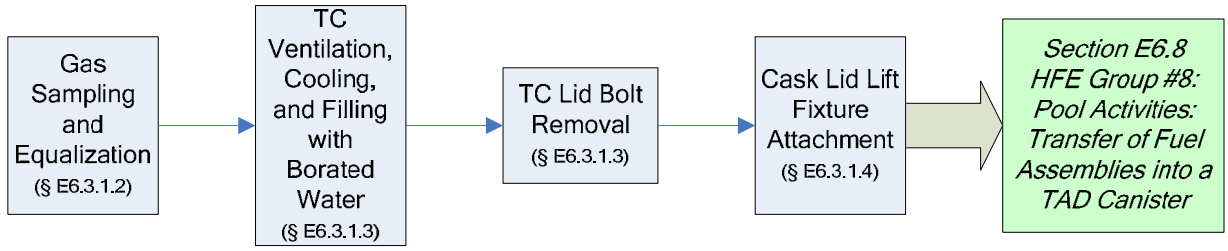
Source: Original

E6.2.3 Detailed Analysis

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E6.3 ANALYSIS OF HUMAN FAILURE EVENT GROUP #3: SNF PREPARATION ACTIVITIES

HFE group #3 corresponds to the operations and initiating events associated with the ESD and HAZOP nodes listed in Table E6.0-1, covering activities that prepare SNF for transfer into the pool for unloading. This operation starts with the SNF in a transportation cask upright in the SNF preparation station. During this operation the transportation cask has a lid lift fixture attached and it undergoes gas sampling, equalization and cooling in preparation for movement into the pool.



NOTE: § = section; HFE = human failure event; TAD = transportation, aging, and disposal; TC = transportation cask.

Source: Original

Figure E6.3-1. Activities Associated with HFE Group #3

E.6.3.1 Base Case Scenario

E6.3.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #3 activities:

1. The transportation cask is sitting upright in the SNF preparation station.
2. The cask handling crane (200-ton) and auxiliary pool crane (20-ton) are in the Cask Preparation Area, and have the following safety features:
   A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.
   B. There are end-of-travel interlocks on the trolley and bridge.
   C. There are speed limiters built into the design of the motors
   D. There is a weight interlock that cuts off power to the hoist when the crane capacity is exceeded.
   E. There is a temperature interlock that cuts off power to the hoist when the temperature is too high; an indicator comes on before this temperature is reached.

F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

Crane operations in this step are not part of a specific procedure outlined in the YMP documentation, but rather reflect critical lift crane operations that are standard in the nuclear industry.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Radiation protection worker[10]
- Supervisor
- Gas sampling crew member

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel in the WHF wear the appropriate PPE for their job.

E6.3.1.2 Gas Sampling and Equalization

To sample the cask, a crew member must plug a hose into the quick-disconnect sampling port and then open the valve to start flow. Once connected, a crew member takes a reading in the gas sampling room of gas that is being removed and verifies that the cask is safe for opening. After the sample is taken**,** and if safe to do so, the remainder of the gas is vented, the valve is closed, and the hose is taken off.

E6.3.1.3 Transportation Cask Ventilation, Cooling, and Filling with Borated Water

After gas sampling is complete, a crew member checks the temperature readout from the sampling process and verifies that the temperature of the gas is less than 212°F. Once verified, a crew member connects the water supply and return lines to the cask via quick disconnect connections and then feeds the return line into the pool. Once the hoses are set up, a crew member slowly turns on the water and fills the cask until it is full. The cask is full when water, instead of air, flows from the return hose; this is indicated by a lack of bubbles coming from the return hose in the pool. When full, a crew member disconnects both hoses.

E6.3.1.3 Transportation Cask Lid Bolt Removal

The crew uses common tools and the SNF preparation platform to remove all but four of the lid bolts. This step is verified on a check list. Movement of the lid bolts may require the use of the jib crane. Once removed, the bolts are counted, and the crew supervisor checks off bolt removal from the check list.

[10]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

E6.3.1.4 Transportation Cask Lid Lift Fixture Attachment to Cask Lid

The crane operator uses the cask preparation platform, common tools, and the jib crane, with the lid lift fixture lifting device (expected to be a grapple), to retrieve and emplace the transportation cask lid lift fixture. Once in place, the crew members close the shield plate and attach the fixture to the lid with bolts via holes in the shield plate. This step is verified via a checklist.

Lid Lift Fixture Retrieval—The crane operator lowers the jib crane into position over the lid lift fixture in the staging area, engages the fixture, and lifts the fixture to proper height for movement, based on a visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Lid Lift Fixture Moved to Cask—The crane operator moves the jib crane so as to locate the fixture over the cask in the Cask Preparation Area, following the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member that can (hand) signal the crane operator to stop at any time. At this time, a crew member opens the shield plate to allow the fixture to be positioned. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lid Lift Fixture Lowered and Disengaged—When properly positioned over the cask, the signaling crew member signals the crane operator to lower the fixture into place. The crane operator then proceeds to lower the fixture at or below the maximum allowable speed. Once the fixture is in place, the crane is disengaged from the fixture and then lifted to its maximum height in preparation for the next operation.

Shield Plate Closed and Lid Lift Fixture Bolted—The crew closes the shield plate and uses the cask preparation platform and common tools to emplace and tighten all the lid fixture bolts according to training and then verifies (via a checklist) that all the bolts have been properly installed.

The next step in WHF operations for SNF is Section E6.8, HFE Group #8.

E6.3.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during SNF preparation are summarized in Table E6.3-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.3-1. HFE Group #3 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCaskDrop01-HFI-NOD	*Operator Drops Cask during Preparation Activities*: The cask is not lifted in this step, and no plausible scenarios that would lead to a cask drop could be identified.	8	N/A	The cask is not lifted in this step and the cask handling crane is not used in this operation. There is no plausible configuration that can result in a cask drop during this operation; therefore, this failure was omitted from analysis
Crane Drop	*Operator Drops Object on Cask during Preparation Activities*: Preparation of a cask entails moving the lid lift fixture over the cask using the jib crane. During this lift, the operator can drop the object onto the cask by improperly connecting the object to the crane, two-blocking the object, or other such failures.	8	N/A [a]	In this step the operator uses the jib crane to move the lid lift fixture over the cask. The lid lift is moved with a grapple or hook. This lift can potentially result in a drop. This HFE was not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for this failure can be found in Attachment C.
050-OpCTCollide1-HFI-NOD	*Operator Causes Low-speed Collision of Auxiliary Vehicle with TC*: During SNF preparation, the TC is loaded and parked under the cask preparation platform for a long period of time. During this time, an operator can cause an auxiliary vehicle to collide with the TC.	8	3E−03	In this step the cask is sitting under the cask preparation platform. The speed of auxiliary vehicle is slow, the platform and cask are very visible, and procedural controls are expected to limit the number of other vehicles in the Cask Preparation Area during cask operations. This HEP was assigned the same preliminary value as railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) because the dominant mechanism of both failures is collision with an auxiliary vehicle. In this case, the preliminary value is conservative because the cask is staged under the platform and the railcar HFE has additional failure modes associated with movement of the SPM which are not applicable here. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted (×3) because there are several ways for a collision to occur.
050-OpFLCollide1-HFI-NOD	*Operator Causes High-speed Collision of Auxiliary Vehicle with TC*: During cask preparation, the TC is loaded and parked under the preparation platform for a long period of time. During this time, an operator can cause an auxiliary vehicle to collide with the TC. If the collision is due to the auxiliary vehicle speed governor malfunctioning, then this is a high-speed collision.	8	1.0	The operator can cause the auxiliary vehicle to over speed, resulting in collision. In order to accomplish this, the speed governor of the vehicle must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.
050-OpTCTImpact01-HFI-NOD	*Operator Causes an Impact Between SSC and Loaded TC due to Crane Operations*: While performing crane operations, the operator can potentially impact the cask if the crane is moved with the hook lowered below the platform.	8	3E−03	In this step the transportation cask is stationed under the preparation station and the lid lift fixture is moved over the cask. For crane operations in this step there are three observers with clear visibility, the operations are simple, the travel distances are short, and the crane speed is slow. There are no interlocks to prevent this error. No part of the cask is above the cask preparation platform. Therefore, the only way the transportation cask can be impacted with the crane is if the crane is moved with the load and hook lower than the platform, and the crane moves into the platform causing the load and hook to swing into the transportation cask. The likelihood of impacting a cask was assessed to be comparable to the crane impact during upending and removal HFE (050-OpTCImpact01-HFI-NOD; Section E6.2, HFE Group #2) and was accordingly assigned the same preliminary value. This is considered a conservative assessment because, in comparison with upending and removal, there are fewer crane movements in this operation, and there is a platform around the cask which makes it harder to impact the cask. This failure is “highly unlikely” (one in a thousand or 0.001, which also corresponds to the generic failure rate for a simple operation that is performed daily) but is adjusted because there are several ways for an impact to occur (×3).
050-OpTipover001-HFI-NOD	*Operator Causes Cask to Tip Over during Cask Preparation Activities*: The operator can improperly stow the crane rigging and it can catch the cask. If this happens, movement of the crane can cause the cask to tip over.	8	1E−04	In this step the transportation cask is stationed under the cask preparation station and the lid lift fixture is attached to the cask lid. In order to get a tipover of the cask, the crane must be attached to the cask and must also move. To be conservative, the jib crane is considered physically capable of tipping over a cask while stationed underneath the platform. At no point in the operations is the crane attached to the cask. Therefore, the only way for the crane to be attached to the cask is if the crane rigging catches the cask during sampling. This is unlikely because the transportation cask is recessed under and protected by the platform during this operation. If the rigging is caught, then it is unlikely that the crane operator would not notice while trying to move the crane. The dominant contributor is the crane hook catching the cask. While it may be unlikely (0.01) that a stray hook or grapple might be hanging from the crane, it would still need to catch on the cask securely enough to pull it over (0.1), and then the cask tipping would have to go unnoticed by all three observers. This task is done under direct observation, there is a platform and a shield plate to protect the cask from stray rigging, and a tipover is a slow process. Therefore, the value was adjusted by a further 0.1. This operation was given the same preliminary value as the cask tipover during upending and removal HFE (050-OpTipover001-HFI-NOD; Section E6.2, HFE Group #2) because it is a very similar operation (movement with a crane using the same type of rigging and attachments) and has similar failure modes. The difference between the two scenarios is that there are more crane operations and more failure modes during upending and removal, and therefore there would be more opportunities for a tipover in that scenario.
050-Liddisplace1-HFI-NOD	*Operator Inadvertently Displaces Lid*: The operator can improperly store the crane rigging such that it catches the lid lift fixture and pulls off the cask lid during cask preparation, resulting in a direct exposure.	29	N/A	In this step the lid lift fixture is attached. Also, in this step, the lid is bolted to the cask. Due to design changes to the preparation platform, improperly stowed rigging during this operation does not catch the lid lift fixture. These design changes included raising the platform so the cask is recessed underneath the platform. This failure was omitted from analysis.

Table E6.3-1. HFE Group #3 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpSampleRel2-HFI-NOD	*Operator Improperly Performs Gas Sampling*: Gas sampling may be performed to determine if the fuel has been damaged by the transportation process. If the gas sampling process is incorrectly performed, such that material is released from the sample line, then a radiation release occurs if the fuel inside is damaged.	16	5E−03	In this step, the crew samples the cask via a quick-disconnect gas sampling port to ensure that the fuel is intact before removing the canister lid. There is one operator in charge of gas sampling. In order to get a release from the line, the line would have to be inappropriately attached such that the quick disconnect valve is engaged and open. This EOC was assessed to be “highly unlikely” (0.001) because the operation is simple and performed on a daily basis by a highly trained individual. This value was adjusted (×5) to account for the fact that this operation is performed by one crew member, and a failure would be very difficult to notice and correct before material is released. Note: this is the probability of release if it is damaged fuel; for release of radioactivity to occur, the probability of damaged fuel would have to be assessed and applied.

NOTE: a HRA preliminary value replaced by use of historic data (Attachment C).
EOC = error of commission; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; ID = identification; N/A = not applicable; SPM = site prime mover; SSC = structure, system, or component; TC = transportation cask.

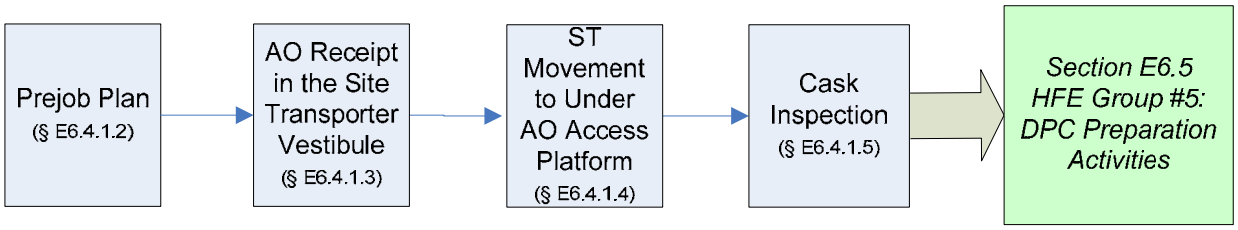
Source: Original

E6.3.3 Detailed Analysis.

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E6.4 ANALYSIS OF HUMAN FAILURE EVENT GROUP #4: SITE TRANSPORTER RECEIPT AND MOVEMENT INTO THE CASK PREPARATION AREA

HFE group #4 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering movement of a site transporter loaded with an aging overpack into the Site Transporter Vestibule to prepare it for unloading. The operations covered in this HFE group are shown in Figure E6.4-1. In this operation, a site transporter, carrying an aging overpack, enters the Site Transporter Vestibule and moves into position under the aging overpack access platform.



NOTE: § = section; AO = aging overpack; CTM = canister transfer machine; HFE = human failure event.

Source: Original

Figure E6.4-1. Activities Associated with HFE Group #4

E6.4.1 Base Case Scenario

E6.4.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #4 activities.

1. The site transporter is securely loaded with an intact aging overpack and is at the entrance of the Site Transporter Entrance Vestibule.

The following personnel are involved in this set of operations:

- Crew members (two people)
- PIC
- Site transporter operator
- Radiation protection worker[11].

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel in the WHF wear the appropriate PPE for their job.

[11]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

E6.4.1.2 Prejob Plan

Before the aging overpack and site transporter reaches the WHF, the PIC is notified of the type of cask and conveyance to expect and how to process it. According to this information, the PIC determines the appropriate procedures and equipment necessary to process this cask type and communicates this information to all the crew members involved in the processing of this cask. The PIC fills out a prelift safety checklist (Ref. E8.1.12) verifying that the equipment is properly staged and is in proper operational condition. All crew members are properly trained and abide by the procedures of the facility.

E6.4.1.3 Aging Overpack Receipt in the Site Transporter Vestibule

Two crew members are located at the Site Transporter Vestibule. When the site transporter approaches the WHF, one crew member opens the outside overhead door and the other crew member directs the site transporter into the Site Transporter Vestibule, ensuring there are no vehicles or obstructions in the path. The crew members follow all relevant restrictions and procedures regarding site transporter speed and direction of travel. Once the site transporter has cleared the door, the first crew member closes the outside door.

E6.4.1.4 Site Transporter Movement to under the Aging Overpack Access Platform

Once the site transporter is in the Site Transporter Vestibule, the ST operator moves the site transport into position under the preparation platform, and stops. The brakes for the site transporter are set, the forks are lowered, the power is turned off, and, if required, the platform is closed over the site transporter.

A checklist is signed to indicate that the facility door has been closed and the site transporter brakes are set.

E6.4.1.5 Cask Inspection

Once the site transporter is parked in the facility, the crew visually inspects and conducts radiological surveys of the exterior of the aging overpack.

E6.4.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during receipt of the site transporter are summarized in Table E6.4-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.4-1. HFE Group #4 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
ST Rollover	*Operator Causes the ST to Rollover in the ST Vestibule:* Operator drives over a significantly uneven surface while moving the ST into the ST Vestibule, causing the ST to rollover.	3	N/A	Although the center of mass for the ST is higher than that of the truck trailer, this failure mode was omitted from analysis for the same reasons as the truck rollover (Section E6.1). For a ST to rollover, the center of mass has to shift laterally. This can be done by traversing a significantly uneven surface or running over a very large object. There are no significantly uneven surfaces in the ST Vestibule. It is incredible for the ST to run over an object large enough necessary to shift its center of mass.
050-OpFailStop-HFI-NOD	*Operator Fails to Stop the ST if the Tread Fails*: If the tread of the ST fails, it is possible the ST can rollover if the operator continues to operate the ST.	3	1.0	If the tread of the ST fails, it is possible the ST can rollover if the operator continues to operate the ST. While it is unlikely that an operator would continue to operate an ST if such a significant and visible failure occurred, to be conservative, unsafe actions that require an equipment failure to cause an initiating event have been assigned an HEP of 1.0.
050-OpSTCollide3-HFI-NOD	*Operator Causes Low-speed Collision of ST with an SSC while Moving to the ST Vestibule*: Operator causes collision of ST with a facility structure or piece of equipment while moving into the ST Vestibule. The ST is physically unable to over speed, therefore any collision of the ST is a low-speed collision.	3	3E−03	When the ST enters the WHF it can collide into an SSC, such as the facility door, an auxiliary vehicle, or improperly stowed crane rigging. Collision of an ST is a similar operation and has the same failure modes as the railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1), and was accordingly assigned the same preliminary value. This failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted because there are several ways for a collision to occur and potentially multiple other vehicles (forklifts) that can collide into the conveyance (×3). In this case, the preliminary value is particularly conservative because no auxiliary vehicles are in the ST Vestibule; therefore, the only failure mode is for the ST to collide into the facility structure or the aging overpack access platform.
050-OpLoadDrop-HFI-NOD	*Operator Causes ST to Drop the AO*: The ST is like a forklift, carrying the AO several inches above the ground on its forks. If the AO is improperly secured onto the ST, it can fall off the forks while in transit.	3	N/A	There are no crane operations in this step, so the only way for an AO to be dropped is if it falls off the ST. The ST is like a fork lift which holds the AO raised several inches above the ground while in transit. The ST cannot lift the AO greater than one foot, so a drop greater than a foot is not plausible in this step. The AO is prevented from moving on or falling off the ST by a securing mechanism which locks the AO into place. The ST travels from the aging pads to the WHF. It is highly unlikely that the AO can drop in the facility due to human error given that it has not dropped in transit to the facility. Also, there are interlocks that prevent the ST from moving if the AO is not properly secured. Therefore, the drop of an AO due to human failure was omitted from the analysis.

NOTE: AO= aging overpack; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; ID = identification; N/A = not applicable; SSC = structure, system, or component; ST = site transporter.

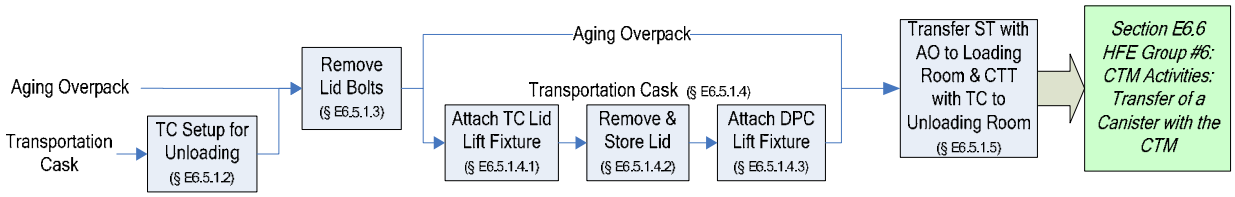
Source: Original

E6.4.3 Detailed Analysis

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E6.5 ANALYSIS OF HUMAN FAILURE EVENT GROUP #5: DPC PREPARATION ACTIVITIES

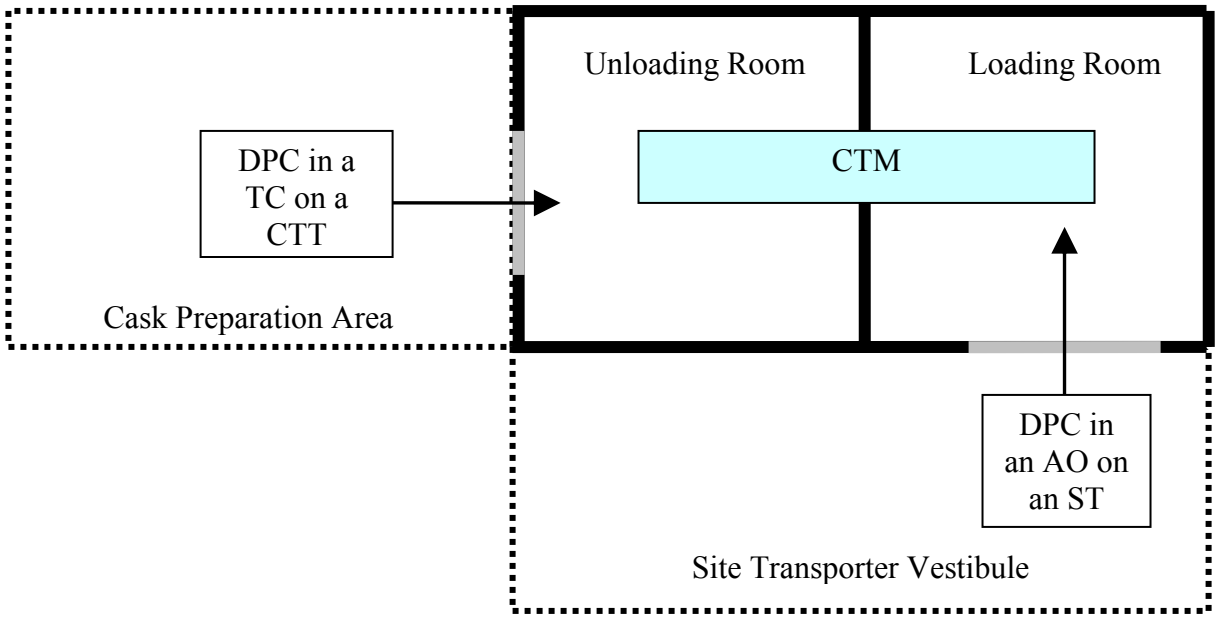
HFE group #5 corresponds to the operations and initiating events associated with the ESD and HAZOP nodes listed in Table E6.0-1, covering the preparation of an aging overpack or transportation cask containing a DPC for unloading from the conveyance and movement into position for removal of the DPC canister. Figure E6.5-1 provides an overview of the operations covered in this HFE group. The process of unloading a DPC from either an aging overpack or a transportation cask (VTC or TTC) is accomplished in one of two rooms on the WHF ground floor that can be accessed by the CTM. DPCs are removed from aging overpacks in the WHF Loading Room, because the Loading Room is the only room with CTM access that the site transporter can physically enter. DPCs are removed from transportation casks in the WHF Unloading Room because it is the only room with CTM access that the CTT can physically enter. This operation starts with the DPC in either an aging overpack under the aging overpack access platform in the Site Transporter Vestibule or in a transportation cask on the CTT in the Cask Preparation Area. During this operation the cask undergoes lid unbolting and other preparation activities necessary for canister transfer. Once the preparation activities are complete, the crew moves the aging overpack and site transporter to the Loading Room or the transportation cask and CTT to the Cask Unloading Room. In DPC is positioned under the cask port and is ready for CTM operations. Operations for this HFE group end at this stage, just prior to the start of CTM activities. Figure E6.5-2 provides a simplified schematic of the rooms involved in this operation.



NOTE: § = section; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure event; TC = transportation cask.

Source: Original

Figure E6.5-1. Activities Associated with HFE Group #5



NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ST = site transporter; TC = transportation cask; WHF = Wet Handling Facility.

Source: Original

Figure E6.5-2. Rooms Involved with the Preparation and Movement of DPCs at the WHF

E6.5.1 Base Case Scenario

E6.5.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #5 activities:

1. The transportation cask is intact and secure in the CTT under the cask preparation platform in the Cask Preparation Area. The aging overpack is intact and secure in the site transporter under the cask preparation platform in the Site Transporter Vestibule.

2. The CTT is an air-pallet trolley apparatus that is guided by two removable rails. The CTT also has end stops to aid in final positioning. A safe load path is marked for the CTT operations, and there are at least three crew members involved in its movement when loaded. The CTT is normally deflated with the controller pendant stowed during preparation activities.

3. The site transporter is a fork-lift like apparatus that carries the aging overpack on prongs that are raised several inches above the ground. A safe load path is marked for the site transporter operations, and there are at least three crew members involved in its movement when loaded. The site transporter is normally powered off with the controller pendant stowed during preparation activities.

4. The shield doors to the Cask Unloading Room and Loading Room are closed. There is an interlock between the port slide gates and the shield doors. The port slide gate to a room cannot be open while the shield door to that room is also open.

5. The jib cranes (for both the preparation platform in the Cask Preparation Area and the aging overpack access platform in the Site Transporter Vestibule) have the following safety features:

   A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final, that is set higher than the upper limit indicator, cuts off the power to the hoist. There is no bypass for the final limit interlock.

   B. There are end of travel interlocks on the trolley and bridge.

   C. There are speed limiters designed into the motors

   D. There is a weight interlock that cuts off power to the hoist when the crane capacity is exceeded.

   E. There is a temperature interlock that cuts off power to the hoist when the motor temperature is too high; an indicator comes on before this temperature is reached.

   F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

   Crane operations in this step are not part of a specific procedure outlined in the YMP documentation, but rather reflect critical lift crane operations that are standard in the nuclear industry.

The following personnel are involved in this set of operations.

- Crew members (two people)
- Crane operator
- Signaling crew member
- Verification crew member
- CTT operator
- Site transporter operator
- Radiation protection worker[12]
- Supervisor.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel in the WHF wear the appropriate PPE for their job.

[12]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

E6.5.1.2 Setup of Transportation Cask for Unloading (Transportation Cask Only)

Cask Preparation Platform Lowering (if Required) and Shield Plate Closure—Once the cask is loaded and secure in the CTT, the crew lowers the cask preparation platform (if necessary) and moves the shield plate over the cask.

Gas Sampling and Equalization (if Required)—To sample the cask, a crew member must plug a hose into the quick-disconnect sampling port and then open the valve to start the flow. Once connected, a crew member takes a reading in the gas sampling room of gas that is being removed and verifies that the cask is safe for opening. After the sample is taken**,** and if safe to do so, the remainder of the gas is vented, the valve is closed, and the hose is taken off.

E6.5.1.3 Remove Aging Overpack or Transportation Cask Lid Bolts

The crew closes the platform shield plate and removes all the cask or aging overpack lid bolts using the cask preparation platform and common tools. Movement of the lid bolts may require the use of the jib crane. Once removed, the bolts are counted and the crew supervisor checks off bolt removal from the check list before the site transporter is moved for CTM activities.

E6.5.1.4 Transportation Cask Preparation Activities

E6.5.1.4.1 Transportation Cask Lid Lifting Fixture Retrieval and Attachment to Cask Lid

The crane operator uses the cask preparation platform, common tools, and the jib crane, with lid lift fixture lifting device (i.e., a grapple) to retrieve and emplace the transportation cask lid lift fixture. Once in place, the crew members close the shield plate and attach the fixture to the lid with bolts. This step is verified via a checklist.

Lid Lift Fixture Retrieval—The crane operator lowers the jib crane into position over the lid lift fixture in the staging area, engages the fixture, and lifts the fixture to proper height for movement, based on a visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Lid Lift Fixture Moved to Cask—The crane operator moves the jib crane so as to locate the fixture over the cask in the Cask Preparation Area, following the indicated safe load path marked on the floor. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member that can (hand) signal the crane operator to stop at any time. At this time, a crew member opens the shield plate to allow the fixture to be positioned. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lid Lift Fixture Lowered and Disengaged—When properly positioned over the cask, the signaling crew member signals the crane operator to lower the fixture into place. The crane operator then proceeds to lower the fixture at or below the maximum allowable speed. Once the fixture is in place, the fixture is disengaged, and the crane is lifted to its maximum height in preparation for the next operation.

Shield Plate Closed and Lid Lift Fixture Bolted—The crew closes the shield plate and uses the cask preparation platform and common tools to emplace and tighten all the lid fixture bolts according to training and then verifies (via a checklist) that all the bolts have been properly installed. The shield plate has holes by which the crew can access the lid fixture bolts.

E6.5.1.4.2 Transportation Cask Lid Removal and Storage on the Cask Lid Stand

Once the lid lift fixture is attached to the cask lid, the crew opens the shield plate and removes the transportation cask lid using the jib crane and standard rigging.

Crane Aligned to Cask—The crane operator retrieves the lid lift fixture lifting device, and the crew opens the shield plate. The crane operator then lowers the jib crane hoist cable into position over the transportation cask. The crane operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member following the load that uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the load, checking alignment of the crane. The verification crew member can only signal to stop the crane. Once positioned, one of the crew members connects the crane to the cask lid using a grapple.

Lid is Lifted Vertically—Upon signal from the signaling crew member that all is well, the crane operator begins to raise the cask lid. Once the lid is raised (i.e., is hanging free), the crane operator clears the cask and CTT and then lowers the lid to the proper movement height based on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. Throughout this operation, the crew is standing several feet away from the platform opening. Once the lid is removed, a crew member then closes the shield plate.

Lid Moved to Staging Area—The crane operator moves the jib crane so as to locate the lid over the lid stand in the staging area. To do this, the crane operator follows the indicated safe load path marked on the floor based on visual cues and confirmatory hand signals from the signaling crew member. The crane operator then sets the lid down and disengages the grapple.

E6.5.1.4.3 Retrieval and Attachment of DPC Lift Fixture to Transportation Cask

The lift fixture is attached to the DPC using the jib crane with a grapple or hook, cask preparation platform, and common tools. The crane operator and the signaling and verification crew members are positioned on the cask preparation platform for this step. There are several DPC types, and the DPC lift adapter is adjustable, with several mounting positions to accommodate all DPC types.

DPC Lift Fixture Retrieval—The crane operator lowers the jib crane into position over the DPC lift fixture in the staging area, engages the grapple, and lifts the fixture to proper height for movement based on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

DPC Lift Fixture Moved to Cask—The crane operator moves the jib crane so as to locate the fixture over the cask in the preparation area. To do this, the crane operator follows the indicated

safe load path marked on the floor based on visual cues and confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member that can (hand) signal the crane operator to stop at any time. At this time, a crew member opens the shield plate to allow the fixture to be positioned. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

DPC Lift Fixture Lowered and Disengaged—When properly positioned over the DPC, the signaling crew member signals the crane operator to lower the fixture into place. The crane operator then proceeds to lower the fixture at or below the maximum allowable speed. Once the fixture is in place, the grapple is disengaged, and the crane is lifted to its maximum height in preparation for the next operation. The crane operator and crew stay several feet away from the platform opening while the shield plate is open.

Shield Plate Closed and DPC Lift Fixture Bolted—A crew member then closes the shield plate, uses the cask preparation platform and common tools to emplace and tighten all the lid fixture bolts according to training, and then verifies (via a checklist) that all the bolts have been properly installed. The shield plate has holes to enable the crew to access the lid fixture bolts.

E6.5.1.5 Transfer of the Site Transporter with an Aging Overpack to the Loading Room and the CTT with a Transportation Cask to the Cask Unloading Room

E6.5.1.5.1 Aging Overpack Movement into the Loading Room

Once the lid bolts are removed, the site transporter operator turns on the site transporter, lifts the fork several inches, and moves the site transporter to the door of the Cask Loading Room. A crew member opens the shield door and the site transporter operator moves the site transporter into position under the cask port in the Loading Room. There are physical stop points which the site transporter must bump up against to ensure proper alignment. The site transporter operator lowers the site transporter forks, turns off the site transporter and closes the shield door.

E6.5.1.5.2 Transportation Cask Movement into Cask Unloading Room

Using the CTT, the crew member moves the transportation cask to the Cask Unloading Room and positions the cask under the cask port. To do this, the CTT operator inflates the CTT, moves the CTT to the Cask Unloading Room door, opens the shield door, moves the CTT through the door, positions it under the cask port, deflates the CTT, stores the pendant, disconnects the air hose, and closes the shield door. There are physical stop points in the Cask Unloading Room that the CTT must bump up against to ensure proper alignment.

E6.5.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during cask preparation and movement to the Cask Unloading or Loading Room are summarized in Table E6.5-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCaskDrop01-HFI-NOD	*Operator Drops the Cask during Preparation Activities*: The cask is not lifted in this step, and no plausible scenarios that would lead to cask drop could be identified.	7, 9	N/A	The cask is not lifted in this step and the 200-ton crane is not used in this operation. For aging overpacks with DPCs, there is no possible configuration that can result in a cask drop because there is no crane capable of lifting an aging overpack in the Site Transporter Vestibule. For transportation casks with DPCs, a cask drop would require several human failures during the same set of activities: during lid removal, the crew must fail to remove some fraction of the lid bolts (EOO), fail to properly use a checklist to verify bolt removal, and must use the wrong crane (EOC) to remove the partially attached lid. In addition to the human failures, the bolts would have to hold the weight of the cask long enough to lift the cask. The crane operator and at least two other crew members would be standing on the platform in direct view of the cask during lid removal, and they would also all have to fail to notice that the entire cask is being lifted before the bolts break. This failure was omitted from the analysis.
Crane Drop	*Operator Drops an Object on Cask during Preparation Activities*: Preparation of a cask entails moving several heavy objects over the cask using a jib crane. These objects include the lid lift fixture and, for TC/DPCs, the cask lid and canister lift fixture. During these lifts, the operator can drop the object onto the cask or canister by improperly connecting the object to the crane, two-blocking the object, or other such failures.	7, 9	N/A[a]	In this step the operator uses the cask handling crane auxiliary hook to move objects over the cask. There are three heavy-object lifts (the lid lift fixture, the cask lid, and the canister lift fixture) using the auxiliary hook. The lid lift and canister lift fixtures are moved with a grapple or hook, the cask lid is moved with a sling. Each of these lifts can potentially result in a drop. These HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for this failure can be found in Attachment C. This failure mode is only applicable to transportation casks with DPCs because lid bolts are not heavy enough to damage an aging overpack.
050-OpCTCollide1-HFI-NOD	*Operator Causes Low-speed Collision of an Auxiliary Vehicle with the CTT*: During cask preparation, the CTT is loaded and parked under the preparation platform for a long period of time. During this time, an operator can cause an auxiliary vehicle to collide with the CTT. There are no auxiliary vehicles in the ST Vestibule, and so this failure mode is not applicable to AOs with DPCs.	7, 9	3E−03	In this step the CTT is loaded and parked under the cask preparation platform. The speed of auxiliary vehicles is slow, the CTT is very visible, and procedural controls are expected to limit the number of other vehicles in the Cask Preparation Area during cask operations. This HEP was assigned the same preliminary value as a railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) because the dominant mechanism of both failures is collision with an auxiliary vehicle. In this case, the preliminary value is conservative because the CTT is staged under the cask preparation platform, and the railcar collision HFE has additional failure modes associated with movement of the SPM that are not applicable here. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted (×3) because there are several ways for a collision to occur.
050-OpFLCollide1-HFI-NOD	*Operator Causes High-speed Collision of Auxiliary Vehicle with the CTT*: During cask preparation, the CTT is loaded and parked under the preparation platform for a long period of time. During this time, an operator can cause an auxiliary vehicle to collide with the CTT. If the collision was due to the auxiliary vehicle speed governor malfunctioning, this failure would be a high-speed collision. There are no auxiliary vehicles in the ST Vestibule, and so this failure mode is not applicable to AO/DPCs.	7, 9	1.0	The operator can cause the auxiliary vehicle to over speed, resulting in collision. In order to accomplish this failure, the speed governor of the vehicle must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
050-OpSpurMove01-HFI-NOD	*Operator Causes Spurious Movement of the CTT or ST during Preparation Activities*: The CTT is supposed to be deflated, with the control pendant stored during this operation. The ST is supposed to be turned off, with the control pendant stored during this operation. However, if the CTT/ST is not in the proper configuration for cask preparation, the operator can inadvertently cause the CTT/ST to move. This spurious movement can cause the CTT/ST to collide into the platform or other SSC.	7, 9	1E−04	In this step the CTT and site transporter are parked under a platform; the CTT is deflated, the site transporter is turned off and both have their control pendant stored. For operations in this step, there are several crew members on the preparation platform and no operators below the platform. This error was considered to be extremely unlikely (0.0001) because it requires multiple human errors: it would require the CTT to be left inflated or the site transporter to be left powered, the observers (i.e., the crane operator, two crew members, or the radiation protection worker) would have to fail to notice or fail to stop operations to deflate the CTT or turn off the site transporter, and an operator would have to access the pendent and signal the CTT or site transporter to move

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCTTImpact1-HFI-NOD	*Operator Causes an Impact between an SSC and a Loaded CTT/ST due to Crane Operations*: While performing crane operations, the operator can potentially impact the cask if the crane is moved with the hook lowered below the platform.	7, 9	3E−03	In this step the CTT is stationed under the preparation platform and the lid lift fixture, lid (DPC only) and canister lift fixture (DPC only) is moved over the cask. The site transporter is parked under the aging overpack platform and has its lid bolts removed. For crane operations in this step, there are three observers with clear visibility, the operations are simple, the travel distances are short, and the crane speed is slow. There are no interlocks to prevent this error. No part of the cask is above the preparation platform, and so the only way the site transporter/CTT (containing a cask) can be impacted with the crane is if the crane is moved with the load/hook lower than the platform and the crane moves into the platform, causing the load/hook to swing into the site transporter/CTT. The crane hook can also be improperly stowed such that the site transporter/CTT, when moving to the Loading/Unloading Room (respectively), collides with the crane hook. However, the site transporter/CTT travels under the platform to the Loading/Unloading Room (respectively) and is the last preparation activity for both types of conveyances and requires the shield plate to be closed. Therefore, it is unlikely in this case that if the crane is improperly stored, the hook would be in the path of the CTT or site transporter. The likelihood of impacting a cask was assessed to be comparable to the crane impact during upending and removal HFE (050-OpTCImpact01-HFI-NOD; Section E6.2, HFE Group #2) and was accordingly assigned the same preliminary value based on the following rationale: this failure is “highly unlikely” (one in a thousand or 0.001, which also corresponds to the generic failure rate for a simple operation that is performed daily) but is adjusted because there are several ways for an impact to occur (×3). This is assessment considered a conservative assessment because, in comparison with upending and removal, there are fewer crane movements in this operation, and there is a platform around both the CTT and site transporter which makes it harder to impact the CTT/site transporter.
050-OpTipover001-HFI-NOD	*Operator Causes Cask to Tip Over during Cask Preparation Activities*: The operator can improperly stow the crane rigging and it can catch the CTT, ST or cask. If this happens, movement of the crane or the CTT/ST can cause the cask to tip over.	7	1E−04	In this step the CTT is stationed under the cask preparation platform, the lid lift fixture is attached to the cask lid and the CTT is then moved to the Unloading Room. For aging overpacks with DPCs, the site transporter is stationed under the aging overpack platform, the lid bolts are removed, and the site transporter is then moved to the Loading Room. In order to get a tipover of the cask/CTT/site transporter, the crane must be attached to the cask or CTT/site transporter and the crane or CTT/site transporter must also move. To be conservative, the jib crane was considered physically capable of causing the cask/CTT to tip over underneath the platform; however, the jib crane cannot cause a loaded ST to tipover (Section 6.0 of the main report). At no point in the operations is the crane attached to the cask. For a transportation cask, the crane is attached to the lid, but the lid is unbolted (Section E6.0.2.3.2 provides a discussion of failure to remove lid bolts). Therefore, the only way for the crane to be attached to the cask is if the crane rigging catches the cask or CTT. This is unlikely because the CTT is protected by the platform and shield plate during this operation. If the rigging is caught, it is unlikely that the crane operator would not notice while trying to move the crane. It is also unlikely that, when the CTT begins movement to the Unloading Room, the operator and observers would not notice that the rigging is attached to the conveyance. The dominant contributor is the crane hook catching the cask. While it may be unlikely (0.01) that a stray hook or grapple might be hanging from the crane, it would still need to catch on the cask securely enough to pull it over (0.1), and then the cask tipping would have to go unnoticed by all three observers. This task is done under direct observation, there is platform and shield plate to protect the cask from stray rigging, and a tipover is a slow process; therefore, the value was adjusted by a further 0.1. This operation was given the same preliminary value as the cask tipover during upending and removal HFE (050-OpTipover001-HFI-NOD; Section E6.2, HFE Group #2) because it is a very similar operation (movement with crane using same type of rigging/attachments) and has similar failure modes. The difference between the two scenarios is that there are more crane operations and more failure modes during upending and removal, and so there would be more opportunities for a tipover in that scenario; also, there is no platform/shield plate in upending to protect the cask from stray rigging.
050-OpTipOver3-HFI-NOD	*Operator Causes a Tipover of CTT/ST during Movement to the Cask Unloading/Loading Room*: The operator can improperly stow the crane rigging, and it can catch the CTT/ST or cask. If this happens while the CTT is moving to the Cask Unloading Room or the ST is moving to the Loading Room, it can cause the CTT/ST to tip over.	10, 11	N/A	The CTT/ST, loaded with a cask, undergoes a set of operations that includes operations under the preparation platform and then movement of the CTT/ST away from the platform to the Cask Unloading or Loading Room (respectively). A tipover of the CTT/ST during this set of activities constitutes one HFE because the most likely scenario is that the crane would be attached during preparation and a tipover would happen during movement of the CTT/ST away from the platform. The event sequences, however, model a tipover during platform activities and a tipover during CTT/ST movement. Because this is only one human failure, the appropriate preliminary value was only modeled in the event sequence associated with platform activities (050-OpTipover001-HFI-NOD, modeled in ESD 7). The HEP for a tipover in the event sequence associated with the subsequent movement of the CTT or ST (050-OpTipOver3-HFI-NOD in ESD 10 and 11) was assigned a probability of zero to avoid double counting.

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpImpact0000-HFI-NOD	*Operator Causes Impact of Cask during Transfer from the Platform to Loading/Unloading Room*: While the ST is moving from the platform to the Loading Room and the CTT is moving to the Unloading Room, the ST/CTT can impact the crane hook or rigging if it is improperly stowed.	10	N/A	While moving from the Preparation Area to the Loading/Unloading Room, the CTT or site transporter can impact the crane hook or rigging if it is improperly stowed. The last step in preparation activities for both DPCs requires the shield plate of the platform to be closed. It is unlikely, then, that the crane rigging can be improperly stowed such that it impacts the CTT or site transporter while it is moving into the Unloading or Loading Room; it is more likely that rigging impacts the cask while the crane is actually in use. Therefore, any crane interference with the CTT/site transporter is already covered by 050-OpCTTImpact1-HFI-NOD (Operator Causes Impact between CTT or Site Transporter and SSC during DPC Preparation) and 050-OpTipover001-HFI-NOD (Operator Causes Cask to Tip Over during DPC Preparation Activities).
050-OpCTCollide2-HFI-NOD	*Operator Causes Low-speed Collision of the CTT during Transfer from the Preparation Station to the Cask Unloading Room*: Once the preparation activities are over, an operator inflates the CTT and moves the cask from the Preparation Area to the Unloading Room. The operator can cause the CTT to collide with the preparation platform structure during this transfer. The CTT is designed such that it physically cannot over speed; therefore, all CTT collisions are below the designed speed.	10	1E−03	In this step the CTT moves from the cask preparation platform to the Unloading Room; the doors of the Cask Preparation Area must be opened to allow the CTT to pass through. There are three observers with clear visibility, the speed of the CTT and other vehicles is low, the CTT is very visible, and there are two guide rails and an end stop to keep the CTT on the safe load path. Procedural controls are expected to limit the number of other vehicles in the Preparation Area during cask operations. The CTT could collide into conveyance or facility structures (i.e., cask preparation platform or shield door). This could happen if the guide rails were not installed properly. This operation is simple, straightforward, and is expected to occur very regularly (daily), and was assigned the default probability of a “highly unlikely” occurrence (0.001). It was considered reasonable and consistent that the preliminary value assigned for this HFE is less likely than a railcar collision because of the guide rail, number of observers, and short travel distance
050-OpSTCollide3-HFI-NOD	*Operator Causes Low-speed Collision of the ST with an SSC while Moving to the Loading Room*: Operator causes a collision of the ST with a facility structure or piece of equipment while moving under the platform to the Loading Room. The ST is physically unable to over speed, so any collision of the ST is a low-speed collision.	11	3E−03	While traveling to the Loading Room from the Site Transporter Vestibule, the site transporter can collide into an SSC, such as the shield door or the platform. Collision of a site transporter is a similar operation and has the same failure modes as the railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1), and was accordingly assigned the same preliminary value based on the following rationale: this failure is “highly unlikely” (one in a thousand or 0.001, which also corresponds to the generic failure rate for a simple operation that is performed daily) but is adjusted because there are several ways for collision to occur (×3).
050-OpFailStop-HFI-NOD	*Operator Fails to Stop ST if Tread Fails*: If the tread of the ST fails, it is possible that the ST can rollover if the operator continues to operate the ST while trying to move through the facility.	11	1.0	If the tread of the site transporter fails, it is possible the site transporter can rollover if the operator continues to operate the site transporter. While it is unlikely that an operator would continue to operate a site transporter if such a significant and visible failure occurred, to be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.
050-OpSDClose001-HFI-NOD	*Operator Closes Shield Door on Conveyance*: Once the preparation activities are over, an operator inflates the CTT or turns on the ST and moves the cask from the Preparation Area to the Loading or Unloading Room, respectively. There is a shield door between the Preparation Area and the Unloading Room and between the ST Vestibule and the Loading Room. The operator can impact the cask by inadvertently closing the shield door on the CTT or ST as they pass through the shield door.	12	1.0	The CTT and site transporter pass through a shield door as they enter the Loading/Unloading Room (respectively). During this transfer, the operator can close the shield door onto the CTT or site transporter. Section E6.0.2.3.3 provides a justification of this preliminary value.
050-OpDPCShield1-HFI-NOW	*Operator Fails to Properly Shield DPC while Installing Canister Lift Fixture, Leading to Direct Exposure (TC only)*: In this step, the DPC canister lift fixture is attached to the canister. There are two ways for the crew to get a direct exposure during this activity: an operator can fail to properly close and verify the closure of the shield plate after the cask lid is removed and the crew continues with the installation, or the operator can inadvertently open the shield plate while the crew is installing the canister lift fixture.	29	1E−03	In this step, the DPC canister lift fixture is attached to the canister. If an operator fails to properly close the shield plate after removing the DPC lid, then the crew can be directly exposed to the shine from the DPC while installing the canister lift fixture. Likewise, if an operator inadvertently opens the shield plate while the crew is installing the canister lift fixture, then the crew can be exposed. In this case, the crew is on top of the shield plate and notices if the shield plate moves. The crew is highly trained and, although they only perform DPC preparation activities weekly, they are accustomed to operating the shield plate during preparation of other transportation casks. In addition to the crew members, there is also a radiation worker present who is monitoring activities. This error was assessed to be highly unlikely and given a preliminary value of 0.001.
050-Liddisplace1-HFI-NOD	*Operator Inadvertently Displaces Lid*: The operator can improperly store the crane rigging such that it catches the lid lift fixture and pulls off the cask lid during cask preparation, resulting in a direct exposure.	29	N/A	In this step, the lid is unbolted and, for transportation casks with DPCs, other crane operations are performed. Due to design changes to the preparation platform, improperly stowed rigging during this operation does not catch the lid lift fixture. These design changes include raising the platform and adding a shield plate so the cask is recessed underneath the platform and protected.

Table E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
Gas Sampling	*Operator Improperly Performs Gas Sampling*: Gas Sampling is performed to determine if an incoming canister has been damaged by the transportation process. If the gas sampling process is incorrectly performed and a damaged canister goes undetected, then a radiation release occurs by continuing with normal operations.	29	N/A	If the gas sampling process is incorrectly performed and a damaged canister goes undetected, then a radiation release occurs by continuing with normal operations. Assessing accident scenarios with pre-damaged canisters is beyond the scope of this analysis.

NOTE: [a] Historical data was used to produce a probability for this HFE (Attachment C).
AO = aging overpack; CTT = cask transport trolley; DPC = dual-purpose canister; SSC = structure, system, or component; ST = site transporter; TC = transportation cask.

Source: Original

E6.5.3 Detailed Analysis

After the preliminary screening analysis and initial quantification are completed, those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives are subjected to a detailed analysis. The overall framework for the HRA is based upon the process guidance provided in ATHEANA (Ref. E8.1.22). Consistent with that framework, the following four steps from the methodology described in Section E3.2 provide the structure for the detailed analysis portion of the HRA:

Step 5: Identify Potential Vulnerabilities

Prior to defining specific scenarios that can lead to the HFEs of interest (Step 6), information is collected to define the context in which the failures are most likely to occur. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in HFEs or unsafe actions. This information collection step discussed in Section E6.5.3.2.

Step 6: Search for HFE Scenarios (Scenarios of Concern)

An HFE scenario is a specific progression of actions with a specific context that leads to the failure of concern; each HFE is made up of one or more HFE scenarios. In this step, documented in Sections E6.5.3.3 and E6.5.3.4, the analyst identifies deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These unsafe actions make up an HFE scenario. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions.

Step 7: Quantify Probabilities of HFEs

Detailed HRA quantification methods are selected as appropriate for the characteristics of each HFE and are applied as explained in Section E6.5.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)
- ATHEANA expert judgment (Ref. E8.1.22).

There is no implication of preference in the order of listing these methods. They are jointly referred to as the "preferred methods" and are applied either individually or in combination as best suited for the unsafe action quantified. The ATHEANA (Ref. E8.1.22) expert judgment method (as opposed to the overall ATHEANA (Ref. E8.1.22) methodology that forms the framework and steps for the performance of this HRA) is used when the other methods are deemed to be inappropriate to the unsafe action, as is often the case for cognitive EOCs.

Appendix E.IV of this analysis explains why these specific methods were selected for quantification and gives some background on when a given method is applicable based on the focus and characteristic of the method.

All judgments used in the quantification effort are determined by the HRA team and are based on their own experience, augmented by facility-specific information and the experience of subject matter experts, as discussed in Section E4. If consensus can be reached by the HRA team on an HEP for an unsafe action, that value is used as the mean. If consensus cannot be reached, the highest opinion is used as the mean.

Step 8: Incorporate HFEs into the PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. The summary table of HFEs by group that lists the final HEP by basic event name provides the link between the HRA and the rest of the PCSA. This table can be found in Section E6.5.4.

E6.5.3.1 HFEs Requiring Detailed Analysis

The detailed analysis methodology, Sections E3.2.5 through E3.2.9, states that HFEs of concern are identified for detailed quantification through the preliminary analysis (Section E3.2.4). An initial quantification of the WHF PCSA model determined that there was one HFE in this group whose preliminary value was too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111. This HFE is presented in Table E6.5-2.

Table E6.5-2. Group #5 HFEs Requiring Detailed Analysis

HFE	Description	Preliminary Value
050-OpDPCShield1-HFI-NOW	Operator fails to properly shield DPC while installing canister lift fixture, leading to direct exposure	1E−03

NOTE: DPC = dual-purpose canister; HFE = human failure event.

Source: Original

E6.5.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the ATHEANA approach to detailed quantification is to identify and characterize factors that could create potential vulnerabilities in the crew's ability to respond to the scenarios of interest and might result in HFEs or unsafe actions. In this sense, the "vulnerabilities" are the context and factors that influence human performance and constitute the characteristics, conditions, rules, and tendencies that pertain to all the scenarios analyzed in detail.

These vulnerabilities are identified through activities including but not limited to the following:

1. The facility familiarization and information collection process discussed in Section E4.1, such as the review of design drawings and concept of operations documents

2. Discussions with subject matter experts from a wide range of areas, as described in Section E4.2

3. Insights gained during the performance of the other PCSA tasks (e.g., initiating events analysis, systems analysis, and event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the preparation operation that relate to potential human failure scenarios relevant to the HFE listed above. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during the preparation operation, but these have no bearing on this analysis.

E6.5.3.2.1 Operating Team Characteristics

Crew members—There are several crew members involved in the installation of the canister lift fixture. One predesignated crew member operates the platform shield plate. This crew member, referred to here as the shield plate operator, is trained as to when the shield plate must be opened or closed. When the operations require the shield plate to be moved, the crew member informs the other crew members on the platform that the shield plate is going to be moved. The other crew members confirm that the shield plate is in the proper position before continuing on to the next step of the operation. All crew members are expected to have the proper training commensurate with nuclear industry standards. This training is followed by a period of observation until the operator is proficient.

Radiation protection worker—The radiation protection worker is a fully certified health physics technician, whose job is to monitor radiation from the cask during movement. The radiation protection worker is responsible for stopping operations if high radiation levels are detected or if there is a situation that would lead to direct exposure.

E6.5.3.2.2 Operation and Design Characteristics

Preparation operations are slow and tedious, and they promote complacency.

The position of the shield plate is very visible. The shield plate is opened to place the canister lift fixture on the DPC, and it is then closed to bolt the fixture. The shield plate remains closed while the DPC is transferred to the Cask Unloading Room.

Shield Plate Operations—The shield plate has two modes: a normal travel mode (forward and reverse) and a jog mode (forward and reverse). The jog mode only allows the plate to move very slowly and in small increments. The shield plate operator uses the travel mode to move the shield plate completely over the cask port until it reaches the end stop. The jog function is then used for fine control of the shield plate to line up the shield plate with the bolt holes in the canister lift fixture. To open the shield plate, the shield plate operator again uses the normal travel mode until it reaches the end stop at the other end of the platform. Before opening or closing the shield plate, the shield plate operator ensures that the path of the shield plate is clear of personnel.

E6.5.3.2.3 Formal Rules and Procedures

Procedures—Formal procedures exist for these operations; however, there are no written, formal procedures that the crew has in front of them during these operations. Operators are trained in the operations, and their proficiency is attested to by the training staff. They perform the operations as a skill.

E6.5.3.2.4 Operator Tendencies and Informal Rules

Observation and Communication—The shield plate crew member communicates the actions to other crew members throughout this operation. The entire crew should be aware of the procedure and order of operations.

E6.5.3.2.5 Operator Expectations

Anticipatory Actions—The preparation process is simple but time consuming. There can be a tendency for the crew to focus on future tasks while preparing the DPC.

Consequences of Failure—The cask is not lifted in this step, and a shield plate is over the cask, so the threat of radiation release or physical injury is very low in this procedure. The crew expects failures to be relatively inconsequential, which promotes complacency in the operations.

E6.5.3.3 HFE Scenarios and Expected Human Failures (Step 6)

Given that the vulnerabilities that provide the operational environment and features that could influence human performance have been specified, then the HFE scenarios within this environment are identified. An HFE scenario is a specific progression of actions during normal operations (with a specific context) that lead to the failure of concern; each HFE is made up of one or more HFE scenarios. In accordance with the methodology, each scenario integrates the unsafe actions with the relevant equipment failures so as to provide the complete context for the understanding and quantification of the HFE.

The HAZOP evaluation is instrumental in initially scoping out the HFE scenarios, but they are then refined through discussions with subject matter experts from a wide range of areas, as described in Section E4.2.

Table E6.5-3 summarizes all of the HFE scenarios developed for the HFE in this group.

Table E6.5-3. HFE Scenarios and Expected Human Failures for HFE Group #5

HFE	HFE Scenarios
050-OpDPCShield1-HFI-NOW *Operator fails to properly shield DPC while installing canister lift fixture, leading to direct exposure*	HFE Scenario 1(a): (1) Shield plate crew member does not place shield plate entirely over the cask, or (2) crew fails to notice improper shield plate closure before approaching the shield plate. HFE Scenario 1(b): (1) Shield plate crew member opens shield plate while crew bolts canister lift fixture, or (2) crew fails to notice shield plate movement in time OR shield plate crew member fails to respond to warnings from crew.

NOTE: HFE = human failure event.

Source: Original

Since there is one HFE identified for detailed analysis in this group, the scenarios are organized under this HFE category, with the scenarios numbered as 1(a) and 1(b).

Each HFE scenario is in turn characterized by several unsafe actions, numbered sequentially as (1), (2), (3), etc. The Boolean logic of the HFE scenarios is expressed with an implicit AND connecting the subsequent unsafe actions and OR notation wherever two unsafe action paths are possible, as shown in Table E6.5-3.

The HFE scenarios summarized in Table E6.5-3 are discussed and quantified in detail below.

E6.5.3.4 Quantitative Analysis (Step 7)

Once the HFE scenarios and the unsafe actions within them are scoped out, it is then possible to review them in detail and apply the appropriate quantification methodology in each case that permits an HEP to be calculated for each HFE. Stated another way, each HFE is quantified through the analysis and combination of the contributing HFE scenarios. Dependencies between the unsafe actions and equipment responses within each scenario and across the scenarios are carefully considered in the quantification process.

This section provides a description of the quantitative analysis performed, structured hierarchically by each HFE category (identified by a basic event name); the HFE scenario; and then the unsafe actions under each scenario, as previously documented in Table E6.5-3.

Prior to the scenario-specific quantification descriptions, a listing is provided of the values used in the quantification that are common across many of the HFE scenarios.

In generating the final HEP values, the use of more than a single significant figure is not justified given the extensive use of judgment required for the quantification of the individual unsafe actions within a given HFE. For this reason, all calculated final HEP values are reduced to one significant figure. When doing this, the value is always rounded upwards to the next highest single significant figure.

E6.5.3.4.1 Common Values Used in the HFE Detailed Quantification

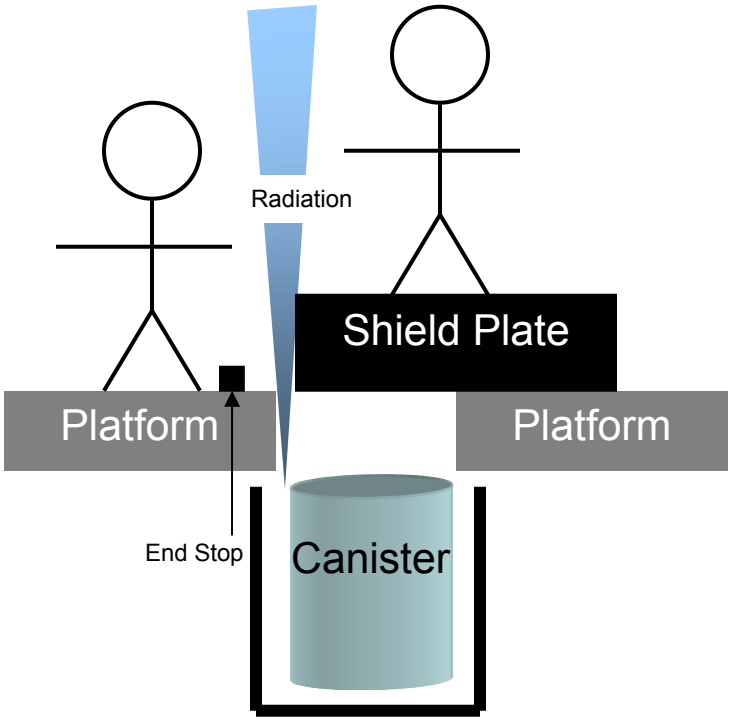
There are some mechanical failures that combine with unsafe actions to form HFEs. In general, these mechanical failures are independent of the specific HFE scenario, and so they can be quantified independently. These values are presented in this section.

Interlock Failures—There are a number of interlock failures in the HFE scenarios. While the status of these events can affect subsequent events in the scenarios in different ways, the likelihood of this event occurring is independent of the scenario. This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for an interlock, from Attachment C, Table C4-1, is approximately 2.7E−05 per demand.

Interlock fails to perform function = 2.7E−05

E6.5.3.4.2 Quantification of HFE Scenarios for 050-OpDPCShield1-HFI-NOW: Operator Fails to Properly Shield DPC while Installing Canister Lift Fixture, Leading to Direct Exposure

Figure E6.5-3 is an illustration of this failure scenario; this figure is not to scale. The DPC itself is shielded on top. The radiation of concern in this scenario is streaming from the small portion of the annulus which is not covered by the preparation platform. Because the shield plate is so visible and because the crew cannot access the canister to bolt the canister lift fixture to the DPC without the shield plate, the only scenarios considered in this analysis are those in which the shield plate is partially open; failure to close the shield plate entirely has been omitted from analysis.



Source: Original

Figure E6.5-3. 050-OpDPCShield1-HFI-NOW Operator Failure Scenario

E6.5.3.4.2.1 HFE Group #5 Scenario 1(a) for 050-OpDPCShield1-HFI-NOW

1. Shield plate crew member fails to cover cask entirely with shield plate.
2. Crew fails to notice improper shield plate closure before approaching the shield plate.

Shield Plate Crew Member Fails to Cover Cask Entirely with Shield Plate—After the canister lift fixture is placed on the DPC, the shield plate operator ensures that the platform area around the shield plate path is clear, announces that the shield plate is closing, and holds down the forward control of the shield plate until it hits the end stop. At that point, the shield plate operator stops moving the shield plate and informs the crew that they can begin their bolting

procedure. This process may have some degree of automation; however, to be conservative, this process is analyzed as if it is entirely manual. This is a simple manual action that the operator performs on a regular basis based on training.

The shield plate operator action of closing the shield plate until it hits the end stop is a simple manual action that the operator performs several times a day based on training. Operation of the shield plate is always the same. The end stop provides an indication, or feedback, that the shield plate has been appropriately moved. This error most closely corresponds to the task execution error NARA (Ref. E8.1.11) generic task type (GTT) A1, and it is adjusted by the following EPCs:

- GTT A1: Carry out a simple single manual action with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The assessed proportion of affect (APOA) anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This assessment appears reasonable for this task since the closure operation takes place in just minutes, so the APOA is set at 0.1.

$$\text{Shield plate crew member fails to cover cask entirely with shield plate} = 0.005 \times [(3-1) \times 0.1 + 1] = 0.006$$

Crew Fails to Notice Improper Shield Plate Closure before Approaching the Shield Plate— If the crew fails to notice that the shield plate is not entirely closed before they approach the shield plate to begin bolting operations, they can potentially get a direct exposure while getting onto the platform. The bolting crew has to get onto the shield plate in order to bolt the canister lift fixture. Part of their training is to visually confirm the shield plate position before approaching the plate. The shield plate, platform opening, and end stop are all easily visible from the preparation platform. This error most closely corresponds to the observation error CREAM (Ref. E8.1.18) cognitive function failure (CFF) O3, adjusted by the following CPCs with values not equal to 1.0.

- CFF O3: Observation not made. The baseline HEP is 0.003.

- CPC "Working Conditions": The crew is physically present with a good view of the area, which qualifies as advantageous. The CPC for advantageous working conditions for an observation task is 0.8.

- CPC "Adequacy of Training/Preparation": Training is adequate, with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Crew fails to notice improper shield plate closure before approaching the shield plate} = 0.003 \times 0.8 \times 0.8 = 0.002$$

This is the HEP if the action is completely independent on the part of the crew. However, there is a dependency between the shield plate operator's failure to close the shield plate properly and the crew's failure to notice based on a certain level of trust between the unbolting crew and their crewmate working the shield plate. In normal, low-consequence circumstances, this dependency might be considered "medium" or "high"; however, in this scenario, the crew is directly at risk if the shield plate operator fails, and thus more likely to actually perform the check. Therefore, this dependency was assessed to be "low." From THERP (Ref. E8.1.26) Table 20-21, item (a)(2), the revised probability of this unsafe action follows:

Crew fails to notice improper shield plate closure
before approaching the shield plate = 0.05

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.5-4.

Table E6.5-4. HEP Model for HFE Group #5 Scenario 1(a) for 050-OpDPCShield1-HFI-NOW

Designator	Description	Probability
A	Shield plate operator fails to cover cask entirely with shield plate	0.006
B	Crew fails to notice improper shield plate closure before approaching the shield plate	0.05

Source: Original

The Boolean expression for this scenario follows:

$$A \times B = 0.006 \times 0.05 = 0.0003 \quad \text{(Eq. E-1)}$$

E6.5.3.4.2.2 HFE Group #5 Scenario 1(b) for 050-OpDPCShield1-HFI-NOW

1. Shield plate crew member opens the shield plate while the crew bolts the canister lift fixture.

2. The crew fails to notice the shield plate movement in time OR the shield plate crew member fails to respond to warnings from the crew.

Shield Plate Crew Member Opens Shield Plate while Crew Bolts Canister Lift Fixture— While it is likely that the entire crew involved in cask preparation is trained in proper shield plate operations, during normal cask preparation operations, the only crew member authorized to open the shield plate is the predesignated shield plate operator. The shield plate operator is trained to ensure that the shield plate and shield plate path are cleared of personnel before moving the shield plate. Also, there is a direct view of the entire shield plate path from the shield plate control location.

The shield plate is not supposed to be moved again during cask preparation activities once the canister lift fixture has been placed on the DPC. The only operations that occur after the canister lift fixture is emplaced and the shield plate is closed are bolting of the fixture and then movement of the CTT to the Cask Unloading Room. Neither of these actions requires actions that can be

confused with the actions that correspond to operating the shield plate; bolting requires tools, and CTT movement is not done from the platform.

Once the canister lift fixture is placed on the DPC and the shield plate is closed, the shield plate is not supposed to be opened for the remainder of the operations. Therefore, this error is an EOC. The crew who are on the shield plate bolting the canister lift fixture would immediately notice that the shield plate was moving and would signal the person committing this error to stop. THERP (Ref. E8.1.26) Table 20-12 describes several EOCs. None of these errors, however, appropriately describes this error. EOCs described in THERP (Ref. E8.1.26) primarily refer to actions where the operator intends to perform an action (e.g., flip a switch or turn a knob) but performs a different action (e.g., flips the wrong switch or turns the knob the wrong way). In this case, none of crew members would be performing an action similar to opening the shield plate during this step. They would only be installing bolts in the canister lift fixture. The most appropriate error that corresponds with this HFE was determined to be the task execution error NARA (Ref. E8.1.11) GTT A5, adjusted by the following EPCs:

- NARA GTT A5: Task execution. Completely familiar, well-designed, highly practiced routine task performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001. While this error is not a task execution error (because there is no task being performed) this error was considered the most appropriate because it describes the operations the best. This value is considered to be conservative when applied to this failure because there is no task being performed in this step.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. This EPC is applicable in its full effect because the whole set of cask preparation activities is slow and tedious, and the operator could get bored and distracted and believe it is time to open the shield before the workers are completely clear. This is the only relevant EPC, and the APOA is set at 1.0.

Using the NARA (Ref. E8.1.11) HEP equation yields the following:

$$\text{Shield plate crew member opens shield plate while crew bolts canister lift fixture} = 0.0001 \times [(3-1) \times 1.0 + 1]) = 0.0003 \quad \text{(Eq. E-2)}$$

Crew Fails to Notice Shield Plate Movement in Time—During this portion of the operation, there are several people on the shield plate bolting the fixture with long reach tools that go through the shield plate. If the shield plate is inadvertently opened, these crew members would notice and provide immediate feedback to the person operating the plate. The crew would have roughly 30 seconds to notice and try to warn the shield plate operator. If they failed to notice the movement or did not realize what it meant, they would be exposed.

The crew works on the platform and stands on the shield plate or very close to it. Their reaction to it is a very simple response to a very obvious indicator; in this case the indicator is movement of the shield plate. This would be very obvious to the workers present, and they would have on

the order of 30 seconds to react. While the NARA task execution error GTT C1 is primarily applicable to response to indicators in a control room, it is seen as the most applicable failure mode to this scenario because the basic action is, again, a very simple response to a very obvious indicator. Specifically, the portions of the description of GTT C1 related to "simple diagnosis required" and "response must be direct execution of simple actions" were considered applicable to this action. The other human failure quantification option for this action might be CREAM generic failure type I3 for "delayed interpretation"; however, the CREAM CPCs did not allow the influence of unfamiliarity to be fully addressed. Therefore, it is considered that NARA GTT C1 captures both the observation and interpretation characteristics of the action, adjusted by the following EPCs:

- GTT C1: Simple response to a range of alarms or indications providing clear indication of situation (simple diagnosis required). The baseline HEP is 0.0004.

- EPC 2: Unfamiliarity (a potentially important situation that occurs infrequently or is novel). The full affect EPC would be ×20, which applies to a rare event not covered in training, but procedures exist. The APOA anchor for 0.5 is for a rare event covered once per year in training. The APOA anchor for 0.1 is for a rare event covered in regular training. Other considerations for a reduction from full affect is something rarely practiced but easy to carry out and for which the crew has some familiarity. This is covered in regular health physics training and in health physics procedures. Proper health physics practices and the importance of shielding is emphasized in the training. It appears reasonable for this task that the APOA be set at 0.1.

- EPC 3: Time pressure. The full affect would be ×11, which applies if, in order to complete the required task, the operator would have to complete each task step correctly and as quickly as possible. The anchor example for the full effect of this EPC being applied (APOA of 1.0) is "just enough time to complete the task when working as quickly as possible," while an APOA of 0.5 is anchored with "operator must work at a fast pace with reduced time for checking." It was considered that the time would not be a full effect but more than half effect and was therefore assessed at an APOA of 0.7.

Using the NARA (Ref. E8.1.11) HEP equation yields the following:

$$\text{Crew fails to notice shield plate movement in time} = 0.0004 \times [(20-1) \times 0.1 + 1] \times [(11-1) \times 0.7 + 1] = 0.01 \quad \text{(Eq. E-3)}$$

Shield Plate Crew Member Fails to Respond to Warnings from Crew—If the crew realized what was happening, they would need to get the attention of the operator in some manner. Their only means of communication is verbal, without the aid of any communication devices. They would need to be heard over the noise of the machinery in the preparation area. The plate control is in direct view of the shield plate, and the operator has roughly 30 to 60 seconds to stop moving the shield plate before a potential direct exposure can occur. If the operator fails to do so, the workers would not have sufficient time to avoid exposure.

The shield plate crew member is on the floor near the platform and is unlikely to be looking up at the workers on the platform, in particular because at this point the shield plate crew member is in

the process of opening the shield plate and expects that no one is on the platform. There is machinery noise from the platform and other things in the preparation area like the CTT. The other members of the crew are trying to communicate the error to the shield plate crew member verbally. The action itself (stopping the shield plate) is very simple, and there is plenty of time to execute it once the need is recognized. This error most closely corresponds to the communication error NARA (Ref. E8.1.11) GTT D1, adjusted by the following EPCs:

- GTT D1: Verbal communication of safety-critical data. The baseline HEP is 0.006.
- EPC 4: Low signal-to-noise ratio. This usually pertains to competing data or signals that obscure the most important ones, but it can also mean masking of the important information by other types of distractions. In this case, the masking affect is the abundance of machine noise and the distance between the crew on the platform and the crew member on the floor. The full affect EPC would be ×10, which applies to a required signal being highly masked (such as when there is a proliferation of other signals). Given the level of noise that is expected and the difficulty in communicating above it, it appears reasonable for this task that the APOA be set at 1.0.

Using the NARA (Ref. E8.1.11) HEP equation yields the following:

$$\text{Shield plate crew member fails to respond to warnings from crew} = 0.006 \times [(10-1) \times 1.0 + 1]) = 0.06 \quad \text{(Eq. E-4)}$$

Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.5-5.

Table E6.5-5. HEP Model for HFE Group #5 Scenario 1(b) for 050-OpDPCShield1-HFI-NOW

Designator	Description	Probability
A	Shield plate crew member opens shield plate while crew bolts canister lift fixture.	0.0003
B	Crew fails to notice shield plate movement in time.	0.01
C	Shield plate crew member fails to respond to warnings from crew.	0.06

Source: Original

The Boolean expression for this scenario follows:

$$A \times (B + C) = 0.0003 \times (0.01 + 0.06) = 2E{-}5 \quad \text{(Eq. E-5)}$$

E6.5.3.4.2.3 HEP for HFE 050-OpDPCShield1-HFI-NOW

The Boolean expression for the overall HFE (all scenarios) follows:

$$\text{HFE 050-OpDPCShield1-HFI-NOW} = \text{HEP 1(a)} + \text{HEP 1(b)} = 0.0003 + 2E{-}5 = 0.00032 \sim 0.0004 \quad \text{(Eq. E-6)}$$

E6.5.4 Results of Detailed HRA for HFE Group #5

The final HEPs for the HFEs that required detailed analysis in HFE Group #5 are presented in Table E6.5-6 (with the original preliminary value shown in parentheses).

Table E6.5-6. Summary of HFE Detailed Analysis for HFE Group #5

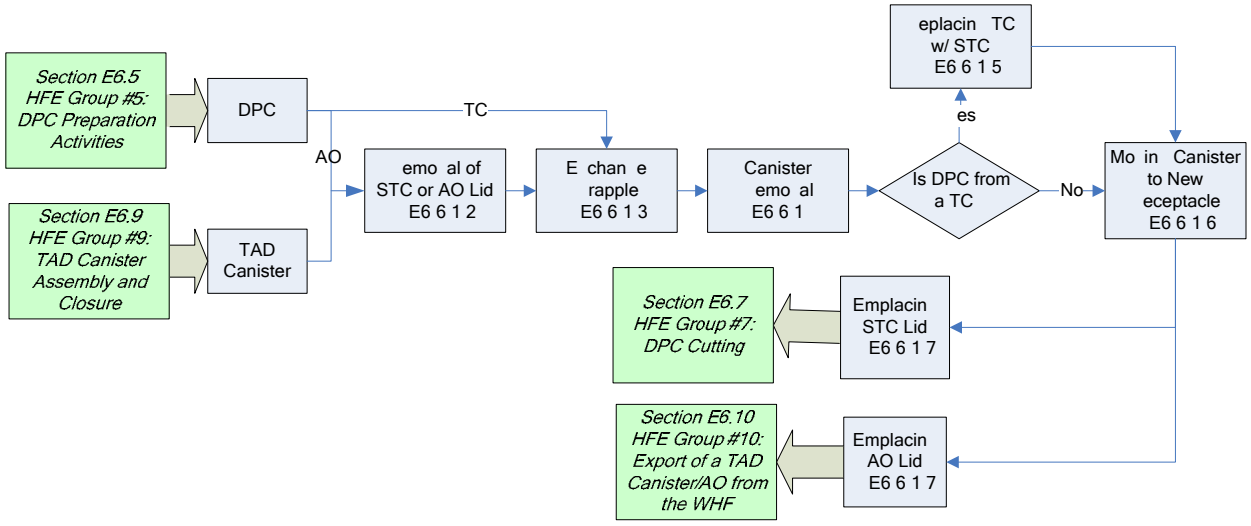
HFE	Description	Final Probability
050-OpDPCShield1-HFI-NOW	Operator fails to properly shield DPC while installing canister lift fixture, leading to direct exposure.	4E−04 (1E−3)

NOTE: DPC = dual-purpose canister; HFE = human failure event.

Source: Original

E6.6 ANALYSIS OF HUMAN FAILURE EVENT GROUP #6: CTM ACTIVITIES: TRANSFER A CANISTER WITH THE CANISTER TRANSFER MACHINE

HFE group #6 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering CTM operations. The overall process associated with these operations is graphically depicted in Figure E6.6-1, which shows how various waste forms are moved by the CTM from their initial to their final destinations.



NOTE: AO = aging overpack; DPC = dual-purpose canister; HFE = human failure event; STC = shielded transportation cask; TAD = transportation, aging, and disposal (canister); TC = transportation cask; WHF = Waste Handling Facility.

Source: Original

Figure E6.6-1. Activities Associated with HFE Group #6

The activities covered in this HFE group begin with a canister in position aligned with a port, ready to be lifted with the CTM. The canister could be in a transportation cask, an aging overpack, or an STC. The operation continues through the tasks of opening the port gate above the canister, removing the canister with the CTM, moving the CTM to the receiving port gate, and placing the canister in the appropriate vessel. Depending on where the canister came from and where it is headed, the vessel could be an aging overpack or STC. This operation ends when the canister has been placed in the vessel, the CTM has been withdrawn, the port gate has been closed, and the canister is ready to move out from under the transfer port.

E6.6.1 Group #6 Base Case Scenario

There are three variations with two loading possibilities for the Group #6 base case scenario:

1. Move DPC from aging overpack to STC
2. Move DPC from transportation cask to STC
3. Move TAD canister from STC to aging overpack.

Loading configurations:

1. STC with DPC
2. Aging overpack with TAD canister.

E6.6.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #6 activities:

1. From transportation cask—The transportation cask is secure in the CTT and is positioned under the cask port in the Cask Unloading Room; the transportation cask has the cask lid removed and a DPC lift fixture attached to the DPC. There is an STC with its lid removed stationed in the preparation area.

2. Transfer of DPC from aging overpack—The empty STC is stationed under the Cask Unloading Room port, secured, with the lid removed; for transfer from a transportation cask, the empty STC is in the preparation area with the lid removed.

3. Transfer of TAD canister from STC to aging overpack—The STC is sitting in the Cask Unloading Room on a CTT, with its lid unbolted; the aging overpack is pre-staged, with its lid off, in the Loading Room, positioned and secured under the cask port on a site transporter.

4. CTM operations are performed remotely from the WHF Control Room unless otherwise specified.

6. The CTM has the following safety features and hardwired interlocks:

    A. Vertical movement and upper limit—The CTM is raised and lowered with the use of an ASD. The ASD has at least three settings: one for lift of canisters, one for lift of objects that do not fit inside the bell (e.g., cask lid), and a maintenance mode. The operator selects the setting and uses the controller to raise the hoist until it automatically stops at the selected setting height.

        1) For the canister mode, the ASD automatically stops once the canister clears the bottom of the bell. There is also an optical sensor at the bottom of the bell that, once cleared, stops the hoist and erases the lift command (i.e., can only lower the hoist).

        2) For the object mode, the ASD automatically stops the hoist once it clears the port gate. The operator can potentially restart the lift operation and further lift the object.

        3) The maintenance mode is fully manual; the ASD does not stop the lift.

        4) Above the ASD stop point is an upper limit switch that, when reached, stops the hoist from lifting. This first limit switch (final hoist lower limit)

effectively erases the lift command. The hoist still has power, but the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (i.e., the final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

B. Horizontal movement and port alignment—There is a visually based system that aligns the CTM with the canister such that the grapple can properly engage a canister. The form of this system may use a scheme as simple as laser/target alignment or a more complex system including image recognition software coupled with PLCs. Likewise, horizontal movement and final alignment of the CTM with the cask ports could potentially be a highly automated process. However, to be conservative, the manual horizontal movement process is analyzed here, generically relying on a visual alignment system and camera for alignment confirmation.

C. There is an interlock between the CTM shield skirt and the port gate that requires the shield skirt to be lowered in order for the port gate to open. If an automated system is used, the CTM alignment is based on a coordinate system, and the CTM would not be able to move at all if the port gate were open. However, if the process is manual, to get exact alignment, the CTM needs a "jog" feature that allows the CTM to move in small increments while the shield skirt is lowered. There is also a maintenance bypass for this interlock.

D. There is an interlock between the CTM bridge and trolley travel and the shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.

E. There is an interlock between the slide gate and shield skirt; the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed for maintenance.

F. There are interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded.

G. There are speed limiters designed into the motors.

H. There are end-of-travel interlocks on the trolley and bridge.

I. There are anti-collision interlocks on the CTMs for the WHF.

J. There is a weight interlock that cuts off power to the hoist when the crane capacity is exceeded.

K. There is an interlock that prevents CTM canister grapple (primary grapple) operation if the grapple is not properly connected to the hoist.

L. There is an interlock between the grapple engagement/position (fully engaged or fully disengaged) and hoist movement. The secondary grapple has the same interlock that is enabled when the power is connected to the grapple.

M. The CTM is mechanically or electrically prevented from inadvertent canister disengagement.

N. The following grapples are associated with these CTM activities:

1) Lid grapple (for transportation cask, aging overpack, and STC lids)

2) DPC canister and TAD canister grapple—The DPC and TAD lift fixtures use the same grapple.

O. It is expected that if the wrong grapple is used, the grapple designs preclude partial or full engagement (i.e., the wrong grapple would be too big, too small, or otherwise mechanically incompatible with the fixture).

P. Grapple installation—When the design is finalized, one option under consideration is that an automatic system would be used to remove and attach the grapples. It is expected that such a system would be more reliable than a local manual process. This analysis retains the local manual process so that compliance can be demonstrated without the automatic system.

6. The shield door is normally closed. There is an interlock between the port slide gates and the shield doors; the port slide gate cannot be opened when the shield doors are also open.

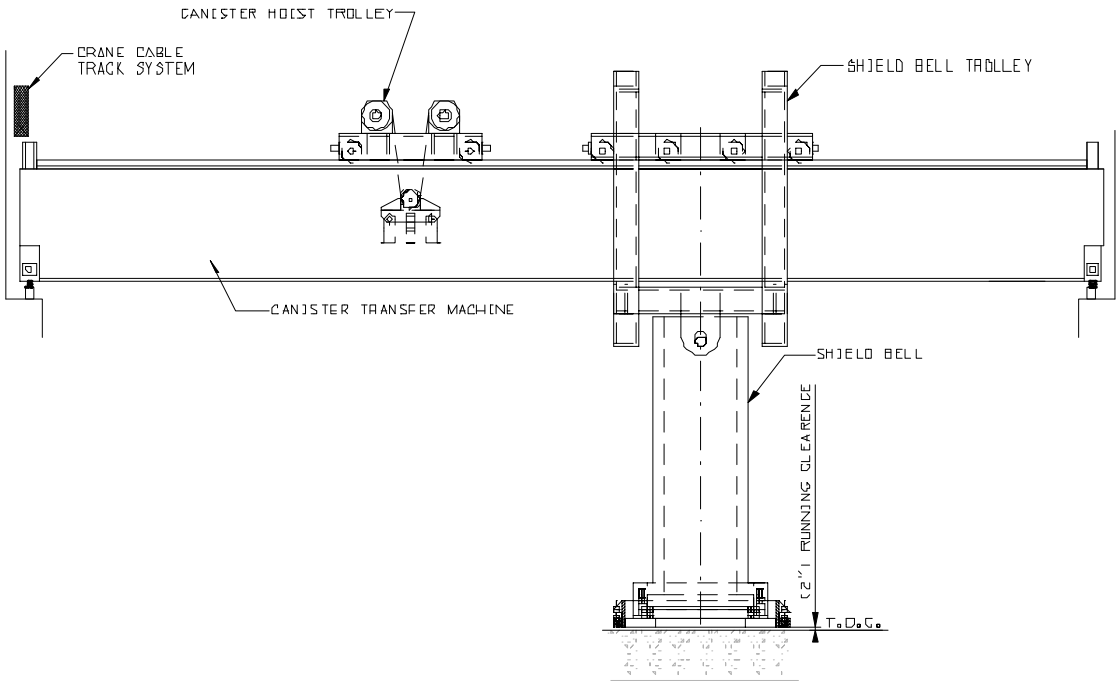
7. There are interlocks that prevent the port slide gate from opening if there is not a cask underneath the port gate.

The following personnel are involved in this set of operations:

- CTM operator
- Crew members (two people)
- Supervisor.

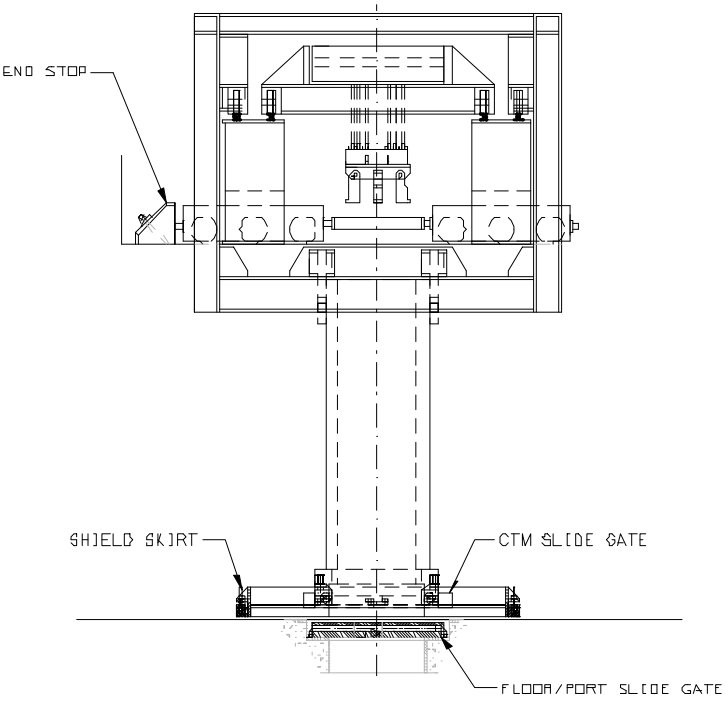
Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

Figure E6.6-2 and Figure E6.6-3 are simple diagrams illustrating the CTM.



Source: Modified from *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. E8.1.6).

Figure E6.6-2. Canister Transfer Machine—Side View



Source: Modified from *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. E8.1.6).

Figure E6.6-3. Canister Transfer Machine—End View

E6.6.1.2 Removal of STC or Aging Overpack Lid with CTM (for TAD Canister or DPC/Aging Overpack)

Proper Grapple Installation—The CTM operator moves the CTM to the CTM maintenance area (Canister Transfer Room floor), where a crew member manually takes off and stores the grapple attached to the CTM (i.e., canister grapple) and replaces it with the lid grapple. The CTM operator also ensures that the ASD is set to the appropriate setting to lift the canister.

Moving CTM to Cask Port—The CTM operator uses a visual alignment system and a camera to position the CTM, with the lid grapple, over the cask port. There is a position indicator, along with a camera view, so the operator knows when the CTM is in position.

Opening CTM Slide Gate and Port Slide Gate—The CTM operator remotely lowers the skirt shield, opens the CTM slide gate, and opens the cask port slide gate once the CTM is in place.

Lifting Cask (STC or Aging Overpack) Lid into CTM and Slide Gate Closure—The operator first sets the ASD to lid lift mode and then lowers and engages the lid grapple; the grapple does not lower unless the slide gate is open and the skirt is lowered. Grapple engagement is manual and is verified visually via camera and an indicator. Once the grapple is engaged and verified, the operator then lifts the cask lid up to the bottom of the CTM bell just past the CTM slide gate. At this point the operator closes the port and CTM slide gates.

Moving CTM to STC or Aging Overpack Lid Station and Lowering Lid to Lid Station—The CTM operator lifts the CTM skirt and moves the CTM with lid to the lid station. Once at the lid station, the operator lowers the lid, disengages the grapple, lifts the grapple, resets the ASD to canister lift setting, closes the slide gate, and lifts the skirt. A camera is used to ensure that the lid is staged in the proper location.

E6.6.1.3 Exchange Grapple (All Variations)

The CTM operator moves the CTM to the CTM maintenance area (Canister Transfer Room floor), where a crew member manually takes off and stores the grapple attached to the CTM and replaces it with the canister grapple. The CTM operator also ensures that the ASD is set to the appropriate setting to lift the canister.

E6.6.1.4 Canister Removal

Moving CTM to Cask Port—The CTM operator uses a visual alignment system and camera to position the CTM, with canister grapple, over the cask port. There is a position indicator, along with a camera view, so the operator knows when the CTM is in position. Once in position, the CTM operator then lowers the shield skirt.

Opening CTM Slide Gate and Port Slide Gate—Once the CTM is in position over the cask port, with the shield skirt lowered, the CTM operator remotely opens the CTM slide gate and the cask port slide gate.

Lifting Canister into CTM—The CTM operator again looks at the relative canister and hoist position and adjusts the alignment if necessary to ensure that the CTM is over the canister. This final adjustment is done with the alignment system, in conjunction with a camera view. Once the CTM is appropriately aligned to the canister, the operator lowers the canister grapple and engages the canister. Grapple engagement is automatic, but it is verified visually via camera and an indicator. The operator then lifts the canister by holding down a controller (i.e., joystick) until the ASD automatically stops the lift.

Closing CTM Slide Gate and Port Slide Gate—Once the canister is raised inside the bell, the operator closes the CTM slide gate, closes the port slide gate, and lifts the CTM skirt in preparation for movement.

E6.6.1.5 Replacing Transportation Cask with STC (DPC/Transportation Cask Only)

In the single case of transferring a DPC from a transportation cask to an STC, the crew must move the empty transportation cask from the Cask Unloading Room into the preparation area, replace the transportation cask on the CTT with a STC, and move the STC on the CTT back into the Cask Unloading Room. This swap of casks is done while the canister is inside the CTM bell with the slide and port gates closed. This is accomplished as follows:

- **Move Empty Transportation Cask from Cask Unloading Room to Preparation Area**—The crew opens the door, plugs in the air hose, moves the CTT through the door, closes the door, and moves the CTT to the cask preparation area. There, the crew uses the cask handling crane to remove the empty transportation cask from the CTT, places

the proper pedestal in the CTT, and places and secures an empty STC, with an unbolted lid, on the CTT.

- **Move Empty STC to Cask Unloading Room**—To do this, the crew moves the CTT to the Cask Unloading Room door, opens the shield door, moves the CTT through the door and into position under the cask port, disconnects the air hose, and closes the door. The crew then removes and stores the STC lid using the CTM maintenance crane.

The STC is now in position to receive the DPC removed from a transportation cask as described in Section E6.6.1.4.

E6.6.1.6 Moving Canister to New Receptacle (All Variations)

Moving CTM to Destination Port—The CTM operator moves the CTM to the appropriate port. The operator uses a visual alignment system and camera to position the CTM over the cask port. There is a position indicator, along with a camera view, so the operator knows when the CTM is in position. Once in position, the CTM operator then lowers the shield skirt.

Opening CTM Slide Gate and Port Slide Gate—The CTM operator then opens the CTM slide gate and the port slide gate.

Lowering Canister—Once the port gate is open, the operator verifies alignment using a visual alignment system in conjunction with a camera view; if not properly aligned, the CTM operator makes fine adjustments to the CTM position until alignment is verified. The operator then lowers the canister into position in the STC or aging overpack, disengages the grapple, verifies disengagement (via camera and indicator), and then retracts the grapple.

Closing CTM Slide Gate and Port Slide Gate—Once the grapple is raised, the operator closes the port slide gate and the CTM slide gate and lifts the CTM skirt in preparation for movement.

E6.6.1.7 Preparing Aging Overpack or STC to Leave Cask Loading/Unloading Room

Grapple Exchange—The CTM operator moves the CTM to the CTM maintenance area, where a crew member removes the canister grapple and attaches the lid grapple. The operator then closes the slide gate and lifts the skirt. The CTM operator also sets the ASD to the proper setting for moving the aging overpack or STC lid.

Installing Aging Overpack Spacer (if Required)—For TAD canisters placed into an aging overpack, a spacer may be required. Once the skirt is lifted, the CTM operator retrieves the aging overpack spacer, moves the CTM to the aging overpack, lowers the shield skirt, opens the port and CTM slide gates, and lowers the hoist. Once the spacer is in place, the CTM operator disengages the grapple, retracts the hoist, closes the CTM port and slide gates, and lifts the shield skirt for movement.

Moving CTM to Aging Overpack or STC Lid Station and Retrieving Lid—Once the skirt is lifted, the operator moves the CTM and positions it over the aging overpack or STC lid station. The operator then lowers the grapple, engages the grapple, verifies the engagement (via camera and indicator), and lifts the lid.

Moving CTM to Cask Port—The CTM operator positions the CTM, with lid, over the aging overpack or STC cask port and lowers the skirt. The operator uses a visual alignment system in conjunction with a camera view to ensure alignment with the port.

Opening Cask Port Slide Gate and Placing Lid on Aging Overpack or STC—Once the skirt is lowered, the operator remotely opens the cask port slide gate, confirms alignment (via the visual alignment system and camera), and lowers the lid into position. The CTM operator then disengages the grapple, verifies that the grapple is disengaged (via indicator and camera), and retracts the grapple.

Closing Cask Port Slide Gate—Once the grapple is retracted, the operator remotely closes the cask port slide gate.

E6.6.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during canister transfer with the CTM are summarized in Table E6.6-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCTMdrop001-HFI-COD	*Operator Drops Object onto Canister during CTM Operations*: Some variations of CTM activities require heavy objects to be move over the canister. STC and AO lids are removed and installed. It is possible that these objects can be dropped onto the canister while being lifted with the CTM.	13	2E−03	In this step, the operator can potentially drop the aging overpack or STC lid onto the TAD canister or DPC. There are several ways for this failure to occur, including the following: • Operator fails to fully engage/disengage the grapple before lifting hoist (partial engagement of grapple). There is an indicator and camera view by which the operator is required to verify engagement. There is also an interlock that does not allow the hoist to move unless the grapple is fully engaged or fully disengaged. This interlock does not have a bypass. • Operator fails to properly connect the grapple to the CTM when switching grapples. • Operator lifts the lid with the CTT significantly misaligned with the cask port. This can cause part of the lid to be caught under the second floor; if the CTM keeps pulling, the cable can snap, and the lid can drop. There are several electromechanical safeguards preventing this, including load cell interlock, motor temperature interlock, and the cable design. (A similar failure can occur if the CTM is moved with an object below the floor; however, this event is treated separately in 050-OpCTMImpact1-HFI-COD.) • Operator lifts the object too high. The only object that is lifted over a canister is the lid. The bell is flared at the bottom to accommodate the cask lid; if the operator puts the ASD in maintenance mode or sets it in canister mode, the operator can lift the lid until it hits the inside of the bell. If the operator continues trying to lift, the cable can snap, causing the lid to drop onto the canister. There are several electromechanical safeguards preventing this, including load cell interlock, motor temperature interlock, and the cable design. The preliminary value was chosen based on the determination that this failure is “highly unlikely” (0.001) and was adjusted because there are several ways for a drop to occur and, because the operation is performed remotely, this is a somewhat complex process (×2), as opposed to an extremely complex process (which would be ×3). This HFE was assessed to be less likely than a cask impact or a railcar collision, and, indeed, the preliminary value reflects this.
050-OpCTMdrop002-HFI-COD	*Operator Causes Drop of Canister during CTM Operations*: All variations of CTM activities require the canister to be lifted and transferred to a new receptacle. During this lift, the operator can drop the canister (e.g., by improper grapple engagement).	13	2E−03	Moving a canister with the CTM is very similar to moving an object (050-OpCTMdrop001-HFI-COD) with the CTM during cask transfer, and it has the same failure modes. The only difference between moving a canister and moving an object (specifically, the lid) is that a canister drop due to lifting too high results in a high drop (two-block) as opposed to a design-limit drop; this drop is analyzed separately. Also, for transportation cask/DPCs, the canister is not moved horizontally but rather suspended for a period of time and then lowered back into the same room. The analysts could not find any additional human failure modes for dropping a canister while the canister is suspended, and the failure modes associated with horizontal travel are not applicable to the transportation cask/DPC. Therefore, it was considered conservative to assign the same preliminary value to this HFE for all canister types.
050-OpCTMDrInt01-HFI-COD	*Operator Lifts Canister too High with CTM*: It is possible that, while lifting objects such as the canister or cask lid, the operator can cause a two-block by lifting the object to high.	13	1.0	When lifting the canister, the operator can lift it too high, resulting in a two-block event and drop of the canister. In order to accomplish this, the interlocks (e.g., optical sensor) and other anti-two-block equipment (e.g., limit switches) must also fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0
050-OpNoUnBolt00-HFI-NOD	*Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tipover*: If the operators fail to remove all or some of the lid bolts from the AO or STC, when they attempt to remove the cask lid with the CTM, the load is significantly heavier than the CTM is rated for, and the result could be a drop of the cask.	13	1E−03	If the lid bolts were not all removed during preparation activities and the CTM operator does not notice, one of two things may happen: the operator attempts to lift the cask and the bolts break, or the CTM operator attempts to lift the cask and the bolts hold. If the bolts hold, the load cell stops the CTM from lifting before the cask can be lifted. The load cell interlock is never bypassed. For this failure to occur, the preparation crew must fail to remove all the bolts and must fail to verify on the checklist that all the bolts have been removed. Independently, the CTM operator would also have to fail to notice that the entire cask is lifting as the operator tries to lift the lid into the CTM. This failure was assessed to be “highly unlikely” (0.001) because it involves two human failures by different teams and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001.
050-OpNoUnBoltDP-HFI-NOD	*Operator Fails to Remove Lid Bolts, Resulting in Impact, Drop, or Tipover (DPCs)*	13	N/A	There is no lid on transportation casks containing a DPC; therefore, this failure mode was omitted from analysis for those canisters.

Table E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCTMImpact1-HFI-COD	*Operator Moves the CTM while Canister or Object is below or between Levels*: If the operator moves the trolley before the canister has cleared the port gate, then the canister can impact the floor if the canister is between levels. If the canister or the lid is completely below the floor, this failure can result in the cable snapping and the canister or object dropping. For canisters, the shear event (movement while the canister is between floors) is the bounding event.	13	1E−03	The operator can inappropriately move the CTM while the canister or lid is below the port gate or while the canister is between levels. If this inadvertent movement occurs while the canister is between levels, it can result in an impact and shear force to the canister. If the movement occurs while the canister is below the port gate, then the cable can snap, resulting in a drop. In order to accomplish this inadvertent movement, the operator would have to fail to follow proper lifting procedure and operate the ASD in manual or lid lift mode. If the operator performs the lift in manual mode, then the operator can fail to lift the canister or object high enough to clear the floor before starting horizontal movement. If it were in lid lift mode, it would automatically stop too soon, but the operator would have to fail to notice that the canister was not high enough when closing the port and CTM slide gates on the canister. For a canister, the operator would also have to fail to rely on the optical sensor, and the operator must also fail to close the slide gate to accomplish this HFE. There are interlocks, such as the load cell interlock, that prevent the CTM from exerting enough force to snap the cable and drop the canister or object. There is also an interlock that prevents horizontal motion if the slide gate is not closed. Due to the complicated nature of this failure, the interlock was not separately modeled for this HFE. Rather, it was included in the preliminary value. This failure was considered highly unlikely and accordingly assigned a preliminary value of 0.001.
050-OpClCTMGate1-HFI-NOD	*Operator Inappropriately Closes Slide or Port Gate during Vertical Canister Movement and Continues Lifting*: If the operator signals the CTM slide gate or port gate to close while the canister is being raised, it can result in a canister impact if the door closes on the canister or in a canister drop if the door closes on the host, severing the cables. The gate motors are required to be sized such that they cannot damage the canisters; the gate cannot sever the cables either. This failure can, however, result in a drop if the operator closes the slide gate on the cables and continues hoisting such that the canister is stuck and the cable snaps.	13	1E−03	In this operation, the CTM operator is lifting and lowering the canister. The slide gate cannot damage the canister or sever the hoist cables, so the failure required here is for the operator to prematurely close the slide gate and keep hoisting such that the canister catches on the slide gate, and the hoist cable snaps. There are two slide gates for each motion: the CTM slide gate and the cask/waste package port slide gate. The operator performs CTM operations daily and has a camera view of the operations. There is no interlock to prevent this error, but if the canister is lifted per the procedure, the operator uses the ASD and does not close the gate until the ASD has stopped. It is unlikely the operator would try to close the slide gate while also lifting the canister; the most likely scenario is for the operator to fail to lift the canister high enough, close the slide gate as if to move the CTM, and then notice that the canister is too low and try to lift the canister without first opening the slide gate. In order for the operator to fail to lift the canister high enough, the ASD has to have a mechanical failure or the ASD has to be in the wrong mode. The manual mode is only accessible by entering a password. Because lifting is a slow procedure, it is unlikely that the operator would, even if it were possible, put the ASD in manual mode. If the operator did so, it is unlikely that the operator would stop the canister too soon because, independent of the ASD, the optical sensor in the bell stops the canister once it has cleared the bell. The more likely case is that the operator would fail to restore the ASD to canister lift mode after moving the lid. For all waste forms except the transportation cask/DPC, the lid is removed in the previous step. If the operator does fail to change ASD mode, the operator must also fail to visually verify the height of the canister before closing the slide gate. In either case, if the operator does stop the canister too soon and closes the slide gate, the operator would still have to forget to reopen the slide gate before resuming the lift in an attempt to correct the error. This failure was assessed to be “highly unlikely” (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001.
050-OpCTMImpact2-HFI-COD	*Operator Causes Canister Impact with Lid during CTM Operations*: The STC/AO lid, when removed by the CTM, is staged such that the canister must travel over it to move to the new receptacle. If the lid is improperly stowed, the CTM can collide with the lid. This failure mode is not applicable to TC/DPCs because the cask lid is removed in the preparation area.	13	N/A	The lid staging area is in the pathway of the CTM; if the lid is improperly stored, the CTM, carrying a canister, can potentially impact the lid. This failure was omitted from analysis because, if the lid were stored such that it was an obstruction to the CTM, the CTM would run into the lid as it returns to the cask from lid staging. At that point, the error would have to be corrected before operations continued.
050-OpCTMImpact5-HFI-COD	*Operator Causes Canister Impact with SSC during CTM Operations (All)*: If the CTM is moved too far while transferring a canister, it can collide into an end stop and impact the inside of the CTM bell or hit an SSC.	13	1.0	In this step, the operator can potentially impact the canister in several ways: • CTM bridge impacts end stops while moving canister • CTM trolley impacts end stops while moving canister. In order to accomplish any of these, however, additional equipment failures must also occur. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.

Table E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpDirExpose1-HFI-NOD	*Operator Causes Direct Exposure during CTM Activities (First Floor, All CTM Movements)*: If an operator were to inadvertently open the shield door and enter the Cask Unloading Room while the canister was being lifted out of the cask, the operator would get a direct exposure.	29	1E−01	Direct exposure during CTM activities can happen if an operator inadvertently opens the shield door to the Canister Transfer Room while the canister is being lifted. In order to accomplish this scenario, an interlock must also fail. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. As was previously discussed, the HRA team has generally assigned unsafe actions that are combined with interlocks an HEP of 1.0. As was also discussed, if this very conservative approach did not demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1), then the HRA team would consider whether a lower preliminary value was justified. That is the case here. In further considering this event, it would be very difficult to make it happen. An extraordinary bypass of the interlock would be required or a random failure of the interlock. Then, a worker would have to violate all administrative controls and training and attempt to enter the room without appropriate clearance from the Central Control Center. To a large extent, all of these things are independent because they are unsafe actions by different individuals doing different things at different times. Therefore, the HRA team feels justified in assigning a lower preliminary value of 0.1 to the unsafe action (still believed to be quite conservative), which in combination with the interlock failure value results in an overall value of 3E−6/demand for an exposure.
050-OPCTMDirExp1-HFI-NOD	*Operator Causes Direct Exposure during CTM Activities (Second Floor, All CTM Movements)*: If the CTM operator fails to close the port gate before lifting the shield skirt after placing a canister in a receptacle (e.g., AO, STC) and a worker violates the procedural control by entering the Canister Transfer Room during canister transfer activities, that worker would be exposed.	29	1E−04	Closure of the port gate is a simple action that is performed multiple times in a day. This action is performed every time the CTM is moved without deviation, and the operator is trained on the consequences associated with this failure. In addition to these failures, a completely independent failure, involving violation of a strict procedural control by a person of a separate “team” inappropriately entering a radiation controlled area must also occur. This HFE was considered “extremely unlikely” and assigned a preliminary value of 0.0001.
050-OpDirExpose2-HFI-NOD	*Operator Causes Direct Exposure During CTM Activities*: For canister loading, if the AO or STC is not staged, the operator can lower the canister to the floor of the Loading Room or Cask Unloading Room and then place the AO or STC lid directly on the canister. The next step in operations is movement of the cask out of the transfer rooms. When the ST or CTT operator goes to perform this step, the operator opens the shield door and enters the Canister Transfer Room as part of normal operations and would be exposed. There is an interlock that prevents the port gate from opening if a receptacle (AO or cask) is not below the port.	29	1E−04	Operators can also cause direct exposure during CTM operations by failing to stage an aging overpack or STC in the Cask Unloading Room or the Loading Room and then placing the canister on the floor and opening the shield door. Placing the receptacle beneath the cask port is part of the staging activities before WHF operations for aging overpack loading and is part of the CTM operation for STC loading. Aging overpack staging is checked off by the staging crew and is also checked off by the operations crew directly before operations begin as part of the prejob plan. If the aging overpack or STC is not staged, the CTM operator has the chance to notice as much when emplacing the canister (via a camera view looking down on the receptacle). For an aging overpack the canister is emplaced on the floor. Then the operator has an additional chance to notice the aging overpack is missing when trying to put the aging overpack lid on the aging overpack with the CTM. This failure received a preliminary value of 0.01 for failure to stage the aging overpack or STC and 0.01 for failure to notice before a direct exposure occurs, resulting in a total preliminary value of 0.0001. There is an interlock preventing this error; however, this interlock may be bypassed during normal maintenance, so the bypass is explicitly modeled in HFE 050-OpFailRstInt-HFI-NOM.
050-OpFailRstInt-HFI-NOM	*Operator Fails to Restore Interlock after Maintenance*: There is an interlock that prevents the port gate from opening before a receptacle is placed underneath the port. If this interlock bypass is not restored, this could result in a direct exposure due to HFE 050-OpDirExpose2-HFI-NOD.	29	1E−02	There is an interlock that prevents the cask port gate from opening before an aging overpack or STC is placed underneath the port. If the interlock bypass is not restored after maintenance, this could result in a direct exposure due to HFE 050-OpDirExpose2-HFI-NOD. This failure would require the crew member to fail to reset the bypass and the crew member to fail to properly perform the prejob check of the CTM equipment. This failure was assigned a preliminary value of 0.01, which corresponds to the generic value for the pre-initiator “failure to properly restore an operating system to service when the degraded state is not easily detectable.”
050-OpFailSG-HFI-NOD	*Operator Fails to Close the CTM Slide Gate before Moving the CTM with the Canister inside the Bell*: If the canister is inside the CTM with the shield skirt raised and the slide gate open, then personnel on the Canister Transfer Room floor may get a direct exposure. This configuration is achieved if the operator fails to close the CTM slide gate and then raises the shield skirt to move the canister to a new receptacle. There is an interlock that does not allow the shield skirt to rise if the slide gate is open; there is no bypass for this interlock.	29	1E−03	Direct exposure during CTM activities can happen if there is a canister in the bell and the CTM slide gate is open while the shield skirt is raised. The most likely way to get this configuration is for the operator to forget to close the slide gate and then raise the shield skirt to move the CTM as per normal operations. There is an interlock that prevents this failure. This operation is performed multiple times a day, and for every CTM lift, the operator closes the slide gate before lifting the shield skirt. This operation is performed by a highly trained operator and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001. No adverse PSFs were identified in this operation that would merit adjusting this preliminary value.

Table E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpNoUnplugST-HFI-NOD	*Operator Causes Spurious Movement of the ST while Canister is Being Loaded*: When the ST is moved to the Cask Unloading Room and positioned under the cask port, the operator is supposed to lower and turn off the ST. If the operator fails to disconnect the ST from the power source, the ST can get a spurious signal during canister lifting that can cause a collision of the ST into the canister.	13	1E−03	While in the Canister Transfer Room, the site transporter is off with the load lowered. The site transporter is controlled locally (i.e., via pendent), and there are no operators in the Canister Transfer Room during CTM operations. In order to cause a spurious movement of the site transporter, the operators must fail to disconnect the site transporter from the power source, and the controller must send a spurious signal to the site transporter. The connection point for the site transporter is outside of the Cask Unloading Room in the preparation area. In order for this failure to occur, when exiting the Cask Unloading Room and closing the shield door, the personnel would have to fail to notice the cord going in through the shield door. If the shield door does not sever the power cord, then there is an interlock that would prevent this error. The interlock prevents the port gate from opening (and thus CTM activities commencing) if the shield door is not completely closed. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. This failure was assessed to be “highly unlikely” (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001.
050-OpNoDiscoAir-HFI-NOD	*Operator Causes Spurious Movement of CTT while Canister is Being Loaded*: When the CTT is moved to the Unloading Room and positioned under the cask port, the operator is supposed to disconnect the air supply from the CTT. If the operator fails to do so, the CTT can get a spurious signal during canister lifting that can cause a collision of the CTT into the canister.	13	1E−03	While in the Canister Transfer Room, the CTT is parked, with the air supply disconnected. The CTT is controlled locally (i.e., via pendent), and there are no operators in the Canister Transfer Room during CTM operations. In order to cause a spurious movement of the CTT, the operators must fail to disconnect the CTT from the air source, and the controller must send a spurious signal to the CTT. The connection point for the CTT is outside of the Cask Unloading Room in the preparation area. In order for this failure to occur, when exiting the Cask Unloading Room and closing the shield door, the personnel would have to fail to notice the hose going in through the shield door. If the shield door does not sever the air hose, then there is an interlock that would prevent this error. The interlock prevents the port gate from opening (and thus CTM activities commencing) if the shield door is not completely closed. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. This failure was assessed to be “highly unlikely” (0.001) because it involves several unlikely failures and significant inattention to the operation. This operation is performed daily and also corresponds closely to the generic human-induced initiator “failure to properly conduct an operation performed on a daily basis,” which also has a default probability of 0.001.
Spurious movement of CTT or ST during CTM activities	*Operator Causes Spurious Movement of CTT or ST while Canister is Being Loaded*	13	N/A	

NOTE: AO = aging overpack; ASD = adjustable speed drive; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; HRA = human reliability analysis; ID = identification; N/A = not applicable; PSF = performance-shaping factor; SSC = structure, system, or component; ST = site transporter; STC = shielded transfer cask; TAD = transportation, aging, and disposal (canister); TC = transportation cask; WHF = Wet Handling Facility.

Source: Original

E6.6.3 Detailed Analysis

After the preliminary screening analysis and initial quantification are completed, those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives are subjected to a detailed analysis. The overall framework for the HRA is based upon the process guidance provided in ATHEANA (Ref. E8.1.22). Consistent with that framework, the following four steps from the methodology described in Section E3.2 provide the structure for the detailed analysis portion of the HRA:

Step 5: Identify Potential Vulnerabilities

Prior to defining specific scenarios which can lead to the HFEs of interest (Step 6), information is collected to define the context in which the failures are most likely to occur. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in HFEs or unsafe actions. This information collection step is discussed in Section E6.6.3.2.

Step 6: Search for HFE Scenarios (Scenarios of Concern)

An HFE scenario is a specific progression of actions with a specific context that leads to the failure of concern; each HFE is made up of one or more HFE scenarios. In this step, documented in Sections E6.6.3.3 and E6.6.3.4, the analyst identifies deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These unsafe actions make up an HFE scenario. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions.

Step 7: Quantify Probabilities of HFEs

Detailed HRA quantification methods are selected as appropriate for the characteristics of each HFE and are applied as explained in Section E6.6.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)
- ATHEANA expert judgment (Ref. E8.1.22).

There is no implication of preference in the order of listing of these methods. They are jointly referred to as the "preferred methods" and are applied either individually or in combination as best suited for the unsafe action being quantified. The ATHEANA (Ref. E8.1.22) expert judgment method (as opposed to the overall ATHEANA (Ref. E8.1.22) methodology that forms the framework and steps for the performance of this HRA) is used when the other methods are deemed to be inappropriate to the unsafe action, as is often the case for cognitive EOCs.

Appendix E.IV of this analysis explains why these specific methods were selected for quantification and gives some background on when a given method is applicable based on the focus and characteristic of the method.

All judgments used in the quantification effort are determined by the HRA team and are based on their own experience, augmented by facility-specific information and the experience of subject matter experts, as discussed in Section E4. If consensus can be reached by the HRA team on an HEP for an unsafe action, that value is used as the mean. If consensus cannot be reached, the highest opinion is used as the mean.

Step 8: Incorporate HFEs into the PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. The summary table of HFEs by group that lists the final HEP by basic event name provides the link between the HRA and the rest of the PCSA. This table can be found in Section E6.6.4.

E6.6.3.1 HFEs Requiring Detailed Analysis

The detailed analysis methodology, Sections E3.2.5 through E3.2.9, states that HFEs of concern are identified for detailed quantification through the preliminary analysis (Section E3.2.4). An initial quantification of the WHF PCSA model determined that there are four HFEs whose preliminary values were too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111. These HFEs are presented in Table E6.6-2.

Table E6.6-2. Group #6 HFEs Requiring Detailed Analysis

HFE	Description	Preliminary Value
050-OpCTMdrop001-HFI-COD	Operator causes drop of object onto canister during CTM operations	2E−03
050-OpCTMdrop002-HFI-COD	Operator causes drop of canister during CTM operations (low-level drop)	2E−03
050-OpCTMImpact1-HFI-COD	Operator moves the CTM while canister or object is below or between levels	1E−03
050-OPCTMDirExp1-HFI-NOD	Operator causes direct exposure during CTM activities (second floor)	1E−04

NOTE: CTM = canister transfer machine; HFE = human failure event.

Source: Original

E6.6.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the ATHEANA approach to detailed quantification is to identify and characterize factors that could create potential vulnerabilities in the crew's ability to respond to the scenarios of interest and might result in HFEs or unsafe actions. In this sense, the "vulnerabilities" are the context and factors that influence human performance and constitute the characteristics, conditions, rules, and tendencies that pertain to all the scenarios analyzed in detail.

These vulnerabilities are identified through activities including but not limited to the following:

1. The facility familiarization and information collection process discussed in Section E4.1, such as the review of design drawings and concept of operations documents

2. Discussions with subject matter experts from a wide range of areas, as described in Section E4.2

3. Insights gained during the performance of the other PCSA tasks (e.g., initiating event analysis, system analysis, and event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the CTM operation that relate to potential human failure scenarios relevant to the four HFEs listed above. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during CTM operation, but these have no bearing on this analysis.

E6.6.3.2.1 Operating Team Characteristics

The operating team consists of the following personnel:

CTM operator—The CTM operator is located in the WHF Control Room. The CTM operator receives standard training for crane operations and observes operations prior to being allowed to operate the CTM on a dry run. After training, the CTM operator is signed off to operate the CTM based on an evaluation of proficiency in a dry run. The CTM operator is observed on initial operations until signed off for solo operation. A single operator is assigned to the CTM operation.

Crew members (two)—Maintenance crew members are trained in tasks required for preparing the CTM for canister transfer, including affixing the appropriate grapple for the canister. Training consists of observation and hands-on instruction for the CTM preparation process. The CTM is prepared by a team of two workers.

Supervisor—The supervisor, or some other personnel with comparable training and certification, is in the WHF Control Room watching CTM operations. This person is in charge of verifying (signing off) that the preoperational checks have been properly performed, including proper attachment of the grapple to the hoist. This person is also in charge of completing an end-of-operations checklist and independently verifying that the Canister Transfer Room is in a safe configuration after canister transfer activities have been completed.

E6.6.3.2.2 Operation and Design Characteristics

Control Panel—The panel consists of a joystick controller for two-dimensional movements of the bridge and trolley. Speed in both directions is fully variable within unit capabilities, based on the extent of joystick deflection. Buttons for the up–down movement of the hoist are spring returned and must be held in for hoist movement. The height of the hoist yoke is displayed digitally on the panel. There is a joystick for fine motion alignment of grapple (e.g., it can move the hoist within the bell). A flat screen display shows view from the camera mounted on the boom above the yoke. A control interface for the ASD is incorporated into the panel.

ASD—The ASD is equipped with a semi automated system for lifts. The ASD has two normal modes and one maintenance (i.e., manual) mode. Normal modes have two settings: canister lift and lid lift. In the canister lift mode, the operator sets the mode and pushes/holds the lift button;

the ASD lifts to the proper height and stops. The maintenance mode allows for full manual operation. The maintenance mode can be engaged only by entering a password.

Interlocks/Alarms—Only hardwired (non-PLC) interlocks are considered.

Hoist Operational Upper Limit—A light curtain located just above (~2 in.) the CTM slide gate. The interlock removes the power from the hoist lift circuit if nothing is sensed within the bell at this height (i.e., when the hoist cables, load cell, grapple, and any load have cleared this height). Indicators on the control panel (red/green lights) indicate whether the limit is cleared or blocked. The upper limit can be bypassed.

Grapple Engagement/Disengagement Interlock—The grapple interlock provides indication to the operator that the grapple is either fully engaged with the load or fully disengaged. Red and green lights indicate position. When both lights are on, this indicates that the grapple is between positions, and the interlock prevents hoist movement under this condition.

Grapple Interlock—The grapple interlock also prevents hoist movement if the secondary grapple is not properly attached to the primary grapple on the hoist. There is an interlock which prevents operation of the CTM canister grapple (primary grapple) if it is not properly attached to the hoist. .

Load Cell Over limit—The load cell over limit stops hoist movement when excessive force is applied to the hoist. This could shut down the hoist if the lid is pulled up against the bottom of the bell, but would not provide any protection against two-blocking because it is located below the lower block (i.e., between the block and the grapple).

Inadvertent Grapple Disengagement—The grapples are mechanically designed such that they cannot disengage while under a load; therefore, inadvertent grapple disengagement is precluded. However, to be conservative, this is modeled as an electric interlock.

Shield Skirt/Slide Gate Interlock—Prevents the shield skirt from lifting if the CTM slide gate is not closed. The failure mode of failing to reset the bypass for this interlock has not been modeled because there is no bypass for this interlock.

E6.6.3.2.3 Operational Conditions

There is no direct view of the CTM operation by any individual. Visual cues are hampered because all observations are made through cameras and observed on screens. The precise locations of the cameras have not been specified in the design, but the intent is to provide cameras that can view the grapple and canister (and move with the hoist) on the hoist trolley (that can see into the bell) and at other locations that can provide views of the outside of the bell and the Canister Transfer Room.

Control panel indications provide positive indication that the grapple has been deployed in the locked position (a red light) or the unlocked position (a green light), but the ability to provide a direct (as opposed to indirect or inferred) confirmation of full engagement in the lift fixture is not proven.

The total operation of the CTM for a canister takes about two hours. The operator has a number of specific tasks to perform during that time, so the overall process can be considered reasonably active. However, the lifting task (relevant to drops) is one of the longest periods of inactivity for the operator (i.e., 10 minutes, of which only the last 30 seconds or so can be considered potentially active). The potential for the onset of boredom, complacency, or distraction is higher than normal during this task.

E6.6.3.2.4 Formal Rules and Procedures

Procedural Controls—Procedural controls associated with the radiation protection program ensure that the operators and maintenance personnel do not enter the Canister Transfer Room during CTM activities. Procedural controls also include a checklist that must be filled out at the end of transfer activities to ensure that all the port slide gates are closed.

E6.6.3.2.5 Operator Tendencies and Informal Rules

Dependency on Hoist Interlocks and Alarms—The CTM operator should actively observe and confirm proper operation of the CTM and not depend on either alarms to inform that limits are being reached or interlocks to stop or prevent improper motion. However, there can be a tendency for the operator to count on these devices to prevent human failure, in particular because the visual information received from the cameras is distorted.

Dependency on Grapple Engagement/Disengagement Indicator—In a similar fashion, the operator should confirm positive engagement of the grapple through the camera, but the lack of clarity expected in the camera view can create a tendency to depend solely on the indicator.

E6.6.3.2.6 Operator Expectations

Consequences of Failure—The CTM operations are performed remotely. No personnel are in the vicinity of the operation, and so the threat of physical injury is absent. Operators expect that failures are mitigated by design features without serious consequences, which could promote complacency in the operations.

Anticipatory Actions—The lifting process is simple, the goal is clear, and problems are not expected. There may be a tendency for the CTM operator to focus on future tasks while the hoist is in motion rather than concentrate on the ongoing task. The operator expects that no one attempts to enter the Canister Transfer Room during CTM activities.

Expectation of Grappling Success—The grapple is a simple device. The operator can expect that once the grapple is actuated, it properly engages or disengages. The operator expects a failure or expects the engagement indicator to show a failure. The operator also does not expect that the grapple is properly attached to the hoist (i.e., the operator can expect and trust that the crew members have properly prepared the CTM).

E6.6.3.3 HFE Scenarios and Expected Human Failures (Step 6)

Given that the vulnerabilities that provide the operational environment and features that could influence human performance have been specified, then the HFE scenarios within this

environment are identified. An HFE scenario is a specific progression of actions during normal operations (with a specific context) that leads to the failure of concern. Each HFE is made up of one or more HFE scenarios. In accordance with the methodology, each scenario integrates the unsafe actions with the relevant equipment failures so as to provide the complete context for the understanding and quantification of the HFE.

The HAZOP evaluation is instrumental in initially scoping out the HFE scenarios, but they are then refined through discussions with subject matter experts from a wide range of areas, as described in Section E4.2.

Table E6.6-3 summarizes all of the HFE scenarios developed for the HFEs in this group.

Table E6.6-3. HFE Scenarios and Expected Human Failures for HFE Group #6

HFE	HFE Scenarios
050-OpCTMdrop001-HFI-COD *Operator causes drop of object (lid)onto canister during CTM operations*	HFE Scenario 1(a): (1) A crew member improperly installs the grapple, (2) the preoperational check fails to note the improper installation, (3) the primary grapple interlock gives a false positive signal, (4) the operator fails to notice the bad connection between the hoist and the grapple through the camera, and (5) the grapple/lid drops from the hoist and strikes the canister. HFE Scenario 1(b): (1) The operator fails to fully engage the grapple, (2) the grapple engagement interlock gives a false positive signal, (3) the operator fails to notice that the grapple is not fully engaged through camera, and (4) the lid drops from the grapple and strikes the canister. HFE Scenario 1(c)[a, b]: (1) The operator leaves the ASD in maintenance mode OR the operator places the ASD in canister mode OR the ASD height control fails, (2) the operator fails to notice that the lift is taking too long OR the operator "locks" the lift button into position, (3) the load cell overload interlock fails, and (4) mechanical failure of the hoist under overload causes the lid to drop. HFE Scenario 1(d)[a, b]: (1) The CTT is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice the lid tilt and continues the lift OR the operator "locks" the lift button into position, (4) the lid catches and jams in port, (5) the load cell overload interlock fails, and (6) mechanical failure of the hoist under overload causes the lid to drop. HFE Scenario 1(e): (1) The operator activates the grapple disengagement switch prematurely, (2) the load cell disengagement interlock fails, and (3) the lid drops from the grapple and strikes the canister.
050-OpCTMdrop002-HFI-COD *Operator causes drop of canister during CTM operations (low-level drop)*	HFE Scenario 2(a): (1) A crew member improperly installs the grapple, (2) a primary grapple interlock gives a false positive signal, (3) the operator fails to notice the bad connection between the hoist and the grapple through the camera, and (4) the grapple/canister drops from the hoist. HFE Scenario 2(b): (1) The operator fails to fully engage the grapple, (2) the grapple engagement interlock gives a false positive signal, (3) the operator fails to notice that the grapple is not fully engaged through camera, and (4) the canister drops from the grapple. HFE Scenario 2(c)[c]: (1) The CTT is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice that the DPC contacting the ceiling and continues the lift OR the operator "locks" the lift button into position, (4) the load cell overload interlock fails, and (5) mechanical failure of the hoist under overload causes the DPC to drop.

Table E6.6-3. HFE Scenarios and Expected Human Failures for HFE Group #6 (Continued)

HFE	HFE Scenarios
050-OpCTMImpact1-HFI-COD *Operator moves the CTM while canister or object is below or between levels*	HFE Scenario 3(a): (1) The operator leaves the CTM in the lid lift mode (DPC/AO or TAD/STC), (2) the operator fails to notice that the lift stops too soon, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, and (5) the CTM slide gate interlock fails. HFE Scenario 3(b): (1) The operator puts the CTM in the lid lift mode (for DPC/TC), (2) the operator fails to notice that the lift stops too soon, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, and (5) the CTM slide gate interlock fails. HFE Scenario 3(c): (1) The operator puts the CTM in the maintenance mode (DPC/AO or TAD/STC), (2) the operator terminates the lift prior to the automatic stop, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, and (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, (5) the CTM slide gate interlock fails. HFE Scenario 3(d)[d]: (1) The operator leaves the CTM in the maintenance mode (for DPC/TC or removing STC/AO lids), (2) the operator terminates the lift prior to the automatic stop, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, and (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, (5) the CTM slide gate interlock fails.
050-OPCTMDirExp1-HFI-NOD *Operator Causes Direct Exposure during CTM Activities (Second Floor)*	HFE Scenario 4(a): (1) A worker violates administrative control by entering the Canister Transfer Room during canister transfer, and (2) the operator fails to close port gate before raising the shield skirt.

NOTE: [a] Scenarios (1c) and (1d) in this event do not apply to DPCs removed from TCs since TC lids are not removed in the CTM.
[b] This scenario does not apply to placing the STC or AO lids since it can only occur over the canister when lifting.
[c] This scenario only applies to a DPC/TC because the transportation cask lid was removed in the preparation area.
[d] For dropping a lid, only scenario 3(d) is applicable.

AO = aging overpack; ASD = adjustable speed drive; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure events; STC = shielded transfer cask; TAD = transportation, aging, and disposal (canister); TC = transportation cask.

Source: Original

Since there are four HFEs identified for detailed analysis in this group, the scenarios are organized under these four HFE categories, with the scenarios under the first HFE category numbered as 1(a), 1(b), etc.; those under the second category numbered 2(a), etc.; and similarly those under the third category numbered 3(a), 3(b), etc.

Each HFE scenario is in turn characterized by several unsafe actions, numbered sequentially as (1), (2), (3), etc. The Boolean logic of the HFE scenarios is expressed with an implicit AND connecting the subsequent unsafe actions and OR notation wherever two unsafe action paths are possible, as shown in Table E6.6-3.

The HFE scenarios summarized in Table E6.6-3 are discussed and quantified in detail in the following sections.

E6.6.3.4 Quantitative Analysis (Step 7)

Once the HFE scenarios and the unsafe actions within them are scoped out, it is then possible to review them in detail and apply the appropriate quantification methodology in each case that permits an HEP to be calculated for each HFE. Stated another way, each HFE is quantified through the analysis and combination of the contributing HFE scenarios. Dependencies between the unsafe actions and equipment responses within each scenario and across the scenarios are carefully considered in the quantification process.

This section provides a description of the quantitative analysis performed, structured hierarchically by each HFE category (identified by a basic event name), the HFE scenario, and the unsafe actions under each scenario, as previously documented in Table E6.6-3.

Prior to the scenario-specific quantification descriptions, a listing is provided of the values used in the quantification that are common across many of the HFE scenarios.

In generating the final HEP values, the use of more than a single significant figure is not justified given the extensive use of judgment required for the quantification of the individual unsafe actions within a given HFE. For this reason, all calculated final HEP values are reduced to one significant figure. When doing this, the value is always rounded upwards to the next highest single significant figure.

E6.6.3.4.1 Common Values Used in the HFE Detailed Quantification

There are some mechanical failures that combine with unsafe actions to form HFEs. In general, these mechanical failures are independent of the specific HFE scenario, and so they can be quantified independently. These values are presented in this section.

Interlock Failures—There are a number of interlock failures in the HFE scenarios. While the status of these events can affect subsequent events in the scenarios in different ways, the likelihood of this event occurring is independent of the scenario. This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for an interlock, from Attachment C, Table C4-1, is approximately 2.7E−05 per demand.

Interlock fails to perform function = 2.7E−05

ASD Height Control Fails—This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for the ASD, from Attachment C, Table C4-1, is approximately 3.4E−05 per demand.

ASD height control fails = 3.4E−5

Load Drops from Hoist—This is the last event in a drop scenario. This event accounts for the safety margins built into the hoist system to accept overload without failure resulting in severed cables, failed clutches, and partially engaged grapples. The various events need to be quantified in relation to each other, using engineering judgment to account for the load being applied to the system versus its capacity to bear the load.

The first drop considered is where a canister (DPC/transportation cask) is being lifted and it catches the ceiling of the Cask Unloading Room. In this case, an overload of the system is created by adding the additional force of the hoist motor straining to lift the unmoving canister (over and above the force created by the canister) to the system. The extent to which this exceeds the ultimate load-bearing capacity of the system is a function of the total force that can be generated by the motor and the amount of time that the motor can exert this force while not turning before the motor overheats. Typical design requirements for NOG-1 cranes (Ref. E8.1.2) provide a significant safety margin against overload failures. The probability of this event is based on analyst judgment in accordance with the PCSA approach to the use analyst judgment for probability estimation. There is limited analysis of this condition. Lacking or inconclusive analysis would argue for assignment of even odds (0.5) for this event. The weight of evidence for the inherent margin in a single failure-proof design could form an argument that the failure is unlikely (0.1). The HRA team is convinced that the best estimate from the available information (given the current state of knowledge) is somewhere in between. The HRA team assigns 0.5 as the 95% confidence level and 0.1 as the 5% confidence level. Using a lognormal distribution, the mean associated with these confidence limits follows:

Mechanical failure of hoist under overload causes DPC (from a transportation cask) drop = 0.25

The other drops are evaluated relative to this. First considered is the similar case where the lid is jammed in the port and the hoist is straining to lift the jammed lid. In this case, the force generated by the hoist is the same, but the weight of the lid is less. The HRA team judges that it is reasonable to reduce the failure probability by a factor of two to account for this difference:

Mechanical failure of hoist under overload causes lid drop = 0.1

Considered next is the condition where the grapple is either not properly connected to the hoist or the grapple itself is only partially engaged with the canister or lid. This failure (i.e., drop of canister or lid from an improperly engaged grapple) is judged to be comparable to mechanical failure of the hoist under overload because in both cases the load-bearing capacity of the system is reduced. Therefore the resulting probability is as follows:

Grapple/canister drops from hoist = 0.25

Canister drops from grapple = 0.25

Regarding the case of a lid, again the force is lower than the canister case and also lower than the jammed lid case, with a similar situation in that the load-bearing capacity of the system is reduced. Using the logic above, this would argue for using the 0.1 value. However, in the case of the lid, there is always the possibility that the drop would occur when the object was not over the canister, or it would occur in a manner that the lid would not impact the canister (i.e., it would only strike the structure of the transportation cask, aging overpack, or STC). In the absence of analysis, the HRA team has applied a 50–50 chance of this occurring, which reduces the probability by a factor of two. Therefore:

Grapple/lid drops from hoist and strikes canister = 0.05

Lid drops from grapple and strikes canister = 0.05

Given the information available about the design, the analyses in existence, and the knowledge of the requirements of NOG-1 (Ref. E8.1.2) and other applicable standards to be applied to the CTM, the HRA team believes this to be both a reasonable assessment and at as fine a level of detail and differentiation as can be justified.

E6.6.3.4.2 Quantification of HFE Scenarios for 050-OpCTMdrop001-HFI-COD: Operator Causes Drop of Object onto Canister during CTM Operations

Operator causes drop of object onto canister during CTM operations. (This event applies to both dropping an STC/aging overpack lid during removal or placement; however, scenarios 1(c) and 1(d) would not apply during lid placement since the failure modes are only applicable to lifts.)

E6.6.3.4.2.1 HFE Group #6 Scenario 1(a) for 050-OpCTMdrop001-HFI-COD

1. Maintenance crew member improperly installs grapple.
2. Preoperational check fails to note improper installation.
3. Primary interlock gives false positive signal.
4. Operator fails to notice bad connection between hoist and grapple through camera.
5. Grapple/lid drops from hoist and strikes canister.

Crew Member Improperly Installs Grapple—Prior to a lift operation, a crew member prepares the CTM for the operation by installing the appropriate grapple for the type of cask lid to be processed. While it is possible that this operation need not be performed (it may be the cask lid grapple is the same grapple used for previous CTM operation and no other work on or with the CTM may have been performed), it is uncertain how often this can occur, so this analysis considers that this action needs to be performed each time. To install the grapple, the primary CTM grapple lowers and engages the secondary grapple. If the primary grapple is only partially engaged, the secondary grapple appears to be secured in place, but it is not.

The operator aligns the grapple visually using the camera view and then engages the grapple. If it is not aligned properly, the grapple does not fully engage. The crew members locally verify engagement and connect the appropriate wire connections from the secondary grapple to the primary grapple. This is a straightforward matter of task execution. The task is simple and routine and can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well designed, highly practiced routine task performed to the highest possible standards by highly motivated, highly trained, and experienced person, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the

task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.

- EPC 8: Poor environment. This EPC is applied not so much because the environment is poor, but rather that it is simply not optimal. The full affect EPC would be ×8, but this applies when working in the plant with suit and breathing apparatus, possible access problems, and for more than 45 minutes so that fatigue sets in. The APOA anchor for 0.1 is for work in the plant with suit and breathing apparatus but none of the other environmental stressors. In this task no breathing apparatus is required, but the task is somewhat physically demanding. Given the tradeoffs, the APOA is set at 0.1.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Crew member improperly installs grapple} = 0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006 \quad \text{(Eq. E-7)}$$

Preoperational Check Fails to Notice Improper Installation—There are two crew members responsible for preparing the CTM for each operation. Each crew member has a distinct set of assignments, although they collaborate when needed and are expected to check each other's work. The second crew member checks the first crew member's installation of the grapple, which provides an opportunity for the error to be detected. The second crew member also has a set of activities to perform, and so checking the first crew member is a secondary function. In addition, the existence of the grapple/hoist interlock provides an expectation that any error can be detected.

The second crew member would have helped initially with the connection of the grapple to line it up but would then move on to other things. At best, the second crew member performs a cursory check at the end of the job. Since the crew member was involved in the early stages, there is a bias that the job was done correctly. It is concluded that the level of dependence is high. The baseline HEP for the checking, for checking routine tasks without a checklist, is best determined from THERP (Ref. E8.1.26), Table 20-22, item (2), which is 0.2. The HEP for high dependence is from THERP, Table 20-21, item (4)(e), which is 0.6.

$$\text{Preoperational check fails to note improper installation} = 0.6$$

Primary Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the primary grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

Primary grapple interlock gives false positive signal = 2.7E−5

Operator Fails to Notice Improper Connection between Hoist and Grapple through Camera—When the CTM operator is in the process of lifting the canister, the camera shows the operator the secondary grapple and its connection to the primary grapple. The operator is not focused on that connection but is focused on lining up the secondary grapple with the lifting device. However, as the lift begins, the operator is supposed to watch through the cameras. This gives the operator the opportunity to note that the grapple is not properly connected (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not expecting any problems in this simple operation, and the operator tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

This action is best represented by the CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made. The baseline HEP is 0.003.
- CPC "Adequacy of Man–Machine Interface": For this particular observation, the use of a camera view (while the only practical means) is somewhere between tolerable and inappropriate. The CPC for an observation task with tolerable man–machine interface is 1.0, and for inappropriate is 5.0. With regard to being able to actually observe the condition of the grapple lock pin, the CPC is set as 4.0.
- CPC "Number of Simultaneous Goals": The operator is primarily focusing on properly aligning the bell and hoist, opening the ports, and grappling the lid. While it could be argued that this is not "more than capacity," it certainly relegates looking at the grapple/hoist connection to a secondary action. It is therefore deemed appropriate to apply the more than capacity CPC, which is 2.0.
- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

The resulting value follows:

Operator fails to notice improper connection between hoist and grapple through camera
$= 0.003 \times 4 \times 2 \times 0.8 = 0.02$

Grapple/Lid Drops from Hoist and Strikes Canister—Just because the lift is occurring with an improper grapple installation does not mean that the lid and grapple fall. The safety margins built into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation, especially given that it is sized for a canister, and the lid is much lighter. Additionally, even if the lid and grapple do fall, they could fall early (a weak connection) or later (sufficient connection that they need time and motion to cause them to break loose). These two cases can result in the lid and grapple breaking loose when they are not above the canister. In addition, it is not a certainty that the lid and grapple, once dropped, would

fall in an orientation that would impact the canister in the STC or aging overpack, even if they are above the canister at the time of the drop (the orientation of the falling lid and grapple may cause them to only impact the STC or aging overpack structure).

This event is quantified in Section E6.6.3.4.1.

Grapple/lid drops from hoist = 0.05

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.6-4.

Table E6.6-4. HEP Model for HFE Group #6 Scenario 1(a) for 050-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Crew member improperly installs grapple	0.0006
B	Preoperational check fails to note improper installation	0.6
C	Primary interlock gives false positive signal	2.7E−5
D	Operator fails to notice improper connection between hoist and grapple through camera	0.02
E	Grapple/lid drops from hoist and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E{-}5 \times 0.02 \times 0.05 = 1E{-}11 \quad \text{(Eq. E-8)}$$

According to NARA, the lower limit of credibility for an HFE accomplished by a single operator or team is 1E−5 per demand. Using this truncated value for the set of unsafe actions, the probability of this scenario is:

$$1E{-}5 \times 2.7E{-}5 < 1E{-}8 \quad \text{(Eq. E-9)}$$

E6.6.3.4.2.2 HFE Group #6 Scenario 1(b) for 050-OpCTMdrop001-HFI-COD

1. Operator fails to fully engage grapple.
2. Grapple engagement interlock gives false positive signal.
3. Operator fails to notice grapple not fully engaged through camera.
4. Lid drops from grapple and strikes canister.

Operator Fails to Fully Engage Grapple—The operator engages the grapple from the control panel. The grapple can be roughly positioned using the alignment guides for the CTM and the hoist height indicator on the control panel, but final alignment must be done visually using the view from the cameras provided on the grapple. Once the operator believes the grapple is aligned, the operator engages the grapple with the lift fixture and confirms through the camera that the grapple has engaged. If the operator sees that the grapple has not properly engaged (generally by checking the interlock condition if it looks engaged visually), then the operator disengages it, repositions the grapple, and tries again to engage.

The operator aligns the grapple visually using the view from the camera and engages the grapple. If it is not aligned properly, it does not fully engage. This unsafe action can be best represented by the task execution error NARA GTT A1, adjusted by the following CPCs:

- NARA GTT A1: Carry out a simple manual task with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005.

- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.

- EPC 11: Poor, ambiguous, or ill-matched system feedback. This EPC is applied to account for the need to observe the operation through cameras. The full affect EPC would be ×4. The full effect is applicable when legibility is poor or label is obscured or where the layout of controls makes visual access and physical access difficult. The use of the camera view is deemed to represent full effect. The APOA is set at 1.0.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Operator fails to fully engage grapple} = 0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad \text{(Eq. E-10)}$$

Grapple Engagement Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

$$\text{Grapple engagement interlock gives false positive signal} = 2.7\text{E}{-5}$$

Operator Fails to Notice Grapple Not Fully Engaged through Camera—As the lift begins, the operator is supposed to watch through the cameras. This allows the opportunity to note that the grapple is not properly engaged (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not

expecting any problems in this simple operation, and the tendency is to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

In this task, the operator is checking the actions taken through the camera. The operator believes that the action was initially performed correctly (because the action was performed by the operator), and this belief is confirmed by the false positive from the interlock, so this last observation is deemed completely dependent on the prior actions. Using THERP Table 20-21 to assess dependency, item (5) for complete dependency:

Operator fails to notice grapple not fully engaged through camera = 1.0

Lid Drops from Grapple and Strikes Canister—Just because the lift is occurring with an incomplete engagement of the grapple does not mean that the grapple would fall. The safety margins built into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation, especially given that it is sized for a canister, and the lid is much lighter. Additionally, even if the lid does fall, it could fall early (a weak connection) or later (sufficient connection that they need time and motion to cause them to break loose). These two cases can result in the lid breaking loose when it is not above the canister. In addition, it is not a certainty that the lid, once dropped, would fall in an orientation that would impact the canister in the STC or aging overpack, even if it is above the canister at the time of the drop (the orientation of the falling lid may cause it to only impact the STC or aging overpack structure).

This event is quantified in Section E6.6.3.4.1.

Lid drops from grapple = 0.05

HEP Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.6-5**.**

Table E6.6-5. HEP Model for HFE Group #6 Scenario 1(b) for 050-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator fails to fully engage grapple	0.07
B	Grapple engagement interlock gives false positive signal	2.7E−5
C	Operator fails to notice grapple not fully engaged through camera	1.0
D	Lid drops from grapple and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D = 0.07 \times 2.7E{-}5 \times 1.0 \times 0.05 = 1E{-}7 \qquad \text{(Eq. E-11)}$$

E6.6.3.4.2.3 HFE Group #6 Scenario 1(c) for 050-OpCTMdrop001-HFI-COD

1. Operator leaves ASD in maintenance mode OR operator places ASD in canister mode OR ASD height control fails.

2. Operator fails to notice lift is taking too long OR operator "locks" lift button into position.

3. Load cell overload interlock fails.

4. Mechanical failure of hoist under overload causes lid drop.

Operator Leaves ASD in Maintenance Mode—The ASD controls the height of the lift. Before beginning the lifting process, the operator should ensure that the ASD is in the lid lift mode. It could be in maintenance mode because of activities performed in the days between canister transfers. It is not clear how often this would occur, so for the purpose of this analysis, the bounding case is that the ASD is always in maintenance mode between canister transfers. Therefore, the operator must change the mode prior to the lid lift. In doing this, the operator could either fail to change the mode (miss this step in the process) or erroneously place it in the canister lift mode, either of which results in the ASD trying to lift the lid too high and impacting the bottom of the bell.

The CTM operator is supposed to set the CTM system to the appropriate lift mode prior to performing a lift. This is fundamental to the operation, not simply a step in a procedure that can be missed. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in maintenance mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3, and adjusted by the following EPCs:

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves ASD in maintenance mode = 0.0007

Operator Places ASD in Canister Lift Mode—Given that the CTM operator has correctly decided to set the CTM system status prior to operations, the appropriate operating mode also needs to be selected. There are only two modes to choose from: lid lift and canister lift. The ASD control is a screen where the operator can scroll between the choices to pick the appropriate lift mode. The act of selecting the wrong mode from these two is best represented by task execution error NARA GTT A1, adjusted by the following EPCs:

- NARA GTT A1: Carry out a simple single manual action with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005.

- This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The ASD control system requests confirmation from the operator (e.g., "You have selected canister lift. Confirm Y/N"). The baseline HEP is used without adjustment.

Operator places ASD in canister lift mode = 0.005

ASD Height Control Fails—This is a mechanical failure of the ASD controller. This event is quantified in Section E6.6.3.4.1.

ASD height control fails = 3.4E−5

Operator Fails to Notice Lift is Taking Too Long—Lifting the lid takes on the order of a few minutes, whereas lifting the canister takes on the order of ten minutes. Because the operator holds the lift button or the lift stops, there is an opportunity to notice that the hoist has not stopped when expected and to release the button and stop the hoist, either before the lid contacts the interior of the bell or before it begins to overload the system. Realistically, the operator would have on the order of 30 seconds between when it should stop and when it would be too late. The hoist position indicator and camera view are in front of the operator on the control panel.

The operator is supposed to hold the lift button until the lift automatically stops. This operation has been performed many times in the past by the operator, who has an instinctive feel for how long the lift takes. If the operator feels it is taking too long, the operator need only look at the camera and the indicators on the control panel for verification. Failing to recognize this situation can be represented by CREAM CFF I3, adjusted by the following CPCs with values not equal to 1.0:

- CFF I3: Delayed interpretation (not made in time). The baseline HEP is 0.01.

- CPC "Working Conditions": The operator has optimal working conditions in the WHF Control Room. The CPC for an interpretation task with advantageous working conditions is 0.8.

Applying these factors yields the following:

Operator fails to notice lift is taking too long = $0.01 \times 0.8 = 0.008$

Operator "Locks" Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to "lock" the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without an ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the operator would not believe that the deviation is unsafe, and it would free up time to prepare for subsequent steps or to perform other duties.

The operator is supposed to hold the lift button until the lift automatically stops. However, it is always possible to rig something up that would hold the button in place, relieving the operator of the "inconvenience" of holding it. The HRA team believes that the preferred methods do not provide baseline HEPs for such unsafe actions. Therefore, the ATHEANA expert judgment approach is used. In considering the judgment, HEART and NARA do provide some insight into the existence of EPCs that can affect this unsafe action, such as the following:

- A mismatch between an operator's model of the world and that imagined by a designer—The designer considers the push-and-hold as a safety feature that keeps the operator's attention on the operation. The operator considers it as an unnecessary inconvenience in what should be an automated function.

- A mismatch between real and perceived risk—Locking the button removes a layer of safety provided by the operator monitoring operations, but the operator perceives the reliability of the limits and interlocks as such that there is no additional risk involved (HEART EPC 12).

- Little or no independent checking or testing of output—A single operator is operating the CTM from a remote location. No one is looking over the operator's shoulder (HEART EPC 17).

- An incentive to use other, more dangerous procedures—Holding the button means that the operator's ability to accomplish other work is limited. The operator can be more efficient (e.g., planning for future activities, completing paperwork) if the operator simply trusts the control system to complete the task (HEART EPC 21, NARA EPC 15).

- Operator underload, boredom—Holding a button when one fully expects that the system automatically controls the operation is not very challenging (NARA EPC 13).

- Little or no intrinsic meaning in a task—The operator really has to wonder why the system was not designed to simply perform the operation on its own. The operator could come to consider the push-and-hold feature as a poorly thought out design flaw. (HEART EPC 28.)

Taking this as a whole, the HRA team judges that the operator locks the button in place about 10% of the time (which can be interpreted as some operators doing it quite frequently and other operators less or not at all, depending on their compunction to do so). However, this action is not unrelated to prior failures in this scenario. An operator who fails to set the CTM system status (leaves the ASD in maintenance mode) has already demonstrated a predilection towards rushing and perhaps a bias towards shortcuts for the particular lift. Therefore, the HRA team judges that the success or failure of this task is related to the way in which the ASD failure occurs. It is judged that if the failure occurs as a result of leaving the ASD in maintenance mode, the HEP for locking the button in place is twice the baseline (0.2). If it occurs for either of the other two reasons, the HEP is one-half the baseline (0.05).

Operator "locks" lift button into place (ASD left in maintenance) = 0.2

Operator "locks" lift button into place (ASD placed in canister mode or fails mechanically) = 0.05

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the lid in contact with the bell (which would put the full load of the bell on the hoist) would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

Load cell interlock fails = 2.7E−5

Mechanical Failure of Hoist under Overload Causes Lid Drop—There are three potential failure modes that could cause the lid to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the grapple or lid. However, just because the hoist keeps pulling does not mean that the lid falls (the hoist motor could overload and fail before the lid becomes detached from the hoist) or that the lid, once dropped, falls in an orientation that would impact the canister in the STC or aging overpack (the orientation of the falling lid may cause it to only impact the STC or aging overpack structure).

This event is quantified in Section E6.6.3.4.1.

Mechanical failure of hoist under overload causes lid drop = 0.1

HEP Calculation for Scenario 1(c)—The events in the HEP model for Scenario 1(c) are presented in Table E6.6-6.

Table E6.6-6. HEP Model for HFE Group #6 Scenario 1(c) for 050-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator leaves ASD in maintenance mode	0.0007
B	Operator places ASD in canister mode	0.005
C	ASD height control fails	3.4E−5
D	Operator fails to notice lift is taking too long	0.008
E1	Operator "locks" lift button into position (ASD left in maintenance)	0.2
E2	Operator "locks" lift button into position (ASD placed in canister mode or fails mechanically)	0.05
F	Load cell overload interlock fails	2.7E−5
G	Mechanical failure of hoist under overload causes lid drop	0.1

NOTE: ASD = adjustable speed drive; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$\{A \times (D + E1) + [(B + C) \times (D + E2)]\} \times F \times G = \{0.0007 \times (0.008 + 0.2) +$$

$$[(0.005 + 3.4E{-}5) \times (0.008 + 0.05)]\} \times 2.7E{-}5 \times 0.1 < 1E{-}8 \qquad \text{(Eq. E-12)}$$

E6.6.3.4.2.4 HFE Group #6 Scenario 1(d) for 050-OpCTMdrop001-HFI-COD

1. CTT or site transporter is not sufficiently centered under port.
2. Operator fails to notice CTT or site transporter not sufficiently centered.
3. Operator fails to notice lid tilt and continues lift OR operator "locks" lift button into position.
4. Lid catches and jams in port.
5. Load cell overload interlock fails.
6. Mechanical failure of hoist under overload causes lid drop.

CTT Is Not Sufficiently Centered Under Port—This unsafe action actually occurs prior to this operation, during movement of the CTT (or site transporter) into the Cask Unloading Room. The CTT (or site transporter) operator brings the unit into the Cask Unloading Room and centers it directly under the cask port by aligning it against end stops that properly locate it and by using markings on the floor. If the cask is not properly centered, it is possible that the lid could strike the ceiling around the cask port rather than rising smoothly through the cask port. The cask would have to be off-center by more than a foot.

The unsafe action results from stopping the CTT prematurely and leaving it at least a foot short of the proper location. This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.
- CPC "Available Time": There is adequate time to perform this task. The only time pressure is the desire to keep the process moving, but the consequences are insignificant. The CPC for an execution task with adequate time is 0.5.
- CPC "Adequacy of Training/Preparation": This routine task is well trained and practiced and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{CTT is not sufficiently centered under port} = 0.003 \times 0.5 \times 0.8 = 0.002$$

Operator Fails to Notice that CTT Is Not Sufficiently Centered—The CTM operator centers the CTM grapple over the cask lid lift fixture using a two-step process. First, the CTM operator does a rough alignment using the bridge and trolley position indicators and sets the bell and

shield skirt in place. Then the operator opens the cask port and performs a fine alignment using a camera alignment system. The operator is not looking for perfect alignment but would expect it to be close. At this point, the operator would have the opportunity to question the amount of distance needed to move the hoist into position. Possible responses include: (1) the position is not off by much, (2) the initial placement of the bell is in question and it is repositioned (which may be easier to accomplish than asking another crew member to move the CTT), or (3) a belief that the position of the CTT is not off center by enough to make a difference.

In this task, the CTM operator roughly centers the CTM over the cask port, lowers the shield, and opens the port and CTM gates. The operator needs to more accurately locate the grapple over the lid by moving the hoist within the bell. At this point, the operator has an opportunity to judge if the amount of movement required to align the grapple is too much for the lid to clear the edges of the port during the lift. In this case, it is not so much an observation error (the operator cannot help but observe the relative locations of the grapple and the lid) or a diagnosis error (the operator knows the canister is not perfectly centered), but rather a decision error, where the operator decides that it doesn't matter that the cask is not centered ("it's close enough"). This can be represented by CREAM CFF I2, adjusted by the following CPCs with values not equal to 1.0:

- CFF I2: Decision error (either not making a decision or making a wrong or incomplete decision). The baseline HEP is 0.01.

- CPC "Available Time": With regard to the general level of time pressure for the task and the situation type, it would be easy to believe that there is plenty of time since the consequences of taking more time are (from a safety perspective) insignificant. However, from a production perspective, this would be a significant setback since the CTM operator would have to get the CTT crew back to move the CTT, a time-consuming process. This time pressure could bias the operator towards a decision that "it's close enough." The CPC for an interpretation task with continuously inadequate available time is 5.0.

Applying these factors yields the following:

$$\text{Operator fails to notice that CTT is not sufficiently centered} = 0.01 \times 5 = 0.05$$

Operator Fails to Notice Lid Tilt—The CTM operator is able to see the lid through the camera display. When the lid strikes the ceiling, it begins to tilt as the hoist continues to rise. The operator has the opportunity to notice the tilting lid before it potentially jams and has the opportunity to stop the lift. The prior unsafe action of failing to notice that the cask is too far off center could still lead the operator to be somewhat more careful and observant during the lift than if it had been closer to center (e.g., like the extra care a driver might show while pulling into a narrower than normal parking space).

If the operator is looking at the camera view during the lift, then the operator has the opportunity to observe the lid contacting the ceiling of the Cask Unloading Room and tilting into the port rather than rising straight through. The most likely failure would be that the operator is not

looking at the screen at the time that this occurs, which can be represented by CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made (omission). The baseline HEP is 0.003.
- CPC "Adequacy of Man–Machine Interface": There are two vulnerabilities in the man–machine interface for this observation. First, there is no alarm or indicator to alert the operator. Second, the camera view is not perfect. These are inherent to this type of operation, but would make it more likely that the operator would not be looking at the screen at the time. Thus, the man–machine interface should be considered inappropriate with regard to success of this observation. The CPC for an observation task with inappropriate man–machine interface is 5.0.

Applying these factors yields the following:

$$\text{Operator fails to notice lid tilt} = 0.003 \times 5 = 0.02$$

Operator "Locks" Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to "lock" the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without an ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the action would not be perceived as unsafe but rather as a clever way to free time to get ready for subsequent steps or perform other duties. Again, the operator might be less likely to do this if there are doubts about the positioning of the cask.

The quantification of this event is discussed in detail under Scenario 1(c). In this scenario, it is judged that there is no bias dependency towards this failure that results from prior failures in the scenario. Therefore, the value used for the no-bias case is applied here:

$$\text{Operator "locks" lift button into place} = 0.05$$

Lid Catches and Jams in Port—Given the size of the lid in relation to the port, it is entirely possible that when it strikes the ceiling and tilts sideways, it still goes through the port at an angle without jamming.

The lid is smaller than the port, and a round object passing through a large round hole would generally be expected not to jam (unlike, for example, a square lid and a square hole where there are a number of orientations where jamming could occur). Nevertheless, for the purpose of this analysis this is assessed as having "even odds" of jamming versus not jamming.

$$\text{Lid catches and jams in port} = 0.5$$

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the lid jammed in the port would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

Load cell interlock fails = 2.7E−5

Mechanical Failure of Hoist under Overload Causes Lid Drop—There are three potential failure modes that could cause the lid to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the grapple or lid. However, just because the hoist keeps pulling does not mean that the lid falls (the hoist motor could overload and fail before the lid becomes detached from the hoist) or that the lid, once dropped, falls in an orientation that impacts the canister in the STC or aging overpack (the orientation of the falling lid may cause it to only impact the STC or aging overpack structure).

This event is quantified in Section E6.6.3.4.1.

Mechanical failure of hoist under overload causes lid drop = 0.1

HEP Calculation for Scenario 1(d)—The events in the HEP model for Scenario 1(d) are presented in Table E6.6-7.

Table E6.6-7. HEP Model for HFE Group #6 Scenario 1(d) for 050-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	CTT is not sufficiently centered under port	0.002
B	Operator fails to notice CTT not sufficiently centered	0.05
C	Operator fails to notice lid tilt and continues lift	0.02
D	Operator “locks” lift button into position	0.05
E	Lid catches and jams in port	0.5
F	Load cell overload interlock fails	2.7E−5
G	Mechanical failure of hoist under overload causes lid drop	0.1

NOTE: CTT = cask transfer trolley; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times (C + D) \times E \times F \times G =$$
$$0.002 \times 0.05 \times (0.02 + 0.05) \times 0.5 \times 2.7E{-}5 \times 0.1 < 1E{-}8 \qquad \text{(Eq. E-13)}$$

E6.6.3.4.2.5 HFE Group #6 Scenario 1(e) for 050-OpCTMdrop001-HFI-COD

1. Operator activates grapple disengagement switch prematurely.
2. Load cell disengagement interlock fails.
3. Lid drops from grapple and strikes canister.

Operator Activates Grapple Disengagement Switch Prematurely—Once engaged with the lid, the grapple is supposed to remain engaged until the lid is placed in its staging area. The operator could prematurely activate grapple disengagement for one of two reasons. Either the

wrong control could be activated (e.g., while closing the port slide gate), or a number of operational steps could be skipped and the operator could actuate the control.

This is a straightforward case of taking an action out of sequence. This can be represented by CREAM CFF E4, adjusted by the following CPCs with values not equal to 1.0:

- CFF E4: Action performed out of sequence (e.g., repetitions, jumps, reversals). The baseline HEP is 0.003.
- CPC "Working Conditions": With regard to this potential unsafe action, the working conditions for the CTM operator are deemed to be advantageous. The CPC for an execution task with advantageous working conditions is 0.8.
- CPC "Adequacy of Training/Preparation": This routine action is well trained and performed often. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator activates grapple disengagement switch prematurely} = 0.003 \times 0.8 \times 0.8 = 0.002$$

Load Cell Disengagement Interlock Fails—One of the load cell interlocks is designed to disable the grapple disengagement circuit if a load is sensed. This interlock would have to fail in order for the operator's action to trigger the disengagement mechanism.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

$$\text{Load cell disengagement interlock fails} = 2.7\text{E}{-5}$$

Lid Drops from Grapple and Strikes Canister—In order for the lid to actually drop, the grapple disengagement mechanism would need to overcome the dead weight friction caused by the weight of the lid. In the case of the canister, this is clearly expected to be true, but the lid weighs much less than the canister; thus, the same expectation is not clear. However, there is still a chance that the grapple would not disengage or would not disengage while the lid is over the open cask port.

There are a number of factors that affect the likelihood of this event. First, in order to strike the canister the disengagement must occur over the canister, including that the slide gates are open. Second, the design of the grapple is such that it may not have the force to disengage when it is loaded (this is certainly true when lifting a canister, but perhaps less so when lifting a lid). Finally, the lid has to fall in an orientation such that it strikes the canister. Taking this all into consideration, the HRA team judges that it is justifiable to assign a 10% chance that this event would occur.

$$\text{Lid drops from grapple and strikes canister} = 0.1$$

HEP Calculation for Scenario 1(e)—The events in the HEP model for Scenario 1(e) are presented in Table E6.6-8.

Table E6.6-8. HEP Model for HFE Group #6 Scenario 1(e) for 050-OpCTMdrop001-HFI-COD

Designator	Description	Probability
A	Operator activates grapple disengagement switch prematurely	0.002
B	Load cell disengagement interlock fails	2.7E−5
C	Lid drops from grapple and strikes canister	0.1

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.002 \times 2.7E{-}5 \times 0.1 < 1E{-}8 \quad \text{(Eq. E-14)}$$

E6.6.3.4.2.6 HEP for HFE 050-OpCTMdrop001-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for lifting a lid off an STC or aging overpack follows:

$$\begin{gathered}\text{050-OpCTMdrop001-HFI-COD (lid lift)} = \\ \text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(c)} + \text{HFE 1(d)} + \text{HFE 1(e)} = \\ (<1E{-}8) + 1E{-}7 + (<1E{-}8) + (<1E{-}8) + (<1E{-}8) = 2E{-}7\end{gathered} \quad \text{(Eq. E-15)}$$

The Boolean expression for the overall HFE (all scenarios) for placing a lid on an aging overpack follows:

$$\begin{gathered}\text{050-OpCTMdrop001-HFI-COD (lid placement)} = \\ \text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(e)} = \\ 2E{-}8 + 1E{-}7 + (<1E{-}8) = 2E{-}7\end{gathered} \quad \text{(Eq. E-16)}$$

Except for transportation cask/DPCs, which only have a lid placement, all canisters have one lid lift and one lid placement as part of their processing. For simplicity, transportation cask/DPCs are conservatively modeled the same as other canisters, and the Boolean expression for the overall HFE for a lid removal and a lid placement follows:

$$\begin{gathered}\text{050-OpCTMdrop001-HFI-COD (total)} = \\ \text{050-OpCTMdrop001-HFI-COD (lid removal)} + \\ \text{050-OpCTMdrop001-HFI-COD (lid placement)} = \\ 2E{-}7 + 2E{-}7 = 4E{-}7\end{gathered} \quad \text{(Eq. E-17)}$$

E6.6.3.4.3 Quantification of HFE Scenarios for 050-OpCTMdrop002-HFI-COD: Operator Causes Drop of Canister during CTM Operations (Low-Level Drop)

E6.6.3.4.3.1 HFE Group #6 Scenario 2(a) for 050-OpCTMdrop002-HFI-COD

1. Crew member improperly installs grapple.
2. Primary grapple interlock gives false positive signal.
3. Operator fails to notice bad connection between hoist and grapple through camera.
4. Grapple/canister drops from hoist.

Crew Member Improperly Installs Grapple—Prior to a lift operation, a crew member prepares the CTM for the operation by installing the appropriate grapple for the type of cask lid to be processed. While it is possible that this operation need not be performed (it may be the cask lid grapple is the same grapple used for previous CTM operation and no other work on or with the CTM may have been performed), it is uncertain how often this occurs, so this analysis considers that this action needs to be performed each time. To install the grapple, the primary CTM grapple lowers and engages the secondary grapple. If the primary grapple is only partially engaged, the secondary grapple would appear to be secured in place when it is not.

The operator aligns the grapple visually using the camera view and then engages the grapple. If it is not aligned properly, the grapple does not fully engage. The crew members locally verify engagement and connect the appropriate wire connections from the secondary grapple to the primary grapple. This is a straightforward matter of task execution. The task is simple and routine and can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well-designed, highly practiced routine task performed to the highest possible standards by highly motivated, highly trained, and experienced person, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure, so the APOA is set at 0.2.

- EPC 8: Poor environment. This EPC is applied not so much because the environment is poor, but rather that it is simply not optimal. The full affect EPC would be ×8, but this applies when working on the plant, with suit and breathing apparatus, possible access problems, and for more than 45 minutes so that fatigue sets in. The APOA anchor for 0.1 is for work in the plant with suit and breathing apparatus, but none of the other environmental stressors. In this task no breathing apparatus is required, but the task is somewhat physically demanding. Given the tradeoffs, the APOA is set at 0.1.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

Crew member improperly installs grapple =
$0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006$ (Eq. E-18)

Preoperational Check Fails to Note Improper Installation—There are two crew members responsible for preparing the CTM for each operation. Each crew member has a distinct set of assignments, although they collaborate when needed and are expected to check each other's work. The second crew member checks the first crew member's installation of the grapple, which provides an opportunity for the error to be detected. The second crew member also has a set of activities to perform, and so checking the first crew member is a secondary function. In addition, the existence of the grapple/hoist interlock provides an expectation that any error can be detected.

The second crew member would have helped initially with the connection of the grapple to line it up but would then move on to other things. At best, the second crew member performs a cursory check at the end of the job. Since the crew member was involved in the early stages, there is a bias that the job was done correctly. It is concluded that the level of dependence is high. The baseline HEP for the checking, for checking routine tasks without a checklist, is best determined from THERP (Ref. E8.1.26), Table 20-22, item (2), which is 0.2. The HEP for high dependence is from THERP, Table 20-21, item (4)(e), which is 0.6.

Preoperational check fails to note improper installation = 0.6

Primary Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the primary grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

Primary interlock gives false positive signal = 2.7E−5

Operator Fails to Notice Bad Connection between Hoist and Grapple through Camera—When the CTM operator is in the process of lifting the canister, the camera shows the operator the secondary grapple and its connection to the primary grapple. The operator is not focused on that connection but is focused on lining up the secondary grapple with the lifting device. However, as the lift begins, the operator is supposed to watch through the cameras. This gives the operator the opportunity to note that the grapple is not properly connected (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not expecting any problems in this simple operation, and the operator tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

This action is best represented by the CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0:

- CFF O3: Observation not made. The baseline HEP is 0.003.
- CPC "Adequacy of Man–Machine Interface": For this particular observation, the use of a camera view (while the only practical means) is somewhere between tolerable and inappropriate. The CPC for an observation task with tolerable man–machine interface is 1.0, and for inappropriate is 5.0. With regard to being able to actually observe the condition of the grapple lock pin, the CPC is set as 4.0.
- CPC "Number of Simultaneous Goals": The operator is primarily focusing on properly aligning the bell and hoist, opening the ports, and grappling the lid. While it could be argued that this is not "more than capacity," it certainly relegates looking at the grapple/hoist connection to a secondary action. It is therefore deemed appropriate to apply the more than capacity CPC, which is 2.0.
- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

The resulting value follows:

Operator fails to notice bad connection between hoist and grapple through camera =
$0.003 \times 4 \times 2 \times 0.8 = 0.02$

Grapple/Canister Drops from Hoist—Just because the lift is occurring with an improper grapple installation does not mean that the lid and grapple fall. The design safety margins built into these systems mean that it is possible that the lift and place can be completed successfully even with improper installation.

This event is quantified in Section E6.6.3.4.1.

Grapple/canister drops from hoist = 0.25

HEP Calculation for Scenario 2(a)—The events in the HEP model for Scenario 2(a) are presented in Table E6.6-9.

Table E6.6-9. HEP Model for HFE Group #6 Scenario 2(a) for 050-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	Crew member improperly installs grapple	0.0006
B	Preoperational check fails to note improper installation	0.6
C	Grapple/hoist interlock gives false positive signal	2.7E−5
D	Operator fails to notice bad connection between hoist and grapple through camera	0.02
E	Grapple/canister drops from hoist	0.25

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E{-}5 \times 0.02 \times 0.25 < 1E{-}8 \qquad \text{(Eq. E-19)}$$

E6.6.3.4.3.2 HFE Group #6 Scenario 2(b) for 050-OpCTMdrop002-HFI-COD

1. Operator fails to fully engage grapple.
2. Grapple engagement interlock gives false positive signal.
3. Operator fails to notice grapple not fully engaged through camera.
4. Canister drops from grapple.

Operator Fails to Fully Engage Grapple—The operator engages the grapple from the control panel. The grapple can be roughly positioned using the alignment guides for the CTM and the hoist height indicator on the control panel, but final alignment must be done visually using the view from the cameras provided on the grapple. Once the operator believes the grapple is aligned, the operator engages the grapple with the lift fixture and confirms through the camera that the grapple has engaged. If the operator sees that the grapple has not properly engaged (generally by checking the interlock condition if it looks engaged visually), then the operator disengages it, repositions the grapple, and tries again to engage.

The operator aligns the grapple visually using the view from the camera and engages the grapple. If it is not aligned properly, it does not fully engage. This unsafe action can be best represented by the task execution error NARA GTT A1, adjusted by the following CPCs:

- NARA GTT A1: Carry out a simple manual task with feedback. Skill-based and therefore not necessarily with procedures. The baseline HEP is 0.005.

- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. The crew member probably feels a little more time pressure than that, so the APOA is set at 0.2.

- EPC 11: Poor, ambiguous, or ill-matched system feedback. This EPC is applied to account for the need to observe the operation through cameras. The full affect EPC would be ×4. The full effect is applicable when legibility is poor or label is obscured or where the layout of controls makes visual access and physical access difficult. The use of the camera view is deemed to represent full effect. The APOA is set at 1.0.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Operator fails to fully engage grapple} = 0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad \text{(Eq. E-20)}$$

Grapple Engagement Interlock Gives False Positive Signal—Before beginning the lifting process, the operator should confirm engagement by checking the grapple engagement interlock. The indicator could give a false positive signal. This could result from a failure in the indicator itself or as the result of a partial engagement that generates a positive signal by triggering the sensor even though only partial engagement has occurred. Since the indicator system has not yet been designed and the specific detection approach has not been defined, this cannot be ruled out.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

$$\text{Grapple engagement interlock gives false positive signal} = 2.7\text{E}{-5}$$

Operator Fails to Notice Grapple Not Fully Engaged through Camera—As the lift begins, the operator is supposed to watch through the cameras. This allows the opportunity to note that the grapple is not properly engaged (e.g., unexpected lid movement to one side or tilting of the grapple). This also gives the operator the opportunity to question the stability of the connection and to lower the lid back down to recheck the connection. However, the operator is not expecting any problems in this simple operation, and the tendency is to believe that any perceived problems are illusions caused by the distortions of viewing through a camera.

In this case, the operator's check is a self-check; again, the operator is checking the actions taken through the camera. The operator believes that the action was initially performed correctly (because the action was performed by the operator), and this belief is confirmed by the false positive from the interlock, so this last observation is deemed completely dependent on the prior actions. Using THERP (Ref. E8.1.26) Table 20-21 to assess dependency, item (5) for complete dependency:

$$\text{Operator fails to notice grapple not fully engaged through camera} = 1.0$$

Canister Drops from Grapple—Just because the lift is occurring with an improper grapple engagement does not mean that the canister falls. The safety margins built into these systems mean that it is possible that the lift and place are completed successfully even with improper installation.

This event is quantified in Section E6.6.3.4.1.

Canister drops from grapple = 0.25

HEP Calculation for Scenario 2(b)—The events in the HEP model for Scenario 2(b) are presented in Table E6.6-10.

Table E6.6-10. HEP Model for HFE Group #6 Scenario 2(b) for 050-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	Operator fails to fully engage grapple	0.07
B	Grapple engagement interlock gives false positive signal	2.7E−5
C	Operator fails to notice grapple not fully engaged through camera	1.0
D	Canister drops from grapple	0.25

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D = 0.07 \times 2.7E{-}5 \times 1.0 \times 0.25 = 5E{-}7 \quad \text{(Eq. E-21)}$$

E6.6.3.4.3.3 HFE Group #6 Scenario 2(c) for 050-OpCTMdrop002-HFI-COD (Applies to DPC/Transportation Cask Only)

1. CTT is not sufficiently centered under port
2. Operator fails to notice CTT not sufficiently centered.
3. Operator fails to notice DPC contacting ceiling and continues lift OR operator "locks" lift button into position.
4. Load cell overload interlock fails.
5. Mechanical failure of hoist under overload causes DPC drop. (NOTE: This scenario only applies to transportation cask/DPCs because the transportation cask lid was removed in the preparation area).

CTT Is Not Sufficiently Centered under Port—This unsafe action actually occurs prior to this operation, during movement of the CTT into the Cask Unloading Room. The CTT operator brings the unit into the Cask Unloading Room and locates it centered directly under the cask port by aligning it against end stops that properly locate it and by using markings on the floor. If the transportation cask is not properly centered, it is possible that the DPC could strike the ceiling around the cask port rather than rising smoothly through the cask port. This only applies to DPCs because their transportation cask lids are removed in the preparation area. For all other waste forms any misalignment would be discovered during the lid lift by the CTM. In order for the DPC to hit the Cask Unloading Room ceiling during lift, the cask would have to be off-center by more than at least a few feet.

The unsafe action results from stopping the CTT prematurely and leaving it at least a number of feet short of the proper location. This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.

- CPC "Available Time": There is adequate time to perform this task. The only time pressure is the desire to keep the process moving, but the consequences are insignificant. The CPC for an execution task with adequate time is 0.5.

- CPC "Adequacy of Training/Preparation": This routine task is well trained and practiced and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.

The above parameters were the same as those applied to failure to properly center the CTT for a lid, where only being about a foot or two out of position could cause a problem. For the case of a canister, the miss must be by at least a few feet in order for the canister to strike the ceiling on the way up. The HRA team believes it is inappropriate to apply the same number to both unsafe actions, and deems it reasonable to further reduce the HEP for the unsafe action by a factor of two to account for this (a multiplier of 0.5).

Applying these factors yields the following:

$$\text{CTT is not sufficiently centered under port (DPC/transportation cask)} = 0.003 \times 0.5 \times 0.8 \times 0.5 = 0.001$$

Operator Fails to Notice that CTT Is Not Sufficiently Centered—The CTM operator centers the CTM grapple over the cask lid lift fixture using a two-step process. First the CTM operator does a rough alignment using the bridge and trolley position indicators and sets the bell and shield skirt in place. Then the operator opens the cask port and performs a fine alignment using a camera alignment system. The operator is not looking for perfect alignment but would expect it to be close. At this point, the operator would have the opportunity to question the amount of distance that the hoist has to be moved to be in position. Possible inappropriate responses include: (1) the initial placement of the bell is in question and it is repositioned (which may be easier to accomplish than asking another crew member to move the CTT), or (2) a belief that the position of the CTT is not off center by enough to make a difference.

In this task, the CTM operator roughly centers the CTM over the cask port, lowers the shield, and opens the port and CTM gates. The operator needs to more accurately locate the grapple over the lid by moving the hoist within the bell. At this point, the operator has an opportunity to judge if the amount of movement required to align the grapple is too much for the lid to clear the edges of the port during the lift. In this case, it is not so much an observation error (the operator cannot help but observe the relative locations of the grapple and the lid) or a diagnosis error (the operator knows the canister is not perfectly centered), but rather a decision error, where the operator decides that it doesn't matter that the cask is not centered ("it's close enough"). This

can be represented by CREAM CFF I2, adjusted by the following CPCs with values not equal to 1.0.

- CFF I2: Decision error (either not making a decision or making a wrong or incomplete decision). The baseline HEP is 0.01.

- CPC "Available Time": With regard to the general level of time pressure for the task and the situation type, it would be easy to believe that there is plenty of time since the consequences of taking more time are (from a safety perspective) insignificant. However, from a production perspective, this would be a significant setback since the CTM operator would have to get the CTT crew back to move the CTT, a time-consuming process. This time pressure could bias the operator towards a decision that "it's close enough." The CPC for an interpretation task with continuously inadequate available time is 5.0.

Applying these factors yields the following:

Operator fails to notice that CTT is not sufficiently centered = $0.01 \times 5 = 0.05$

Operator Fails to Notice DPC Contacting Ceiling and Continues Lift—The CTM operator is able to see the DPC through the camera display. When the DPC strikes the ceiling, it stops as the hoist continues to try to rise. The operator has an opportunity to notice the stopped CTM before it stops the lift. The prior unsafe action of failing to notice that the cask is too far off center could lead the operator to be somewhat more careful and observant during the lift than if it had been closer to center (e.g., like the extra care a driver might show while pulling into a narrower than normal parking space).

If the operator is looking at the camera view during the lift, there is an opportunity to observe the DPC contacting the ceiling of the Cask Unloading Room and stopping rather than rising straight through. The most likely failure is not looking at the screen at the time this occurs, which can be represented by CREAM CFF O3, adjusted by the following CPCs with values not equal to 1.0.

- CFF O3: Observation not made (omission). The baseline HEP is 0.003.

- CPC "Adequacy of Man–Machine Interface": There are two vulnerabilities in the man–machine interface for this observation. First, there is no alarm or indicator to alert the operator. Second, the camera view is not perfect. These are inherent to this type of operation, but would make it more likely that the operator would not be looking at the screen at the time. Thus, the man–machine interface could be considered inappropriate with regard to success of this observation (as it was for scenario 1(e)). However, the fact that the magnitude of the CTT offset required to cause a problem is so much greater in this case argues for a somewhat lesser adjustment. That is, the man–machine interface is somewhat better with regard to this failure, and it is more likely that the operator is looking and sees the contact. The CPC for an observation task with inappropriate man–machine interface is 5.0. The HRA team has determined that a CPC of 3.0 is more appropriate in this case.

Applying these factors yields the following:

$$\text{Operator fails to notice DPC contacting ceiling and continues lift} = 0.003 \times 3 = 0.01$$

Operator "Locks" Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to "lock" the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the action would not be perceived as unsafe but rather as a clever way to free time to get ready for subsequent steps or perform other duties. Again, the operator might be less likely to do this if there are doubts about the positioning of the cask.

The quantification of this event is discussed in detail under Scenario 1(c). In this scenario, it is judged that there is no bias dependency towards this failure that results from prior failures in the scenario. Therefore, the value used for the no-bias case (0.05) could be applied here. However, similar to the previous discussion, the HRA team believes that the magnitude of the CTT offset required to cause a problem actually creates a bias in the operator against taking any shortcuts (as opposed to no bias), so that a further reduction of 0.5 should be applied.

$$\text{Operator "locks" lift button into place} = 0.05 \times 0.5 = 0.03$$

Load Cell Overload Interlock Fails—The load cell has an interlock that shuts off the hoist if it senses that the load exceeds the approved load for the hoist. The hoist straining to lift the DPC in contact with the ceiling would be one such condition. Since this would shut the hoist down prior to exceeding the ultimate capacity of the system, it would have to fail in order to cause a drop.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

$$\text{Load cell interlock fails} = 2.7\text{E}{-5}$$

Mechanical Failure of Hoist under Overload Causes DPC Drop—There are three potential failure modes that could cause the canister to detach from the hoist. The cable could fail, the grapple could break free from the lower block, or the lifting fixture could break free from the grapple or DPC. However, just because the hoist keeps pulling does not mean that the DPC falls (the hoist motor could overload and fail before the DPC becomes detached from the hoist).

This event is quantified in Section E6.6.3.4.1.

$$\text{Mechanical failure of hoist under overload causes DPC drop} = 0.25$$

HEP Calculation for Scenario 2(c)—The events in the HEP model for Scenario 2(c) are presented in Table E6.6-11.

Table E6.6-11. HEP Model for HFE Group #6 Scenario 2(c) for 050-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	CTT is not sufficiently centered under port	0.001
B	Operator fails to notice CTT not sufficiently centered	0.05
C	Operator fails to notice DPC contacting ceiling and continues lift	0.01
D	Operator "locks" lift button into position	0.03
E	Load cell overload interlock fails	2.7E−5
F	Mechanical failure of hoist under overload causes DPC drop	0.25

NOTE: CTT = cask transfer trolley; DPC = dual-purpose canister; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times (C + D) \times E \times F = 0.001 \times 0.05 \times (0.01 + 0.03) \times 2.7E{-}5 \times 0.25 < 1E{-}8 \quad \text{(Eq. E-22)}$$

E6.6.3.4.3.4 HEP for HFE 050-OpCTMdrop002-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for lifting a DPC/transportation cask follows:

$$\text{050-OpCTMdrop002-HFI-COD (DPC/transportation cask)} = \text{HFE 2(a)} + \text{HFE 2(b)} + \text{HFE 2(c)} = (<1E{-}8) + 5E{-}7 + (<1E{-}8) = 5E{-}7 \quad \text{(Eq. E-23)}$$

The Boolean expression for the overall HFE (all scenarios) for lifting all other canisters follows:

$$\text{050-OpCTMdrop002-HFI-COD (non-DPC/transportation cask)} = \text{HFE 2(a)} + \text{HFE 2(b)} = (<1E{-}8) + 5E{-}7 = 5E{-}7 \quad \text{(Eq. E-24)}$$

E6.6.3.4.4 Quantification of HFE Scenarios for 050-OpCTMImpact1-HFI-COD: Operator Moves the CTM while Canister or Object Is below or between Levels

E6.6.3.4.4.1 HFE Group #6 Scenario 3(a) for 050-OpCTMImpact1-HFI-COD

1. Operator leaves CTM in lid lift mode (nontransportation cask/DPCs).
2. Operator fails to notice that lift stops too soon.
3. Operator fails to close port slide gate OR fails to notice that it does not fully close.
4. Operator fails to close CTM slide gate OR fails to notice it does not fully close.
5. CTM slide gate interlock fails.

Operator Leaves CTM in Lid Lift Mode (Nontransportation Cask/DPCs)—The operator is supposed to set the ASD to canister lift mode prior to lifting the canister. It should be in lid lift mode because the lid was lifted right before the canister. Failing to reset for canister lift would result in the canister stopping part way through the port.

Setting the CTM system to the appropriate lift mode prior to performing a lift is fundamental to the operation, not simply a step in a procedure that can be missed. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in lid lift mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3, adjusted by the following EPCs:

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves CTM in lid lift mode = 0.0007

Operator Fails to Notice that Lift Stops too Soon—Lifting the canister takes on the order of ten minutes, whereas lifting the lid takes only on the order of three minutes. Since the operator has to hold the lift button in or the lift stops, there is an opportunity to notice that the hoist has stopped sooner than expected. On the control panel the operator would have the camera view and also the hoist position indication, either of which can confirm that the canister has not been fully lifted. Failure to do so would result in continuing the operations with the canister between floors.

The operator is supposed to hold the lift button until the lift automatically stops. The operator has performed this operation many times in the past and has an instinctive feel for how long the lift takes. A canister lift should take around three times as long as a lid lift. If the operator feels it has not taken long enough, the camera and the indicators on the control panel can provide confirmation that the lift was prematurely terminated. Failing to recognize the short lift (and thus an implied failure to question the result of the action) could be an observation error (CREAM CFF O2, wrong identification made, or O3, observation not made). But the more conservative and more applicable approach is represented by the interpretation error CREAM CFF I1, adjusted by the following CPCs with values not equal to 1.0:

- CFF I1: Faulty diagnosis (either a wrong diagnosis or an incomplete diagnosis). The baseline HEP is 0.2.

- CPC “Working Conditions”: The operator has optimal working conditions in the control room. The CPC for an interpretation task with advantageous working conditions is 0.8.

- CPC “Available Time”: The operator clearly has adequate time before beginning the next steps in the process to realize that the amount of time spent in the lift is not reasonable for a canister lift. The CPC for an interpretation task with adequate available time is 0.5.

- CPC “Adequacy of Training/Preparation”: Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to notice lift is taking too long} = 0.2 \times 0.8 \times 0.5 \times 0.8 = 0.07$$

Operator Fails to Close Port Slide Gate—The operator is supposed to close the port slide gate as soon as the lift is completed. This gives the operator an opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the canister). In the latter case, the slide gate open/close indicator lights are in an incorrect state (either both on or both off, depending on design).

The operator is supposed to close the port slide gate prior as a part of the lift and transfer process. This is an EOO that can most closely be represented by CREAM CFF E5, adjusted by the following CPCs with values not equal to 1.0:

- CFF E5: Action missed, not performed (omission), including the omission of the last actions in a series. The baseline HEP is 0.03.
- CPC "Available Time": There is adequate time available. The CPC for an execution task with adequate time is 0.5.
- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to close port slide gate} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—The action of closing the port slide gate is simple. In this scenario, the gate does not close all the way because the canister is in the way. The operator has visible feedback on the failure of the gate to close because the "open" (or "green") light on the control panel stays on and the "closed" (or "red") light also comes on and stays on. Both lights on at the same time signifies that the port is neither fully open nor fully closed. The problem can be easily confirmed by looking at the camera or checking the status of the light curtain at the bottom of the bell. This unsafe action can be represented by NARA GTT C1, adjusted by the following EPCs:

- GTT C1: Simple response to a range of alarms/indications providing clear indication of situation (simple diagnosis required). The baseline HEP is 0.0004.
- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. This appears reasonable for this task, so the APOA is set at 0.1.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Operator fails to notice that port slide gate does not fully close} = 0.0004 \times [(11-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.001 \quad \text{(Eq. E-25)}$$

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the CTM slide gate as soon as the port slide gate is closed. This gives the operator another opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the hoist cables or load cell). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

The baseline HEP for failure to close this gate would be the same as for the similar unsafe action for the port slide gate.

Operator fails to close CTM slide gate (independent) = 0.01

However, this would only apply in the case where the earlier unsafe action was failure to notice that the port slide gate had failed to close. In the case where the earlier unsafe action was failure to close the port slide gate, there is a dependence on the failure to perform a similar task next in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP Table 20-21, the HEP follows:

Operator fails to close CTM slide gate (given failure to close the port slide gate) = 0.5

Operator Fails to Notice CTM Slide Gate Does Not Fully Close—The baseline HEP for failure to notice this gate did not fully close would be the same as for the similar unsafe action for the port slide gate.

Operator fails to notice CTM slide gate does not fully close (independent) = 0.001

However, this would only apply in the case where the earlier unsafe action was failure to close the port slide gate. In the case where the earlier unsafe action was failure to notice that the port slide gate did not fully close, there is a dependence on the failure to perform a similar task next in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP Table 20-21, the HEP follows:

Operator fails to notice CTM slide gate does not fully close
(given failure to notice that port slide gate did not fully close) = 0.5

CTM Slide Gate Interlock Fails—The CTM slide gate interlock prevents CTM movement with the slide gate open (i.e., the shield skirt cannot be raised). If the interlock itself fails, the operator can move the CTM with the canister between levels.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

CTM slide gate interlock fails = 2.7E−5

HEP Calculation for Scenario 3(a)—The events in the HEP model for Scenario 3(a) are presented in Table E6.6-12.

Table E6.6-12. HEP Model for HFE Group #6 Scenario 3(a) for 050-OpCTMImpact1-HFI-COD

Designator	Description	Probability
A	Operator leaves CTM in lid lift mode	0.0007
B	Operator fails to notice that lift stops too soon	0.07
C	Operator fails to close port slide gate	0.01
D	Operator fails to notice that port slide gate does not fully close	0.001
E1	Operator fails to close CTM slide gate (independent)	0.01
E2	Operator fails to close CTM slide gate (given failure to close the port slide gate)	0.5
F1	Operator fails to notice CTM slide gate does not fully close (independent)	0.001
F2	Operator fails to notice CTM slide gate does not fully close (given failure to notice that port slide gate did not fully close)	0.5
G	CTM slide gate interlock fails	2.7E−05

NOTE: CTM = canister transfer machine; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times \{[C \times (E2 + F1)] + [D \times (E1 + F2)]\} \times G = 0.0007 \times 0.07 \times \{[0.01 \times (0.5 + 0.001)] + [0.001 \times (0.01 + 0.5)]\} \times 2.7E{-}05 = 0.0007 \times 0.07 \times 0.006 \times 2.7E{-}05 = (<1E{-}8) \quad \text{(Eq. E-26)}$$

E6.6.3.4.4.2 HFE Group #6 Scenario 3(b) for 050-OpCTMImpact1-HFI-COD

1. Operator places CTM in lid lift mode (transportation cask/DPCs).
2. Operator fails to notice that lift stops too soon.
3. Operator fails to close port slide gate OR fails to notice that it does not fully close.
4. Operator fails to close CTM slide gate OR fails to notice it does not fully close.
5. CTM slide gate interlock fails.

Operator Inadvertently Places CTM in Lid Lift Mode (DPCs)—The operator is supposed to set the ASD to canister lift mode prior to lifting the canister. For transportation cask/DPC operations, the ASD is in maintenance (or manual) lift mode because this is the default positioning. Failing to reset for canister lift would result in the canister stopping part way through the port.

Setting the CTM system to the appropriate lift mode prior to performing a lift is fundamental to the operation, not simply a step in a procedure that can be missed. For the situation involving transportation cask/DPCs, the ASD has been in maintenance mode as a default condition; therefore, the operator must inadvertently set the ASD to lid lift mode rather than canister lift mode. There are only two modes to choose from: lid lift and canister lift. The ASD control is a screen where the operator can scroll between the choices to pick the appropriate lift mode. The act of selecting the wrong mode from these two can be best represented by the task execution error NARA GTT A1, adjusted by the following CPC:

- NARA GTT A1: Carry out a simple single manual action with feedback. Skill-based and, therefore, not necessarily with procedures. The baseline HEP is 0.005.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The ASD control system requests confirmation from the operator (e.g., "You have selected canister lift. Confirm Y/N"). The baseline HEP is used without adjustment.

Operator inadvertently places CTM in lid lift mode (DPCs) = 0.005

Operator Fails to Notice that Lift Stops too Soon—Lifting the canister takes on the order of ten minutes, whereas lifting the lid takes only on the order of three minutes. Since the operator has to hold the lift button in or the lift stops, there is an opportunity to notice that the hoist has stopped sooner than expected. On the control panel the operator would have the camera view and also the hoist position indication, either of which can confirm the suspicion that the canister has not been fully lifted. Failure to do so would result in continuing the operations with the canister between floors.

The operator is supposed to hold the lift button until the lift automatically stops. The operator has performed this operation many times in the past and has an instinctive feel for how long the lift takes. A canister lift should take around three times as long as a lid lift. If the operator feels it has not taken long enough, the camera and the indicators on the control panel can provide confirmation that the lift was prematurely terminated. Failing to recognize the short lift (and thus an implied failure to question the result of the action) could be an observation error (CREAM CFF O2, wrong identification made, or O3, observation not made). But the more conservative and more applicable approach is represented by the interpretation error CREAM CFF I1, adjusted by the following CPCs with values not equal to 1.0:

- CFF I3: Faulty diagnosis (either a wrong diagnosis or an incomplete diagnosis). The baseline HEP is 0.2.

- CPC "Working Conditions": The operator has optimal working conditions in the control room. The CPC for an interpretation task with advantageous working conditions is 0.8.

- CPC "Available Time": The operator clearly has adequate time before beginning the next steps in the process to realize that the amount of time spent in the lift is not reasonable for a canister lift. The CPC for an interpretation task with adequate available time is 0.5.

- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an observation task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to notice lift is taking too long} = 0.2 \times 0.8 \times 0.5 \times 0.8 = 0.07$$

Operator Fails to Close Port Slide Gate—The operator is supposed to close the port slide gate as soon as the lift is completed. This gives the operator an opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the canister). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

The operator is supposed to close the port slide gate prior as a part of the lift and transfer process. This is an EOO that can most closely be represented by CREAM CFF E5, adjusted by the following CPCs with values not equal to 1.0:

- CFF E5: Action missed, not performed (omission), including the omission of the last actions in a series. The baseline HEP is 0.03.

- CPC "Available Time": There is adequate time available. The CPC for an execution task with adequate time is 0.5.

- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to close port slide gate} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—The action of closing the port slide gate is simple. In this scenario, the gate does not close all the way because the canister is in the way. The operator has visible feedback on the failure of the gate to close because the "open" (or "green") light on the control panel stays on and the "closed" (or "red") light also comes on and stays on. Both lights on at the same time signify that the port is neither fully open nor fully closed. The problem can be easily confirmed by looking at the camera or checking the status of the light curtain at the bottom of the bell. This unsafe action can be represented by NARA GTT C1, adjusted for the following EPCs.

- GTT C1: Simple response to a range of alarms/indications providing clear indication of situation (simple diagnosis required). The baseline HEP is 0.0004.

- EPC 3: Time pressure. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is

that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. This appears reasonable for this task, so the APOA is set at 0.1.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields the following:

$$\text{Operator fails to notice that port slide gate does not fully close} = 0.0004 \times [(11-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.001 \quad \text{(Eq. E-27)}$$

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the CTM slide gate as soon as the port slide gate is closed. This gives the operator another opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the hoist cables or load cell). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

The baseline HEP for failure to close this gate would be the same as for the similar unsafe action for the port slide gate.

$$\text{Operator fails to close CTM slide gate (independent)} = 0.01$$

However, this would only apply in the case where the earlier unsafe action was failure to notice that the port slide gate had failed to close. In the case where the earlier unsafe action was failure to close the port slide gate, there is a dependence on the failure to perform a similar task next in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP Table 20-21, the HEP follows:

$$\text{Operator fails to close CTM slide gate (given failure to close the port slide gate)} = 0.5$$

Operator Fails to Notice CTM Slide Gate Does Not Fully Close—The baseline HEP for failure to notice this gate did not fully close would be the same as for the similar unsafe action for the port slide gate.

$$\text{Operator fails to notice CTM slide gate does not fully close (independent)} = 0.001$$

However, this would only apply in the case where the earlier unsafe action was failure to close the port slide gate. In the case where the earlier unsafe action was failure to notice that the port slide gate did not fully close, there is a dependence on the failure to perform a similar task next in the sequence. It is judged that the dependence between these two actions is high. Using item (4)(a) from THERP Table 20-21, the HEP follows:

Operator fails to notice CTM slide gate does not fully close
(given failure to notice that port slide gate did not fully close) = 0.5

CTM Slide Gate Interlock Fails—The CTM slide gate interlock prevents CTM movement with the slide gate open (i.e., the shield skirt cannot be raised). If the interlock itself fails, the operator can move the CTM with the canister between levels.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

CTM slide gate interlock fails = 2.7E−5

HEP Calculation for Scenario 3(b)—The events in the HEP model for Scenario 3(b) are presented in Table E6.6-13.

Table E6.6-13. HEP Model for HFE Group #6 Scenario 3(b) for 050-OpCTMImpact1-HFI-COD

Designator	Description	Probability
A	Operator inadvertently places CTM in lid lift mode	0.005
B	Operator fails to notice that lift stops too soon	0.07
C	Operator fails to close port slide gate	0.01
D	Operator fails to notice that port slide gate does not fully close	0.001
E1	Operator fails to close CTM slide gate (independent)	0.01
E2	Operator fails to close CTM slide gate (given failure to close the port slide gate)	0.5
F1	Operator fails to notice CTM slide gate does not fully close (independent)	0.001
F2	Operator fails to notice CTM slide gate does not fully close (given failure to notice that port slide gate did not fully close)	0.5
G	CTM slide gate interlock fails	2.7E−05

NOTE: CTM = canister transfer machine; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times \{[C \times (E2 + F1)] + [D \times (E1 + F2)]\} \times G = 0.005 \times 0.07 \times \{[0.01 \times (0.5 + 0.001)] + [0.001 \times (0.01 + 0.5)]\} \times 2.7E{-}05 = 0.005 \times 0.07 \times 0.006 \times 2.7E{-}05 = (<1E{-}8) \quad \text{(Eq. E-28)}$$

E6.6.3.4.4.3 HFE Group #6 Scenario 3(c) for 050-OpCTMImpact1-HFI-COD

1. Operator puts CTM in maintenance mode (nontransportation cask/DPCs)
2. Operator terminates lift prior to automatic stop
3. Operator fails to close port slide gate OR fails to notice that it does not fully close
4. Operator fails to close CTM slide gate OR fails to notice it does not fully close.
5. CTM slide gate interlock fails.

Operator puts CTM in maintenance mode (Nontransportation cask/DPCs). The operator is supposed to set the ASD to canister lift mode prior to lifting the canister. It should be in lid lift

mode because the lid was lifted right before the canister. Placing it in the maintenance mode instead of the canister lift mode removes the ASD height control set point and also defeats the CTM slide gate interlock (since maintenance mode would allows CTM movement with the slide gate open). In order to place it into maintenance mode the operator is required to enter a password.

In this case, the operator commits the unsafe action of placing the CTM in maintenance mode. This is not easy to do, since if the operator inadvertently selects this mode, the operator is asked to confirm the selection and is also required to enter a password, which is not required for the selection of canister mode. This can be represented by NARA GTT A5, adjusted for the following EPCs:

- GTT A5: Completely familiar, well designed highly practiced, routine task performed to highest possible standards by highly motivated, highly trained and experienced personnel, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 6: A means of suppressing or overriding information or features that are too easily accessible. In this case, while a warning is given and a password is required, the operator still can override the feature and enter manual mode. The full affect is ×9. The APOA anchor for 0.5 is for something overridden on a regular basis. The APOA anchor for 0.1 is for something overridden once in a while. Other considerations for a reduction from full affect are a good interface design and good safety culture. Since maintenance mode is required on a regular basis but there are other mitigating factors, it appears reasonable for this task that the APOA be set at 0.3.

Using the NARA HEP equation yields the following:

$$\text{Operator puts CTM in maintenance mode} = 0.0001 \times [(9-1) \times 0.3 + 1] = 0.0004 \quad \text{(Eq. E-29)}$$

Operator Terminates Lift Prior to Automatic Stop—The operator is supposed to hold the lift button until the lift automatically stops. This happens even in the maintenance mode since the interlocks that prevent two-blocking are still active, and the CTM transfer sequence can still be completed successfully. However, if the operator terminates the lift prematurely, the canister could still be between floors.

The unsafe action results from stopping the hoist prematurely and leaving the canister below or between the floors (a number of feet short of the proper location). This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed or direction). The baseline HEP is 0.003.

There are no CPCs that are deemed to have values not equal to 1.0 for this action.

Applying these factors yields the following:

Operator terminates lift prior to automatic stop =0.003

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the port slide gate as soon as the lift is completed. This gives the operator an opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the canister). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

This value is the same as for Scenario 3(a):

Operator fails to close port slide gate = 0.01

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—This value is the same as for Scenario 3(a).

Operator fails to notice that port slide gate does not fully close = 0.001

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the CTM slide gate as soon as the port slide gate is closed. This gives the operator another opportunity to determine that the canister is not fully withdrawn. The operator would fail to notice this if either the operator skipped this step or if the operator performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the hoist cables or load cell). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

This value is the same as for Scenario 3(a):

Operator fails to close CTM slide gate (independent) = 0.01

Operator fails to close CTM slide gate (given failure to close the port slide gate) = 0.5

Operator Fails to Notice CTM Slide Gate Does Not Fully Close—This value is the same as for Scenario 3(a):

Operator fails to notice CTM slide gate does not fully close (independent) = 0.001

Operator fails to notice CTM slide gate does not fully close (given failure to notice that port slide gate did not fully close) = 0.5

CTM Slide Gate Interlock Fails

The CTM slide gate interlock prevents CTM movement with the slide gate open (the shield skirt cannot be raised). If the interlock itself fails, the operator can move the CTM with the canister between levels. Note: the maintenance mode does not bypass the shield skirt/slide gate interlock; this interlock cannot be bypassed.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

CTM slide gate interlock fails = 2.7E−5

HEP Calculation for Scenario 3(c)—The events in the HEP model for Scenario 3(c) are presented in Table E6.6-14.

Table E6.6-14. HEP Model for HFE Group #6 Scenario 3(c) for 050-OpCTMImpact1-HFI-COD

Designator	Description	Probability
A	Operator puts CTM in maintenance mode	0.0004
B	Operator terminates lift prior to automatic stop	0.003
C	Operator fails to close port slide gate	0.01
D	Operator fails to notice that port slide gate does not fully close	0.001
E1	Operator fails to close CTM slide gate (independent)	0.01
E2	Operator fails to close CTM slide gate (given failure to close the port slide gate)	0.5
F1	Operator fails to notice CTM slide gate does not fully close (independent)	0.001
F2	Operator fails to notice CTM slide gate does not fully close (given failure notice that port slide gate did not fully close)	0.5
G	CTM slide gate interlock fails	2.7E−05

NOTE: CTM = canister transfer machine; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times \{[C \times (E2 + F1)] + [D \times (E1 + F2)]\} \times G = 0.0004 \times 0.003 \times \{[0.01 \times (0.5 + 0.001)] + [0.001 \times (0.01 + 0.5)]\} \times 2.7E{-}05 = 0.0004 \times 0.003 \times .006 \times 2.7E{-}05 = 7E{-}09 \times 2.7E{-}05 = (<1E{-}08) \quad \text{(Eq. E-30)}$$

Truncating the human failure component, the HEP for this scenario becomes:

$$1E{-}5 \times 2.7E{-}5 = (<1E{-}08) \quad \text{(Eq. E-31)}$$

E6.6.3.4.4.4 HFE Group #6 Scenario 3(d) for 050-OpCTMImpact1-HFI-COD

1. Operator leaves CTM in maintenance mode (transportation cask/DPCs).
2. Operator terminates lift prior to automatic stop.
3. Operator fails to close port slide gate OR fails to notice that it does not fully close.
4. Operator fails to close CTM slide gate OR fails to notice it does not fully close.
5. CTM slide gate interlock fails.

Operator Leaves CTM in Maintenance Mode (transportation cask/DPCs)—The operator is supposed to set the ASD to canister lift mode prior to lifting the canister. For transportation cask/DPC operations, the ASD is in maintenance (or manual) lift mode because this is the default positioning. Leaving it in the maintenance mode instead of the canister lift mode removes the

ASD height control set point and also defeats the CTM slide gate interlock (since maintenance mode allows CTM movement with the slide gate open).

In this case, this leaves the ASD in maintenance mode, which is the default position for DPC operations. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in maintenance mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3, adjusted by the following EPCs:

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves CTM in maintenance mode = 0.0007

Operator Terminates Lift Prior to Automatic Stop—The operator is supposed to hold the lift button in until the lift automatically stops. This happens even in the maintenance mode since the interlocks that prevent two-blocking are still active, and the CTM transfer sequence can still be completed successfully. However, if the operator terminates the lift prematurely, the canister could still be between floors.

The unsafe action results from stopping the hoist prematurely and leaving the canister below or between the floors (i.e., a number of feet short of the proper location). This can be represented by CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.

There are no CPCs that are deemed to have values not equal to 1.0 for this action.

Applying these factors yields the following:

Operator terminates lift prior to automatic stop = 0.003

Operator Fails to Close Port Slide Gate—The operator is supposed to close the port slide gate as soon as the lift is completed. This gives the operator the opportunity to determine that the canister is not fully withdrawn. This failure would go unnoticed if the operator either skipped this step or performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the canister). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

This value is the same as for Scenario 3(a):

Operator fails to close port slide gate = 0.01

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—This value is the same as for Scenario 3(a):

Operator fails to notice that port slide gate does not fully close = 0.001

Operator Fails to Close CTM Slide Gate—The operator is supposed to close the CTM slide gate as soon as the port slide gate is closed. This gives the operator another opportunity to determine that the canister is not fully withdrawn. This would go unnoticed if the operator either skipped this step or performed the action and failed to notice that the gate had not closed all the way (e.g., because it is blocked from doing so by the hoist cables or load cell). In the latter case, the slide gate open/close indicator lights would be in an incorrect state (either both on or both off, depending on design).

This value is the same as for Scenario 3(a):

Operator fails to close CTM slide gate (independent) = 0.01

Operator fails to close CTM slide gate (given failure to close the port slide gate) = 0.5

Operator Fails to Notice CTM Slide Gate Does Not Fully Close—This value is the same as for Scenario 3(a):

Operator fails to notice CTM slide gate does not fully close (independent) = 0.001

Operator fails to notice CTM slide gate does not fully close
(given failure notice that port slide gate did not fully close) = 0.5

CTM Slide Gate Interlock Fails

The CTM slide gate interlock prevents CTM movement with the slide gate open (the shield skirt cannot be raised). If the interlock itself fails, the operator can move the CTM with the canister between levels. Note: the maintenance mode does not bypass the shield skirt/slide gate interlock; this interlock cannot be bypassed.

This is a mechanical failure of the interlock. This event is quantified in Section E6.6.3.4.1.

CTM slide gate interlock fails = 2.7E−5

HEP Calculation for Scenario 3(d)—The events in the HEP model for Scenario 3(d) are presented in Table E6.6-15.

Table E6.6-15. HEP Model for HFE Group #6 Scenario 3(d) for 050-OpCTMImpact1-HFI-COD

Designator	Description	Probability
A	Operator leaves CTM in maintenance mode	0.0007
B	Operator terminates lift prior to automatic stop	0.003
C	Operator fails to close port slide gate	0.01
D	Operator fails to notice that port slide gate does not fully close	0.001
E1	Operator fails to close CTM slide gate (independent)	0.01
E2	Operator fails to close CTM slide gate (given failure to close the port slide gate)	0.5
F1	Operator fails to notice CTM slide gate does not fully close (independent)	0.001
F2	Operator fails to notice CTM slide gate does not fully close (given failure to notice that port slide gate did not fully close)	0.5
G	CTM slide gate interlock fails	2.7E−05

NOTE: CTM = canister transfer machine; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times \{[C \times (E2 + F1)] + [D \times (E1 + F2)]\} \times G =$$
$$0.0007 \times 0.003 \times \{[0.01 \times (0.5 + 0.001)] + [0.001 \times (0.01 + 0.5)]\} \times 2.7E{-}05 =$$
$$0.0004 \times 0.003 \times 0.006 \times 2.7E{-}05 = 7E{-}09 \times 2.7E{-}05 = (<1E{-}08) \quad \text{(Eq. E-32)}$$

Truncating the human failure component, the HEP for this scenario becomes:

$$1E{-}5 \times 2.7E{-}5 = (<1E{-}08) \quad \text{(Eq. E-33)}$$

E6.6.3.4.4.5 HEP for HFE 050-OpCTMImpact1-HFI-COD

The Boolean expression for the overall HFE (all scenarios) follows:

$$\text{050-OpCTMImpact1-HFI-COD} = \text{HFE 3(a)} + \text{HFE 3(b)} + \text{HFE 3(c)} +$$
$$\text{HFE 3(d)} = (<1E{-}8) + (<1E{-}8) + (<1E{-}8) + (<1E{-}8) = 4E{-}8 \quad \text{(Eq. E-34)}$$

NOTE: For lifting objects (STC or aging overpack lids), the only failure mode that is applicable is 3(d); therefore, 4E−8 conservatively models movement with the lid below the floor.

E6.6.3.4.5 Quantification of HFE Scenarios for 050-OPCTMDirExp1-HFI-NOD: Operator Causes Direct Exposure during CTM Activities (Second Floor)

E6.6.3.4.5.1 HFE Group #6 Scenario 4(a) for 050-OPCTMDirExp1-HFI-NOD

1. Worker violates administrative control by entering the Canister Transfer Room during canister transfer.

2. Operator fails to close port gate before raising shield skirt.

Worker Violates Administrative Control by Entering the Canister Transfer Room during Canister Transfer—If a worker enters the Canister Transfer Room during canister transfer operations, there is a potential for direct exposure. There are several administrative controls restricting personnel from entering the Canister Transfer Room during canister transfer. These controls include the following:

- Personnel are only allowed in the Canister Transfer Room during prescheduled times.
- All personnel must check in with the control room (where the CTM is controlled) before entering the Canister Transfer Room.

If these controls are violated and a person enters the Canister Transfer Room when transfer operations are occurring, that person increases the potential to be exposed.

Any worker that wishes to enter the Canister Transfer Room needs to get permission to do so from a supervisor. If a worker violates this requirement, there is nothing that stops the worker from entering the room. However, this administrative control is fundamental to the operation of the facility and applies to entry to all important (i.e., radiation-controlled) areas of the facility. This is best represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well-designed, highly practiced routine task performed to highest possible standards by highly motivated, highly trained, and experienced personnel, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.
- EPC 7: No obvious means of reversing an unintended action. The GTT HEP is based on there being time to correct potential errors. This does not exist for this task. The maximum effect of the EPC is 9, which applies when there is no means of recovering from an unintended action once executed. Given that the error is not correctable, the APOA is set at 1.0.

This assessment does not give credit for the worker believing that there is a need to enter the Canister Transfer Room in the first place.

Applying the NARA HEP equation yields the following:

$$\text{Worker violates administrative control by entering the Canister Transfer Room during canister transfer} = 0.0001 \times [(9-1) \times 1.0 + 1] = 0.0009 \qquad \text{(Eq. E-35)}$$

Operator Fails to Close Port Gate before Lifting Shield Skirt—Just entering the Canister Transfer Room during canister transfer cannot result in an exposure since the entire operation is shielded. Therefore, to result in an exposure, the shielding must be compromised. After the canister is placed in a receptacle (e.g., aging overpack, STC), the CTM operator is supposed to close the port gate and then raise the shield skirt and move the CTM. If the operator fails to close the port gate before the shield skirt is raised and before the CTM is moved, then the crew members on the floor of the Canister Transfer Room would get a direct exposure. This is a skill-based action that is performed as part of every CTM movement over a port gate. This action is completely independent of the worker entering the room.

This is a task execution error with no feedback and its consequences are immediate (i.e., no potential for recovery). This most closely corresponds to the task execution error CREAM CFF E5, adjusted for the following CPCs with values not equal to 1.0.

- CFF E5: Missed action. The baseline HEP is 0.03.
- CPC "Working Conditions": The working conditions for the operator are in a control room with a favorable environment. The CPC for advantageous working conditions for an execution task is 0.8.
- CPC "Availability of Procedures": With regard to the notification step, the procedures and checklist clearly list that this task needs to be performed. The CPC for appropriate availability of procedures for an execution task is 0.8.
- CPC "Available Time": There is more than enough time to successfully perform this task. The CPC for adequate available time for an execution task is 0.5.
- CPC "Adequacy of Training/Preparation": This is a routine task that is clearly trained and emphasized in training. Because it is routine, there is a high level of experience. The CPC for adequate training and high experience for an execution task is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to close port gate before lifting shield skirt} = 0.03 \times 0.8 \times 0.8 \times 0.5 \times 0.8 = 0.008$$

HEP Calculation for Scenario 4(a)—The events in the HEP model for Scenario 4(a) are presented in Table E6.6-16.

Table E6.6-16. HEP Model for HFE Group #6 Scenario 4(a) for 050-OPCTMDirExp1-HFI-NOD

Designator	Description	Probability
A	Worker violates administrative control by entering the Canister Transfer Room during canister transfer	0.0009
B	Operator fails to close port gate before lifting shield skirt	0.008

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B = 0.0009 \times 0.008 = 8E{-}06 \quad \text{(Eq. E-36)}$$

E6.6.3.4.5.2 HEP for HFE 050-OpCTMDirExp1-HFI-NOD

The Boolean expression for the overall HFE (all scenarios) follows:

$$\text{050-OpCTMDirExp1-HFI-NOD} = \text{HEP 4(a)} = 8E{-}6 \quad \text{(Eq. E-37)}$$

E6.6.4 Results of Detailed HRA for HFE Group #6

The final HEPs for the HFEs that required detailed analysis in HFE Group #6 are presented in Table E6.6-17 (with the original preliminary value shown in parentheses):

Table E6.6-17. Summary of HFE Detailed Analysis for HFE Group #6

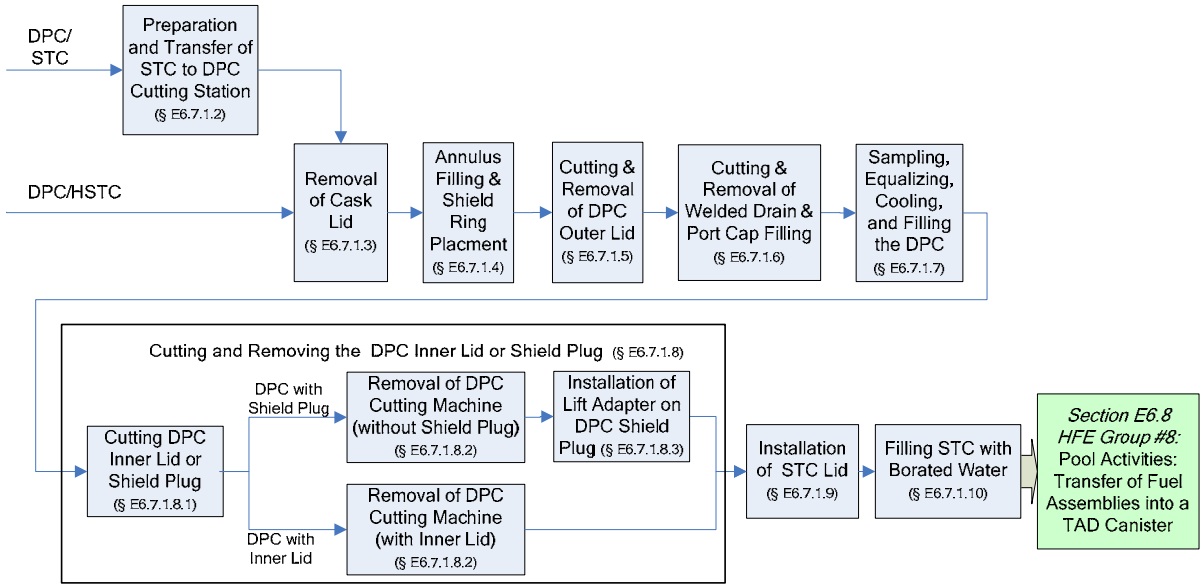
HFE	Description	Final Probability
050-OpCTMdrop001-HFI-COD	Operator causes drop of object onto canister during CTM operations	4E−7 (2E−03)
050-OpCTMdrop002-HFI-COD	Operator causes drop of canister during CTM operations (low level drop)	5E−7 (2E−03)
	Applied to removing a DPC from a TC	5E−7 (2E−03)
	Applied to removing any other canister from a TC or any canister from an AO	5E−7 (2E−03)
050-OpCTMImpact1-HFI-COD	Operator moves the CTM while canister or object is below or between levels	4E−8 (1E−03)
050-OpCTMDirExp1-HFI-NOD	Direct exposure during CTM activities (second floor)	8E−6 (1E−4)

NOTE: AO = aging overpack; CTM = canister transfer machine; DPC = dual-purpose canister; HFE = human failure event; TC = transportation cask.

Source: Original

E6.7 ANALYSIS OF HUMAN FAILURE EVENT GROUP #7: DPC CUTTING

HFE group #7 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering DPC cutting. There are two variations on this step: (1) a DPC in an STC (Section E6.6) is moved to the DPC cutting station from the Cask Unloading Room and is opened, and (2) a DPC in an HSTC (Section E6.2) is already at the DPC cutting station and is opened. For a DPC in an STC this operation begins with the CTT, loaded with a STC/DPC, in the Cask Unloading Room. The STC/DPC is moved to the preparation platform where the lid is bolted. The STC/DPC is then moved with the cask handling crane to the DPC cutting station. From this point on the HSTC/DPC, which is already at the DPC cutting station, and STC/DPC are handled in the same manner. The DPC is sampled, cooled, and filled with borated water and then the DPC lid is removed. The operation ends with the open DPC sitting in the DPC cutting station with STC lid bolted on, ready for transport into the pool. Figure E6.7-1 provides an overview of the operations in HFE group #7.



NOTE: § = Section; DPC = dual-purpose canister; HSTC = horizontal shielded transfer cask; HFE = human failure event; STC = shielded transfer cask; TAD = transportation, aging, and disposal.

Source: Original

Figure E6.7-1. Activities Associated with HFE Group #7

E6.7.1 Group #7 Base Case Scenario

E6.7.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #7 activities:

1. The STC with DPC is secured to the CTT and is positioned in the Cask Unloading Room. The STC has a lid on, is unbolted, and the DPC lifting device is still attached to the DPC.

2. The HSTC with DPC is sitting in the DPC cutting station with lid bolted on and no DPC lifting device attached to the DPC.
3. There is an interlock between the port slide gates and the Cask Unloading Room shield door. The port slide gate cannot be opened while the shield door to the Cask Unloading Room is also open.
4. The CTT is an air-pallet apparatus that is guided by two removable rails. The CTT also has end stops to aid in final positioning. A safe load path is marked for the CTT operations, and there are at least three crew members involved in its movement when loaded.
5. The cask handling crane (200-ton) is in the Cask Preparation Area and has the following safety features:

    A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.

    B. There are end-of-travel interlocks on the trolley and bridge.

    C. There are speed limiters built into the motors

    D. There is a weight interlock that cuts off power to the crane when the crane capacity is exceeded.

    E. There is a temperature interlock that cuts off power to the hoist when the temperature is too high. An indicator comes on before this temperature is reached.

    F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

6. The jib crane at the DPC cutting station and the jib crane at the preparation station are expected to have the same safety features as the cask handling crane with the exception of the yoke interlock.

Crane operations in this step are not part of a specific procedure outlined in the YMP documentation, but rather reflect critical lift crane operations that are standard in the nuclear industry.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Crew members (two)

- Radiation protection worker[13]
- Supervisor
- DPC cutter
- CTT operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel in this operation wear the appropriate PPE.

E6.7.1.2 Preparation and Transfer of STC to DPC Cutting Station

This step is only applicable to DPCs in an STC coming from the Cask Unloading Room (not HSTCs).

E6.7.1.2.1 Movement of an STC to Preparation Station in Cask Preparation Area

After a DPC has been transferred into the STC in the Cask Unloading Room, the Cask Unloading Room door is opened and the CTT operator moves the CTT, loaded with an STC/DPC to the Cask Preparation Area. The Cask Unloading Room door is then closed.

E6.7.1.2.2 Removal and Storage of STC Lid on Lid Rack

Once the cask is in place under the platform, the crew opens the shield plate and removes the STC lid using the jib crane and standard rigging.

Align Crane to Cask Lid—The crew opens the shield plate. The crane operator then lowers the jib crane into position over the STC. The operator is positioned on the platform in view of the crew members on either side of the lid. There is a signaling crew member next to the lid who uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask checking alignment of the crane. The verification crew member can only signal to stop the crane. Once positioned, one of the crew members connects the crane to the cask lid using the grapple.

Lid is Lifted Vertically—Upon signal from the signaling crew member that all is well, the crane operator begins to raise the cask lid. Once the lid is raised (i.e., is hanging free), the crane operator clears the cask and CTT and then lowers the lid to the proper movement height (roughly 6 in. above the highest obstacle in the movement path) based upon a visual inspection and confirmation by the signaling crew member via hand signals. Throughout this operation, the crew is standing several feet away from the platform opening. Once the lid is removed, a crew member then closes the shield plate.

Lid Moved to Staging Area—Using the jib crane, the crane operator positions the lid over the lid stand in the staging area. The crane follows the indicated safe load path marked on the floor visually, with confirmatory hand signals from the signaling crew member. The crane operator then sets down the lid and disengages the hook.

[13]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

E6.7.1.2.3 Removal of DPC Lift Fixture

The DPC lift fixture is removed from the DPC using the jib crane with grapple or hook, cask preparation platform, and common tools. The crane operator and the signaling and verification crew members are positioned on the cask preparation platform for this step.

DPC Lift Fixture Unbolting—A crew member closes the shield plate and uses the cask preparation platform and common tools to unbolt and remove all the lid fixture bolts according to training and then verifies (using a checklist) that all the bolts have been properly removed. Once the checklist has been marked off, the shield plate operator opens the shield plate in preparation for the next step.

Movement of Crane to Cask—The crane operator positions the jib crane over the cask/DPC fixture in the Cask Preparation Area. The crane operator visually follows the indicated safe load path marked on the floor, with confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member that can (hand) signal the crane operator to stop at anytime. At this time, the shield plate crew member opens the shield plate to allow the fixture to be positioned. The crane operator can roughly align the fixture over the DPC, but final alignment is directed by the signaling crew member.

Lowering and Engaging Lift Fixture—When properly positioned over the DPC, the signaling crew member signals the crane operator to lower the crane into place. The crane operator then proceeds to lower the crane at or below the maximum allowable speed. Once the crane is in place, the crane operator engages the DPC lift fixture, lifts the crane to operational height, and moves the lift fixture to the staging area. The crane operator and crew stay several feet away from the platform while the shield plate is open. The crew then closes the shield plate.

E6.7.1.2.4 Installation of STC Lid

Retrieval and Movement of STC Lid to Cask – The crane operator positions the jib crane hook over the STC lid. The crane operator engages the hoist to the lid, lifts the lid vertically to the proper operational height, and moves the lid to the cask following a safe load path based on visual inspection and with confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the lid over the cask, but final alignment is directed by the signaling crew member. Once aligned, a crew member opens the shield plate.

Lid Placement—Once the shield plate has been opened and the lid is properly aligned, the crane operator lowers the STC lid, disengages the hook/grapple, and retracts the hoist to the maximum height for the next crane operation.

Lid Bolting—With the lid in place, the crew closes the shield plate and, using long-reach tools, bolts the lid onto the STC. Before moving the cask, a checklist is used to ensure that at least four bolts have been used to secure the lid.

E6.7.1.2.5 Release of STC from CTT

The STC is released from the CTT by personnel using common tools. This is done on the preparation platform in the Cask Preparation Area.

E6.7.1.2.6 Movement of STC to DPC Cutting Station

The STC is moved from the CTT to the DPC cutting station using the 200-ton cask handling crane with the cask handling yoke.

Movement of Crane to STC—The operator positions the 200-ton crane over the STC. The crane operator visually follows the indicated safe load path marked on the floor, with confirmatory hand signals from the signaling crew member. The operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Aligning the Crane to the Cask—The crane operator lowers the 200-ton crane into position so that the yoke arms are lined up with the trunnions. The operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask who uses hand signals to guide the crane operator's movements (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask checking alignment of the second trunnion; the verification crew member can only signal the crane operator to stop.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. The crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). If the arms are sufficiently engaged on both sides, the crane operator knows by an indicator on the controller and the signaling crew member signals the operator to raise the crane a slight amount to put pressure on the arms. The crane operator sees on the controller that the 200-ton crane is bearing weight. Both crew members verify that the yoke remains level. If the arms do not engage on the initial attempt either crew member can signal the operator to stop, and the crane operator then sets the cask down and opens the yoke arms to disengage them from the cask. The signaling crew member directs the movement of the crane with hand signals, and then once aligned, signals the operator to close the yoke arms.

Movement of Cask to DPC Cutting Station—The crane operator raises the cask, clears the CTT, and then lowers the cask to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The crane operator confirms the height visually and obtains confirmation from the signaling crew member before beginning movement to the DPC cutting station. The operator visually follows the indicated safe load path marked on the floor, with confirmatory hand signals from the signaling crew member. There is a verification crew member on the opposite side of the cask from the signaling crew member who is the only one authorized to give the crane operator a signal to stop. The operator can roughly align the cask with the DPC cutting station, but final alignment is directed by the crew member, since the operator's view of the alignment with the platform may be obstructed. Once properly positioned, the crew member signals the crane operator to lower the cask. The crane operator then

disengages the yoke, lifts the crane to the proper height for movement, and moves it to the yoke stand.

E6.7.1.3 Removal of Cask Lid (All Variations)

E6.7.1.3.1 Removal of Lid Bolts

The crew uses the DPC cutting station platform and common tools to unbolt the cask lid. The bolts are removed, counted, and verified on a checklist.

E6.7.1.3.2 Removal and Storage of Cask Lid

From the second floor of the DPC cutting station, the crane operator removes the STC lid using the jib crane with grapple and stages it on the lid stand.

Lid Removal—The crane operator lowers the jib crane into position over the lid and engages the grapple. Once engaged properly (indicator), the crane operator lifts the lid and clears the cask, then lowers the lid to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path) based on a visual inspection and confirmation by the signaling crew member via hand signals.

Movement of Lid to Lid Stand—The crane operator moves the jib crane to the lid stand following the safe load path indicated on the floor. The operator does this visually, and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator then places the lid on the lid stand and disengages the grapple.

E6.7.1.4 Annulus Filling and Shield Ring Placement

E6.7.1.4.1 Fill Annulus with Borated Water

The crew attaches two hoses to the STC (one to the vent port and one to the fill port) via the quick disconnect ports. The other ends of the hoses are in the pool with filters attached. The crew turns on a pump to fill the annulus between the DPC and the STC with borated water. Once the annulus is full, a crew member turns off the pump, disconnects the hoses, and closes the ports. The annulus is full when there are no bubbles coming out of the return line in the pool.

E6.7.1.4.2 Placement of the Shield Ring between the DPC Canister and the STC

From the DPC cutting platform, the crane operator retrieves the shield ring using a jib crane with standard rigging, and places it over the DPC canister.

Retrieval of Shield Ring—The crane operator remotely lowers the jib crane into position over the shield ring in the staging area and attaches the slings. Once the slings are attached, the signaling crew member signals the crane operator to slightly lift the shield ring. The crew members then check to see that the shield ring is balanced on the sling and that the sling is properly engaged. Both crew members verify that the shield ring remains level and the crane

operator lifts the shield ring to the proper height for movement (i.e., roughly 6 in. above the highest obstacle in the movement path). The crane operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals.

Movement of Shield Ring to Cask—Using the jib crane, the crane operator positions the shield ring over the cask. The operator does this based on visual inspection and also receives confirmatory hand signals from the signaling crew member. There is also a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the shield ring over the cask, but final alignment is directed by the signaling crew member.

Lowering the Shield Ring and Disengaging the Sling—When properly positioned, the signaling crew member signals the crane operator to lower the shield ring into place. The crane operator then proceeds to lower the shield ring at or below the maximum allowable speed. Once the shield ring is in place, the crew member disengages the sling from the shield ring.

E6.7.1.5 Cutting and Removal of DPC Outer Lid

E6.7.1.5.1 Attachment of DPC Cutting Machine to DPC

The crane operator uses the DPC cutting platform, common tools, and the jib crane with hook to retrieve and emplace the adapter plate and cutting machine. Once in place, the crew members attach the adapter plate to the DPC with bolts. This step is verified with a checklist.

Attach DPC Cutting Machine to Adapter Plate—The crane operator and crew members use the jib crane with standard rigging to move the DPC cutting machine from its staging area to the adapter plate staging area. The crew uses common tools to bolt the DPC cutting machine to the adapter plate, without detaching the crane from the DPC cutting machine. This step is verified with a check list.

Retrieval of Adapter Plate/Cutting Machine—The jib crane is attached to the DPC cutting machine, which is bolted to the adapter plate. The crane operator lifts the adapter plate/cutting machine to proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals.

Movement of the Adapter Plate/Cutting Machine to the DPC— Using the jib crane, the crane operator positions the adapter plate over the DPC in the DPC cutting station, following the indicated safe load path marked on the floor. The operator does this visually, and also receives confirmatory hand signals from the signaling crew member. There is also a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the adapter plate over the cask, but final alignment is directed by the signaling crew member.

Lowering the Adapter Plate/Cutting Machine and Disengaging the Crane—When properly positioned over the cask, the signaling crew member signals the crane operator to lower the adapter plate into place. The crane operator then proceeds to lower the adapter plate at or below

the maximum allowable speed. Once the adapter plate is in place, the crew member disengages the hoist and the crane lifts to its maximum height in preparation for the next operation.

A crew member uses the cask preparation platform and common tools to emplace and tighten all the adapter plate bolts according to training and then verifies (checklist) all the bolts have been properly installed.

E6.7.1.5.2 Cutting of DPC Outer Lid with DPC Cutter

The operator is on the platform and uses a camera for this operation. Once the DPC cutting machine is securely in place on the DPC, the operator starts the cutting machine and cuts the outer lid weld. The cutting machine is semi automated and cannot damage the canister.

E6.7.1.5.3 Removal of DPC Cutting Machine/Adapter Plate/Outer Lid

From the second floor of the DPC cutting station, the crane operator removes the DPC cutting machine, adapter plate and outer lid using the jib crane with hook, and stages it on the cutting machine stand.

The crane operator lowers the jib crane into position over the cutting machine and engages the hook with the cutting machine. Once engaged properly, the crane operator lifts the cutting machine (that is still attached to the adapter plate and outer lid) and clears the cask; the cutting machine is then lowered to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals. The crane operator moves the jib crane to the staging area, following the safe load path indicated on the floor. The operator does this visually, and also receives confirmatory hand signals from the signaling crew member. There is also a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator then places the cutting machine with outer lid on the outer lid stand.

Once the cutting machine/adapter plate/outer lid unit has been removed from the DPC and placed in the staging area, without disengaging the cutting machine from the crane, a crew member uses common tools to unbolt the adapter plate (with cutting machine) from the outer lid.

E6.7.1.6 Cutting and Removal of Welded Drain and Port Cap Filling

E6.7.1.6.1 Reinstallation of Adapter Plate/Cutting Machine on DPC Inner Lid

The crane operator uses the cask preparation platform, common tools, and the jib crane with hook to emplace the adapter plate/cutting machine. Once in place, the crew members attach the adapter plate to the DPC inner lid/shield plug with bolts. This step is verified with a checklist.

Retrieval of Adapter Plate/Cutting Machine—The crane is already attached to the lid adapter. The crane operator lifts the adapter plate to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals.

Movement of the Adapter Plate/Cutting Machine to DPC—Using the jib crane, the crane operator positions the adapter plate over the DPC in the DPC cutting station, following the indicated safe load path marked on the floor. The operator does this visually, and also receives confirmatory hand signals from the signaling crew member. There is also a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the adapter plate over the cask, but final alignment is directed by the signaling crew member.

Lowering the Adapter Plate/Cutting Machine and Disengaging the Crane—When the adapter plate/cutting machine is properly positioned over the DPC, the signaling crew member signals the crane operator to lower the adapter plate into place. The crane operator lowers the adapter plate at or below the maximum allowable speed. Once the adapter plate is in place on the DPC inner lid, the crew member disengages the hook and the lifts the crane to its maximum height in preparation for the next operation.

A crew member uses the cask preparation platform and common tools to emplace and tighten all the adapter plate bolts (according to training), and verifies (using a checklist) that all the bolts have been properly installed.

E6.7.1.6.2 Cutting and Removal of Welded Cap over Drain and Filling Lines

The operator is on the platform and has to use a camera to perform this operation. Once the DPC cutting machine is in place on the DPC inner lid/shield plug, the operator starts the machine and cuts the welded cap over the DPC drain and fill lines. The crew then removes the cap using common tools. The cutting machine is semi automated and cannot damage the canister.

E6.7.1.7 Sampling, Equalizing, Cooling, and Filling the DPC

To sample the DPC, a crew member must plug a hose into the quick-disconnect drain port to start flow. Once connected, a crew member takes a reading of the gas that is being removed and verifies that the DPC is safe for opening. After the sample is taken, the remainder of the gas is vented, the valve is closed, and the hose taken off. If the DPC needs cooling, it is also cooled.

To fill/flush the DPC, the crew attaches two hoses to the DPC (one to the drain port and one to the fill port) via the quick disconnect ports. The other ends of the hoses are in the pool with filters attached. The DPC is then filled with borated waster until bubbles are no longer coming out of the return line. The pump is subsequently turned off, the valves are closed, and the hoses are disconnected. Continuous filling and flushing of the DPC may be necessary, in which case, a crew member would turn on a pump to cycle borated water through the DPC while the inner lid weld is being cut.

E6.7.1.8 Cutting and Removing Inner Lid or Shield Plug

E6.7.1.8.1 Cutting DPC Inner Lid or Shield Plug

The operator is on the platform and has to use a camera to perform this operation. Once the DPC cutting machine is in place on the DPC, the operator starts the machine and cuts the inner lid or

shield plug weld. It takes several cycles of the cutting machine to cut through the weld. The cutting machine is semi automated and cannot damage the canister.

Just prior the final cutting cycle, the crew stops the cutting machine and stops cycling water through the DPC. The crew turns off the pump, lets the hoses drain back into the pool, disconnects the hoses, and closes the valves. The crew then restarts the cutting machine. The cutting crew member determines it is time to stop the cutting machine based on visual inspection (via camera) of the cut depth.

E6.7.1.8.2 Removal of the DPC Cutting Machine

From the second floor of the DPC cutting station, the crane operator removes the DPC cutting machine using the jib crane with hook, and stages it on the cutting machine stand. There are two variations of this step: (1) remove the DPC cutting machine with inner lid attached, and (2) disconnect the shield plug from the DPC cutting machine and then remove the DPC cutting machine only.

If the DPC has a shield plug, then a crew member unbolts the adapter plate/cutting machine unit from the shield plug and then removes the adapter plate/cutting machine unit only; if the DPC has an inner lid, the crew removes the adapter plate/cutting machine unit with the inner lid attached. To remove the cutting machine unit, the crane operator lowers the jib crane into position over the cutting machine and engages the hook. Once engaged properly, the crane operator lifts the cutting machine and clears the cask, then lowers the machine to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals. The crane operator moves the jib crane to the inner lid stand (if the inner lid is attached) or the cutting machine stand (if there is a shield plug) following the safe load path indicated on the floor. The operator does this visually, and also receives confirmatory hand signals from the signaling crew member.

E6.7.1.8.3 Installation of Lift Adapter on DPC Shield Plug (DPC with shield plug only)

For DPCs with shield plugs, the crane operator uses the jib crane and standard rigging to retrieve the shield plug lift adapter from the staging area and move to the DPC. Once the shield plug adapter is put in place on the shield plug, the crew uses the platform and common tools to bolt the adapter to the shield plug. The shield plug is removed in the pool, but the lift adapter is installed on the platform.

Retrieval and Movement of Lift Adapter to the DPC—Following the indicated safe load path marked on the floor, the crane operator uses the jib crane to retrieve the shield plug lift adapter and position the adapter over the DPC shield plug in the DPC cutting station The operator does this visually, and also receives confirmatory hand signals from the signaling crew member. There is also a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the adapter over the cask, but final alignment is directed by the signaling crew member.

Lowering the Lift Adapter and Disengaging the Crane—When properly positioned over the DPC, the signaling crew member signals the crane operator to lower the adapter into place. The

crane operator then proceeds to lower the adapter at or below the maximum allowable speed. Once the adapter is in place on the DPC shield plug, the crew member disengages the grapple, and the crane lifts to its maximum height in preparation for the next operation.

Bolting the Lift Adapter to the Shield Plug—A crew member uses the cask preparation platform and common tools to emplace and tighten all the lift adapter bolts (according to training), and then verifies (using a checklist) that all the bolts have been properly installed.

E6.7.1.9 Installation of STC Lid

E6.7.1.9.1 Removal and Storage of the STC Shield Ring

From the DPC cutting platform, the crane operator removes the shield ring using the jib crane and standard rigging, and places it back in the staging area.

The crane operator lowers the jib crane into position over the shield ring and aligns the hook. Once the hook is aligned, the signaling crew member attaches the rigging. Both crew members verify that the load remains level during the lift. If the load is not level on the initial attempt, either crew member can signal the operator to stop and the crane operator then sets the cask down and the crew adjusts the rigging. Once the shield ring is attached properly, the crane operator lifts the shield ring to clear the cask. Once the shield ring is moved clear of the cask, the crane operator lowers the shield ring to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path) and moves the shield ring to the ring stand. The operator bases this on a visual inspection and confirmation by the signaling crew member via hand signals.

E6.7.1.9.2 Placement and Bolting of STC Lid

The crane operator uses the jib crane and lid grapple to place the STC lid on the STC. The crew uses common tools to bolt the lid to the STC (using at least four bolts). This step is verified by quality control. In preparation of this step, the lid grapple must be attached to the crane.

Retrieval of Lid—The crane operator lowers the jib crane with grapple into position over the lid in the staging area, engages the grapple, and lifts the lid to the proper height for movement (roughly 6 in. above the highest obstacle in the movement path). The operator bases this on a visual inspection and confirmation is provided by the signaling crew member via hand signals.

Movement of Lid to the STC—The crane uses the jib crane to position the lid over the STC in the DPC cutting station. The operator follows the indicated safe load path marked on the floor visually, and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member opposite the signaling crew member who can (hand) signal the crane operator to stop at anytime. The crane operator can roughly align the lid over the cask, but final alignment is directed by the signaling crew member.

Lowering Lid and Disengaging the Crane—When properly positioned over the DPC, the signaling crew member signals the crane operator to lower the lid into place. The crane operator then proceeds to lower the lid at or below the maximum allowable speed. Once the lid is in place

on the STC, the crew member disengages the grapple and lifts the crane to its maximum height in preparation for the next operation.

Installation of Lid Bolts—Once the lid is in place, the crew member uses the cask preparation platform and common tools to emplace and tighten at least four lid bolts (according to training), and then the supervisor verifies (using a checklist) that the bolts have been properly installed.

E6.7.1.10 Filling the STC with Borated Water

To fill the remainder of the STC, the crew attaches two hoses to the STC (one to the drain port and one to the fill port) via the quick disconnect ports. The other ends of the hoses are in the pool with filters attached. The STC is filled until bubbles are no longer coming out of the return line. The pump is then turned off, the valves are closed, and the hoses are disconnected.

E6.7.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during DPC Cutting are summarized in Table E6.7-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.7-1. HFE Group #7 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
Crane Drops	*Operator Causes Drop of Cask, Canister, or Object during DPC Cutting*: Throughout the DPC cutting operation, several objects are moved over an open cask and the cask itself is moved at least once. These operations utilize the cask handling crane and jib cranes. Each of these lifts can result in a drop which impacts the cask or canister.	15, 17, 18	N/A [a]	In this step, the operator uses the cask handling crane and jib cranes to move the cask and other heavy objects. STCs have one cask lift using the cask handling crane with cask handling yoke; HSTCs have no cask lifts in this HFE group. There are numerous object lifts associated with removing the canister lift fixture (STC/DPC unit) and with DPC cutting: lift of the cask lid (×4), lift of the canister and shield plug lift fixtures, and four movements of the DPC cutting machine (with adapter plate and inner or outer lid). Each of these lifts can potentially result in a drop. These HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for this failure can be found in Attachment C.
050-OpCTCollide2-HFI-NOD	*Operator Causes Low-Speed Collision of CTT during Transfer from Unloading Room to Preparation Station (STC/DPC only)*: Once the DPC is in an STC with the lid on, an operator inflates the CTT and moves the cask from the Cask Unloading Room to the Cask Preparation Area. The operator can cause the CTT to collide with the preparation platform during this transfer. The CTT is designed such that it physically cannot over speed; therefore, all CTT collisions are below the designed speed.	14	1E−03	In this step, the CTT moves from the Cask Unloading Room to the preparation station; the doors of the preparation station must be opened to allow the CTT to pass through. There are three observers with clear visibility, the speed of the CTT is low, the CTT is very visible, and there are two guide rails and an end stop to keep the CTT on the safe load path. The CTT could collide into conveyance or facility structures (i.e., preparation station platform or shield door). This could happen if the guide rails were not installed properly. This operation is simple, straightforward, and is expected to occur very regularly (daily), and was assigned the default probability of a “highly unlikely” occurrence (0.001) and not adjusted further. It was considered reasonable and consistent that the preliminary value assigned for this HFE be less likely than a railcar collision because of the guide rail, number of observers, and short travel distance.
050-OpImpact0000-HFI-NOD	*Operator Causes Impact of Cask during Transfer from Cask Unloading Room to Cask Preparation Station (STC/DPC only)*: While moving from the Cask Unloading Room to the cask preparation station, the CTT can impact the crane hook or rigging if it is improperly stowed.	14	N/A	While moving from the Cask Unloading Room to the cask preparation station, the CTT can impact the crane hook or rigging if it is improperly stowed. The shield plate is closed at the end of every operation involving the cask preparation platform. It is unlikely, then, that the crane rigging can be improperly stowed such that it impacts the CTT while it is moving out of the Cask Unloading Room to the cask preparation station; it is more likely that rigging could impact the cask while the crane is actually in use. Therefore, any crane interference with the CTT is already covered by 050-OpTCImpact01-HFI-NOD (Operator Causes Cask Impact during DPC cutting) and 050-OpTipover001-HFI-NOD (Operator Causes Cask to Tip Over). This failure was omitted from analysis.
050-OpSDClose001-HFI-NOD	*Operator Closes Shield Door on Conveyance (STC/DPC only)*: Once the CTM activities are over, an operator opens the shield door, turns on the CTM, lifts the forks, and moves the cask from the Cask Unloading Room to the Cask Preparation Area. There is a shield door between the Cask Preparation Area and the Cask Unloading Room. The operator can impact the cask by inadvertently closing the shield door on the CTT as the CTT passes through the door.	12	1.0	The CTT passes through a shield door as it moves between the cask preparation station and the Cask Unloading Room. During this transfer, the operator can cause the CTT to collide into the shield door or can close the shield door on the CTT. Section E6.0.2.3.3 provides a justification of this preliminary value.
050-OpFLCollide2-HFI-NOD	*Operator Causes Collision of Auxiliary Vehicle with the Cask*: Operator can cause an auxiliary vehicle to collide into a cask while it is stationed at the cutting station. If the collision is due to the auxiliary vehicle speed governor malfunctioning, this would be a high-speed collision.	15	N/A	The operator can cause an auxiliary vehicle (i.e., forklift) to collide with the cask while it is stationed in the DPC cutting station during DPC cutting. This failure was omitted from analysis because the design of the DPC cutting station precludes the cask from being impacted by an auxiliary vehicle.
050-OpTipOver001-HFI-NOD	*Operator Causes Tipover of Cask*: If the operator improperly stows the crane rigging, during DPC cutting or precutting preparation, it can catch the CTT, cask, or canister. If the crane becomes attached to the CTT, cask or canister and the operator continues to move the CTT (i.e., exiting the Cask Preparation Area) or crane, the cask could tip over.	15	1E−04	In this step, there are several crane operations using the cask handling crane and jib cranes. For crane operations there are three observers with clear visibility, the operations are simple, the travel distances are short, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. There are no interlocks to prevent this error. The contributors to cask tipover include: • Crane hook, grapple, or rigging catches conveyance/cask • Horizontal movement of cask with the hook lowered and attached to the cask • Crane travels in the wrong direction • Cask not lifted high enough to clear the conveyance. The dominant contributor is the crane hook catching the cask. While it may be unlikely (0.01) that a stray hook or grapple might be hanging from the crane, it would still need to catch on the cask securely enough to pull it over (0.1) and then the cask tipping would have to go unnoticed by all three observers. This is done under direct observation, there are not many surfaces which are “catchable,” and tipover is a slow process; therefore the value was adjusted by a further 0.1.

Table E6.7-1. HFE Group #7 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpTCImpact01-HFI-NOD	*Operator Causes an Impact Between Cask and SSC*: While moving the STC with the cask handling crane from the Cask Preparation Area to the DPC cutting station, the crane operator can impact the cask by moving the crane outside the safe load path or by colliding the cask with an SSC in the safe load path. Once the cask is at the cutting station, several objects are moved to and from the cask. Likewise, the crane operator can impact the cask with an object if the crane is moved with the hook too low or otherwise outside of the safe load path.	15	3E−03	In this step an STC is moved from the CTT to the DPC cutting station. There are also several object movements around the cask during DPC cutting. For crane operations in this step there are three observers with clear visibility, the operations are simple, the travel distances are short, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. There are no interlocks to prevent this error. The dominant contributors to the impact of a cask include: • Crane is moved outside its safe load path (i.e. operators cut corners) • Crane is moved in the wrong direction • Failure to maintain proper vertical and horizontal distance between the cask and SSCs during crane operations. The operator must manually maintain movement within the safe load path. It is not unlikely that the operator would stray slightly from that path, or that an object may be slightly within that path. However, these crane operations are very slow and within clear direct view of three observers. The likelihood of impacting a cask was assessed to be comparable to the crane impact during upending and removal HFE (050-OpTCImpact01-HFI-NOD; Section E6.2, HFE Group #2) and was accordingly assigned the same preliminary value: this failure is “highly unlikely” (one in a thousand or 0.001, which also corresponds to the generic failure rate for a simple operation that is performed daily) but is adjusted because there are several ways for an impact to occur (×3).
050-OpDPCShield2-HFI-NOW	*Operator Causes Loss of Shielding during DPC Cutting*: In this step, the DPC cutting activities are carried out. The crane operator can improperly place the DPC shield ring on the STC during cutting activities, resulting in a direct exposure to the DPC cutting crew.	29	1E−02	In this step, the DPC shield ring is placed over the annulus so the crew can perform DPC cutting activities. During this operation there are three observers plus a supervisor, the crane operations are simple, the ring is attached via sling to the crane, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a weekly basis. There are no interlocks to prevent this error. To add to the complexity of this task, the actual alignment is done via camera; however, if the shield ring is misaligned, it can be seen from the platform. This operation was given the default preliminary value for an event performed on a regular basis (weekly) that is not particularly complex. This is classified as an “unlikely” event and a value of 0.01 applied.
050-OpDPCShield3-HFI-NOW	*Operator Causes Loss of Shielding while Removing DPC Lift Fixture (TC/DPC only)*: In this step, the DPC canister lift fixture is removed from the canister. An operator can fail to properly close and verify the closure of the shield plate. The crew continues with the installation, or can inadvertently open the shield plate while the crew is installing the canister lift fixture.	29	1E−03	In this step, the DPC canister lift fixture is removed from the canister. If an operator fails to properly close the shield plate, then the crew can be directly exposed to the shine from the DPC while removing the canister lift fixture. Likewise, if an operator inadvertently opens the shield plate while the crew is removing the canister lift fixture, then the crew can be exposed. In this case, the crew is on top of the shield plate and would notice if the shield plate moves. The crew is highly trained and, although they only perform DPC preparation activities weekly, they are accustomed to operating the shield plate during preparation of other transportation casks. In addition to the crew members, there is also a radiation protection worker present who is monitoring activities. This error was assessed to be highly unlikely and given a preliminary value of 0.001. This failure is identical to loss of shielding during DPC preparation activities (050-OpDPCShield1-HFI-NOW; HFE Group #5).
050-LidDisplace1-HFI-NOD	*Operator Inadvertently Displaces Lid.*	29	N/A	In this step the lid is unbolted and, for transportation casks/DPCs, other crane operations are performed. Due to design changes to the preparation platform, improperly stowed rigging during this operation would not catch the lid lift fixture. These design changes include raising the platform and adding a shield plate so that the cask is recessed underneath the platform and protected.
050-OpSampleRel2-HFI-NOD	*Operator Improperly Performs Gas Sampling*: Gas sampling may be performed to determine if the fuel has been damaged by the transportation process. If the gas sampling process is incorrectly performed, such that material is released from the sample line, then a radiation release would result if the fuel inside is damaged.	17	5E−03	In this step, the crew samples the cask via a quick-disconnect gas sampling port to ensure that the fuel is intact before removing the canister lid. There is one operator in charge of gas sampling. In order to get a release from the line, the line would have to be inappropriately attached such that the quick disconnect valve is engaged and open. This EOC was assessed to be “highly unlikely” (0.001) because the operation is simple and performed on a daily basis by a highly trained individual. This value was adjusted (×5) to account for the fact that this operation is performed by one crew member, and a failure would be very difficult to notice and correct before material is released. Note: this is the probability of release given damaged fuel; for release of radioactivity to occur, the probability of damaged fuel would have to be assessed and applied.
050-OpDPC-OVP01-HFI-NOW	*Operator Causes DPC Overpressurization*: While cooling the DPC, the operators can cause the DPC to over pressurize by pumping the water too fast. The system is designed to accommodate the hot DPCs (temperatures greater than 350°C); therefore there is not a human-induced overpressurization event if the DPC is not at a low temperature before cooling begins (i.e., due to steam pressure).	17	5E−03	In this step, the crew cools the DPC by running borated water through the canister. While cooling the DPC, the operators can cause the DPC to over pressurize by pumping the water too fast. In order to get the overpressurization, the operator would have to fail to set the water flow rate properly and fail to notice and reduce the flow once the alarms indicated that there was a problem. This EOC was assessed to be “highly unlikely” (0.001) because the operation is simple, performed by a highly trained individual and has associated alarms. This value was adjusted (×5) to account for the fact that this operation is performed by one crew member and is only performed weekly. This was assessed to be comparable to failure of the operator to properly perform gas sampling (050-OpSampleRel2-HFI-NOD), and the preliminary values reflect this

Table E6.7-1. HFE Group #7 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpExpose-Splash	*Operator Exposed Due to Pool Splash*: If the cask is dropped into the pool while the operator is standing too close to the edge of the pool, then the operator can get a direct exposure from the water.	30	1.0	If the cask is dropped into the pool while the operator is standing too close to the edge of the pool, then the operator can get a direct exposure from the water. The probability of an operator being in splash-range of the pool was conservatively assessed to be 1.0.

NOTE: [a] HRA preliminary value replaced by use of historic data (Attachment C).
CTM = canister transfer machine; CTT = cask transport trolley; DPC = dual-purpose canister; EOC = error of commission; ESD = event sequence diagram; HFE = human failure event; N/A = not applicable; SSC = structure, system, or component; SSCs = structures, systems, and components; STC = shielded transfer cask; TC = transportation cask.

Source: Original

E6.7.3 Detailed Analysis

After the preliminary screening analysis and initial quantification are completed, those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives are subjected to a detailed analysis. The overall framework for the HRA is based upon the process guidance provided in ATHEANA (Ref. E8.1.22). Consistent with that framework, the following four steps from the methodology described in Section E3.2 provide the structure for the detailed analysis portion of the HRA.

Step 5: Identify Potential Vulnerabilities

Prior to defining specific scenarios that can lead to the HFEs of interest (Step 6), information is collected to define the context in which the failures are most likely to occur. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in HFEs or unsafe actions. This information collection step is discussed in Section E6.7.3.2.

Step 6: Search for HFE Scenarios (Scenarios of Concern)

An HFE scenario is a specific progression of actions with a specific context that leads to the failure of concern; each HFE is made up of one or more HFE scenarios. In this step, documented in Sections E6.7.3.3 and E6.7.3.4, the analyst identifies deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These unsafe actions make up an HFE scenario. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions.

Step 7: Quantify Probabilities of HFEs

Detailed HRA quantification methods are selected as appropriate for the characteristics of each HFE and are applied as explained in Section E6.7.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)
- ATHEANA expert judgment (Ref. E8.1.22).

There is no implication of preference in the order of listing these methods. They are jointly referred to as the "preferred methods" and are applied either individually or in combination as best suited for the unsafe action quantified. The ATHEANA (Ref. E8.1.22) expert judgment method (as opposed to the overall ATHEANA (Ref. E8.1.22) methodology that forms the framework and steps for the performance of this HRA) is used when the other methods are deemed to be inappropriate to the unsafe action, as is often the case for cognitive EOCs.

Appendix E.IV of this analysis explains why these specific methods were selected for quantification and gives some background on when a given method is applicable based on the focus and characteristic of the method.

All judgments used in the quantification effort are determined by the HRA team and are based on their own experience, augmented by facility-specific information and the experience of subject matter experts, as discussed in Section E4. If consensus can be reached by the HRA team on an HEP for an unsafe action, that value is used as the mean. If consensus cannot be reached, the highest opinion is used as the mean.

Step 8: Incorporate HFEs into the PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. The summary table of HFEs by group that lists the final HEP by basic event name provides the link between the HRA and the rest of the PCSA. This table can be found in Section E6.7.4.

E6.7.3.1 Human Failure Events Requiring Detailed Analysis

The detailed analysis methodology, Sections E3.2.5 through E3.2.9, states that HFEs of concern are identified for detailed quantification through the preliminary analysis (Section E3.2.4). An initial quantification of the WHF PCSA model determined that there were only three HFEs whose preliminary values were too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111. These HFEs are presented in Table E6.7-2.

Table E6.7-2. Group #7 HFEs Requiring Detailed Analysis

HFE	Description	Preliminary Value
050-OpDPCShield2-HFI-NOW	Operator causes exposure due to failure to install DPC shield ring	1E−02
050-OpDPC-OVP01-HFI-NOW	Operator causes overpressurization of DPC during DPC Cutting	5E−03
050-OpDPCShield3-HFI-NOW	Operator causes loss of shielding while removing DPC lift fixture (STC/DPC only)	1E−03

NOTE: DPC = dual-purpose canister; HFE = human failure event; STC = shielded transfer cask.

Source: Original

E6.7.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the approach to conducting a detailed quantification is to identify and characterize factors that could create potential vulnerabilities in the crew's ability to respond to the scenarios of interest and might result in HFEs or unsafe actions. In this sense, the "vulnerabilities" are the context and factors that influence human performance and constitute the characteristics, conditions, rules and tendencies that pertain to all the scenarios analyzed in detail.

These vulnerabilities are identified through activities including but not limited to the following:

1. The facility familiarization and information collection process discussed in Section E4.1, such as the review of design drawings and concept of operations documents

2. Discussions with subject matter experts from a wide range of areas, as described in Section E4.2

3. Insights gained during the performance of the other PCSA tasks (e.g., initiating event analysis, system analysis, and event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the DPC cutting operation that relate to potential human failure scenarios relevant to the three HFEs listed in Table E6.7-2. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during DPC cutting operations, but these have no bearing on this analysis.

E6.7.3.2.1 Operating Team Characteristics

The operating team consists of the following personnel:

Crane Operator—The crane operator has received standard training for crane operations and observed operations prior to being allowed to operate the crane on a dry run. Based on evaluation of the crane operator's proficiency in a dry run, the crane operator is signed off to operate the crane. On initial operations, the crane operator is observed until signed off for solo operation. A single operator is assigned to the crane operation.

Crew Members (two)—Crew members are trained in tasks required for DPC cutting operations. Training consists of observation and "hands-on" instruction. The crew members assist in various tasks of the operation, including bolting and unbolting activities. There is a crew member designated to operate the shield plate on the cask preparation platform, but this crew member is also involved in bolting, unbolting, and other related operations.

Signaling Crew Member—During shield ring movement to the DPC/STC, the signaling crew member provides hand signals to the crane operator to direct the movement of the crane

Verification Crew Member—The verification crew member is stationed in view of the DPC/STC and shield ring and covers those areas that the signaling crew member cannot see. The verification crew member gives hand signals to the signaling crew member if there are any problems with the alignment of the shield ring.

Radiation Protection Worker—The radiation protection worker is a fully certified health physics technician, whose job is to monitor radiation from the cask during cask handling operations. The radiation protection worker is responsible for stopping operations if high radiation levels are detected or if there is a situation that would lead to direct exposure.

Supervisor—The supervisor, or some other personnel with comparable training and certification, is present during DPC cutting activities. This person supervises and checks critical operations, including shield ring installation and DPC filling. No credit for supervisor checks has been given for this HFE group.

E6.7.3.2.2 Operation and Design Characteristics

Control Panel— The control panel consists of a standard jib control panel for movement of the crane. Controls are provided for both coarse and fine motion. A camera view is provided to augment the operator's direct view from a distance. The crane operator and crew members are located on the platform, several feet away from the cask.

Interlocks/Alarms—An interlock shuts off the DPC cooling pump motor upon overpressurization and an alarm sounds when the pressure gets too high. There are no interlocks or alarms associated with radiation protection that are credited in this task. A radiation protection worker takes a manual reading of radiation levels and prevents operations from proceeding if high radiation levels are detected.

Pressure Relief Capability—There is pressure relief capability associated with the DPC cooling system. This capability is either integral to the quick disconnect valves or a separate pressure relief valve is in series with each quick disconnect valve. These pressure relief valves do not vent directly to atmosphere, but are vented to the HVAC off-gas lines in the case of vapor or to the DPC drain line to filtration prior to water return to the pool in the case of liquid.

E6.7.3.2.3 Operational Conditions

Verbal communication—Verbal communication between crew members and the crane operator is considered to be ineffective. A significant amount of machine noise is present, so hand signals are the only practical means of communication during DPC cutting operations.

E6.7.3.2.4 Formal Rules and Procedures

Procedures—Procedures exist for DPC cutting operations; however, there are no written, formal procedures that the crew has in front of them during cask preparation. Operators and crew members are trained in the operations, and their proficiency is attested to by the training staff. They perform the operations as a skill.

Formal Rule—This operation involves potential radiation exposure, so a formal rule exists that the radiation protection worker must measure the radiation in the area of the DPC where the workers are conducting operations. However, the radiation protection workers do not have to formally sign off on the measurement; they simply need to inform the crane operator and crew that it is safe to continue.

E6.7.3.2.5 Operator Tendencies and Informal Rules

Crane Operator Dependency on Crew Members—The view from the control panel and through the camera are reasonable for rough placement of the shield ring, but final alignment is directed through hand signals from crew members.

Crew Member Deference to the Crane Operator—The crane operator is essentially the foreman of the team, and is seen by the crew members as being in a more skilled position than them. The crew tends to defer to the crane operator's judgment and have some level of reluctance to question the crane operator's directions.

E6.7.3.2.6 Operator Expectations

Shield ring installation is a simple task ancillary to the main task of DPC cutting. The operator and crew expect that it should go smoothly.

E6.7.3.3 HFE Scenarios and Expected Human Failures (Step 6)

Given that the vulnerabilities that provide the operational environment and features that could influence human performance have been specified, then the HFE scenarios within this environment are identified. An HFE scenario is a specific progression of actions during normal operations (with a specific context) that lead to the failure of concern; each HFE is made up of one or more HFE scenarios. In accordance with the methodology, each scenario integrates the unsafe actions with the relevant equipment failures so as to provide the complete context for the understanding and quantification of the HFE.

The HAZOP evaluation is instrumental in initially scoping out the HFE scenarios, but they are then refined through discussions with subject matter experts from a wide range of areas, as described in Section E4.2.

Table E6.7-3 summarizes all of the HFE scenarios developed for the HFEs in HFE Group #7.

Table E6.7-3. HFE Scenarios and Expected Human Failures for HFE Group #7

HFE	HFE Scenarios
050-OpDPCShield2-HFI-COW *Operator Causes Loss of Shielding During DPC Cutting*	HFE Scenario 1(a): (1) Crane operator fails to install the shield ring; (2) Crew members fail to realize that the shield ring installation has been skipped, and (3) Crew members fail to notice that the shield ring is not in place prior to approaching the DPC. HFE Scenario 1(b): (1) Crane operator installs shield improperly, (2) Radiation protection worker fails to check radiation levels OR radiation protection worker misreads radiation levels OR radiation monitor fails, and (3) Crew member fails to note that the shield ring is out of position before approaching the DPC.
050-OpDPC-OVP01-HFI-NOW *Operator Causes DPC Overpressurization*	HFE Scenario 2(a): (1) Operator pumps borated water at faster than acceptable rate, (2) Operator fails to notice pressure increase or fails to stop operation given the pressure increase; ,and (3)Pressure relief valve fails to operate OR pump motor fails to shut off upon overpressure.
050-OpDPCShield3-HFI-NOW *Operator Causes Loss of Shielding While Removing DPC Lift Fixture*	This HFE is identical to the direct exposure during DPC lift fixture installation (050-OpDPCShield1-HFI-COW; E 6.5, HFE Group #5: DPC Preparation Activities) and the detailed analyses are also identical; therefore, the analysis is not repeated here.

NOTE: DPC = dual-purpose canister; HFE = human failure event.

Source: Original

Since there are three HFEs identified for detailed analysis in this group, the scenarios are organized under these HFE categories, with the scenarios numbered for the first category as 1(a) and 1(b), and the second category numbered as 2(a).

Each HFE scenario is in turn characterized by several unsafe actions, numbered sequentially as (1), (2), and (3). The Boolean logic of the HFE scenarios is expressed with an implicit AND

connecting the subsequent unsafe actions and OR notation wherever two unsafe action paths are possible, as shown in Table E6.7-3.

The HFE scenarios summarized in Table E6.7-3 are discussed and quantified in detail in the following sections.

E6.7.3.4 Quantitative Analysis (Step 7)

Once the HFE scenarios and the unsafe actions within them are scoped out, it is then possible to review them in detail and apply the appropriate quantification methodology in each case that permits an HEP to be calculated for each HFE. Stated another way, each HFE is quantified through the analysis and combination of the contributing HFE scenarios. Dependencies between the unsafe actions and equipment responses within each scenario and across the scenarios are carefully considered in the quantification process.

This section provides a description of the quantitative analysis performed. This quantitative analysis is structured hierarchically by each HFE category (identified by a basic event name), followed by the HFE scenario, and then followed by the unsafe actions under each scenario as documented in Table E6.7-3.

Prior to the scenario-specific quantification descriptions, a listing is provided of the values used in the quantification that are common across many of the HFE scenarios.

In generating the final HEP values, the use of more than a single significant figure is not justified given the extensive use of judgment required for the quantification of the individual unsafe actions within a given HFE. For this reason, all calculated final HEP values are reduced to one significant figure. When doing this, the value is always rounded upwards to the next highest single significant figure.

E6.7.3.4.1 Common Values used in the HFE Detailed Quantification

There are no mechanical failures that appear in multiple HFE scenarios.

E6.7.3.4.2 Quantification of HFE Scenarios for 050-OpDPCShield2-HFI-NOW: Operator Causes Exposure due to Failure to Install DPC Shield Ring

E6.7.3.4.2.1 HFE Group #7 Scenario 1(a) for 050-OpDPCShield2-HFI-NOW:

1. Crane operator fails to install shield ring.
2. Crew members fail to realize that the shield ring installation has been skipped.
3. Crew members fail to notice that the shield ring is not in place prior to approaching the DPC.

Crane Operator Fails to Install Shield Ring—The crane operator is responsible for ensuring that the shield ring is installed prior to the crew members unbolting the DPC lifting device. The crew members assist in this process by handling the rigging and providing hand signals to the

crane operator to help in placement of the shield ring. Since this is a radiation protection task, the operator must contact the Health Physics Department and inform them that the operation is about to take place so that a radiation protection worker can check radiation levels after shield placement. The unsafe action in this case is that the crane operator fails to perform this entire step and tells the crew to unbolt the lifting device. The operator's motivation for doing this could be that the shield ring is viewed as unnecessary for this task, the operator "remembers" already installing it from having done this operation many times before, the operator is anxious to get the job done, or the operator is distracted by other activities and simply forgets.

The jib crane operator is required to install the shield ring prior to the DPC cutting. The unsafe action in this case is that the jib crane operator skips this entire part of the process and tells the crew member to begin cutting preparation. This can be represented by CREAM CFF E5, adjusted for the following CPCs with value not equal to 1.0, as follows:

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03
- CPC "Available Time": The general level of time pressure for the overall process of preparing the DPC is very low. There is no particular impetus for getting the task done that would potentially drive the operator to skipping this task. The CPC weighting factor for an execution task with adequate time is 0.5.
- CPC "Adequacy of Training and Preparation": This routine task is well trained and practiced and performed quite frequently. The CPC weighting factor for an execution task with adequate training and high experience is 0.8.

Note that in skipping this entire task, it is deemed that the operator also fails to inform the Health Physics Department that they are needed to perform monitoring after the shield ring is installed.

Applying these factors yields the following:

$$\text{Crane operator fails to install shield ring} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Crew Members Fail to Realize That Shield Ring Installation Has Been Skipped—The crew members who aid in DPC cutting are an integral part of the overall task process, including the placement of the shield ring. They should be aware that the ring needs to be placed, and should question the crane operator if the crane operator tells them to begin the unbolting task when they have not participated in the placement process. In addition, the crew members should also be expecting to see a radiation protection worker check radiation levels and give them the "all clear" signal to approach the DPC. The crew members have a particular motivation to ensure that this is done, since the crew members (not the crane operator) are exposed to radiation if the shield ring is not installed. The unsafe action in this case is that they do not question the crane operator when told to begin the unbolting task. It is expected that their motivation for this unsafe action is most likely to be a reluctance to question the crane operator, who is above them in the operational hierarchy of the facility (i.e., the crane operator is essentially the foreman of the team). The crew member's deference to the crane operator's instruction would come from a belief that the crane operator was in charge and aware of the situation.

Because the crew members that are involved in DPC cutting process are the same crew members that assist in the shield ring installation process (i.e., preparing the crane, signaling the operator, etc.), the crew members need to miss this entire task for this event to occur. As a baseline value for this event, the same probability as crane operator fails to install shield ring can be used (0.01). However, the crew members would not be totally independent of the crane operator. The crew members could be distracted, or they could be starting a new shift and be convinced by the crane operator that they are ready to begin cutting preparation (i.e., a bias towards believing that the crane operator, who would generally be considered above them in the operations hierarchy, must be aware of the status of the operation). On the other hand, crew members would clearly expect to participate in this task and because it is important to their personal safety (i.e., they are the ones who are depending on the shielding) they are more cognizant of the operational status. Taking all of this into consideration, it is deemed that the level of dependence is low. For low dependence when a baseline HEP is 0.01, the adjusted HEP is taken from THERP Table 20-21, item (2)(a) (Ref. E8.1.26) as follows:

Crew members fail to note that shield ring installation has been skipped = 0.05

Crew Members Fail to Notice That Shield Ring is Not In Place Prior to Approaching DPC—After the crew members are cleared to begin the cutting task, they gather the required tools and approach the DPC. The crew members would have performed this task many times before, and would have an image in their minds of how everything should look. The ring is a large and rather obvious device that the crew members would have to walk on or over in order to perform the unbolting. However, if the ring were not in place they would be exposed well before they got this close to it, so they would have to notice from some reasonable distance away. The crew members are carrying the tools they need, focusing on the performance of the task, and likely talking to each other about the performance of the task or having a casual conversation (since the work is not particularly difficult or challenging and they are not expecting any complications). The unsafe action results from the crew members not noticing that the configuration of the shield ring is not correct. Most likely, the crew members would have a bias that the operational conditions are in order and it is time to perform the task; the crew does not detect the differences in appearance (i.e., they see what they expect to see). To put this in a more colloquial context, this type of missed observation would be comparable to an individual walking out to a car and failing to see from a distance that the car has a flat tire. Noticing it when getting within a few feet of the car would be a failure in this case (the individual would already be "exposed").

Although there is no specific check that takes place when the crew begins setting up the cutting machine on the DPC, there is ample opportunity to notice that the shield ring is not in place. Rather than missing a check, it is more in the nature of failing to notice that something is not right. It would be similar to someone noticing a low tire on their car when they go out to start it. There are no failures in the primary quantification methods that reasonably fit this unsafe action, so it is necessary to provide a value based on expert judgment (ATHEANA). It is clear that some credit needs to be given for this since the crew members perform this task often and should recognize what the configuration should look like when they perform the task. However, in opposition to this, the crew begins operations carrying the necessary tools with them believing everything is in place. The HRA team believes that the failure is less than likely (0.5), but greater than unlikely (0.1). A value of 0.3 is selected.

Crew members fail to notice that shield ring is not in place prior to approaching DPC = 0.3

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.7-4.

Table E6.7-4. HEP Model for HFE Group #7 Scenario 1(a) for 050-OpDPCShield2-HFI-NOW

Designator	Description	Probability
A	Crane operator fails to install shield ring	0.01
B	Crew members fail to realize that shield ring installation has been skipped	0.05
C	Crew members fail to notice that shield ring is not in place prior to approaching DPC	0.3

NOTE: DPC = dual-purpose canister; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.01 \times 0.05 \times 0.3 = 0.0002 \quad \text{(Eq. E-38)}$$

E6.7.3.4.2.2 HFE Group #7 Scenario 1(b) for 050-OpDPCShield2-HFI-NOW

1. Crane operator installs shield improperly.

2. Radiation protection worker fails to check radiation levels OR radiation protection worker misreads radiation level OR radiation monitor fails.

3. Crew member fails to note that the shield ring is out of position before approaching the DPC.

Crane Operator Installs Shield Ring Improperly—The installation process is relatively simple and straightforward. Once the crew members attach the shield ring to the jib crane sling, the operator moves it over the DPC. The crew members help the operator to align the shield ring properly over the DPC using hand signals. The crew members signal the crane operator throughout the lowering process to ensure proper alignment. Although the operation is simple, the shield ring must have a close fit in order to completely block the annulus between the DPC and the STC to prevent radiation from escaping and exposing workers when they approach the DPC. If the shield ring is not exactly aligned, it could partially jam or hang up at a slight angle that would allow radiation to escape. The unsafe action is that the operator causes the shield ring to partially jam or hang up. Included in this is the implicit condition that the crane operator and crew members do not notice that the shield ring is jammed or hung up as they perform the task.

In this case, the crane operator is performing the shield installation task, but the shield ring is not seated properly. This is a very routine task, and is practiced often. Failures can be corrected without consequences since the operator has the opportunity to lift and place the shield ring as many times as necessary until the operator is satisfied that it is properly aligned. This can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well designed, highly practiced, and routine task performed to highest possible standards by highly motivated, highly trained, and experienced personnel, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 11: Poor, ambiguous, or ill-matched system feedback. This EPC addresses the issue that the crane operator views this operation from a distance. The maximum effect is ×4, which applies to a very difficult situation where visibility is poor, and visual and physical access if difficult. It is not believed that this case is this severe, but the full effect is still applied. The APOA is set to 1.0.

Applying the NARA HEP equation yields:

$$\text{Crane operator installs shield ring improperly} =$$

$$0.0001 \times [(4-1) \times 1 + 1] = 0.0004 \qquad \text{(Eq. E-39)}$$

Radiation Protection Worker Fails to Check Radiation Levels—The crane operator contacts the Health Physics Department before initiating the shield ring placement task, and awaits clearance that radiation levels are acceptable before ordering the crew members to unbolt the lift fixture. There are three potential ways that the radiation protection worker could fail to properly determine that the shield ring is not properly in place. First, the radiation protection worker could forget to perform the measurement; however, since the only reason the radiation protection worker was called to the WHF was to perform this task, the radiation protection worker would need to be distracted by something or someone to not perform this measurement. The radiation protection worker has performed this task a number of times in the past, and it is possible that the radiation protection worker could remember performing this task before and get confused and signal the operator that the levels are acceptable, believing that the radiation measurement has been performed. To put this in a more colloquial context, this type of omission would be comparable to an individual leaving their home or office without setting an alarm system. This individual performs this task every time they exit, and it has become second nature, so they cannot believe that they did not do it this time.

In this case, the unsafe action results from the radiation protection worker not checking radiation levels, after being called in specifically to perform this task. This can be represented by CREAM CFF E5, adjusted by the following CPCs with value other than 1.0.

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03.

- CFP "Adequacy of Training/Preparation": This routine task is well trained, practiced, and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.

- CFP "Available Time": There is adequate time to perform this task and no significant time pressure. The CPC value for adequate time for an execution task is 0.5.

Applying these factors yields the following:

Radiation protection worker fails to check radiation levels = 0.03 × 0.8 × 0.5 = 0.02

Radiation Protection Worker Misreads Radiation Levels—The second potential way that the radiation protection worker could fail to properly determine that the shield ring is not properly in place is by simply misreading the meter on the radiation gauge and believing the level is acceptable. Therefore, this failure is misreading the digital display on the radiation monitor. This can be represented by THERP table 20-11, item 1 (HEPs for EOCs in check-reading digital indicator displays) (Ref. E8.1.26).

Radiation protection worker misreads radiation level = 0.001

Radiation Monitor Fails—The radiation protection worker could also fail to properly determine that the shield ring is not properly in place due to a problem with the radiation monitor. The radiation monitor could give a false low reading as the result of a hardware failure. This is a mechanical rather than a human failure. From the Attachment C, Table C4-1, the failure rate for radiation sensors is approximately 2E−5/hour. It is expected that the monitor is used at least once each day. Using the equation for standby equipment (0.5λt) yields:

Radiation monitor fails = 0.5 × 2E−5 × 24 = 2.4E−4

Crew Member Fails to Note Shield Ring Out Of Position Before Approaching DPC—The crew members, after being cleared to begin the cutting task, bring the required tools and approach the DPC. They have performed this task many times before, and they would have an image in their minds of how everything should look. Unlike the previous scenario, the ring is essentially in place and the misalignment is a more subtle deviation from the image they expect. Even so, if the ring were out of position they would be exposed well before they got close to it, so they would still have to notice from some reasonable distance away. The crew carries the tools they need, they are focused on the performance of the task, and likely talking to each other about the performance of the task or involved in casual conversation (since the work is not particularly difficult or challenging and they are not expecting any complications). The unsafe action is that they do not notice that the shield ring is out of position. The crew members would have a bias that the previous activities have been performed correctly, the shield ring is configured properly, and they are ready to proceed with their operations; any differences in appearance do not register (i.e., they see what they expect to see). To put this in a more colloquial context, this type of missed observation would be comparable to an individual walking out to a car and failing to see from a distance that the car has a flat tire. Noticing it when getting within a few feet of the car would be a failure in this case, since the person would already be exposed.

Although there is no specific check that takes place when the crew begins cutting preparations, there is ample opportunity to notice that the shield ring is not properly in place (i.e., that it is over the DPC, but out of position). Rather than missing a check, it is more in the nature of failing to notice that the operational conditions were not correct. It would be similar to someone noticing a low tire on their car when they go out to start their car. There are no failures in the primary quantification methods that reasonably fit this unsafe action, so it is necessary to provide a value based on expert judgment (ATHEANA). It is clear that some credit needs to be given for this action since the crew members perform this task often, and should recognize what the

configuration should look like when they perform the task. However, in opposition to this, the crew begins operations on the DPC believing the shield ring is properly configured and they are focused on the task that they are about to perform. Taking all of this into consideration, the HRA team believes that the failure is less than likely (0.5), but greater than unlikely (0.1). A value of 0.3 is selected.

Crew members fail to notice that shield ring is out of position prior to approaching DPC = 0.3

HEP Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.7-5.

Table E6.7-5. HEP Model for HFE Group #7 Scenario 1(b) for 050-OpDPCShield2-HFI-NOW

Designator	Description	Probability
A	Crane operator installs shield ring improperly	0.0004
B	Radiation protection worker fails to check radiation levels	0.02
C	Radiation protection worker misreads radiation level	0.001
D	Radiation monitor fails	2.4E−4
E	Crew member fails to note shield ring out of position before approaching DPC	0.3

NOTE: DPC = dual-purpose canister; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times (B + C + D) \times E =$$
$$0.0004 \times (0.02 + 0.001 + 2.4E{-}4) \times 0.3 = 3E{-}6 \quad \text{(Eq. E-40)}$$

E6.7.3.4.2.3 HEP for HFE 050-OpDPCShield2-HFI-NOW

The Boolean expression for the overall HFE (all scenarios) follows:

$$\text{050-OpDPCShield2-HFI-NOW} =$$
$$\text{HFE 1(a)} + \text{HFE 1(b)} =$$
$$0.0002 + 3E{-}6 = 0.0002$$

E6.7.3.4.3 Quantification of HFE Scenarios for 050-OpDPC-OVP01-HFI-NOW Operator Causes Overpressure when Filling/Flushing the DPC with Borated Water (DPC Only)

E6.7.3.4.3.1 HFE Group #7 Scenario 2(a) for 050-OpDPC-OVP01-HFI-NOW:

1. Operator pumps borated water at faster than acceptable rate.

2. Operator fails to notice pressure increase OR fails to stop operation given the pressure increase.

3. Pressure relief valve fails to operate OR pump motor fails to shut off upon overpressure.

Operator Pumps Borated Water at Faster Than Acceptable Rate—During preparation, the DPC is filled and flushed with water to prevent a crud burst when put into the pool. This step is straight forward, integral to the sampling and cutting, and on a checklist. The crew attaches two hoses to the DPC (one to the fill port and one to the drain port), via the quick disconnect ports and then starts the water flow according to procedures. The crew starts the cooling water feed pump to send borated pool water through the 1 in. treatment discharge piping into the DPC to cool it down. It is anticipated that this cool down would require one shift (8 hours) at minimum and up to 3 shifts (24 hours) to accomplish. Overpressurization can happen by setting the cooling water feed pump at or near its maximum rate of 20 gpm. The operator could make this error due to a perceived schedule pressure or because of some distraction.

The most likely scenario is that the crew rushes the process due to perceived schedule pressure and floods the DPC at a faster rate than the 8 to 24 hour timeframe. This would be accomplished by setting the cooling water feed pump at or near its maximum rate of 20 gpm.

This action is best represented by the CREAM CFF E1, adjusted by the following CPCs with values not equal to 1.0:

- CFF E1: Execution of wrong type performed (with regard to force, distance, speed, or direction). The baseline HEP is 0.003.

It is presumed that a second crew member is present during this task, but while that second crew member could note that the pumping rate is excessive, it is considered a dependent failure for them to not correct the situation since they are likely to depend upon the judgment of the initial operator. Based on Table 20-21 of THERP, for a baseline HEP of <.01 and medium dependence, the appropriate dependence value would be item (3)(a) or 0.15 (Ref. E8.1.26).

$$\text{Operator pumps borated water at faster than acceptable rate} = 0.003 \times 0.15 = 0.0005$$

Operator Fails to Notice Pressure Increase

If the pump rate is set too high, then the overpressurization manifests itself fairly quickly (within the shift). There are alarms associated with overpressurization. The operator may be occupied with other tasks, but is located in the immediate vicinity of the DPC. The operator can fail to respond to the overpressure alarms because of distraction from other tasks or because the operator has inappropriately left the area for a prolonged period of time. If there is an overpressurization, it would most likely occur in the first hour or so of cooling, and the operator would have on the order of a minute or more to respond to the alarm before the DPC would be damaged.

The potential exists to monitor pressure during the fill/flush operation via either the pressure indicator on the inlet line to the DPC, or the indicator on the outlet line back toward the pool. This unsafe action can be represented by NARA GTT C1, adjusted for the following EPCs:

- GTT C1: Simple response to a range of alarms/indications providing clear indication of a situation (simple diagnosis required). The baseline HEP is 0.0004

- EPC 3: Time pressure. The full effect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. This appears reasonable for this task, so the APOA is set at 0.1.

- EPC 13: Operator underload/boredom. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, a single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

Using the NARA HEP equation yields:

$$\text{Operator fails to notice pressure increase} = 0.0004 \times [(11-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.001$$

Operator Fails to Stop Operation Given Pressure Increase

If the operator responds to the alarm, it is possible that the operator fails to properly stop the operation. For example, the pressure can be misread or the operator could insufficiently turn down the flow and assume the alarm is malfunctioning. Alternately, the alarm could be responded to in an untimely manner and the operator could fail to stop the overpressurization before there is damage to the canister. If there is an overpressurization, it would most likely occur in the first hour or so of cooling and the operator would have on the order of a minute or more to respond to the alarm before the DPC is damaged.

This is an error of omission that can most closely be represented by CREAM CFF E5, adjusted by the following CPC's with values not equal to 1.0:

- CFF E5: Action missed, not performed (omission), including the omission of the last actions in a series. The baseline HEP is 0.03.

- CPC "Available Time": There is adequate time available. The CPC for an execution task with adequate time is 0.5.

- CPC "Adequacy of Training/Preparation": Training is adequate with high experience. The CPC for an execution task with adequate training and high experience is 0.8.

Applying these factors yields:

$$\text{Operator fails to stop operation given pressure increase} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Pump Motor Fails to Shut Off Upon High Pressure Signal

The pump used to fill the canister receives a signal to shut off upon high pressure, but if the motor fails to shut off, an overpressure condition could result.

This is a mechanical failure to shut off of a motor, included in the PCSA active component reliability database provided in Attachment C, Table C4-1 as MOE-FSO.

Pump motor fails to shut off = 1.35E−8 = 1E−8

Pressure Relief Valve Fails to Operate Upon Overpressure

A pressure relief valve is provided on the pipe assembly that connects directly to the canister connection to protect against canister failure due to overpressure; however, failure of this valve could lead to an overpressure condition.

This is a mechanical failure of a pressure relief valve included in the PCSA active component reliability database provided in Attachment C, Table C1-4 as PRV-FOD.

Pressure relief valve fails = 6.5 E−3 = 7E−3

HEP Calculation for Scenario 2(a)—The events in the HEP model for Scenario 2(a) are presented in Table E6.7-6.

Table E6.7-6. HEP Model for HFE Group #7 Scenario 2(a) for 050-OpDPC-OVP01-HFI-NOW

Designator	Description	Probability
A	Operator pumps borated water at faster than acceptable rate	0.0005
B	Operator fails to notice pressure increase	0.001
C	Operator fails to stop operation given pressure increase	0.01
D	Pressure relief valve fails to operate upon overpressure	7E−03
E	Pump motor fails to shut off upon high pressure signal	1E−08

NOTE: DPC = dual-purpose canister; HEP = human error probability; HFE = human failure event.

Source: Original

The Boolean expression for this scenario follows:

$$A \times [B + C] \times [D + E] =$$
$$0.0005 \times [0.001 + 0.01] \times [7E{-}3 + 1E{-}08] =$$
$$0.0005 \times 0.011 \times 7E{-}3 \qquad \text{(Eq. E-41)}$$

E6.7.3.4.3.2 HEP for HFE 050-OpDPC-OVP01-HFI-NOW

The human portion of the HEP quantification is 0.0005 × 0.011 and the mechanical portion is 7E−3.

With truncation of human portion for 1 team to 1E−5:
$$1E{-}5 \times 0.007 = 7E{-}08 \qquad \text{(Eq. E-42)}$$

E6.7.4 Results of Detailed HRA for HFE Group #7

The final HEPs for the HFEs that required detailed analysis in HFE Group #7 are presented in Table E6.7-7 (with the original preliminary value shown in parentheses):

Table E6.7.-7. Summary of HFE Detailed Analysis for HFE Group #7

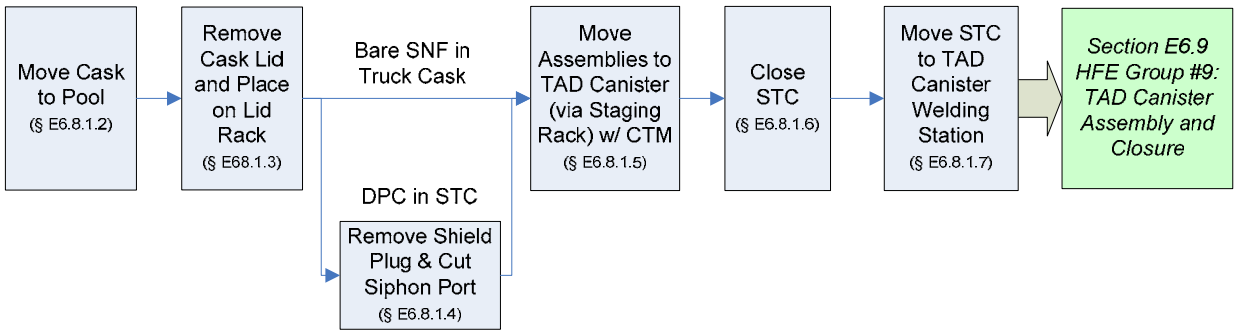
HFE	Description	Final Probability
050-OpDPCShield2-HFI-COW	Operator causes exposure due to failure to install DPC shield ring	2E−4 (1E−02)
050-OpDPC-OVP01-HFI-NOW	Operator causes overpressurization of DPC during DPC Cutting	7E−8 (5E−03)
050-OpDPCShield3-HFI-NOW	Operator fails to properly shield DPC while removing canister lift fixture, leading to direct exposure	4E−04 [a] (1E−3)

NOTE: a This value is taken from the detailed analysis for 050-OpDPCShield1-HFI-NOW (Table E6.5-6) because that HFE is identical to the HFE considered here (050-OpDPCShield3-HFI-NOW)
DPC = dual-purpose canister; HFE = human failure event.

Source: Original

E6.8 ANALYSIS OF HUMAN FAILURE EVENT GROUP #8: POOL ACTIVITIES: TRANSFER OF FUEL ASSEMBLIES INTO A TAD CANISTER

HFE group #8 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering the transfer of fuel assemblies into a TAD canister. The operations covered in this HFE group are shown in Figure E6.8-1. The process of transferring fuel assemblies into a TAD canister begins with fuel assemblies in either a truck cask at the SNF preparation platform or in a DPC in a STC at the DPC cutting station. Both types of the transportation casks have their lids bolted on. In this operation, the cask is transferred to the pool, the cask lid is removed, the spent fuel assemblies are transferred to a TAD canister (which is also in a STC), the TAD canister lid is emplaced, and the STC lid is bolted on. After the STC lid is bolted on, the STC containing the TAD is lifted out of the pool. This operation ends when the STC/TAD canister is stationed at the TAD canister closure station ready for TAD canister assembly and closure activities.



NOTE: § = section; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure event; STC = shielded transportation cask; TAD canister = transportation, aging, and disposal canister.

Source: Original

Figure E6.8-1. Activities Associated with HFE Group #8

E6.8.1 Base Case Scenario

E6.8.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #8 activities:

1. The DPC is sitting in the DPC cutting area in a STC, with the STC lid bolted on. The DPC has no lid (but may have a shield plug) and is filled with borated water.

2. The SNF is sitting in the preparation station in a truck cask with the truck cask lid bolted on, and is located in a transportation cask handling frame.

3. The cask handling crane (200-ton) and auxiliary pool crane (20-ton) are in the pool area and have the following safety features:

   A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.

   B. There are end-of-travel interlocks on the trolley and bridge.

   C. There are speed limiters built into the motors.

   D. There is a weight interlock that cuts off power to the crane when the crane capacity is exceeded.

   E. There is a temperature interlock that cuts off power to the hoist when the temperature is too high. An indicator comes on before this temperature is reached.

   F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

4. An STC with an empty TAD canister is positioned and ready in the Cask Preparation Area prior to the arrival of non-truck cask fuel assemblies. For all casks, the annulus between the TAD canister and the STC is pre-filled with demineralized water and sealed with a bladder on top to prevent borated water from seeping into the annulus.

5. The PWR fuel assemblies are significantly larger than the BWR fuel assemblies and should not be easily confused. Likewise, the staging racks for the PWR assemblies are noticeably taller than those for the BWR fuel.

6. The SNF transfer machine operator has the correct TAD canister loading plan (map) for a specific TAD.

7. The SNF transfer machine is located over the pool, and has the following safety features:

   A. Upper limits—There are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.

   B. There are end-of-travel interlocks on the trolley and bridge.

   C. There is a speed limiter built into the motor.

   D. There is a weight interlock that cuts off power to the crane when the crane capacity is exceeded.

E. There is a temperature interlock that cuts off power to the crane when the motor temperature is too high. An indicator comes on before this temperature is reached.

F. There is an interlock which prevents the crane from moving the SNF too high.

8. The SNF transfer machine has five possible grapples:
   A. PWR lifting grapple #1.
   B. PWR lifting grapple #2.
   C. PWR lifting grapple #3.
   D. BWR lifting grapple #1.
   E. BWR lifting grapple #2.
9. The SNF transfer machine operator is located on the bridge over the pool, and can look down at the pool and see the operations. The operator also has a camera view of the pool operations.

Crane and SNF transfer machine operations in this operation are not part of a specific procedure outlined in the YMP documentation, but rather reflect the comparable standard operations in the nuclear industry.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Radiation protection worker[14]
- Supervisor
- Nuclear engineer
- Quality control.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel involved in pool operations wear the appropriate PPE.

E6.8.1.2 Movement of Cask to Pool

E6.8.1.2.1 Cask Movement to Staging Shelf in Pool

The transportation casks are moved to the staging shelf in the pool using the cask handling crane with the cask handling yoke; in the case of a truck cask, the cask is moved in the cask handling frame. In preparation for this step, the cask handling yoke is attached to the cask handling crane.

[14]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

Crane Alignment to Cask— The operator positions the crane over the cask. The crane operator is on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask who uses hand signals to guide the operator's movements (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask, checking alignment of the second trunnion. The crew member signals the crane operator to stop, as required.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. Crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). The crane operator knows if the arms are sufficiently engaged on both sides by an indicator on the controller, and the signaling crew member signals the operator to raise the crane a slight amount to put pressure on the arms. The crane operator can see on the controller that the crane is bearing weight. Crew members verify that the yoke remains level. If the arms do adequately not engage on the initial attempt, either crew member signals the operator to stop, and the crane operator sets the cask down and opens the yoke arms to disengage. The signaling crew member then directs movement of the crane (again with hand signals) to compensate, and then signals the operator to close the yoke arms.

Cask Lifting and Movement to the Pool Staging Shelf – Once the cask is attached to the yoke, the signaling crew member signals the crane operator to lift the cask vertically. The crane operator lifts the cask vertically until it reaches the proper height for movement, basing this on a visual inspection, confirmed by hand signals from the signaling crew member. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path. This requires the crane operator to clear the cask from the platform before lowering the cask to movement height. The crane operator then begins to move the crane to the pool staging shelf, following the indicated safe load path marked on the floor to the pool ledge. The crane operator performs this task visually and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member on the opposite side of the cask of the signaling crew member who can only give the crane operator a signal to stop. Once the cask has cleared the pool ledge, the crane operator lowers the cask down onto the pool staging shelf. The crane operator can roughly align the cask on the shelf, but final alignment is directed by the signaling crew member, since the crane operator's view of the alignment in the pool may be obstructed. Once properly positioned, the signaling crew member signals the crane operator to finish lowering the cask. Finally, with the confirmation of the signaling crew member, the crane operator disengages the yoke and lifts the crane to proper moving height.

The crane operator is able to see crane movements inside the pool by looking over the edge of the pool and also via a camera fed to a monitor located on the crane controller.

E6.8.1.2.2 Move Cask to Position in Bottom of Pool

The transportation cask, or truck cask in a cask handling frame, is moved to position in the bottom of the pool using the cask handling crane with the cask pool handling yoke (with extension). In preparation of this step, the crew must remove the cask handling yoke from the cask handling crane, wash the yoke, attach the yoke extension piece, and then reattach the cask

handling yoke. For this operation, the crane operator is standing at the ledge of the pool, there is a camera on the crane, and the camera monitor is located on the crane operator's controller.

Crane Alignment with Cask—The crane operator lowers the crane into position over the cask such that the yoke arms line up with the trunnions. The crane operator is positioned on the pool ledge looking down, and has a camera view of the crane operations on the crane controller.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the crane operator closes the yoke arms and checks to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). The crane operator knows if the arms are sufficiently engaged on both sides by an indicator on the controller and by the camera view. The crane operator raises the hoist to put a slight amount of pressure on the arms and then checks the controller to verify that the crane is bearing weight. The crane operator also verifies that the yoke remains level. If the arms do adequately not engage on the initial attempt the crane operator sets the cask down, opens the yoke arms to disengage, readjusts the yoke and then closes the yoke arms again.

Movement of Cask to Bottom of the Pool—Once the yoke is properly engaged, the crane operator lifts and moves the cask to clear the staging shelf, then lowers the cask to the proper height for movement. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. The operator confirms the height visually via camera. The operator then moves the cask into position on the bottom of the pool, disengages the yoke, lifts the crane out of the pool and washes the yoke. Correct positioning of the cask is verified by quality control.

E6.8.1.3 Removal and Storage of the Cask Lid on the Lid Rack

The auxiliary pool crane is used with the long reach grapple adapter and lid lifting grapple to pick up and place the cask lid (truck cask or STC lid) on the appropriate lid stand. In preparation of this step, the crew members attach the lid lifting grapple with extension to the auxiliary pool crane. For this operation, the crane operator is standing at the ledge of the pool, there is a camera on the crane, and the camera monitor is located on the crane operator's controller.

Removal of Cask Lid Bolts—The cask lid bolts are remotely removed by personnel using underwater common tools and the auxiliary pool crane. The removed bolts are counted and verified before continuing.

Crane Alignment with Cask—The crane operator lowers the crane into position over the cask. The crane operator is positioned on the pool ledge looking down, and has a camera view (underwater) of the crane operations on the crane controller. Once positioned, the crane operator engages the lid lifting grapple to the lid adapter on the cask lid. There is an indicator to verify engagement.

Vertical Lift of the Lid—Once the grapple is engaged, the crane operator begins to raise the cask lid out of the pool. Once the lid is out of the pool, a crew member washes off the grapple and lid, and the crane operator lowers the lid to the proper movement height based on visual inspection. The proper height for movement is roughly 6 in. above the highest obstacle in the

movement path. The crane operator then moves the lid to the appropriate lid stand in the staging area, following the indicated safe load path marked on the floor.

E6.8.1.4 Removal of the DPC Shield Plug and Cutting of the Siphon Port (DPC in STC Only)

The crane operator uses the auxiliary pool crane with the appropriate extensions to lift the DPC shield plug above the siphon tube shear tool (approximately 1 to 2 ft). A crew member uses the siphon tube shear tool to cut the siphon tube. The crane operator then proceeds to move the shield plug to the staging area. The siphon tube shear tool is like an arm that swings over the STC and cuts the siphon tube. The siphon tube is taller than the STC and cannot impact it.

E6.8.1.5 Movement of SNF Assemblies to TAD Canister (via Staging Rack) with SNF Transfer Machine

The TAD canister loading plan is prepared before the TAD canister is placed into the pool and the loading sequence is verified by both Nuclear Engineering and quality control. The TAD canister cannot be placed into the pool until all the SNF assemblies identified in the loading plan are in the pool and ready for transfer into the TAD canister. A full TAD canister contains 21 PWR assemblies or 44 BWR assemblies. A DPC has more fuel assemblies than can fit into one TAD canister. For bare SNF arriving in truck casks, 5 truck casks full of BWR fuel assemblies or 9 truck casks full of PWR fuel assemblies are needed to fill one TAD canister. Section E6.1 provides a more detailed explanation of "campaigns." Movement of the SNF assemblies with the SNF transfer machine is described in the following sections:

E6.8.1.5.1 Preparation for TAD Canister Loading

All the fuel assemblies in the TAD canister loading plan must be present in the staging rack before the TAD canister/STC unit is placed in the pool. Once all the SNF assemblies are staged in the staging racks, then the TAD canister/STC unit is placed into the pool as follows:

E6.8.1.5.1.1 Movement of SNF Assemblies to Storage Rack

The SNF transfer machine is used with the BWR lifting grapple #1 or #2, or PWR lifting grapple #1, #2, or #3 to move the SNF assemblies from a DPC or a truck cask into the SNF staging rack.

The SNF transfer machine operator attaches the correct fuel assembly grapple to the SNF transfer machine (crane like) and then position the grapple over the SNF assembly to be moved. Once in position, the operator engages the grapple (verified by indicator and visual inspection via camera) and lifts the assembly to the proper height for movement under the water. The operator then moves the SNF transfer machine laterally to position it over the staging rack. Once positioned, the operator lowers the assembly onto the rack, disengages the grapple, and lifts the SNF transfer machine.

E6.8.1.5.1.2 Movement of STC and TAD Canister into the Pool

Once all the fuel assemblies necessary to fill a TAD canister are in the staging rack, the crane operator uses the cask handling crane with cask handling yoke and long reach adapter to move

the empty STC/TAD canister into the pool. The annulus of the STC/TAD canister is pre-filled with demineralized water and sealed with a bladder. For this operation, the crane operator is standing at the ledge of the pool; there is a camera on the crane and the corresponding monitor is located on the crane operator's controller.

Crane Alignment to Cask—The operator positions the crane (with cask handling yoke and extension) over the cask. The crane operator is positioned on the building floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask using hand signals to guide the operator's movements (no hardwired or wireless communication system is used) to position the woke on the first trunnion. A verification crew member on the opposite side of the cask checks the alignment of the second trunnion. Once this is achieved the crew member signals the crane operator to stop.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. Crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). The crane operator knows if the arms are sufficiently engaged on both sides by an indicator on the controller, and the signaling crew member signals the operator to raise the crane a slight amount to put pressure on the arms. The crane operator can see on the controller that the crane is bearing weight. Crew members verify that the yoke remains level. If the arms do adequately not engage on the initial attempt, either crew member signals the operator to stop. The crane operator sets the cask down and opens the yoke arms to disengage. The signaling crew member then directs the movement of the crane with hand signals, and then signals the operator to close the yoke arms.

Lift and Move Cask to Pool Bottom —Once the cask is attached to the yoke, the signaling crew member signals the crane operator to lift the cask vertically. The crane operator lifts the cask vertically until it reaches the proper height for movement (based on a visual inspection) that is confirmed by hand signals from the signaling crew member. The proper height for movement is defined as roughly 6 in. above the highest obstacle in the movement path. The crane operator then begins movement to the pool, following the indicated safe load path marked on the floor to the pool ledge. The crane operator does this visually and also receives confirmatory hand signals from the signaling crew member. There is a verification crew member on the opposite side of the cask as the signaling crew member which can only give the crane operator a signal to stop. Once the cask has cleared the pool ledge and is roughly over the portion of the pool where the TAD canister is staged, the crane operator lowers the cask down to the pool bottom. The crane operator can roughly align the cask by eye, but final alignment is done using the camera view. Once the TAD is correctly placed, the crane operator disengages the yoke, lifts the crane out of the pool and washes the yoke. Correct positioning of the cask is verified by quality control.

E6.8.1.5.2 Move SNF Assemblies to TAD Canister with SNF Transfer Machine

The SNF transfer machine is used with BWR lifting grapple #1 or #2 or PWR lifting grapple #1, #2, or #3 to move the SNF assemblies from a DPC, a transportation cask, or the SNF staging rack into a TAD canister.

The SNF transfer machine operator attaches the correct fuel assembly grapple to the SNF transfer machine and then positions the grapple over the SNF assembly to be moved. Once in position, the operator engages the grapple (verified by indicator and visual inspection via camera) and lifts the assembly to the proper height for movement underwater. The operator then moves the SNF transfer machine laterally to position it over the TAD canister, lowers the assembly into the TAD canister, disengages the grapple and lifts the SNF transfer machine. For DPCs, the fuel assemblies are moved through the DPC unloading bay gate that is normally open.

The SNF transfer machine operator has a loading plan (map) for the TAD canister that indicates the serial number of the fuel assembly to be placed in each position of the TAD canister. When a fuel assembly is placed in the TAD canister, the SNF transfer machine operator documents the serial number and both operator and the quality control personnel verify the serial number and positioning.

This operation repeats this process until the TAD canister is full with 21 PWR assemblies or 44 BWR assemblies.

E6.8.1.6 Closure of an STC

E6.8.1.6.1 Installation of TAD Canister Lid

The auxiliary pool crane is used with the long reach grapple adapter to pick up the lid lifting grapple and place the TAD canister lid onto the TAD canister. In preparation of this step, the crew members attach the lid lifting grapple, with extension, to the auxiliary pool crane. For this operation, the crane operator is standing at the ledge of the pool; there is a camera on the crane and the corresponding monitor is located on the crane operator's controller.

The crane operator uses the auxiliary pool crane to retrieve the TAD canister lid. The crane operator moves the crane to the lid, engages the grapple (indicator), then lifts the lid to proper position for movement. The operator then moves the lid over the pool and lowers it into position over the TAD canister. The operator is positioned on the floor at the ledge of the pool. There is a camera underwater that the crane operator can use to verify positioning. Once positioned, the crane operator disengages the lid lifting grapple and uses an indicator to verify disengagement.

E6.8.1.6.2 Installation of STC Lid

The auxiliary pool crane with the long reach grapple adapter is used to pick up the lid lifting grapple and place the STC lid onto the STC.

Once the lid lifting grapple is disengaged from the TAD canister lid, the crane operator lifts the crane and washes off the grapple and long reach adapter. The operator then moves the auxiliary pool crane over to the STC lid rack, engages the grapple to the STC lid (indicator), and lifts the STC lid to the proper height for movement. The crane operator moves the lid over the pool in position over the cask and then lowers the lid onto the STC. The operator assesses the alignment visually with the aid of a camera. Once in place, the crane operator disengages the grapple from the lid and lifts the crane. The operator lifts the crane and washes the grapple and adapter.

E6.8.1.6.3 Bolting STC Lid

Using at least four bolts, the lid is bolted to the STC by personnel using common underwater tools and the auxiliary pool crane. This step is verified on a checklist.

E6.8.1.7 Movement of an STC to the TAD Canister Welding Station

E6.8.1.7.1 STC Lifting to the Staging Shelf

The STC is moved to the staging shelf in the pool using the cask handling crane with the cask pool handling yoke and crane extension. In preparation for this step, the cask pool handling yoke, with extension, must be attached to the cask handling crane. For this operation, the crane operator is standing at the ledge of the pool; there is a camera on the crane and the corresponding monitor is located on the crane operator's controller.

Crane Alignment to Cask—The crane operator positions the crane over the cask. The crane operator is standing at the ledge of the pool looking down, and has a camera view of the crane operations from the controller. The crane operator lowers the crane into position so that the yoke arms are lined up with the trunnion.

Yoke Arm Engagement on Trunnions—Once the yoke is aligned, the crane operator closes the yoke arms. The operator checks to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). An indicator on the controller lets the crane operator know when the arms are sufficiently engaged and the operator raises the crane a slight amount to put pressure on the arms. The crane operator can see on the controller that the crane is bearing weight. The operator verifies that the yoke remains level. If the arms do adequately not engage on the initial attempt the operator stops, sets the cask down, opens the yoke arms to disengage, readjusts the yoke, and then closes the yoke arms.

Cask Movement to the Staging Shelf in the Pool—Once the yoke is properly engaged, the crane operator moves the cask into position on the staging shelf of the pool, lowers the cask onto the shelf, disengages the yoke, and lifts the crane out of the pool.

E6.8.1.7.2 Cask Pool Handling Yoke Washing and Placement on the Cask Pool Handling Yoke Stand

Once the cask pool handling yoke is disengaged from the STC, the crane is lifted out of the pool. The yoke (with extension) is washed over the pool using the wash lance. The crane operator uses the cask handling crane to place the cask pool handling yoke extension onto the cask pool handling yoke stand, following the indicated safe load path marked on the floor. A crew member then reattaches the cask handling yoke to the cask handling crane.

E6.8.1.7.3 Lifting the STC Out of the Pool

The STC is lifted out of the pool using the cask handling crane with the cask handling yoke. In preparation for this step, the cask handling yoke is attached to the cask handling crane.

Aligns Crane to STC – The crane operator positions the crane over the STC. The operator is positioned at the ledge of the pool looking down, and has a camera view of the crane operations from the controller. The crane operator lowers the crane into position so that the yoke arms are lined up with the trunnion.

Yoke Arm Engagement on Trunnion and Lifting of STC Out of the Pool – Once the yoke is aligned, the crane operator closes the yoke arms. The operator checks to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm), with the use of an indicator on the controller. The crane operator raises the crane a slight amount to put pressure on the arms and can see on the controller that the crane is bearing weight. The operator verifies that the yoke remains level. If the arms do adequately not engage on the initial attempt the operator stops the process, sets the cask down, disengages the yoke arms by opening them, readjusts the yoke, and then closes the yoke arms. Once the yoke is properly engaged, the crane operator lifts the cask vertically out of the pool. The crane operator is able to see crane movements inside the pool by looking over the edge of the pool and also via a camera feed to a monitor located on the controller.

E6.8.1.7.4 Wash Lifting Yoke and Exterior of STC over the Pool

While the STC is suspended over the pool, a crew member washes the cask handling yoke and the exterior of the STC over the pool using the wash lance. The crew is cognizant of the boron pool concentration during this operation. The wash lance has a trigger mechanism that won't stay on unless the crew member is pressing on the trigger.

E6.8.1.7.5 Move STC to the TAD Canister Welding Station

The operator lowers the cask to the proper height for movement (i.e., 6 in. above the highest obstacle in the movement path) and then moves the STC to the TAD canister welding station, using the cask handling crane with the cask handling yoke. The operator visually follows the indicated safe load path marked on the floor, and also receives confirmatory hand signals from the signaling crew member. Once at the welding station, a crew member opens the hinged platform to allow the STC to pass through. Once in proper position in the weld station, the crane operator lowers the cask to the floor of the welding station and disengages the yoke. The crew member closes the hinged platform so there is a proper working platform around the STC.

E6.8.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during pool activities are summarized in Table E6.3-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.8-1. HFE Group #8 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
Crane Drops	*Operator Drops Cask or Object onto Cask/Fuel Assembly*: During the pool activities, several objects are moved, including: the cask, the fuel assemblies, the cask lid, the DPC shield plug, etc. Each of these lifts could result in a drop and damage to the fuel/canister.	19, 20, 21, 22, 23, 24, 30	N/A[a]	There are several lifts in this operation, including several lifts of the cask itself. These lifts of casks and heavy objects can all potentially result in a drop. Crane drop related HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for these failures can be found in Attachment C. Note: Except for the movement from the pool shelf to the pool bottom, the cask lid is bolted with at least four bolts for each cask lift in this operation.
Drops from SNF Transfer Machine	*Operator Drops Fuel Assembly*: During the pool activities, many fuel assemblies are moved using the SNF transfer machine. Each of these lifts could result in a drop and damage to the fuel/canister.	22	N/A[a]	There are several fuel assembly lifts in this operation performed using the SNF transfer machine. These lifts of fuel assemblies can all potentially result in a drop. Historical data is used to quantify the probability of dropping a fuel assembly with the SNF transfer machine. Documentation for this failure can be found in Attachment C.
050-OpTCImpact06-HFI-NOD	*Operator Causes an Impact between the Cask and an SSC during Movement between the Pool Ledge and the Outside of the Pool*: In this step, the DPC/STC and SNF/TC are moved to the pool ledge from the DPC cutting station or SNF preparation platform (respectively), and the TAD canister/STC unit is moved from the pool ledge to the TAD canister closure station outside the pool. In terms of failure modes and conditions, these two movements are identical. During this movement, the crane operator can cause the cask to collide with an SSC, such as the side of the pool or the TAD canister closure station, DPC cutting station, or SNF preparation platform.	19, 20, 24	3E−03	In this step, the DPC/STC and SNF/TC are moved to the pool ledge from the DPC cutting station or SNF preparation platform (respectively), and the TAD canister/STC unit is moved from the pool ledge to the TAD canister closure station outside the pool. For crane operations in this step, there are three observers with clear visibility, the operations are simple, the travel distances are short, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a very regular (daily) basis. There are no interlocks to prevent this error. The dominant contributors to the impact of a cask include the following: • Crane moved outside its safe load path (e.g., operators cut corners) • Crane moved in wrong direction • Operator failed to maintain proper vertical and horizontal distance between cask and SSCs during crane operations • Bridge or trolley impacts end stop. The operator must manually maintain movement within the safe load path. It is not unlikely that the operator would stray slightly from that path or that an object would be slightly within that path. However, the crane operations are very slow and within clear, direct view of three observers. This operation is very similar to and has the same failure modes as operator causes an impact between cask and SSC during upending and removal (050-OpTCImpact01-HFI-NOD; Section E6.2, HFE Group #2), and was thus assigned the same preliminary value with the same rationale: the preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001) and was adjusted because there are several ways for an impact to occur (×3).
050-OpTipOver002-HFI-NOD	*Operator Causes Cask to Tip Over during Movement between Pool Ledge and Outside the Pool*: In this step, the DPC/STC and SNF/TC are moved to the pool ledge from the DPC cutting station or the SNF preparation platform (respectively), and the TAD canister/STC unit is moved from the pool ledge to the TAD canister closure station outside the pool. In terms of failure modes and conditions, these two movements are identical. During this movement, the crane operator can catch the ledge of the pool while moving the cask into or out of the pool. If the crane operator and crew members do not notice, the cask can start to tipover. If a trunnion or yoke arm fails due to the lateral force from the tipping, then the cask can fall over.	19, 20, 24	3E−03	In this step, The DPC/STC and SNF/TC are moved to the pool ledge from the DPC cutting station or SNF preparation platform, and the TAD canister/STC is moved from the pool ledge to the TAD canister closure station outside the pool. During this movement, the cask can be tipped over if it catches the ledge of the pool as the cask is moved onto the pool shelf. Unlike other cask tipover events (050-OpTipover001-HFI-NOD), the most likely cause of this tipover is that the crane operator catches the edge of the pool while lowering the cask into the pool or taking the cask out of the pool, and the crew members and crane operator fail to notice before the cask tips over. This failure requires the crane operator and the two crew members to be inattentive. This operation was given the same preliminary value as cask impact (050-OpTCImpact06-HFI-NOD) because it has the same basic cause and failure modes of inattention of the crane operator and the crew members. This preliminary value is considered particularly conservative because there is time (on the order of 30 to 90 seconds) for one of the three workers to notice and correct the error. The error is easy to correct, is very visible and may also require a mechanical failure to result in an actual tipover.
050-OpTCImpact07-HFI-COD	*Operator Causes an Impact Between Cask and SSC during Cask Movement between Pool Shelf and Pool Bottom*: In this step, The DPC/STC and SNF/TC are moved from the pool ledge to the pool bottom and the TAD canister/STC is moved from the pool bottom to the pool ledge. In terms of failure modes and conditions, these two movements are identical. During cask movement, the crane operator can cause the cask to collide with an SSC, such as the side of the pool, the staging rack or a staged STC.	21	6E−03	In this step, the DPC/STC and SNF/TC are being moved from the pool ledge to the pool bottom and the TAD canister/STC unit is moved from the pool bottom to the pool ledge. This operation is very similar to and has the same failure modes as operator causes an impact between cask and SSC during movement to pool shelf (3E−3, 050-OpTCImpact06-HFI-NOD), but this operation is done from the pool ledge looking over into the pool. The crane operator also has a camera view by which to observe the operations. The preliminary value was adjusted (×2) to account for visual distortion due to parallax effects and the camera view.

Table E6.8-1. HFE Group #8 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpTipOver004-HFI-COD	*Operator Causes Cask to Tip Over during Cask Movement between Pool Shelf and Pool Bottom*: In this step, the DPC/STC and SNF/TC are moved from the pool ledge to the pool bottom and the TAD canister/STC is moved from the pool bottom to the pool ledge. In terms of failure modes and conditions, these two movements are identical. During this movement, the crane operator can catch the ledge of the pool shelf while moving the cask onto or off of the pool shelf. If the crane operator and crew members do not notice, the cask can start to tipover. If a trunnion or yoke arm fails due to the lateral force from the tipping, then the cask can fall over.	21	6E−03	In this step, The DPC/STC and SNF/transportation cask are moved from the pool ledge to the pool bottom and the TAD canister/STC unit is moved from the pool bottom to the pool ledge. This operation is very similar to and has the same failure modes as operator causes a cask to tip over during movement to pool shelf (3E−3, 050-OpTipover002-HFI-NOD), but this operation is done from the pool ledge looking over into the pool. The crane operator also has a camera view by which to observe the operations. The preliminary value was adjusted (×2) to account for visual distortion due to parallax effects and the camera view.
050-OpFuelImpact-HFI-NOD	*Operator Impacts Fuel Assembly During Transfer*: If the spent fuel transfer machine operator does not lift the fuel assembly high enough or does not follow a clear path during fuel assembly transfer, the operator can impact and damage the fuel assembly.	22	N/A	If the SNF transfer machine operator does not lift the fuel assembly high enough or does not follow a clear path during fuel assembly transfer, an impact can occur that damages the fuel assembly. This failure event was screened out by the WHF analysts because: (1) criticality due to impact was screened out based on pool boration, criticality in this case is only an issue if it is accompanied by a loss of boration (screened out in Table 6.0-2 of the main report); (2) gaseous radiation release due to impact is bounded by the drop event addressed above. This HFE was omitted from the HRA analysis.
Improper Boration	*Operator Fails to Maintain Proper Boron Concentration*: If the operators fail to maintain the proper boron concentration, then it can result in a potential criticality.	N/A	N/A	If the operators fail to maintain the proper boron concentration, then it can result in a potential criticality. This failure event was screened out by the WHF analysts and is not part of this HRA; Table 6.0-2 of the main report provides the screening justification. This HFE was omitted from the HRA analysis.
Fuel Transpose	*Operator Misloads TAD Canister*: The SNF transfer machine operator can misload the TAD canister by failing to follow the loading map, transposing two or more fuel assemblies, or otherwise loading the TAD canister with the wrong fuel assemblies. This failure has possible criticality and thermal implications.	N/A	N/A	Misloading a TAD canister with the wrong fuel assemblies or transposing fuel assemblies has no criticality consequence (Table 4.3-1) and was therefore omitted from analysis.

NOTE: a HRA value replaced by use of historic data (Attachment C).
DPC = dual-purpose canister; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; HRA = human reliability analysis; N/A = not applicable; SNF = spent nuclear fuel; ssc = structure, system, or component; SSCs = structures, systems, and components; STC = shielded transfer cask; TC = transportation cask; TAD = transportation, aging, and disposal canister.

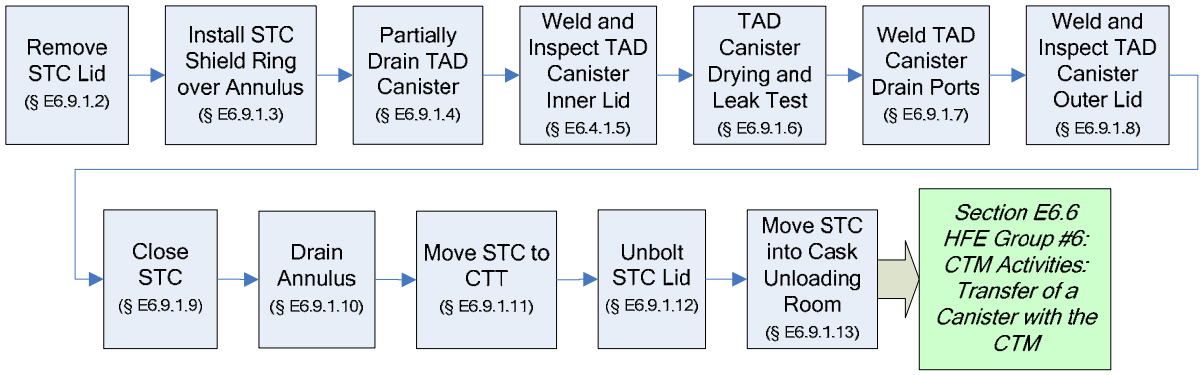
Source: Original

E6.8.3 Detailed Analysis

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E6.9 ANALYSIS OF HUMAN FAILURE EVENT GROUP #9: TAD CANISTER ASSEMBLY AND CLOSURE

HFE group #9 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering TAD canister closure and movement into the Cask Unloading Room. The operations covered in this HFE group are shown in Figure E6.9-1. This operation begins with the STC/TAD canister stationed in the TAD canister closure platform with the STC lid bolted on. TAD canister closure operations include the drying and welding of the TAD canister, the transfer of a TAD canister/STC unit to a CTT, and the movement of the loaded CTT to the CTM Unloading Room.



NOTE: § = section; CTM = canister transfer machine; CTT = cask transfer trolley; HFE = human failure event; STC = shielded transfer cask; TAD = transportation, aging, and disposal.

Source: Original

Figure E6.9-1. Activities Associated with HFE Group #9

E6.9.1 Base Case Scenario

E6.9.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #9 activities.

1. The STC/TAD canister is sitting in the welding station in the Cask Preparation Area; the TAD canister lid is not welded, but the STC lid is bolted down.

2. The STC has been thoroughly washed down. The radiation protection worker has ensured that there is not excessive radiation due to contamination from the STC.

3. The CTT is an air-pallet apparatus that is guided by two removable rails. The CTT also has end stops to aid in final positioning. A safe load path is marked for the CTT operations, and there are at least three crew members involved in its movement when loaded. The CTT is normally deflated, with control pendant stowed, during preparation activities. The empty CTT is staged underneath the cask preparation platform.

4. The TAD canister closure activities are performed on an elevated platform approximately 28 by 32 ft. Hinged platform sections open to allow the STC to enter the platform area. All equipment and workstations are provided on the work platform.

5. The cask handling crane (200-ton) is in the Cask Preparation Area, and has the following safety features:

   A. Upper limits—there are two upper limit marks: the initial is an indicator, and the final (which is set higher than the upper limit indicator) cuts off the power to the hoist. There is no bypass for the final limit interlock.

   B. There are end-of- travel interlocks on the trolley and bridge.

   C. There are speed limiters built into the motors

   D. There is a weight interlock that cuts off power to the hoist when the crane capacity is exceeded.

   E. There is a motor drive temperature interlock that cuts off power to the hoist when the temperature is too high. An indicator comes on before this temperature is reached.

   F. There is an indicator to signal the operators that the cask handling yoke is fully engaged, and an interlock (yoke engagement) that prevents the crane from moving unless and the yoke is either fully engaged or disengaged.

Crane operations in this step are not part of a specific procedure outlined in the YMP documentation, but rather reflect critical lift crane operations that are standard in the nuclear industry.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Crew members (two)
- Radiation protection worker
- Supervisor
- Quality control
- Level 2 and 3 NDE personnel
- Welding operator
- CTT operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel. Personnel in this operation wear the appropriate PPE.

E6.9.1.2 Removal of STC Lid

E6.9.1.2.1 Partially Drain TAD Canister STC

The crew connects a hose to the STC drain port (quick disconnect) and allows the annulus between the STC and TAD canister to partially drain into the pool. The cask is drained to just below the STC lid to prevent undue contamination when opening the cask lid.

E6.9.1.2.2 Removal of STC Lid Bolts

Once the STC is in place at the welding station, the crew uses common tools to remove the STC lid bolts. The removed bolts are counted and verified on a checklist.

E6.9.1.2.3 Removal of STC Lid and Placement in the Laydown Area

The jib crane is used with the lid lifting grapple to remove the STC lid. The STC lid is placed in the laydown area according to the following steps:

Crane Alignment to Cask—The crane operator lowers the jib crane into position over the STC. The operator is positioned on the platform in view of the crew members on either side of the cask. There is a signaling crew member next to the crane who uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the crane checking alignment of the crane. The verification crew member can only signal to stop the crane. Once positioned, one of the crew members connects the crane hoist to the cask lid using a grapple.

Vertical Lifting of Lid—Upon signal from the signaling crew member that all is well, the crane operator begins to raise the cask lid. Once the lid is raised (i.e., is hanging free), the crane operator clears the cask and then lowers the lid to the proper movement height based on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. Throughout this operation, the crew is standing several feet away from the platform opening.

Lid Movement to Staging Area—Using the jib crane, the crane operator positions the lid over the lid stand in the laydown area. To do this, the crane operator follows the indicated safe load path marked on the floor, based on visual cues and confirmatory hand signals from the signaling crew member. The crane operator then sets the lid down and disengages the grapple.

Once the lid is removed, a crew member wipes down the inside of the lid and removes the bladder seal with a long-reach tool.

E6.9.1.3 Installation of STC Shield Ring

The crew uses the jib crane to install a STC shield ring over the annulus.

The crane operator retrieves the STC shield ring from the staging area with the jib crane and lowers the crane into position over the STC. The operator is positioned on the platform in view of the crew members on either side of the cask. There is a signaling crew member next to the

crane who uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the crane checking the alignment. The verification crew member can only signal to stop the crane. Once positioned, the crane operator lowers the shield ring into place and disengages the grapple.

E6.9.1.4 Partially Drain TAD Canister

The crew attaches a hose to the shield plug siphon port (quick disconnect). The other side of the hose leads to the pool; there is also be a pump connected to the hose to create a vacuum. Once the hose is connected, the crew member turns on the pump and watches the water level in STC. Once the water level reaches just below the TAD canister lid, but before the fuel is exposed, the crew member stops the pump and disconnects the hose.

E6.9.1.5 Welding and Inspection of TAD Canister Inner Lid

E6.9.1.5.1 Movement of TAD Canister Welding Machine to the TAD Canister and Positioning the TAD Canister Welding Machine on the TAD Canister Lid

The jib crane is used to lift the TAD canister welding machine and move it to the TAD canister. This operation is done from the platform. The TAD canister welding machine is set up by personnel using common tools. The welding machine's weight is sufficient to maintain the machine in place, and the welding machine does not need to be bolted down.

Retrieval of the TAD Canister Welding Machine—The crane operator lowers the jib crane with the hook into position over the TAD canister welding machine in the staging area, engages the hook, and lifts the TAD canister welding machine to the proper height for movement based on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Movement of the TAD Canister Welding Machine to TAD Canister—Using the jib crane, the crane operator positions the TAD canister welding machine over the TAD canister in the welding area. The operator follows the indicated safe load path marked on the floor based on visual inspection, and confirmation by the signaling crew member via hand signals. A verification crew member, located opposite the signaling crew member, can signal the crane operator to stop at anytime. The crane operator can roughly align the TAD canister welding machine over the TAD canister, but final alignment is directed by the signaling crew member.

Lowering the TAD Canister Welding Machine—When the TAD canister welding machine is properly positioned over the TAD canister, the signaling crew member signals the crane operator that it is okay to lower the TAD canister welding machine into place. The crane operator proceeds to lower the TAD canister welding machine at or below the maximum allowable speed. Once the TAD canister welding machine is securely in place, the crew member disengages the hook, and the crane operator lifts the crane to its maximum height in preparation for the next operation.

E6.9.1.5.2 TAD Canister Inner Lid Weld and Inspection

The TAD canister inner lid is welded in place using the TAD canister welding machine. All TAD canister welds are stainless steel (spool fed).

The weld machine is semiautomatic and, once set up, makes automatic weld passes around the periphery of the lid while being operated from a remote location.

The welding operator performs visual and ultrasonic testing hand tool inspections of the inner lid The weld is verified and signed off by level 2 and level 3 NDE personnel.

E6.9.1.6 Drain TAD Canister Fully, Vacuum Dry, Helium Fill and Leak Test TAD Canister Weld

The crew installs a drying and inerting system on the vent and siphon ports of the inner lid to drain and dry the interior of the TAD canister using pressurized helium. The canister is then backfilled with helium gas. There is a moisture indicator associated with the helium drying system. Once dry and inerted, the weld is leak tested and the drying and inerting system hose is disconnected. This process takes place over several shifts (36 hours or more).

E6.9.1.7 Weld TAD Canister Drain Ports

The TAD canister drain ports are welded in place using the TAD canister welding machine. All TAD canister welds are stainless steel (spool fed).

The welding machine is semiautomatic and, once set up, makes automatic weld passes around the periphery of the port while operated from a remote location. The welding machine does not need to be repositioned in order to weld the drain ports.

E6.9.1.8 Welding and Inspection of TAD Canister Outer Lid

E6.9.1.8.1 Removal of TAD Canister Welding Machine from the TAD Canister

The jib crane is used to remove the TAD canister welding machine from the TAD canister and stage it on the welding machine stand.

Removal of TAD Canister Welding Machine—The crane operator lowers the jib crane into position over the welding machine and engages the hook. Once engaged properly, the crane operator lifts the welding machine and clears the cask, then lowers the machine to the proper height for movement based on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Movement of TAD Canister Welding Machine to Stand—The crane operator moves the jib crane to the welding machine stand, following the safe load path indicated on the floor. The crane operator places the welding machine on the stand and disengages the hook.

E6.9.1.8.2 Placement of Outer Lid on TAD Canister

The jib crane is used to lift the outer lid and move it to the TAD canister. This operation is done from the platform.

Retrieval of the TAD Canister Outer Lid—In the staging area, the crane operator lowers the jib crane with the hook into position over the TAD canister outer lid, engages the hook, and lifts the outer lid to proper height for movement based on visual inspection and confirmation via hand signals by the signaling crew member. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Movement of the TAD Canister Outer Lid to TAD Canister—Using the jib crane, the crane operator positions the TAD canister outer lid over the TAD canister in the welding area. The operator follows the indicated safe load path marked on the floor based on visual inspection and confirmation via hand signals by the signaling crew member. There is a verification crew member opposite the signaling crew member that can signal the crane operator to stop at anytime. The crane operator can roughly align the TAD canister outer lid over the TAD canister, but final alignment is directed by the signaling crew member.

Lowering the TAD Canister Outer Lid—When properly positioned over the TAD canister, the signaling crew member signals the crane operator that it is okay to lower the TAD canister outer lid into place. The crane operator proceeds to lower the TAD canister outer lid at or below the maximum allowable speed. Once the TAD canister outer lid is securely in place, the crew member disengages the hook, and the crane operator lifts the crane to its maximum height in preparation for the next operation.

E6.9.1.8.3 Movement of TAD Canister Welding Machine to the TAD Canister and Positioning the TAD Canister Welding Machine on the TAD Canister Lid

The jib crane is used to place the TAD canister welding machine on the TAD canister lid. The TAD canister welding machine is set up by personnel using common tools. The outer lid has a flat lifting feature on its top with which the weld machine must interface. The TAD canister welding machine is positioned on top of the outer lid's 6-in.-high lifting fixture to perform the closure weld on the outer lid. The welder has at least three pawls that engage the inside of the lifting feature to anchor the welding machine to the TAD canister.

Retrieval of the TAD Canister Welding Machine—In the staging area, the crane operator lowers the jib crane with the hook into position over the TAD canister welding machine, engages the hook, and lifts the TAD canister welding machine to the proper height for movement based on visual inspection and confirmation via hand signals by the signaling crew member. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Movement of the TAD Canister Welding Machine to TAD Canister—Using the jib crane, the crane operator positions the TAD canister welding machine over the TAD canister in the welding area. The operator follows the indicated safe load path marked on the floor based on visual inspection and confirmation by the signaling crew member via hand signals. A verification crew member, opposite the signaling crew member, can signal the crane operator to stop at anytime.

The crane operator can roughly align the TAD canister welding machine over the TAD canister, but final alignment is directed by the signaling crew member.

Lowering the TAD Canister Welding Machine—When properly positioned over the TAD canister, the signaling crew member signals the crane operator that it is okay to lower the TAD canister welding machine into place. The crane operator proceeds to lower the TAD canister welding machine at or below the maximum allowable speed. Once the TAD canister welding machine is securely in place on the lifting feature of the outer lid, the crew member engages the pawls that connect the welding machine to the outer lid's lifting fixture. The crew member then disengages the crane hook and signals the crane operator to lift the crane to its maximum height in preparation for the next operation.

E6.9.1.8.4 TAD Canister Outer Lid Welding and Inspection

The TAD canister outer lid is welded in place using the TAD canister welding machine. All TAD canister welds are stainless steel (spool fed).

The weld machine is semiautomatic and, once set up, makes automatic weld passes around the periphery of the lid while being operated from a remote location.

The welding operator performs visual and ultrasonic testing inspections of the outer lid weld using hand tools. The weld is verified and signed off by level 2 and level 3 NDE personnel.

E6.9.1.8.5 Removal of TAD Canister Welding Machine from the TAD Canister

The jib crane is used to remove the TAD canister welding machine from the TAD canister and stage it on the welding machine stand.

Removal of TAD Canister Welding Machine—The crane operator lowers the jib crane into position over the welding machine and a crew member engages the hook. Once engaged properly, the crew member disengages the pawls from the outer lid and then signals the crane operator to lift the welding machine. The crane operator lifts the machine and clears the cask, then lowers the machine to the proper height for movement based this on visual inspection and confirmation by the signaling crew member via hand signals. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Movement of TAD Canister Welding Machine to Stand—The crane operator moves the jib crane to the welding machine stand, following the safe loading path indicated on the floor. The crane operator places the welding machine on the stand and disengages the hook.

E6.9.1.9 Closure of STC

E6.9.1.9.1 Removal of STC Shield Ring

The crane operator uses the jib crane and standard rigging to remove the STC shield ring from the STC. This operation is done from the cask preparation platform with the aid of two crew members. The crane operator moves the crane to the STC and the crew members attach the rigging to the shield ring. The crew members then step several feet away from the cask and the

crane operator lifts the shield ring, ensures that it is steady, and moves the shield ring to its staging area.

E6.9.1.9.2 Installation of STC Lid

The jib crane and lid lifting grapple are used to lift the STC lid and place it onto the STC. This operation is done on the cask preparation platform. In preparation of this step, the lid lifting grapple is attached to the jib crane, and there is a lid lifting fixture attached to the STC lid.

The crane operator retrieves the STC lid from the staging area with the jib crane and lowers crane into position over the STC. The operator is positioned on the platform in view of the crew members on either side of the cask. There is a signaling crew member next to the crane that uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the crane checking alignment of the crane. The verification crew member can only signal to stop the crane. Once positioned, the crane operator lowers the lid into place and disengages the grapple.

E6.9.1.9.3 Install STC Lid Bolts

The STC lid is bolted (using at least four bolts) to the STC by personnel using common tools. This step is verified on a checklist.

E6.9.1.10 Draining the Annulus between the STC and TAD Canister

The crew attaches a hose to the shield plug siphon port (quick disconnect), while the other side of the hose leads to the pool. There is a pump connected to the hose to create a vacuum. Once the hose is connected, the crew member turns on the pump and waits until the annulus is fully drained (in the pool a crew member can see bubbles coming from the hose). The crew member then stops the pump and disconnects the hose. The STC drain port is then closed by a crew member using common tools.

E6.9.1.11 Movement of the STC to CTT

The STC is moved to the Cask Preparation Area using the cask handling crane with the cask handling yoke. In preparation for this step, the cask handling yoke is attached to the cask handling crane. The CTT is deflated under the preparation platform.

Movement of Crane to STC—The operator positions the crane over the STC. The operator follows the indicated safe load path marked on the floor based on visual inspection and hand signal confirmation from the signaling crew member. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Crane Alignment with Cask—The crane operator lowers the crane into position so that the yoke arms are lined up with the trunnions. The operator is positioned on the floor in view of the crew members on either side of the cask. There is a signaling crew member next to the cask who uses hand signals to guide the crane operator (no hardwired or wireless communication system is used). There is a verification crew member on the opposite side of the cask checking alignment of the second trunnion. The verification crew member can only signal the crane operator to stop.

Engagement of Yoke Arms on Trunnions—Once the yoke is aligned, the signaling crew member signals the operator to close the yoke arms. The crew members check to see that the yoke arms have attained at least the minimum amount of engagement (minimum distance from edge of trunnion to edge of yoke arm). The crane operator can see by an indicator on the controller that the arms are fully engaged on both sides. The signaling crew member signals the operator to raise the crane a slight amount to put pressure on the arms. Again, the crane operator can see on the controller that the crane is bearing weight. Once the cask is lifted slightly, both crew members verify that the yoke is level. If the arms do not engage on the initial attempt either crew member signals the operator to stop, and the crane operator sets the cask down, and opens the yoke arms to disengage. The signaling crew member then directs movement of the crane (again with hand signals) to compensate, and signals the operator to close the yoke arms.

Movement of Cask to CTT—The crane operator raises the cask to the proper height for movement. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path. The operator confirms the height visually and gets confirmation from the signaling crew member before beginning movement to the Cask Preparation Area. The crane operator follows the indicated safe load path marked on the floor based on visual inspection and confirmation from the signaling crew member. There is a verification crew member that is on the opposite side of the cask as the signaling crew member. With the help of both crew members, the crane operator aligns the cask to the CTT and then lowers the cask in the CTT.

Secure Cask to CTT—Prior to disengaging the yoke from the cask, the crew members use common tools to secure the cask to the CTT. The crane operator then disengages the yoke, lifts the crane to the proper height for movement and moves the yoke to the yoke stand.

E6.9.1.12 Unbolting STC Lid

Once secure in the CTT, the crew lowers the preparation platform and unbolts the STC lid using common tools and the preparation platform.

E6.9.1.13 Movement of STC into Cask Unloading Room

Using the CTT, the CTT operator moves the STC to the Cask Unloading Room and positions the cask under the cask port. To do this, the CTT operator inflates the CTT, moves the CTT to the Cask Unloading Room door, opens the shield door, moves the CTT through the door and positions it under the cask port, deflates the CTT and stores the pendant, disconnects the air hose, and closes the shield door. There are physical stop points in the Cask Unloading Room which the CTT must bump up against to ensure proper alignment.

E6.9.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during TAD canister closure and movement to the Cask Unloading Room are summarized in Table E6.9-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.9-1. HFE Group #9 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpTCImpact10-HFI-NOD	*Operator Causes an Impact between a Cask and an SSC during TAD Canister Closure*: While performing crane operations, the operator can impact the cask in the following ways: • Impacting the cask while moving an object with the crane • Impacting the cask with the crane hook	25	6E−03	This HFE is very similar to the standard impact due to crane operations (050-OpTCImpact01-HFI-NOD; 0.003) in regards to the operations involved and failure modes. The justification for those failures is as follows: the preliminary value was chosen based on the determination that this failure is "highly unlikely" (one in a thousand or 0.001) and was adjusted because there are several ways for an impact to occur (×3). However, for this operation, there is a cask lift and (comparatively) several more equipment lifts that may be done over multiple shifts; therefore this HEP was adjusted by an additional factor (×2).
050-OpTCImpact01-HFI-NOD	*Operator Causes an Impact between a Cask and an SSC during TAD Movement to CTT*: While moving the TAD to the CTT from the TAD closure station, the crane operator can cause the cask to impact an SSC in the following ways: • Move crane in wrong direction • Move crane with hoist too low • Move load out of safe load path • Object is left in the safe load path.	28	3E−03	This HFE is identical to the standard impact due to crane operations (i.e., impact during upending and removal from conveyance, HFE Group #2, 050-OpTCImpact01-HFI-NOD; 0.003) in regards to the operations involved and failure modes. The justification for those failures is as follows: the preliminary value was chosen based on the determination that this failure is "highly unlikely" (one in a thousand or 0.001) and was adjusted because there are several ways for an impact to occur (×3).
050-OpSTCShield1-HFI-COD	*Operator Causes a Direct Exposure Due to Failure to Properly Install the STC Shield Ring*: In this step, the TAD canister is dried and the TAD canister lids are welded on. The crew can get a direct exposure if the crane operator improperly places the STC shield ring on the STC during TAD canister closure activities.	29	1E−02	In this step, the STC shield ring is placed over the annulus so the crew can perform the welding operations. During this operation the crane operations are simple, the ring is attached via standard rigging to the crane, the crane speed is slow, the crew is well trained, and the operators are expected to perform these operations on a daily basis. There are no interlocks to prevent this error. To add to the complexity of this task, the actual alignment is done at a distance with the aid of a camera. If the shield ring is misaligned, it can be seen from the platform. This operation was given the default value for an "unlikely" event. This operation is nearly identical to operator fails to properly install DPC shield ring (050-OpDPCShield1-HFI-NOW; Section E6.7, HFE Group #7), and the preliminary values reflect this.
050-TadDry-Fail	*Operator Leaves Water in the TAD Canister*: If the operator prematurely terminates TAD canister drying or otherwise fails to ensure the TAD canister is fully dry before closure, this can result in damage to the canister or fuel assemblies.	26	N/A	If the operator prematurely terminates the TAD canister drying or otherwise fails to ensure the TAD canister is fully dry before closure, there can be resulting damage to the canister or fuel assemblies. This failure event was screened out by the WHF analysts and is not part of this HRA; Sections 6.0 of the main report provides the screening justification.
050-WeldDetect-Fail	*Operator Causes Defective Weld or Fails to Detect a Bad Weld*: The welding system is highly automated, with few opportunities for humans to intervene. The weld check system is highly automated using an ultrasonic tester, but at least one human is supposed to visually inspect each weld and sign off on it. If the TAD canister inner and outer lids both have a bad weld that is cracked all the way through, then a radiation release can occur.	27	N/A	If the TAD canister inner and outer lids both have a bad weld that is cracked all the way through, then a radiation release can occur. This failure event was screened out by the WHF analysts and is not part of this HRA; Sections 6.0 of the main report provides the screening justification.
050-OpTipover001-HFI-NOD	*Operator Causes CTT to Tip Over while Moving into the Preparation Station*: During this operation, the CTT is moved from the TAD canister closure station to the preparation station and then to the Cask Unloading Room. Several crane operations are carried out during TAD canister closure both at the closure station and at the preparation station. If the crane rigging is attached to the cask or CTT (either accidentally or purposefully) and the crane or CTT moves, the cask can potentially tip over. The following are contributors to this HFE: • Crane hook, grapple or rigging catches conveyance/cask • Horizontal movement of the crane with the hook lowered and attached to cask • Crane travels in wrong direction.	28	1E−04	In this step the CTT is moved from the Cask Preparation Area to the preparation station for lid bolt removal, and then to the Cask Unloading Room where it is positioned under the cask port. This HFE was assigned the same preliminary value as other cask tipover events (050-OpTipover001-HFI-NOD; Section E6.2, HFE Group #2) because the operations and failure modes are identical; the CTT can catch improperly stowed crane rigging in the Cask Preparation Area and the crane or CTT can continue moving and result in a tipover. The following is the rationale behind this preliminary value: the dominant contributor is the crane hook catching the cask. While it may be unlikely (0.01) that a stray hook or grapple might be hanging from the crane, it would still need to catch on the cask securely enough to pull it over (0.1), and then the cask tipping would have to go unnoticed by all three observers. This is done with direct observation, and a tipover is a slow process; therefore, the value was adjusted by a further 0.1.

Table E6.9-1. HFE Group #9 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpCTCollide1-HFI-NOD	*Operator Causes Low-Speed Collision of Auxiliary Vehicle with STC*: During STC unbolting at the preparation station, the STC is loaded and parked under the preparation platform. During this time, an operator can cause an auxiliary vehicle to collide with the STC. The TAD canister closure station design precludes an auxiliary vehicle from colliding with the TAD canister stationed in the closure station.	25	3E−03	In this step the CTT is loaded and parked under the cask preparation platform. The TAD canister cannot be impacted in the TAD canister closure station because it is protected by the platform itself. The speed of auxiliary vehicles is slow, the CTT is very visible, and procedural controls are expected to limit the number of other vehicles in the Cask Preparation Area during cask operations. This HEP was assigned the same preliminary probability as a railcar collision HFE (050-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) because the dominant mechanism of both failures is collision with an auxiliary vehicle. In this case, the preliminary value is conservative because the CTT is staged under the platform and the railcar collision HFE has additional failure modes associated with movement of the SPM that are not applicable here. This failure is identical for the preparation activities in a CTT (050-OpCTCollide1-HFI-NOD; Section E6.3, HFE Group #3 and Section E6.4, HFE Group #4) and has the following justification: the preliminary value was chosen based on the determination that this failure is “highly unlikely” (one in a thousand or 0.001), was adjusted because there are several ways for a collision to occur, and there are potentially multiple other vehicles (forklifts) that can collide into the conveyance (×3).
050-OpFLCollide1-HFI-NOD	*Operator Causes High-Speed Collision of Auxiliary Vehicle with STC*: During STC unbolting at the preparation station, the STC is loaded and parked under the preparation platform. During this time, an operator can cause an auxiliary vehicle to collide with the STC. If the collision is due to the auxiliary vehicle speed governor malfunctioning, then this is a high-speed collision.	25	1.0	An auxiliary vehicle (i.e., forklift) can over speed, resulting in collision with the CTT while the CTT is parked under the preparation platform or in transit to or from the platform. In order to accomplish this, the speed governor of the auxiliary vehicle must fail. The CTT itself is limited by design from over speeding. To be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0
050-OpCTCollide2-HFI-NOD	*Operator Causes Low-Speed Collision of CTT during Transfer from the Preparation Station to the Unloading Room*: Once the TAD canister is closed and the STC bolts are removed, an operator inflates the CTT and moves the cask from the Cask Preparation Area to the Cask Unloading Room. The operator can cause the CTT to collide with the preparation platform structure or other SSCs during this transfer. The CTT is designed such that it physically cannot over speed; therefore, all CTT collisions are below the designed speed.	10	1E−03	In this step the CTT is moved from the Cask Preparation Area to the preparation station for lid bolt removal and then to the Transfer Room where it is positioned under the cask port. This HFE was assigned the same preliminary value as other collisions during CTT movement (050-OpCTCollide2-HFI-NOD; Section E6.5, HFE Group #5) because the operations, opportunities for collision, and failure modes are very similar. This operation is simple, is straightforward, is expected to occur very regularly (daily), and was assigned the default probability of a “highly unlikely” occurrence (0.001). It was considered reasonable and consistent that the preliminary value assigned for this HFE be less likely than a railcar or auxiliary vehicle collision because of the CTT guide rail, number of observers, and short travel distance.
050-OpSDClose001-HFI-NOD	*Operator Closes Shield Door on Conveyance*: Once the TAD canister is closed and the STC lid is unbolted, the TAD canister is moved from the Cask Preparation Area to the Cask Unloading Room. There is a shield door between the Cask Preparation Area and the Cask Unloading Room. The operator can impact the cask by inadvertently closing the shield door on the CTT/STC as the CTT passes through the door.	12	1.0	The CTT passes through a shield door as it moves from the preparation station into the Cask Unloading Room. During this transfer, the operator can cause the CTT to collide into the shield door or can close the shield door on the CTT. Section E6.0.2.3.3 provides a justification of this preliminary value.

NOTE: CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; HRA = human reliability analysis; N/A = not applicable; ssc = structure, system, or component; STC = shielded transfer cask; TAD = transportation, aging, and disposal canister; WHF = Wet Handling Facility.

Source: Original

E6.9.3 Detailed Analysis

After the preliminary screening analysis and initial quantification are completed, those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives are subjected to a detailed analysis. The overall framework for the HRA is based upon the process guidance provided in ATHEANA (Ref. E8.1.22). Consistent with that framework, the following four steps from the methodology described in Section E3.2 provide the structure for the detailed analysis portion of the HRA:

Step 5: Identify Potential Vulnerabilities

Prior to defining specific scenarios that can lead to the HFEs of interest (Step 6), information is collected to define the context in which the failures are most likely to occur. In particular, analysts search for potential vulnerabilities in the operators' knowledge and information base for the initiating event or base case scenario(s) under study that might result in HFEs or unsafe actions. This information collection step discussed in Section E6.9.3.2.

Step 6: Search for HFE Scenarios (Scenarios of Concern)

An HFE scenario is a specific progression of actions with a specific context that leads to the failure of concern; each HFE is made up of one or more HFE scenarios. In this step, documented in Sections E6.9.3.3 and E6.9.3.4, the analyst identifies deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These unsafe actions make up an HFE scenario. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions.

Step 7: Quantify Probabilities of HFEs

Detailed HRA quantification methods are selected as appropriate for the characteristics of each HFE and are applied as explained in Section E6.9.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)
- ATHEANA expert judgment (Ref. E8.1.22).

There is no implication of preference in the order of listing these methods. They are jointly referred to as the "preferred methods" and are applied either individually or in combination as best suited for the unsafe action quantified. The ATHEANA (Ref. E8.1.22) expert judgment method (as opposed to the overall ATHEANA (Ref. E8.1.22) methodology that forms the framework and steps for the performance of this HRA) is used when the other methods are deemed to be inappropriate to the unsafe action, as is often the case for cognitive EOCs.

Appendix E.IV of this analysis explains why these specific methods were selected for quantification and gives some background on when a given method is applicable based on the focus and characteristic of the method.

All judgments used in the quantification effort are determined by the HRA team and are based on their own experience, augmented by facility-specific information and the experience of subject matter experts, as discussed in Section E4. If consensus can be reached by the HRA team on an HEP for an unsafe action, that value is used as the mean. If consensus cannot be reached, the highest opinion is used as the mean.

Step 8: Incorporate HFEs into the PCSA

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. The summary table of HFEs by group that lists the final HEP by basic event name provides the link between the HRA and the rest of the PCSA. This table can be found in Section E6.9.4.

E6.9.3.1 HFEs Requiring Detailed Analysis

The detailed analysis methodology, Sections E3.2.5 through E3.2.9, states that HFEs of concern are identified for detailed quantification through the preliminary analysis (Section E3.2.4). An initial quantification of the WHF PCSA model determined that there was one HFE in this group whose preliminary value was too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111. This HFE is presented in Table E6.9-2.

Table E6.9-2. Group #9 HFE Requiring Detailed Analysis

HFE	Description	Preliminary Value
050-OpSTCShield1-HFI-COD	Operator causes direct exposure due to failure to properly install STC shield ring	1E−02

NOTE: STC = shielded transfer cask.

Source: Original.

E6.9.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the approach to conducting a detailed quantification is to identify and characterize factors that could create potential vulnerabilities in the crew's ability to respond to the scenarios of interest and might result in HFEs or unsafe actions. In this sense, the "vulnerabilities" are the context and factors that influence human performance and constitute the characteristics, conditions, rules, and tendencies that pertain to all the scenarios analyzed in detail.

These vulnerabilities are identified through activities including but not limited to the following:

1. The facility familiarization and information collection process discussed in Section E4.1, such as the review of design drawings and concept of operations documents

2. Discussions with subject matter experts from a wide range of areas, as described in Section E4.2

3. Insights gained during the performance of the other PCSA tasks (e.g., initiating events analysis, systems analysis, and event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the preparation operation that relate to potential human failure scenarios relevant to the HFE listed in Table E6.9.2. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during the preparation operation, but these have no bearing on this analysis.

E6.9.3.2.1 Operating Team Characteristics

Crane Operator—The crane operator has received standard training for crane operations and observed operations prior to being allowed to operate the crane on a dry run. Based on evaluation of the crane operator's proficiency in a dry run, the crane operator is signed off to operate the crane. On initial operations, the crane operator is observed until signed off for solo operation. A single operator is assigned to the crane operation.

Signaling Crew Member—During the shield ring movement to the TAD canister/STC, the signaling crew member provides hand signals to the crane operator to direct the movement of the crane.

Verification Crew Member—The verification crew member is stationed in view of the TAD canister/STC and shield ring and covers the areas that the signaling crew member cannot see. The verification crew member gives hand signals to the signaling crew member if there are any problems with the alignment of the shield ring.

Radiation Protection Worker—The radiation protection worker is a fully certified health physics technician, whose job is to monitor radiation from the cask during cask handling operations. The radiation protection worker is responsible for stopping operations if high radiation levels are detected or if there is a situation that would lead to direct exposure.

E6.9.3.2.2 Operation and Design Characteristics

Control Panel—The control panel consists of a standard jib control panel for movement of the crane. Controls are provided for both coarse and fine motion. A camera view is provided to augment the operator's direct view from a distance. The crane operator and crew members are located on the platform, several feet away from the cask.

Interlocks/Alarms—There are no interlocks or alarms that control this task. A radiation protection worker takes a manual reading of radiation levels and prevents operations if high radiation is detected.

Verbal Communication—Verbal communication between crew members and the crane operator is ineffective. A significant amount of machine noise is present, so hand signals are the only practical means of communication.

E6.9.3.2.3 Formal Rules and Procedures

Procedures—Procedures exist for these operations; however, there are no written, formal procedures that the crew has in front of them during cask preparation. Operators and crew members are trained in the operations, and their proficiency is attested to by the training staff. They perform the operations as a skill.

Formal Rule—This operation involves potential radiation exposure, so a formal rule exists that the radiation protection worker must measure the radiation in the area of the TAD canister where the workers are located. Radiation protection workers do not have to formally sign off on the measurement of the radiation level; however, they need to inform the crane operator and crew members that it is safe to continue working in the area.

E6.9.3.2.4 Operator Tendencies and Informal Rules

Crane Operator Dependency on Crew Members—The view from the control panel and through the camera are reasonable for rough placement of the shield ring, but final alignment is directed through hand signals from crew members.

Crew Member Deference to the Crane Operator—The crane operator is essentially the foreman of the team, and is seen by the crew members as being in a more skilled position than them. The crew tends to defer to the crane operator's judgment and have some level of reluctance to question the operator's directions.

E6.9.3.2.5 Operator Expectations

Shield ring installation is a simple task ancillary to the main task of draining the TAD canister. The operator and crew expect the operation to go smoothly.

E6.9.3.3 HFE Scenarios and Expected Human Failures (Step 6)

Given that the vulnerabilities that provide the operational environment and features that could influence human performance have been specified, then the HFE scenarios within this environment are identified. An HFE scenario is a specific progression of actions during normal operations (with a specific context) that lead to the failure of concern; each HFE is made up of one or more HFE scenarios. In accordance with the methodology, each scenario integrates the unsafe actions with the relevant equipment failures so as to provide the complete context for the understanding and quantification of the HFE.

The HAZOP evaluation is instrumental in initially scoping out the HFE scenarios, but the HFEs are then refined through discussions with subject matter experts from a wide range of areas, as described in Section E4.2.

Table E6.9-3 summarizes all of the HFE scenarios developed for the HFEs in this group.

Table E6.9-3. HFE Scenarios and Expected Human Failures for HFE Group #9

HFE	HFE Scenarios
050-OpSTCShield1-HFI-COD *Operator Causes Direct Exposure Due to Improper Installation of STC Shield Ring*	HFE Scenario 1(a): (1) Crane operator fails to install shield ring; (2) Crew members fail to note that shield ring installation has been skipped; (3) Crew members fail to notice that shield ring is not in place prior to approaching TAD canister. HFE Scenario 1(b): (1) Crane operator installs shield improperly; (2) radiation protection worker fails to check radiation levels OR radiation protection worker misreads radiation level OR radiation monitor fails; (3) Crew member fails to note shield ring out of position before approaching TAD canister.

NOTE: HFE = human failure event; STC = shielded transfer cask; TAD = transportation, aging, and disposal.

Source: Original

Since there is one HFE identified for detailed analysis in this group, the scenarios are organized under this HFE category, with the scenarios numbered as 1(a) and 1(b).

Each HFE scenario is in turn characterized by several unsafe actions, numbered sequentially as (1), (2), or (3). The Boolean logic of the HFE scenarios is expressed with an implicit AND connecting the subsequent unsafe actions and OR notation wherever two unsafe action paths are possible, as shown in Table E6.9-3.

The HFE scenarios summarized in Table E6.9-3 are discussed and quantified in the following sections.

E6.9.3.4 Quantitative Analysis (Step 7)

Once the HFE scenarios and the unsafe actions within them are scoped out, it is then possible to review them in detail and apply the appropriate quantification methodology in each case that permits an HEP to be calculated for each HFE. Stated another way, each HFE is quantified through the analysis and combination of the contributing HFE scenarios. Dependencies between the unsafe actions and equipment responses within each scenario and across the scenarios are carefully considered in the quantification process.

This section provides a description of the quantitative analysis performed. This quantitative analysis is structured hierarchically by each HFE category (identified by a basic event name), followed by the HFE scenario, and then followed by the unsafe actions under each scenario as documented in Table E6.9-3.

Prior to the scenario-specific quantification descriptions, a listing is provided of the values used in the quantification that are common across many of the HFE scenarios.

In generating the final HEP values, the use of more than a single significant figure is not justified given the extensive use of judgment required for the quantification of the individual unsafe actions within a given HFE. For this reason, all calculated final HEP values are reduced to one significant figure. When doing this, the value is always rounded upwards to the next highest single significant figure.

E6.9.3.4.1 Common Values used in the HFE Detailed Quantification

There are no mechanical failures that appear in multiple HFE scenarios.

E6.9.3.4.2 Quantification of HFE Scenarios for 050-OpSTCShield1-HFI-COD: Operator Causes Direct Exposure Due to Failure to Install STC Shield Ring

E6.9.3.4.2.1 HFE Group #9 Scenario 1(a) for 050-OpSTCShield1-HFI-COD

1. Crane operator fails to install shield ring.
2. Crew members fail to realize that the shield ring installation has been skipped.
3. Crew members fail to notice that the shield ring is not in place prior to approaching the TAD canister.

Crane Operator Fails to Install Shield Ring—The crane operator is responsible for ensuring that the shield ring is installed prior to the crew members setting up the TAD canister draining system and partially draining the TAD canister. The crew members assist in this process by handling the rigging and providing hand signals to the crane operator to help in placement of the shield ring. Since this is a radiation protection task, the operator must contact the Health Physics Department and inform them that the operation is about to take place so that a radiation protection worker can check radiation levels after shield placement. The unsafe action in this case is that the crane operator fails to perform this entire step and tells the crew to partially drain the TAD canister. The operator's motivation for doing this could be that the shield ring is viewed as unnecessary for this task, the operator "remembers" already installing it from having done this operation many times before, the operator is anxious to get the job done, or the operator is distracted by other activities and simply forgets.

The jib crane operator is required to install the shield ring prior to the crew members partially draining the TAD canister. The unsafe action in this case is that the jib crane operator skips this entire part of the process and tells the crew members to drain the TAD canister. This can be represented by CREAM CFF E5, adjusted for the following CPCs with a value not equal to 1.0, as follows:

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03
- CPC "Available Time": The general level of time pressure for the overall process of draining the TAD canister is very low. There is no particular impetus for getting the task done that would potentially drive the operator to skipping this task. The CPC weighting factor for an execution task with adequate time is 0.5.
- CPC "Adequacy of Training and Preparation": This routine task is well trained and practiced and performed quite frequently. The CPC weighting factor for an execution task with adequate training and high experience is 0.8.

Note that in skipping this entire task, it is deemed that the operator also fails to inform the Health Physics Department that they are needed to perform monitoring after the shield ring is installed.

Applying these factors yields the following:

$$\text{Crane operator fails to install shield ring} = 0.03 \times 0.5 \times 0.8 = 0.01$$

Crew Members Fail to Realize that Shield Ring Installation Has been Skipped—The crew members that drain the TAD canister are an integral part of the overall task process, including the placement of the shield ring. They should be aware that the ring needs to be placed, and should question the crane operator if the crane operator tells them to begin the unbolting task when the crew has not been a part of the placement process. In addition, the crew members should also be expecting to see a radiation protection worker check radiation levels and give them the "all clear" signal to approach the TAD canister. The crew members have a particular motivation to ensure that this is done, since the crew members (not the crane operator) are exposed if the shield ring is not installed. The unsafe action in this case is that they do not question the crane operator when told to begin the draining task. It is expected that their motivation for this unsafe action is most likely to be a reluctance to question the crane operator, who is above them in the operational hierarchy of the facility (i.e., the crane operator is essentially the foreman of the team). The crew member's deference to the crane operator's instruction would come from a belief that the crane operator was in charge and aware of the situation.

Because the crew members that partially drain the TAD canister are the same crew members that assist in the shield ring installation process (i.e., preparing the crane, signaling the operator, etc.), the crew members need to miss this entire task for this event to occur. As a baseline value for this event, the same probability as crane operator fails to install shield ring can be used (0.01). However, the crew members would not be totally independent of the crane operator. The crew members could be distracted, or they could be starting a new shift and be convinced by the crane operator that the TAD canister is ready to be drained (i.e., a bias towards believing that the operator, who would generally be considered above them in the operational hierarchy, must be aware of the status of the operation). On the other hand, the crew members would clearly expect to participate in this task and because it is important to their personal safety (i.e., they are the ones who are depending on the shielding) they are more cognizant of the operational status. Taking all of this into consideration, it is deemed that the level of dependence is low. For low dependence when a baseline HEP is 0.01, the adjusted HEP is taken from THERP Table 20-21, item (2)(a) (Ref. E8.1.26) as follows:

$$\text{Crew members fail to note that shield ring installation has been skipped} = 0.05$$

Crew Members Fail to Notice that the Shield Ring Is Not in Place Prior to Approaching the TAD Canister—After the crew members are cleared to begin the draining task, they gather the required tools and approach the TAD canister. The crew members would have performed this task many times before, and would have an image in their minds of how everything should look. The ring is a large and rather obvious device that the crew members would have to walk on or over in order to perform the draining. Since they would not be exposed until the TAD canister was partially drained (because the water provides shielding) they could walk up to the TAD canister before noticing the missing shield ring and even start the task (i.e., connect the system) and still not be exposed. The crew members are carrying the tools they need, focusing on the performance of the task, and likely talking to each other about the performance of the task or

having a casual conversation (since the work is not particularly difficult or challenging and they are not expecting any complications). The unsafe action results from the crew members not noticing that the configuration of the shield ring is not correct. Most likely, the crew members would have a bias that the operational conditions are in order and it is time to perform the task; the crew does not detect the differences in appearance (i.e., they see what they expect to see). To put this in a more colloquial context, this type of missed observation would be comparable to an individual walking up to their car and failing to notice that the door of the car is open, up to the point of opening the door and getting in.

Although there is no specific check that takes place when the crew goes to partially drain the TAD canister, there is opportunity to notice that the shield ring is not in place. They would have ample opportunity to detect that the shield ring is not in place, since there is no risk of exposure until the TAD canister is partially drained (prior to that, the water would provide adequate shielding). Therefore, the crew would be located at the TAD canister and have a clear view. The crew would have to not notice that the shield ring is not there before they begin draining water. Rather than missing a check, it is more in the nature of failing to notice that something is not correct.

There are no failures in the primary quantification methods that reasonably fit this unsafe action, so it is necessary to provide a value based on expert judgment (ATHEANA). It is clear that some credit needs to be given for this since the crew members perform this task often and should recognize what the configuration should look like when they perform the task, especially given that they would be within a few feet of the TAD canister for several minutes performing preparatory tasks before the drain. However, in opposition to this, the crew begins operations on the TAD canister believing the shield ring is in place and they are focused on the task that they are about to perform. Taking all of this into consideration, the HRA team believes that the failure is unlikely, which corresponds to an HEP of 0.1.

Crew members fail to notice that the shield ring is not in place
prior to approaching the TAD canister = 0.1

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.9-4.

Table E6.9-4. HEP Model for HFE Group #9 Scenario 1(a) for 050-OpSTCShield1-HFI-COD

Designator	Description	Probability
A	Crane operator fails to install shield ring	0.01
B	Crew members fail to realize that shield ring installation has been skipped	0.05
C	Crew members fail to notice that shield ring is not in place prior to approaching TAD canister	0.1

NOTE: TAD = transportation, aging, and disposal.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.01 \times 0.05 \times 0.1 = 0.00005 \quad \text{(Eq. E-43)}$$

E6.9.3.4.2.2 HFE Group #9 Scenario 1(b) for 050-OpSTCShield1-HFI-COD

1. Crane operator installs shield improperly.

2. Radiation protection worker fails to check radiation levels OR the radiation protection worker misreads the radiation level OR the radiation monitor fails.

3. Crew member fails to note shield ring is out of position before approaching the TAD canister.

Crane Operator Installs Shield Ring Improperly—The installation process is relatively simple and straightforward. Once the crew members attach the shield ring to the jib crane sling, the operator moves it over the TAD canister. The crew members help the operator to align the shield ring properly over the TAD canister using hand signals. The crew members signal the crane operator throughout the lowering process to ensure proper alignment. Although the operation is simple, the shield ring must have a close fit in order to completely block the annulus between the TAD canister and the STC to prevent radiation from escaping and exposing workers when they approach the TAD canister/STC unit. If the shield ring is not exactly aligned, it could partially jam or hang up at a slight angle that would allow radiation to escape. The unsafe action is that the operator causes the shield ring to partially jam or hang up. Included in this is the implicit condition that the crane operator and crew members do not notice that the shield ring is jammed or hung up as they perform the task.

In this case, the crane operator is performing the shield installation task, but the shield ring is not seated properly. This is a very routine task and is practiced often. Failures can be corrected without consequences since the operator has the opportunity to lift and place the shield ring as many times as necessary until it is properly aligned. This can be represented by NARA GTT A5, adjusted by the following EPCs:

- GTT A5: Completely familiar, well designed, highly practiced, and routine task performed to highest possible standards by highly motivated, highly trained, and experienced personnel, totally aware of implications of failure, with time to correct potential errors. The baseline HEP is 0.0001.

- EPC 11: Poor, ambiguous, or ill-matched system feedback. This EPC addresses the issue that the crane operator views this operation from a distance. The maximum effect is ×4, which applies to a very difficult situation where visibility is poor, and visual and physical access if difficult. It is not believed that this case is this severe, but the full effect is still applied. The APOA is set to 1.0.

Applying the NARA HEP equation yields the following:

$$\text{Crane operator installs shield ring improperly} = 0.0001 \times [(4-1) \times 1 + 1] = 0.0004 \quad \text{(Eq. E-44)}$$

Radiation Protection Worker Fails to Check Radiation Levels—The crane operator contacts the Health Physics Department before initiating the shield ring placement task, and awaits clearance that radiation levels are acceptable before ordering the crew members to unbolt the lift

fixture. There are three potential ways that the radiation protection worker could fail to properly determine that the shield ring is not properly in place. First, the radiation protection worker could forget to perform the measurement; however, since the only reason the radiation protection worker was called to the WHF was to perform this task, the radiation protection worker would need to be distracted by something or someone to not perform this measurement. The radiation protection worker has performed this task a number of times in the past, and it is possible that the radiation protection worker could remember performing this task before and get confused and signal the operator that the levels are acceptable, believing that the radiation measurement has been performed. To put this in a more colloquial context, this type of omission would be comparable to an individual leaving their home or office without setting an alarm system. This individual performs this task every time they exit, and it has become second nature, so they cannot believe that they did not do it this time.

In this case, the unsafe action results from the radiation protection worker not checking radiation levels, after being called in specifically to perform this task. This can be represented by CREAM CFF E5, adjusted by the following CPCs with a value other than 1.0.

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03.
- CFP "Adequacy of Training/Preparation": This routine task is well trained, practiced, and performed quite frequently. The CPC for an execution task with adequate training and high experience is 0.8.
- CFP "Available Time": There is adequate time to perform this task and no significant time pressure. The CPC value for adequate time for an execution task is 0.5.

Applying these factors yields the following:

$$\text{Radiation protection worker fails to check radiation levels} = 0.03 \times 0.8 \times 0.5 = 0.02$$

Radiation Protection Worker Misreads Radiation Level—The second potential way that the radiation protection worker could fail to properly determine that the shield ring is not properly in place is by simply misreading the meter on the radiation gauge and believing the level is acceptable. Therefore, this failure is misreading the digital display on the radiation monitor. This can be represented by THERP table 20-11, item 1 (HEPs for EOCs in check-reading digital indicator displays) (Ref. E8.1.26).

$$\text{Radiation protection worker misreads radiation level} = 0.001$$

Radiation Monitor Fails—The radiation protection worker could also fail to properly determine that the shield ring is not properly in place due to a problem with the radiation monitor. The radiation monitor could give a false low reading as the result of a hardware failure. This is a mechanical rather than a human failure. From the Attachment C, Table C4-1, the failure rate for radiation sensors is approximately 2E−5/hour. It is expected that the monitor is used at least once each day. Using the equation for standby equipment ($0.5\lambda t$) yields:

$$\text{Radiation monitor fails} = 0.5 \times 2E{-}5 \times 24 = 2.4E{-}4$$

Crew Member Fails to Note Shield Ring Is Out of Position Before Approaching TAD Canister—The crew members, after being cleared to begin the unbolting task, bring the required tools and approach the TAD canister. They have performed this task many times before, and they would have an image in their minds of how everything should look. Unlike the previous scenario, the ring is essentially in place and the misalignment is a more subtle deviation from the image they expect. The crew carries the tools they need, they are focused on the performance of the task, and likely talking to each other about the performance of the task or involved in casual conversation (since the work is not particularly difficult or challenging and they are not expecting any complications). The unsafe action is that they do not notice that the shield ring is out of position. The crew members would have a bias that the previous activities have been performed correctly, the shield ring is configured properly, and they are ready to proceed with their operations; any differences in appearance do not register (i.e., they see what they expect to see). To put this in a more colloquial context, this type of missed observation would be comparable to an individual walking up to their car and failing to notice that the door of the car is slightly ajar, up to the point of opening the door and getting in.

Although there is no specific check that takes place when the crew begins operations to partially drain the TAD canister, there is ample opportunity to notice that the shield ring is not properly in place (i.e., is over the TAD canister, but out of position). There is no risk of exposure until the TAD canister is partially drained because prior to that, the water would provide adequate shielding. The crew would be located in the vicinity of the TAD canister and have a clear view of any problems. They would have to not notice that the shield ring is out of place before they began draining the water. Rather than missing a check, it is more in the nature of failing to notice that the operational conditions were not correct. There are no failures in the primary quantification methods that reasonably fit this unsafe action, so it is necessary to provide a value based on expert judgment (ATHEANA). It is clear that some credit needs to be given for this since the crew members perform this task often and should recognize what the configuration should look like when they perform the task, especially given that they would be within a few feet of the TAD canister for several minutes performing preparatory tasks before the drain. However, in opposition to this, the crew begins operations on the TAD canister believing the shield ring is properly configured and they are focused on the task that they are about to perform. Taking all of this into consideration, the HRA team believes that the failure is unlikely, which corresponds to an HEP of 0.1.

Crew members fail to notice that shield ring is out of position
prior to approaching TAD canister = 0.1

Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.9-5.

Table E6.9-5. HEP Model Events for HFE Group #9 Scenario 1(b) for 050-OpSTCShield1-HFI-COD

Designator	Description	Probability
A	Crane operator installs shield ring improperly	0.0004
B	Radiation protection worker fails to check radiation levels	0.02
C	Radiation protection worker misreads radiation level	0.001
D	Radiation monitor fails	0.00024
E	Crew member fails to note shield ring out of position before approaching TAD canister	0.1

NOTE: TAD = transportation, aging, and disposal.

Source: Original

The Boolean expression for this scenario follows:

$$A \times (B + C + D) \times E =$$
$$0.0004 \times (0.02 + 0.001 + 0.00024) \times 0.1 = 1E{-}6 \quad \text{(Eq. E-45)}$$

E6.9.3.4.2.3 HEP for HFE 050-OpSTCShield1-HFI-COW

The Boolean expression for the overall HFE (all scenarios) follows:

$$\text{050-OpSTCShield1-HFI-COW} =$$
$$\text{HFE 1(a)} + \text{HFE 1(b)} =$$
$$5E{-}5 + 1E{-}6 = 6E{-}5$$

E6.9.4 Results of Detailed HRA for HFE Group #9

The final HEPs for the HFEs that required detailed analysis in HFE Group #9 are presented in Table E6.9-6 (with the original preliminary value shown in parentheses):

Table E6.9-6. Summary of Detailed Analysis for HFE Group #9

HFE	Description	Final Probability
050-OpSTCShield1-HFI-COD	Operator causes exposure due to failure to properly install STC shield ring	6E−5 (1E−02)

NOTE: HFE = human failure event; STC = shielded transfer cask.

Source: Original

E6.10 ANALYSIS OF HUMAN FAILURE EVENT GROUP #10: EXPORT OF A TAD CANISTER/AGING OVERPACK FROM THE WHF

HFE group #10 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6-0.1, covering export of a TAD canister in an aging overpack from the facility. The operations covered in this HFE group are shown in Figure E6.10-1. This operation begins with the aging overpack/TAD canister sitting in the CTM Loading Room with the aging overpack lid on, unbolted. The operation proceeds through movement of the aging overpack, on a site transporter, to the Site Transporter Vestibule where the aging overpack lid is bolted. The operation ends with the export of the aging overpack/site transporter from the facility.

NOTE: § = section; AO = aging overpack; CTM = canister transfer machine; HFE = human failure event; ST = site transporter; WHF = Wet Handling Facility.

Source: Original

Figure E6.10-1. Activities Associated with HFE Group #10

E6.10.1 Base Case Scenario

E6.10.1.1 Initial Conditions and Design Considerations Affecting the Analysis

The following conditions and design considerations were considered in evaluating HFE group #10 activities.

1. The aging overpack (secured on a site transporter) is in the Cask Loading Room, loaded with a TAD canister, with an aging overpack lid on top, unbolted.

2. The site transporter is off with forks lowered.

4. There is an interlock between the port slide gates and the Cask Loading Room shield doors; the port slide gate cannot be open while the shield doors to the Cask Loading Room are also open.

The following personnel are involved in this set of operations:

- Crew members (two people)
- Supervisor
- Site transporter operator

- Radiation protection worker[15].

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.10.1.2 Aging Overpack Movement to Aging Overpack Access Platform

A crew member opens the Cask Loading Room shield door, and the site transporter operator energizes the site transporter, raises the site transporter forks, moves the loaded aging overpack out of the cask Loading Room, and positions it under the aging overpack access platform in the Site Transporter Vestibule. The site transporter operator follows the indicated safe load path marked on the floor. The operator does this visually and also receives confirmatory hand signals from the crew member. Once the site transporter is cleared out of the Loading Room, the crew member closes the shield door.

E6.10.1.3 Aging Overpack Lid Bolt Installation

Using the aging overpack access platform and common tools, a crew member(s) emplaces and tightens all the aging overpack lid bolts according to the proper procedure and then verifies (via a checklist) that all the bolts have been properly installed.

E6.10.1.4 Aging Overpack Inspection

Once the cask is ready to leave the facility, the radiation protection worker conducts a visual inspection and a radiological survey of the exterior of the cask.

E6.10.1.5 Aging Overpack Movement from Site Transporter Vestibule to Outside

Once the site transporter is in the Site Transporter Vestibule with the aging overpack/TAD canister closed, a crew member opens the outside door of the Site Transporter Vestibule, and the site transporter operator proceeds to move the site transporter to the outside. Once the site transporter has cleared the outside overhead door, a crew member closes the door.

E6.10.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during closure and export of an aging overpack are summarized in Table E6.10-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

[15]The radiation protection worker, or health physicist, is not mentioned specifically in each step of this operation; however, there is always at least one radiation protection worker present during this step.

Table E6.10-1. HFE Group #10 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpSTCollide3-HFI-NOD	*Operator Causes Low-Speed Collision of ST with SSC while Moving from the Loading Room to the ST Vestibule*: Operator causes collision of ST with facility structure or equipment while moving the ST under the platform from the Loading Room.	11	3E−03	This operation is identical to site transporter collision while moving into the Loading Room (050-OpSTCollide3-HFI-NOD; Section E6.3, HFE Group #3); therefore, it was assigned the same preliminary value: this failure is “highly unlikely” (one in a thousand or 0.001) but was adjusted because there are several ways for a collision to occur (×3).
050-OpSTCollide4-HFI-NOD	*Operator Causes Low-Speed Collision of ST with SSC while Exporting the ST*: Operator causes collision of ST with facility structure or equipment while moving through the ST Vestibule to outside the facility. This is a separate HFE from 050-OpSTCollide3-HFI-NOD because this movement of the ST is temporally separate from the ST movement to the ST Vestibule; movement is separated by lid bolting activities.	11	3E−03	This operation is identical to (but the reverse of) site transporter collision while moving into the facility (050-OpSTCollide3-HFI-NOD; Section E6.3, HFE Group #3); therefore, it has the same preliminary value: this failure is “highly unlikely” (one in a thousand or 0.001) but was adjusted because there are several ways for a collision to occur (×3). This is a separate HFE from “Operator Causes Low-Speed Collision of ST with SSC while Moving from the Loading Room to the ST Vestibule” (050-OpSTCollide3-HFI-NOD) because the site transporter movement is temporally separated by lid bolting.
050-OpImpact0000-HFI-NOD	*Operator Causes Impact of Cask during Transfer from Loading Room to ST Vestibule or from ST Vestibule to Outside*: While moving from the Loading Room to the lid bolting platform or from the lid bolting platform to outside the facility, the ST can impact the crane hook or rigging if it is improperly stowed.	11	N/A	While moving from the Loading Room to the lid bolting platform or from the lid bolting platform to outside the facility, the site transporter can impact the crane hook or rigging if it is improperly stowed. It is unlikely that the crane rigging can be improperly stowed such that it would impact the site transporter while it is moving out of the Loading Room; it is more likely that rigging would impact the cask while the crane is actually in use. Therefore, any crane interference with the site transporter is already covered by 050-OpTCImpact01-HFI-NOD (Operator Causes Impact of AO during AO Closure) and 050-OpTipover3-HFI-NOD (Operator Causes Tipover of ST).
050-OpSDClose001-HFI-NOD	*Operator Closes Shield Door on Conveyance*: Once the CTM activities are over, an operator opens the shield door, turns on the ST, lifts the forks, and moves the cask from the Loading Room to the ST Vestibule. There is a shield door between the ST Vestibule and the Cask Loading Room. The operator can impact the cask by inadvertently closing the shield door on the ST as the ST passes through the door.	12	1.0	The site transporter passes through a shield door as it moves from the Loading Room to the Site Transporter Vestibule. During this transfer, the operator can cause the site transporter to collide into the shield door or a crew member can close the shield door on the site transporter. Section E6.0.2.3.3 provides a justification of this preliminary value.
050-OpFLCollide1-HFI-NOD	*Operator Causes High-Speed Collision of ST with SSC*: The operator can cause an auxiliary vehicle to collide into a loaded ST while the conveyance is parked in the ST Vestibule. If the collision is due to the auxiliary vehicle speed governor malfunctioning, this is a high-speed collision.	11	1.0	An auxiliary vehicle (e.g., forklift) can overspeed, resulting in a collision with the site transporter while the site transporter is parked under the platform or in transit to or from the platform. In order to accomplish this, the speed governor of the auxiliary vehicle must fail. The site transporter itself is limited by design from over speeding. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
050-OpTipOver3-HFI-NOD	*Operator Causes Tipover of ST*: If the operator improperly stows the crane rigging, it can catch the ST or cask during AO lid bolting. If the crane becomes attached to the ST or cask and the operator continues to move the ST (e.g., exiting the ST Vestibule) or crane, the ST could tip over.	11	N/A	In this step the site transporter is moved from the Cask Loading Room to the ST Vestibule, the aging overpack lid bolts are removed, and then the site transporter is exported from the facility. In order to get a tipover of the site transporter, the crane must be attached to the cask or site transporter, and the crane or site transporter must also move. If there is a crane involved in the lid unbolting activities, it is a jib crane. A jib crane cannot tipover a loaded ST; see Section 6.0 for the screening justification. This failure was omitted from the HRA.
050-OpTCImpact01-HFI-NOD	*Operator Causes Impact of AO during AO Closure*: During AO closure the AO lid is bolted. If the lid bolts are installed with the crane, it is possible that the AO/ST can be impacted by the crane hook due to improper crane operations.	11	3E−03	In this step, the aging overpack lid bolts are installed. If the crane is used to move the lid bolts, it is possible that the crane can impact the side of the site transporter/aging overpack. This operation is identical to (but the reverse of) preparation of a DPC/aging overpack and, thus, was given the same name and preliminary value as impact during preparation of the DPC/aging overpack (050-OpTCImpact01-HFI-NOD; Section E6.5, HFE Group #5): this failure was assessed as “highly unlikely” (one in a thousand or 0.001) but is adjusted because there are several ways for an impact to occur (×3).
050-OpCTCollide1-HFI-NOD	*Operator Causes Low-Speed Collision of Auxiliary Vehicle with ST during Closure Activities*: While the ST is parked under the lid bolting platform for closure activities, the operator of an auxiliary vehicle can collide into the ST. If the speed governor is functioning, this is a low-speed collision.	11	3E−03	In this step the site transporter is loaded and parked under the platform. There are no auxiliary vehicles expected in this area; however if there is one, the speed of auxiliary vehicle would be slow and the site transporter and platform are very visible. This HEP was assigned the same preliminary probability as railcar collision HFE 050-OpRCCollide1-HFI-NOD (Section E6.1, HFE Group #1) because the dominant mechanism of both failures is collision with an auxiliary vehicle. In this case, the preliminary value is conservative because the site transporter is staged under the platform, and the railcar collision HFE has additional failure modes associated with movement of the SPM that are not applicable here. This failure is identical for the preparation activities in a CTT or site transporter (050-OpCTCollide1-HFI-NOD; Section E6.3, HFE Group #3): this failure was assessed as “highly unlikely” (one in a thousand or 0.001) but is adjusted because there are several ways for a collision to occur (×3).

Table E6.10-1. HFE Group #10 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
050-OpSpurMove01-HFI-NOD	*Operator Causes Spurious Movement of ST during Closure Activities*: The ST is supposed to be turned off during this operation, with the control pendant stored. However, if the ST is not in the proper configuration for AO closure, the operator can inadvertently cause the ST to move. This spurious movement can cause the ST to collide into the lid bolting platform.	11	1E−04	In this step the site transporter is parked under the preparation platform; the power is off, with the control pendant stored. For operations in this step there are several crew members on the preparation platform and no operators below the platform. This error was considered to be extremely unlikely (0.0001) because it requires multiple human errors: it would require the site transporter to be left on, the observers (the crane operator, two crew members, or the radiation protection worker) would have to fail to notice or fail to stop operations and turn off the site transporter, and an operator would have to access the pendent and signal the site transporter to move. This failure is identical for the preparation activities in a CTT or site transporter (050-OpSpurMove01-HFI-NOD; Section E6.3, HFE Group #3).
050-Liddisplace1-HFI-NOD	*Operator Inadvertently Displaces Lid*: The operator can improperly store the crane rigging such that it catches the lid lift fixture and pulls off the AO lid when bolts are installed, resulting in a direct exposure.	29	N/A	In this step the aging overpack lid is bolted with, perhaps, the use of the crane. Due to design changes to the preparation platform, improperly stowed rigging during this operation would not catch the lid lift fixture. These design changes include raising the platform so the cask is recessed underneath the platform. Therefore, this failure was omitted from analysis.
050-OpLoadDrop-HFI-NOD	*Operator Causes ST to drop AO*: The ST is like a forklift, carrying the AO several inches above the ground on its forks. If the AO is improperly secured onto the ST, it can fall off the forks while in transit or during closure activities.	N/A	N/A	The aging overpack is not lifted in this step, so the only way for an aging overpack to be dropped is if it were to fall off the site transporter. The site transporter is like a fork lift that holds the aging overpack several inches above the ground while in transit. The site transporter cannot lift the aging overpack greater than 1 ft, so a drop greater than 1 ft is not plausible in this step. The aging overpack is prevented from moving on or falling off the site transporter by a securing mechanism that locks the aging overpack into place. The site transporter has traveled to WHF from where the aging overpacks are stored. It is highly unlikely that the aging overpack would drop in the facility due to human error, given that it has not dropped in transit to the facility because the aging overpack is not removed from the site transporter in the WHF. Also, there are interlocks that prevent the site transporter from moving if the aging overpack is not properly secured. Therefore, drop of an aging overpack due to human failure was omitted from analysis.
ST rollover	*Operator Causes ST to Roll over*: The operator drives over a significantly uneven surface while exporting the ST, causing the ST to rollover.	11	N/A	Although the center of mass for the site transporter is higher than that of the truck trailer, this failure mode was omitted from analysis for the same reasons as the truck rollover in Section E6.1. For a site transporter to roll over, the center of mass has to shift laterally. This can be done by traversing a significantly uneven surface or running over a very large object. There are no significantly uneven surfaces in the Site Transporter Vestibule. It is incredible for the site transporter to run over an object large enough necessary to shift its center of mass.
050-OpFailStop-HFI-NOD	*Operator Fails to Stop ST if Tread Fails*: If the tread of the ST fails, it is possible that the ST can roll over if the operator continues to operate the ST while trying to exit the facility.	11	1.0	If the tread of the site transporter fails, it is possible the site transporter can rollover if the operator continues to operate the site transporter. While it is unlikely that an operator would continue to operate a site transporter if such a significant and visible failure occurred, to be conservative, unsafe actions that require an equipment failure to cause an initiating event are generally assigned an HEP of 1.0.

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HEP = human error probability; HFE = human failure event; HCTT = cask tractor and cask transfer trailer; ID = identification; N/A = not applicable; SSC = structure, system, or component; ST = site transporter; WHF = Wet Handling Facility.

Source: Original

E6.10.3 Detailed Analysis

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with 63.111the performance objectives of 10 CFR 63.111; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

E7 RESULTS: HUMAN RELIABILITY ANALYSIS DATABASE

Table E7-1 presents a summary of all of the human failures identified in this analysis, and it provides a link between the HFE group and the ESD in which the human failure is modeled.

Table E7-1. HFE Data Summary

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-#EEE-LDCNTRA-BUA-ROE	Operator Fails to Restore Load Center (Train A) Post Maintenance	Electrical	OA (Pre-Initiator)	1.03E−05	10	Preliminary
050-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore Load Center (Train B) Post Maintenance	Electrical	OA (Pre-Initiator)	1.03E−05	10	Preliminary
050-Liddisplace1-HFI-NOD	Operator Inadvertently Displaces Lid	29	3, 5, 7, 10	N/A[b]	N/A	Omitted from Analysis
050-LLW-Cleanup	Operator Exposed during LLW cleanup	23	OA	N/A[b]	N/A	Omitted from Analysis
050-LLW-Collision	Operator Causes Collision with LLW Container	23	OA	N/A[b]	N/A	Omitted from Analysis
050-LLW-Decon-Fail	Operator Improperly Performs Decontamination Procedures	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpCaskDrop01-HFI-NOD	Operator Drops Cask during Preparation Activities	7, 8, 9	3, 5	N/A[b]	N/A	Omitted from Analysis
050-OpClCTMGate1-HFI-NOD	Operator Inappropriately Closes Slide or Port Gate during Vertical Canister Movement and Continues Lifting	13	6	1.00E−03	5	Preliminary
050-OpCollide001-HFI-NOD	Operator Causes Low-speed Collision with RC, TT, HCTT, CTT or TTC	5, 6	2	3.00E−03	5	Preliminary
050-OpCTCollide1-HFI-NOD	Operator Causes Low-speed Collision of Auxiliary Vehicle with Cask, CTT or ST	7, 8, 9, 11, 25	3, 5, 9, 10	3.00E−03	5	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpCTCollide2-HFI-NOD	Operator Causes Low-speed Collision of the CTT during Transfer between the Preparation Station to the Cask Unloading Room	10, 14	5, 7, 9	1.00E−03	5	Preliminary
050-OpCTMDirExp1-HFI-NOD	Operator Causes Direct Exposure during CTM Activities (Second Floor, All CTM Movements)	29	6	8.00E−06	10	Detailed
050-OpCTMDrInt01-HFI-COD	Operator Lifts Canister too High with CTM	13	6	1.0	N/A	Preliminary
050-OpCTMdrop001-HFI-COD	Operator Drops Object onto Canister during CTM Operations	13	6	4.00E−07	10	Detailed
050-OpCTMdrop002-HFI-COD	Operator Causes Drop of Canister during CTM Operations	13	6	5.00E−07	10	Detailed
050-OpCTMImpact1-HFI-COD	Operator Moves the CTM while Canister or Object is below or between Levels	13	6	4.00E−08	10	Detailed
050-OpCTMImpact2-HFI-COD	Operator Causes Canister Impact with Lid during CTM Operations [AO, STC]	13	6	N/A[b]	N/A	Omitted from Analysis
050-OpCTMImpact5-HFI-COD	Operator Causes Canister Impact with SSC during CTM Operations (All)	13	6	1.0	N/A	Preliminary
050-OpCTTImpact1-HFI-NOD	Operator Causes an Impact between an SSC and a Loaded CTT/ST due to Crane Operations	7, 9	5	3.00E−03	5	Preliminary
050-OpDirExpose1-HFI-NOD	Operator Causes Direct Exposure during CTM Activities (First Floor, All CTM Movements)	29	6	1.00E−01	3	Preliminary
050-OpDirExpose2-HFI-NOD	Operator Causes Direct Exposure During CTM Activities	29	6	1.00E−04	10	Preliminary
050-OpDPC-OVP01-HFI-NOW	Operator Causes DPC Overpressurization	17	7	7.00E−08	10	Detailed

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpDPCShield1-HFI-NOW	Operator Fails to Properly Shield DPC while Installing Canister Lift Fixture, Leading to Direct Exposure (TC/DPC only)	29	5	4.00E−04	10	Detailed
050-OpDPCShield2-HFI-NOW	Operator Causes Loss of Shielding During DPC Cutting	29	7	2.00E−04	10	Detailed
050-OpDPCShield3-HFI-NOW	Operator Causes Loss of Shielding While Removing DPC Lift Fixture (TC/DPC only)	29	7	4.00E−04	10	Detailed
050-OpExpose-Decon	Operator Exposed During Decontamination	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpExpose-Splash	Operator Exposed Due to Pool Splash	30	7	1.0	N/A	Preliminary
050-OpFailRstInt-HFI-NOM	Operator Fails to Restore Interlock after Maintenance	29	6	1.00E−02	3	Preliminary
050-OpFailSG-HFI-NOD	Operator Fails to Close the CTM Slide Gate before Moving the CTM with the Canister inside the Bell	29	6	1.00E−03	5	Preliminary
050-OpFailStop-HFI-NOD	Operator Fails to Stop the ST if the Tread Fails	3, 11	4, 5, 10	1.0	N/A	Preliminary
050-Op-Filter-Expose	Operator Exposed During Filter Change out	23	OA	N/A[b]	N/A	Omitted from Analysis
050-OpFLCollide1-HFI-NOD	Operator Causes High-speed Collision of Loaded Conveyance or Cask with Auxiliary Vehicle	5, 6, 7, 8, 9, 11, 25	2, 3, 5, 9, 10	1.0	N/A	Preliminary
050-OpFLCollide2-HFI-NOD	Operator Causes Collision of Auxiliary Vehicle with Cask at DPC Cutting Station	15	7	N/A[b]	N/A	Omitted from Analysis
050-OpFuelImpact-HFI-NOD	Operator Impacts Fuel Assembly During Transfer	22	8	N/A[b]	N/A	Omitted from Analysis
050-OpHTCollide1-HFI-NOD	Operator Causes Low-speed Collision between HCTT and facility SSC	4	1	3.00E−03	5	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpHTIntCol01-HFI-NOD	Operator Causes High-speed Collision between HCTT and facility SSC	4	1	1.0	N/A	Preliminary
050-OpImpact0000-HFI-NOD	Operator Causes Impact of Cask during Transfer from the Platform to Loading/Unloading Room	10, 11, 14	5, 7, 10	N/A[b]	N/A	Omitted from Analysis
050-OpLoadDrop-HFI-NOD	Operator Causes ST to Drop the AO	3	4, 10	N/A[b]	N/A	Omitted from Analysis
050-OpNoDiscoAir-HFI-NOD	Operator Causes Spurious Movement of CTT while Canister is Being Loaded	13	6	1.00E−03	5	Preliminary
050-OpNoUnBolt00-HFI-NOD	Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tipover (AO or STC)	13	6	1.00E−03	5	Preliminary
050-OpNoUnBoltDP-HFI-NOD	Operator Fails to remove Lid Bolts, Resulting in Impact, Drop, or Tipover (TC/DPC)	13	6	N/A[b]	N/A	Omitted from Analysis
050-OpNoUnplugST-HFI-NOD	Operator Causes Spurious Movement of the ST while Canister is Being Loaded	13	6	1.00E−03	5	Preliminary
050-OpRCCollide1-HFI-NOD	Operator Causes Low-speed Collision between RC and facility SSC	2	1	3.00E−03	5	Preliminary
050-OpRCIntCol01-HFI-NOD	Operator Causes High-speed Collision between RC and facility SSC	2	1	1.0	N/A	Preliminary
050-OpRCIntCol02-HFI-NOD	Operator Causes the Mobile Access Platform to Collide into a RC	2	1	1.0	N/A	Preliminary
050-OpSampleRel2-HFI-NOD	Operator Improperly Performs Gas Sampling of Canister or Cask with Bare SNF	16, 17	3, 7	5.00E−03	5	Preliminary
050-OpSDClose001-HFI-NOD	Operator Closes Shield Door on Conveyance	12	OA (5, 7, 9, 10)	1.0	N/A	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpSpurMove01-HFI-NOD	Operator Causes Spurious Movement of the CTT in the Preparation Area or ST in the ST Vestibule	6, 7, 9, 11	2, 5, 10	1.00E−04	10	Preliminary
050-OpSTCollide3-HFI-NOD	Operator Causes Low-speed Collision of ST with an SSC while Moving to the ST Vestibule or Loading Room	3, 11	4, 5, 10	3.00E−03	5	Preliminary
050-OpSTCollide4-HFI-NOD	Operator Causes Low-Speed Collision of ST with SSC while Exporting the ST	11	10	3.00E−03	5	Preliminary
050-OpSTCShield1-HFI-COD	Operator Causes a Direct Exposure Due to Failure to Properly Install the STC Shield Ring	29	9	6.00E−05	10	Detailed
050-OpTCImpact01-HFI-NOD	Operator Causes an Impact Between Cask and SSC (Preparation Area)	5, 6, 8, 11, 15, 28	2, 3, 7, 9, 10	3.00E−03	5	Preliminary
050-OpTCImpact06-HFI-NOD	Operator Causes an Impact between the Cask and an SSC during Movement between the Pool Ledge and the Outside of the Pool	19, 20, 24	8	3.00E−03	5	Preliminary
050-OpTCImpact07-HFI-COD	Operator Causes an Impact Between Cask and SSC during Cask Movement between Pool Shelf and Pool Bottom	21	8	6.00E−03	5	Preliminary
050-OpTCImpact10-HFI-NOD	Operator Causes an Impact between a Cask and an SSC during TAD Canister Closure	25	9	6.00E−03	5	Preliminary
050-OpTipover001-HFI-NOD	Operator Causes Cask to Tip Over (Preparation Area)	5, 6, 7, 8, 15, 28	2, 3, 5, 7, 9	1.00E−04	10	Preliminary
050-OpTipOver002-HFI-NOD	Operator Causes Cask to Tip Over during Movement between Pool Ledge and Outside the Pool	19, 20, 24	8	3.00E−03	5	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
050-OpTipOver004-HFI-COD	Operator Causes Cask to Tip Over during Cask Movement between Pool Shelf and Pool Bottom	21	8	6.00E−03	5	Preliminary
050-OpTipOver3-HFI-NOD	Operator Causes a Tipover of CTT during Movement to the Cask Unloading Room or Tipover of ST with Jib Crane	10, 11	5, 10	N/A[b]	N/A	Omitted from Analysis
050-OpTTCollide1-HFI-NOD	Operator Causes Low-speed Collision between TT and facility SSC	1	1	3.00E−03	5	Preliminary
050-OpTTIntCol01-HFI-NOD	Operator Causes High-speed Collision between TT and facility SSC	1	1	1.0	N/A	Preliminary
050-OpTTIntCol02-HFI-NOD	Operator Causes the Mobile Access Platform to Collide into a TT	1	1	1.0	N/A	Preliminary
050-OpTTRollover-HFI-NOD	Operator Causes a TT or HCTT to Rollover as the Conveyance Moves into the Cask Preparation Area	1, 4	1	N/A[b]	N/A	Omitted from Analysis
050-TadDry-Fail	Operator Leaves Water in the TAD Canister	26	9	N/A[b]	N/A	Omitted from Analysis
050-VCSO-DR00001-HFI-NOD	Operators Open 2 or More Vestibule Doors in WHF	HVAC	OA (Pre-initiator)	1.00E−02	3	Preliminary
050-VCSO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	HVAC	OA (Pre-initiator)	1.0	N/A	Preliminary
050-VCSO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	HVAC	OA (Pre-initiator)	1.00E−01	3	Preliminary
050-WeldDetect-Fail	Operator Causes Defective Weld or Fails to Detect a Bad Weld	27	9	N/A[b]	N/A	Omitted from Analysis
26D-#EEY-ITSDG-A-#DG-RSS	Operator Fails to Restore Diesel Generator to Service (Train A)	Electrical	OA (Pre-initiator)	1.95E−04	10	Preliminary
26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator to Service (Train B)	Electrical	OA (Pre-initiator)	1.95-04	10	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
Crane Drops	Operator Causes Drop of Cask or Drop of Object onto Cask	OA (5-9, 15, 17-24, 30)	OA (2, 3, 5, 7, 8)	N/A [a]	N/A	Historical Data
Drop from SNF Transfer Machine	Operator Causes Drop of Fuel Assembly	22	8	N/A [a]	N/A	Historical Data
Fuel Transpose	Operator Misloads TAD Canister	N/A	8	N/A[b]	N/A	Omitted from Analysis
Gas Sampling	Operator Improperly Performs Gas Sampling of Cask with Canister	29	5	N/A[b]	N/A	Omitted from Analysis
Improper Boration	Operator Fails to Maintain Proper Boron Concentration	N/A	8	N/A[b]	N/A	Omitted from Analysis
Load too Heavy	Operator attempts to lift load which is greater than crane rating	OA	OA	N/A[b]	N/A	Omitted from Analysis
Moderator	Operator Introduces Moderator Source in to Moderator-Controlled Areas of the WHF	OA	OA	N/A[b]	N/A	Omitted from Analysis
RC Derailment	Operator Causes RC to Derail as the RC travels into the Cask Preparation Area	1	1	N/A [a]	N/A	Historical Data
Spurious Movement of CTT or ST during CTM Activities	Operator Causes Spurious Movement of CTT or ST while Canister is Being Loaded	13	6	N/A[b]	N/A	Omitted from Analysis
ST Rollover	Operator Causes the ST to Rollover in the ST Vestibule	3, 11	4, 10	N/A[b]	N/A	Omitted from Analysis

NOTE: [a] Historical data was used to produce a probability for this HFE; this is not covered as part of the HRA, but rather addressed in Attachment C.
[b] These HFEs were initially identified, but omitted from analysis for various reasons, including a design change precluding the human failure, or the failure would require a series of unsafe actions in combination with mechanical failures, such that the event is no longer credible. See the appropriate HFE group for a case-by-case justification for these omissions.
AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; ESD = event sequence diagram; HCTT = cask tractor and cask transfer trailer; HFE = human failure event; HSTC = horizontal shielded transfer cask; LLW = low-level radioactive waste; N/A = not applicable; OA = over arching (applies to multiple HFE groups, Section E6.0.2); RC = railcar; SNF = spent nuclear fuel; ST = site transporter; SSC = structure, system, or component; SSCs = structures, systems, and components; STC = shielded transfer cask; TAD = transportation, aging, and disposal; TC = transportation cask; TT = truck trailer; TTC = a transportation cask that is upended using a tilt frame; VTC = a transportation cask that is upended on a railcar; WHF = Wet Handling Facility.

Source: Original

E8 REFERENCES

E8.1 DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

E8.1.1* AIChE (American Institute of Chemical Engineers) 1992. *Guidelines for Hazard Evaluation Procedures.* 2nd Edition with Worked Examples. New York, New York: American Institute of Chemical Engineers. TIC: 239050. ISBN (0-8169-0491-X.

E8.1.2* ASME (American Society of Mechanical Engineers) NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.

E8.1.3* ASME NUM-1-2004. 2005. *Rules for Construction of Cranes, Monorails, and Hoists (with Bridge or Trolley or Hoist of the Underhung Type).* New York, New York: American Society of Mechanical Engineers. TIC: 259317. ISBN: 0-7918-2938-3.

E8.1.4* ASME RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.* New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.

E8.1.5* Benhardt, H.C.; Eide, S.A.; Held, J.E.; Olsen, L.M.; and Vail, R.E. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U*). WSRC-TR-93-581. Aiken, South Carolina: Westinghouse Savannah River Company, Savannah River Site. ACC: MOL.20061201.0160.

E8.1.6 BSC (Bechtel SAIC Company) 2006. *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope.* 000-MJ0-HTC0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061120.0011

E8.1.7* BSC 2006. *Engineering Standard for Repository Component Function Identifiers.* 000-30X-MGR0-00900-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20060816.0001.

E8.1.8* BSC 2007. *Engineering Standard for Repository Area Codes.* 000-3DS-MGR0-00400-000 REV 004. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070911.0015.

E8.1.9*BSC 2007. *Repository System Codes.* 000-30X-MGR0-01200-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071101.0022.

E8.1.10 BSC 2008. *Wet Handling Facility Event Sequence Development Analysis.* 050-PSA-WH00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080225.0010.

E8.1.11* CRA (Corporate Risk Associates) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique.* CRA-BEGL-POW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.

E8.1.12 DOE-STD-1090-2004. 2004. *Hoisting and Rigging (Formerly Hoisting and Rigging Manual).* Washington, D.C.: U.S. Department of Energy. ACC: ENG.20060407.0002.

E8.1.13* Dougherty, E.M., Jr. and Fragola, J.R. 1988. *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications.* New York, New York: John Wiley & Sons. TIC: 3986. ISBN: 0-471-60614-6.

E8.1.14* Gertman, D.; Blackman, H.; Marble, J.; Byers, J.; and Smith, C. 2005. *The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0009.

E8.1.15* Hall, R.E.; Fragola, J.R.; and Wreathall, J. 1982. *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlations.* NUREG/CR-3010. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0211.

E8.1.16* Hamlin, T.L. 2005. *Space Shuttle Probabilistic Risk Assessment - Human Reliability Analysis (HRA) Data Report.* VOL. III, Rev. 2.0. Washington, D.C.: NASA. ACC: MOL.20080311.0023.

E8.1.17* Hannaman, G.W. and Spurgin, A.J. 1984. *Systematic Human Action Reliability Procedure (SHARP).* EPRI-NP-3583. Palo Alto, California: Electric Power Research Institute. TIC: 252015.

E8.1.18* Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM.* 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487

E8.1.19* Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

E8.1.20 NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

E8.1.21 NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants.* NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

E8.1.22 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.

E8.1.23 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis.* HLWRS-ISG-04. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071211.0230.

E8.1.24* Rasmussen, J. 1983. "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models." *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13*, (3), 257–266. [New York, New York]: Institute of Electrical and Electronics Engineers. TIC: 259863.

E8.1.25* Swain, A.D. 1987. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. NUREG/CR-4772. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0026.

E8.1.26* Swain, A.D. and Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report.* NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.

E8.1.27* Vesely, W. 2008. "Re: CREAM Errata." E-mail from W.E.Vesely to M.Presley, February, 20, 2008. ACC: MOL.20080220.0081.

E8.1.28* Williams, J.C. 1986. "HEART - A Proposed Method for Assessing and Reducing Human Error." *9th Advances in Reliability Technology Symposium - 1986.* Bradford, England: University of Bradford. TIC: 259862.

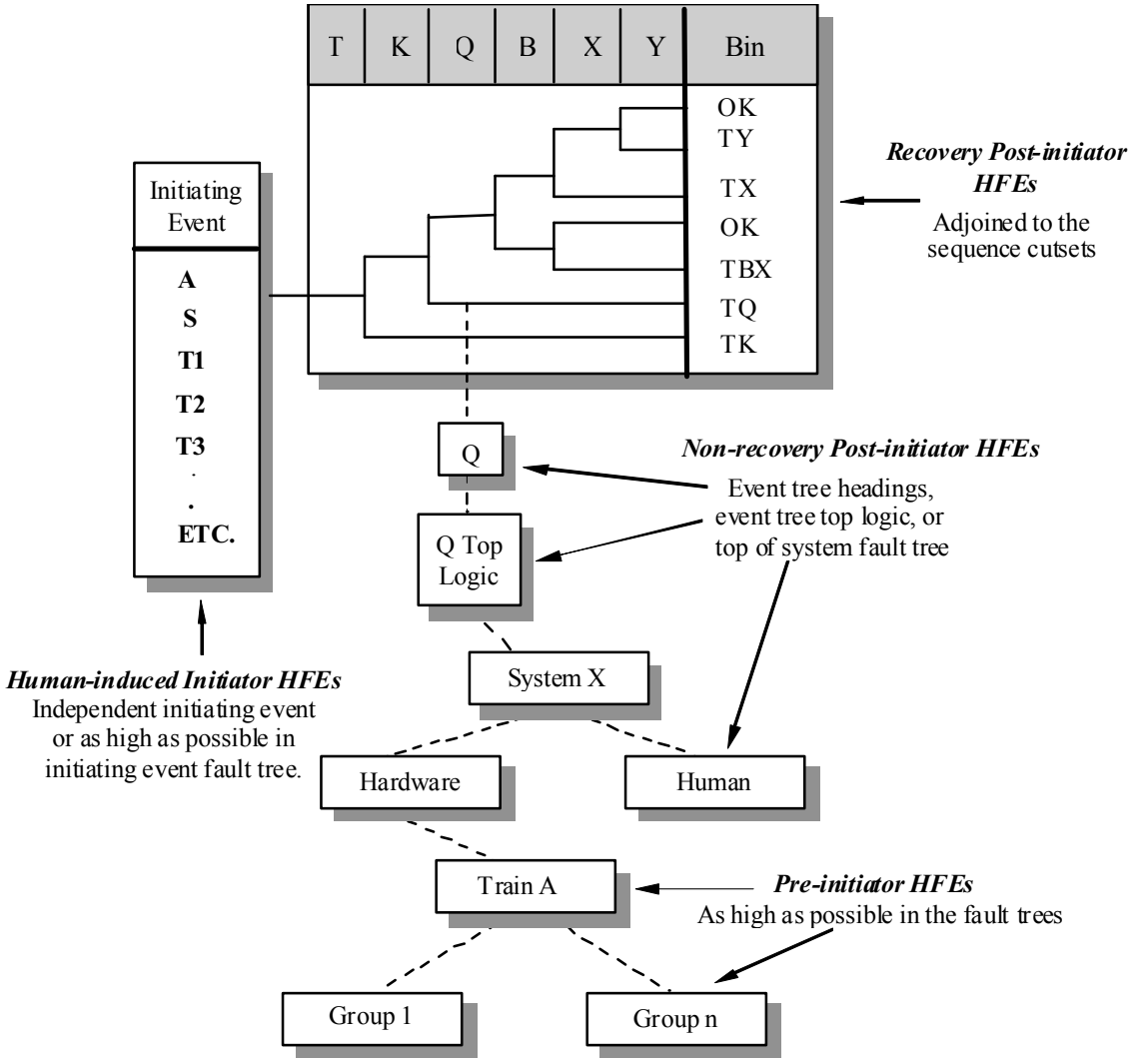
E8.1.29* Williams, J.C. 1988. "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance." *[Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants]*. Pages 436–450. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259864.

E8.2 DESIGN CONSTRAINTS

E8.2.1 10 CFR (Code of Federal Regulations) Part 63. 2007. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. U.S. Nuclear Regulatory Commission.

APPENDIX E.I
RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA

Figure E.I-1 provides a graphical illustration of how HFEs are incorporated into the PCSA.

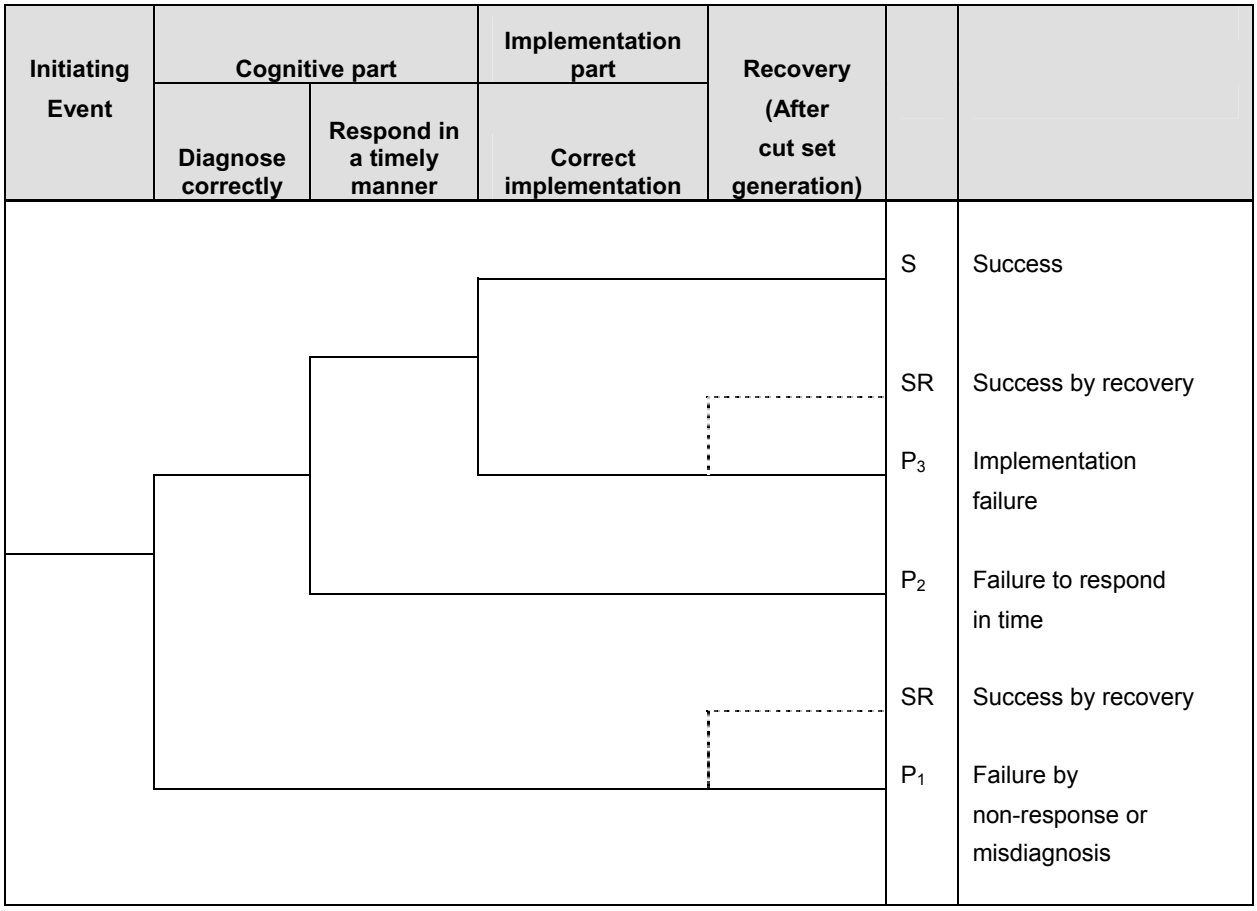


NOTE: HFE = human failure event.

Source: Original

Figure E.I-1. Modeling Strategy for HFE Types

APPENDIX E.II
GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS



Source: Original

Figure E.II-1 Post Initiator Operator Action Event Tree

The representation in Figure E.II-1 consists of two elements, corresponding to a cognitive part (detection, diagnosis, and decision making) and an implementation (i.e., action) part.

P_1 represents the probability that operators make an incorrect diagnosis and decision and do not realize that they have done so. Some of the reasons for such mistakes are: incorrect interpretation of the procedures, incorrect knowledge of the plant state owing to communication difficulties, and instrumentation problems.

Given that the crew decides what to do correctly, there is still a possibility of failure to respond in time (represented by P_2) or making an error in implementation (represented by P_3).

However, it may be probable in certain scenarios that a recovery action can be taken. This consideration is taken into account after the initial quantification is completed and is applied as appropriate to the dominant cut sets.

APPENDIX E.III
PRELIMINARY (SCREENING) QUANTIFICATION PROCESS FOR HUMAN FAILURE EVENTS

The preliminary quantification process consists of the following:

Step 1—Complete the Initial Conditions Required for Quantification.

The preliminary quantification process requires the following:

- The baseline scenarios are available.
- The HFEs and their associated context have been defined.
  - Collect any additional information that is not already collected and that is needed to describe and define the HFEs (and associated contexts).
  - Review all information for clarity, completeness, etc.
  - Interpret and prioritize all information with respect to relevance, credibility, and significance.

Table E.III-1 provides examples of information normally identified using the ATHEANA method (*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis* (Ref. E8.1.22) that serves as inputs to the quantification process. The HFE/context descriptions in Table E.III-1 touch briefly on the information that is relevant to the screening-level quantification of the HFE. Since the baseline scenario generally touches on much of this information, the point of including the HFE/context descriptions is to summarize the information that pertains to the specific HFE to minimize the need for the analysts to refer back to the baseline scenario, except to obtain additional detail.

Table E.III-1. Examples of Information Useful to HFE Quantification

Information Type	Examples
Facility, conditions, and behavior for possible deviations of the scenarios	Reasonably possible unusual plant behavior and failures of systems; equipment, and indications, especially those that may be unexpected or difficult to detect by operators. Includes presence of interlocks that would have to fail to promote the deviation.
Operating crew characteristics (i.e., crew characterization)	Crew structure, communication style, emphasis on crew discussion of the “big picture.”
Features of procedures	Structure, how implemented by operating crews, opportunities for “big picture” assessment and monitoring of critical safety functions, emphasis on relevant issue, priorities, any potential mismatches with deviation scenarios.
Relevant informal rules	Experience, training, practice, ways of doing things - especially those that may conflict with informal rules or otherwise lead operators to take inappropriate actions.
Timing	Plant behavior and requirements for operator intervention versus expected timing of operator response in performing procedure steps, etc.

Table E.III-1. Examples of Information Useful to HFE Quantification (Continued)

Information Type	Examples
Relevant vulnerabilities	Any potential mismatches between the scenarios and expected operator performance with respect to timing, formal and informal rules, biases from operator experience, and training, etc.
Error mechanisms	Any that may be particularly relevant by plant context or implied by vulnerabilities; applicable mechanisms depend upon whether HFE is a slip or mistake. Examples include: failures of attention, possible tunnel vision, conflicts in priorities, biases, missing or misleading indications, complex situations, lack of technical knowledge, timing mismatches and delays, workload, and human–machine interface concerns.
Performance-shaping factors	Those deemed associated with, or triggered by, the relevant plant conditions and error mechanisms.

NOTE: HFE = human failure event.

Source: Original

In Step 1, interpreting and prioritizing all information with respect to relevance, credibility, and significance is especially important if:

- Some information is applicable only to certain scenarios, HFEs, or contexts
- There are conflicts among information sources
- Information is ambiguous, confusing, or incomplete
- Information must be extrapolated, interpolated, etc.

Completion of the "lead-in" initial conditions is primarily performed by a single individual, using the results of the YMP HAZOP evaluation process and reviews of other relevant information sources. Discussions are also held with the Operations Department to augment that information and the resulting write-ups are reviewed by the PCSA facility leads and the HRA team. The initial conditions are refined as part of an open discussion among the experts (in this case, the HRA team for the study) involved in the expert opinion elicitation process. The goal of this discussion is not to achieve a consensus but, rather, to advance the understanding of all the experts through the sharing of distributed knowledge and expertise. In each case, the scenario (or group of similar scenarios) and the HFE in question are described and the vulnerabilities and strong points associated with taking the right action are discussed openly among the HRA team.

Step 2—Identify the Key or Driving Factors of the Scenario Context.

The purpose of Step 2 is to identify the key or driving factors on operator behavior/performance for each HFE and associated context. Each expert participating in the elicitation process individually identifies these factors based on the expert's own judgment. Usually, these factors are not formally documented until Step 4.

Typically, there are multiple factors deemed most important to assessing the probability for the HFE in question. This is due to the focus of the ATHEANA search process on combinations of factors that are more likely to result in an integrated context (Ref. E8.1.22). When there is only a single driving factor, it is usually one that is so overwhelming that it alone can easily drive the estimated probability. For example, if the time available is shorter than the time required to

perform the actions associated with the HFE, quantification becomes much simpler and other factors need not be considered.

Step 3—Generalize the Context by Matching it With Generic, Contextually-Anchored Rankings, or Ratings.

In Step 3, each expert participating in the elicitation process must answer the following question for each HFE: based upon the factors identified in Step 2, how difficult or challenging is this context relative to the HFE being analyzed?

Answering this question involves independent assessments by each expert. In order to perform this assessment, the specifics of the context defined for an HFE must be generalized or characterized. These characterizations or generalizations then must be matched to general categories of failures and associated failure probabilities.

To assist the experts in making their judgments regarding the probability of events, some basic guidance is provided. In thinking about what a particular HEP associated with an HFE may be, they are encouraged to think about similar situations or experiences and use that to help estimate how many times out of 10, 100, 1,000, etc., would they expect crews to commit the HFE, given the identified conditions. The following examples of what different probabilities mean are provided to the experts to help them scale their judgments:

"Likely" to fail (extremely difficult/challenging)	~0.5	(5 out of 10 would fail)
"Infrequently" fails (highly difficult/challenging)[16]	~0.1	(1 out of 10 would fail)
"Unlikely" to fail (somewhat difficult/challenging)	~0.01	(1 out of 100 would fail)
"Highly unlikely" to fail (not difficult/challenging)	~0.001	(1 out of 1000 would fail)

The experts are allowed to select any value to represent the probability of the HFE. That is, other values (e.g., 3E−2, 5E−3) can be used. The qualitative descriptions above are provided initially to give analysts a simple notion of what a particular probability means. For exceptional cases, the quantification approach allows an HEP of 1.0 to be used when failure was deemed essentially certain. The following general guidance in Table E.III-2 is also provided to help calibrate the assessment by providing specific examples that fall into each of the above bins, and is based on the elicited judgment and consensus of the HRA team based on their past experience. This guidance applies to contexts where generally optimal conditions exist during performance of the action. Therefore, the experts should modify these values if they believe that the action may be performed under non-optimal conditions or under extremely favorable conditions. Values may also be adjusted to take credit for design features, controls and interlocks, or procedural safety controls[17,18]. Examples of such adjustments are also provided below; however these values are not taken to be firm in any sense of the word, but rather simply as examples of

[16] The default value is 0.1. This value is used if no preliminary assessment is performed.

[17] As an initial preliminary value, unsafe actions that are backed up by interlocks are assigned a human error probability of 1.0 such that no credit for human performance is taken (i.e., only the interlocks are relied upon to demonstrate 10 CFR Part 63 (Ref. E8.2.1) compliance). If this proves insufficient, a more reasonable preliminary value is assigned to the unsafe action in accordance with this Appendix.

[18] Note that if such credit is taken, then it may be necessary (based on the PCSA results) to include these items in the nuclear safety design basis or the procedural safety controls for the YMP facilities.

where in general terms HEPs may fall and how they may relate to each other. Types of HFEs not listed here can be given values based on being "similar to" HFEs that are listed. Whatever value is selected, the basis is briefly documented.

Table E.III-2. Types of HFEs

PRE-INITIATOR HFEs	
Fail to properly restore a standby system to service	0.1
Failure to properly restore an operating system to service when the degraded state is not easily detectable	0.01
Failure to properly restore an operating system to service when the degraded state is easily detectable	0.001
Calibration error	0.01
HUMAN-INDUCED INITIATOR HFEs	
Failure to properly conduct an operation performed on a daily basis	0.001
Failure to properly conduct an operation performed on a very regular basis (on the order of once/week)	0.01
Failure to properly conduct an operation performed only very infrequently (once/month or less)	0.1
Operation is extremely complex OR conducted under environmental or ergonomic stress	×3
Operation is extremely complex AND conducted under environmental or ergonomic stress	×10
NON-RECOVERY POST-INITIATOR HFEs	
Not trained or proceduralized, time pressure	0.5
Not trained or proceduralized, no time pressure	0.1
Trained and/or proceduralized, time pressure	0.1
Trained and/or proceduralized, no time pressure	0.01

Source: Original

Step 4—Discuss and Justify the Judgments Made in Step 3

In Step 3, each expert independently provides an estimate for each HFE. Once all the expert estimates are recorded, each expert describes the reasons why they chose a particular failure probability. In describing their reasons, each expert identifies what factors (positive and negative) are thought to be important to characterizing the context and how this characterization fit the failure category description and the associated HEP estimate.

After the original elicited estimates are provided, a discussion is held that addresses not only the individual expert estimates but also differences and similarities among the context characterizations, key factors, and failure probability assignments made by all of the experts. This discussion allows the identification of any differences in the technical understanding or interpretation of the HFE versus differences in judgment regarding the assignment of failure probabilities. Examples of factors important to HFE quantification that might be revealed in the discussion include:

- Differences in key factors and their significance, relevance, etc., based upon expert-specific expertise and perspective.

- Differences in interpretations of context descriptions.
- Simplifications made in defining the context.
- Ambiguities and uncertainties in context definitions.

A consensus opinion is not required following the discussion.

Step 5—Refinement of HFEs, associated contexts, and assigned HEPs (if needed)

Based upon the discussion in Step 4, the experts form a consensus on whether or not the HFE definition must be refined or modified, based upon its associated context. If the HFE must be refined or re-defined, this is done in Step 5. If such modifications are necessary, the experts "reestimate" based upon the newly defined context for the HFE (or new HFEs, each with an associated context).

The experts participating in the elicitation process are also allowed to change their estimate after the discussion in Step 4 based on the discussions during that step, whether or not the HFE definition and context are changed. Once again, a consensus is not required.

Step 6—Determine final preliminary HEP for HFE and associated context

The final preliminary value to be incorporated into the PCSA for each HFE is determined in Step 6.

The failure probabilities assigned in the preliminary HRA quantification are based on the context outlined in the base case scenarios and deemed to be "realistically conservative." To help ensure this conservatism, if a consensus value could not be reached, the final failure probability that was assigned to each HFE was determined by choosing the highest assigned probability among the final estimates of the experts participating in the expert elicitation process.

APPENDIX E.IV
SELECTION OF METHODS FOR DETAILED QUANTIFICATION

There are a number of methods available for the detailed quantification of HFEs (preliminary quantification is discussed in Appendix E.III of this analysis). Some are more suited for use for the YMP PCSA than others. A number of methods were considered, but many were rejected as inapplicable or insufficient for use in quantification. Several sources were examined as part of the background analysis for selecting a method for detailed quantification (Ref. E8.1.17; Ref. E8.1.13; Ref. E8.1.24; and Ref. E8.1.21). As discussed in Section E3.2 the following four were chosen:

- ATHEANA expert judgment (Ref. E8.1.22).
- CREAM (Ref. E8.1.18)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11)
- THERP (Ref. E8.1.26)

This appendix discusses the selection process.

Basis for Selection—The selection process was conducted with due consideration of the HRA quantification requirements set forth in the ASME Level 1 PRA standard (Ref. E8.1.4) to the extent that those requirements, which were written for application to NPP PRA, apply to the types of operations conducted at the YMP. Certainly, all of the high level HRA quantification requirements were considered to be applicable. Further, all of the supporting requirements to these high level requirements were considered applicable, at least in regards to their intent. In some cases, the specifics of the supporting requirements are only applicable to NPP HRA and some judgment is needed on how to apply them. This was particularly true of those supporting requirements that judged certain specific quantification methods acceptable. This appendix lays out the specific case for the methods selected for use at the YMP (or, more to the point, the exclusion of certain methods that would normally be considered acceptable under the standard, but are deemed inappropriate for use for the YMP PCSA).

Differences between NPP and the YMP Relevant to HRA Quantification—There are a number of contrasts between the operations at the YMP and the operations at an NPP that affect the selection of approaches to performing detailed HRA quantification (Table E.IV-1).

Table E.IV-1. Comparison between NPP and YMP Operations

NPP	YMP
Central control of operations maintained in control room.	Decentralized (local), hands on control for most operations.
Most important human actions are in response to accidents.	Most important human actions are initiating events.
Post-accident response is important and occurs in minutes to hours. Short time response important to model in HRA.	Post-accident response evolves more slowly (hours to days). Short time response not important to model.
Multiple standby systems are susceptible to pre-initiator failures.	Standby systems do not play major role in the YMP safeguards, therefore few opportunities for pre-initiator failures.

Table E.IV-1. Comparison between NPP and YMP Operations (Continued)

NPP	YMP
Auxiliary operators sent by central control room operators to where needed in the plant.	Local control reduces time to respond.
Most actions are controlled by automatic systems.	Most actions are controlled by operators.
Reliance on instrumentation /gauges as operators' "eyes".	Most actions are local, either hands on or televised. Less reliance on man–machine interface.
High complexity of systems, interactions, and phenomena. Actions may be skill, rule, or knowledge based.	Relatively simple process with simple actions. Actions are largely skill based.
Many in operation for decades; HRA may include walk-downs and consultation with operators.	First of a kind; HRA performed for construction application, therefore walk-downs and consultation with operators not feasible.

NOTE: HRA = human reliability analysis; NPP = nuclear power plant; YMP = Yucca Mountain Project.

Source: Original

Assessment of Available Methods—There are essentially four general types of quantification approaches available:

1. Procedure focused methods:

    a. Basis: These methods concentrate on failures that occur during step-by-step tasks (i.e., during the use of written procedures). They are generally based on observations of human performance in the completion of manipulations without much consideration of the root causes or motivations for the performance (e.g., how often does an operator turn a switch to the left instead of to the right).

    b. Methods considered: THERP (Ref. E8.1.26).

    c. Applicability: This method is of limited use for the YMP because important actions are not procedure-driven. Many operations are skill-based and/or semi-automated (e.g., crane operation, trolley operation, CTM operation, transport and emplacement vehicle operation). However, there are some instances where such an approach would be applicable to certain unsafe actions within an HFE. In addition, the THERP dependency model is adopted by NARA as being appropriate to use within a context-based quantification approach.

    d. Assessment: THERP is retained as an option in the detailed quantification for its dependency model and for limited use when simple, procedure-driven unsafe actions are present within an HFE.

2. Time-response focused methods:

    a. Basis: These methods focus on the time available to perform a task, versus the time required, as the most dominant factor in the probability of failure. They are, for the most part, based on NPP control room observations, studies, and simulator exercises. They also tend to be correlated with short duration simulator exercises

(i.e., where there is a clear time pressure in the range of a few minutes to an hour to complete a task in response to a given situation).

b. As discussed in *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications* (Ref. E8.1.13), examples of time-response methods include: HCR (Ref. E8.1.13) and TRCs (Ref. E8.1.15).

c. Applicability: These methods are not applicable to the YMP because most actions do not occur in a control room and, in addition, are generally not subject to time pressure. This is particularly true of the most important HFEs, those that are human-induced initiators. Other than a desire to complete an action in a timely fashion to maintain production schedules, time is irrelevant to these actions, especially in the context of the type of time pressure considered by these methods. Even those actions at the YMP that may take place in a control room in response to an event sequence and have time as a factor would only require response in the range of hours or days, which is outside the credible range for these methods.

d. Assessment: No use can be identified for these methods within the YMP PCSA. None of them are retained.

3. Context and/or cognition driven methods:

a. Basis: These methods focus on the context and motivations behind human performance rather than the specifics of the actions, and as such are independent of the specific facility and process. To the extent that some of the methods are data-driven (i.e., they collect and use observations of human performance) the data utilized is categorized by GTT rather than by the type of facility or equipment where the human failure occurred. This makes them more broadly applicable to various industries, tasks, and situations, in large part because they allow context-specific PSFs to be considered. This allows for them to support a variety of contexts, individual performance factors (e.g., via PSFs) and human factor approaches.

b. Methods considered: HEART (Ref. E8.1.28; Ref. E8.1.29)/NARA (Ref. E8.1.11), CREAM (Ref. E8.1.18), and ATHEANA (Ref. E8.1.22) expert judgment.

c. Applicability: The broad applicability of these methods and their flexibility of application make them most suited for application at the YMP. The use of information from a broad range of facilities and other performance regimes (e.g., driving, flying) support their use as facility-independent methods. The generic tasks considered can be applied to the types of actions of most concern to the YMP (i.e., human-induced initiators) as opposed to the more narrow definitions used in other approaches that make it difficult to use them for other than post-initiator or pre-initiator actions.

d. Assessment: Optimally it would be convenient to use only one of the three methods of this type for all the detailed quantification. However, HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11) and CREAM (Ref. E8.1.18) approach their GTTs slightly differently and also use different PSFs and adjustment factors. There are unsafe actions within the YMP HFEs that would best fit the HEART (Ref. E8.1.28)/NARA (Ref. E8.1.11) approach and others that would best fit the CREAM (Ref. E8.1.18) approach. In addition, the union of the two approaches still has some gaps that would not cover a small subset of unsafe actions for the YMP (primarily in the area of unusual acts of commission). One gap relates to dependencies between actions, but in this case NARA (Ref. E8.1.11) specifically endorses the THERP (Ref. E8.1.26) approach and so this is used. However, other gaps exist. For these cases, the ATHEANA (Ref. E8.1.22) expert judgment approach provides a viable and structured framework for the use of judgment to establish the appropriate HEP values in a manner that would meet the requirements of the ASME RA-S-2002 (Ref. E8.1.4) standard. Therefore, all three of these methods are retained for use and the selection of one versus the other is made based on the specific unsafe action being quantified. This is documented as appropriate in the actual detailed quantification of each HFE.

4. Simplified methods:

A. Basis: These methods use the results of past PRAs to focus attention on those HFEs that have dominated risk. These are essentially PRA results from NPPs. As such, they pre-suppose NPP situations and actions, and define important PSFs based on these past NPP PRAs. They have very limited (if any) ability to investigate context, individual and human factors that are beyond NPP experience. The HEPs that result from applying these methods are calibrated to other NPP methods.

B. Methods considered: ASEP (Ref. E8.1.25), SPAR-H (Ref. E8.1.14).

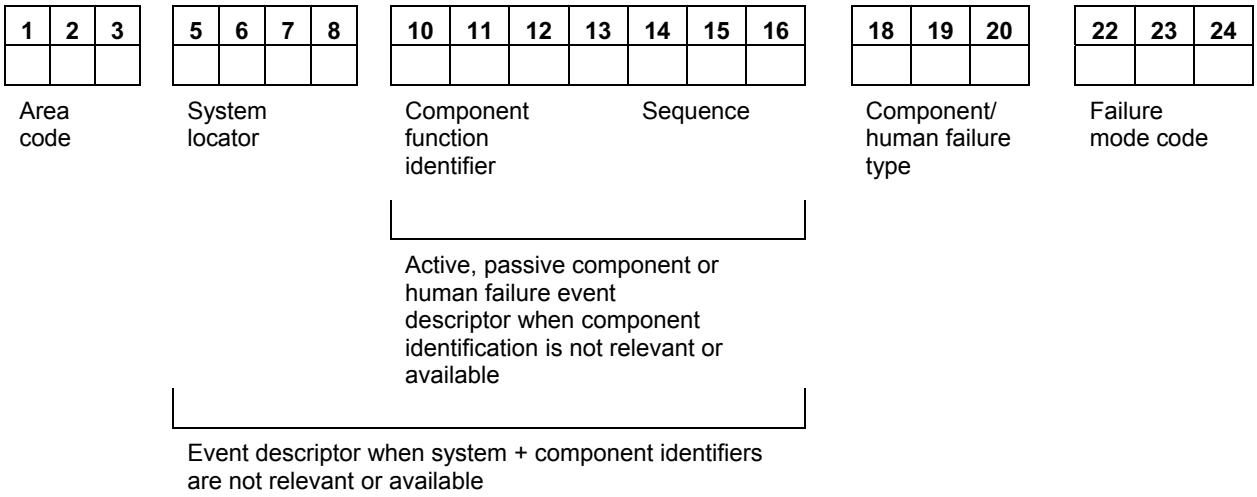
C. Applicability: These methods are clearly biased by their very close dependence on the results of past NPP PRAs. They are too limited for application beyond the NPP environment. They are not simply inappropriate for this application, but it would be extremely difficult to make a sound technical case regarding technical validity.

D. Assessment: No use can be identified for these methods within the YMP PCSA or any technical case made supporting them for a non-NPP application. None of them are retained.

APPENDIX E.V
HUMAN FAILURE EVENTS NAMING CONVENTION

Event names for HFEs in the YMP PCSA model follow the general structure of the naming convention for fault tree basic events. This is true whether the HFE is modeled in a fault tree, directly on an event tree, or as an initiating event. The convention, as adapted for HFEs, is as follows:

This basic event naming convention in Figure E.V-1 below is provided to ensure consistency with project standards and to permit this information to fit into a 24-character SAPHIRE field such that each basic event can be correlated to a unique component or human failure.



Source: Original

Figure E.V-1. Basic Event Naming Convention

The area code defines the physical design or construction areas where a component would be installed. Area codes are listed in *Engineering Standard for Repository Area Codes,* (Ref. E8.1.8). These codes are used rather than the facility acronyms to maintain consistency with Engineering. In this system, the Canister Receipt and Closure Facility is designated by area code 060, the WHF is 050, the Receipt Facility is 200, the Initial Handling Facility is 51A, and Subsurface is 800. Intra-Site Operations could fall under one of several repository area codes and therefore the most appropriate code to use was the repository general area code. However, this code was insufficient for the purposes of this analysis, and a designator of ISO was substituted instead. For the majority of cases, the area coding of HFEs in Attachment E reflects the location of the operations being evaluated, such as ISO for Intra-Site Operations. However, for certain HFEs, the coding corresponds to the location of the systems impacted by the human failure, such as HVAC, which is specific to the CRCF and therefore retains the 060 coding, and AC power, which retains the 26x and 27x coding. For these specific instances, such coding provides better traceability of the HFE back to the affected equipment.

The system locator code identifies operational systems and processes. System locator codes (four characters) are listed in Table 1 of *Repository System Codes* (Ref. E8.1.9). These are generally three or four characters long, such as VCT for tertiary confinement HVAC.

The component function identifiers identify the component function and are listed in the *Engineering Standard for Repository Component Function Identifiers* (Ref. E8.1.7). These are generally three or four characters long. Some Bechtel SAIC Company, LLC component function identifiers for typical components are shown in Table E.V-1, but in cases where there is not an equivalent match, the most appropriate PCSA type code should be used (also given in Table E.V-1).

The sequence code is a numeric sequence and train assignment (suffix), if appropriate, that uniquely identifies components within the same area, system, and component function.

If an HFE is related to the failure of an individual component with an existing component function identifier and sequence code, the naming scheme should utilize these codes in the event name. If an HFE is such that these codes do not apply, the basic event name can be a free form field for describing the nature of the event, such as HCSKSCF for operator topples cask during scaffold movement or HFCANLIDAJAR for operator leaves canister lid ajar, utilizing either seven characters when there is a relevant system locator code, or 12 characters when no system codes are applicable.

The human failure type and failure mode codes are three characters each, consistent with the coding provided in Table E.V-1 below.

For HFEs, the type code always begins with HF and continues with a one letter designator for the HFE temporal phase: P for pre-initiator, I for human-induced initiator, N for non-recovery post-initiator, R for recovery post-initiator (this latter code is not used during preliminary analysis).

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes

PRE-INITIATOR HFEs; TYP=HFP		FMC=
Fail to properly restore a standby system to service		RSS
Failure to properly restore an operating system to service when the degraded state is not easily detectable		ROH
Failure to properly restore an operating system to service when the degraded state is easily detectable		ROE
Calibration error		CAL
HUMAN-INDUCED INITIATOR HFEs; TYP=HFI		
Failure to properly conduct an operation	Operation is performed on a daily basis.	NOD
	Operation is performed on a very regular basis (on the order of once per week)	NOW
	Operation is performed only very infrequently (once per month or less)	NOM
Operation is extremely complex OR conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	COD
	Operation is performed on a very regular basis (on the order of once per week)	COW
	Operation is performed only very infrequently (once per month or less)	COM
Operation is extremely complex AND conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	CSD
	Operation is performed on a very regular basis (on the order of once per week)	CSW
	Operation is performed only very infrequently (once per month or less)	CSM
NON-RECOVERY POST-INITIATOR HFEs; TYP=HFN		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN
RECOVERY POST-INITIATOR HFEs; TYP=HFR		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN

NOTE: FMC = failure mode code; HFE = human failure event; HFI = human-induced initiator HFE; HFN = human failure non-recovery post-initiator HFE; HFP = pre-initiator HFE; HFR = human failure recovery post-initiator HFE; TYP = type.

Source: Original

ATTACHMENT F
FIRE ANALYSIS

CONTENTS

Page

FIGURES

Page

TABLES

Page

TABLES (Continued)

Page

ACRONYMS

ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
BFD	block flow diagram
CTM	canister transfer machine
CTT	cask transport trolley
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EPRI	Electrical Power Research Institute
HEPA	high-efficiency particulate air
HVAC	heating, ventilation, and air-conditioning
ITS	important to safety
MCC	motor control center
NFPA	National Fire Protection Association
NRC	U.S. Nuclear Regulatory Commission
PCSA	Preclosure Safety Analysis
PRA	probabilistic risk assessment
RWF	residence weighting factor
SNF	spent nuclear fuel
TAD	transportation, aging, and disposal canister
WHF	Wet Handling Facility
YMP	Yucca Mountain Project

F1 INTRODUCTION

This document describes the work scope, definitions and terms, method, and results for the fire analysis performed as a part of the Yucca Mountain Project (YMP) Preclosure Safety Analysis (PCSA). Fire analysis is divided into four major areas:

- Initiating event identification
- Initiating event quantification (including both ignition frequency and propagation probability)
- Fragility analysis (including convolution of fragility and hazard curves)
- Fire analysis model development and quantification.

Within the task, the internal events PCSA model is evaluated with respect to fire initiating events and modified as necessary to address fire-induced failures that lead to exposures. The lists of fire-induced failures that are included in the model are evaluated as to fire vulnerability, and fragility analyses are conducted as needed. All calculations are performed in Excel and included in Attachment H in *WHF Fire Frequency - no suppression.xls* and *WHF CB Report.xls.*

F2 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

F2.1 *Ahrens, M. 2000. *Fires in or at Industrial Chemical, Hazardous Chemical and Plastic Manufacturing Facilities, 1988-1997 Unallocated Annual Averages and Narratives.* Quincy, Massachusetts: National Fire Protection Association. TIC: 259997.

F2.2 ANSI/ANS 58.23-2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.

F2.3 ASME RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications.* New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.

F2.4 BSC 2007. *CRCF, RF, WHF, and IHF Cask Transfer Trolley Process and Instrumentation Diagram*. 000-M60-HM00-00301-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071119.0013.

F2.5 BSC 2007. *Equipment Motor Horsepower and Electrical Requirements Analysis.* 000-M0A-H000-00100-000-00A. Las Vegas, Nevada. Bechtel SAIC Company. ACC: ENG.20070816.0001.

F2.6 *BSC 2007. *Preliminary Wet Handling Facility Throughput Study.* 050-30R-MGR0-00300-000-003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0019.

F2.7 *BSC 2007. *Wet Handling Facility 480V Load Center 050-EEN0-LC-00001 Single Line Diagram*. 050-E10-EEN0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0019.

F2.8 *BSC 2007. *Wet Handling Facility 480V Load Center 050-EEN0-LC-00002 Single Line Diagram*. 050-E10-EEN0-00801-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0026.

F2.9 *BSC 2007. *Wet Handling Facility 480V Load Center 050-EEN0-LC-00003 Single Line Diagram*. 050-E10-EEN0-01101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0029.

F2.10 BSC 2007. *Wet Handling Facility 480V ITS Load Center 050-EEE0-LC-00001 Train A Single Line Diagram*. 050-E10-EEE0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0017.

F2.11 BSC 2007. *Wet Handling Facility 480V ITS Load Center 050-EEE0-LC-00002 Single Line Diagram*. 050-E10-EEE0-00401-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0018.

F2.12 BSC 2007. *Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00001 Train A Single Line Diagram*. 050-E10-EEE0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0015.

F2.13 BSC 2007. *Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00002 Train B Single Line Diagram*. 050-E10-EEE0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0016.

F2.14 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00001 Single Line Diagram*. 050-E10-EEN0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0020.

F2.15 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00002 Single Line Diagram*. 050-E10-EEN0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0021.

F2.16 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00003 Single Line Diagram*. 050-E10-EEN0-00401-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0022.

F2.17 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00004 Single Line Diagram*. 050-E10-EEN0-00501-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0023.

F2.18 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00005 Single Line Diagram*. 050-E10-EEN0-00601-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0024.

F2.19 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00006 Single Line Diagram*. 050-E10-EEN0-00701-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0025.

F2.20 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00007 Single Line Diagram*. 050-E10-EEN0-00901-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0027.

F2.21 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00008 Single Line Diagram*. 050-E10-EEN0-01001-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0028.

F2.22 *BSC 2007. *Wet Handling Facility 480V MCC 050-EEN0-MCC-00009 Single Line Diagram*. 050-E10-EEN0-01201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0030.

F2.23 *BSC 2007. *Wet Handling Facility Chilled Water System Piping & Instrument. Diagram.* 050-M60-PSC0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070925.0006.

F2.24 BSC 2007. *Wet Handling Facility Composite Vent Flow Diagram HVAC Electrical & Battery Rooms.* 050-M50-VCT0-00301-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0016.

F2.25 BSC 2007. *Wet Handling Facility Composite Vent Flow Diagram HVAC Supply & ITS Exhaust.* 050-M50-VC00-00101-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0001.

F2.26 *BSC 2008. *Wet Handling Facility Composite Vent Flow Diagram Non-Confinement HVAC Trans Vest & Support Areas.* 050-M50-VNI0-00101-000-00B. Las Vegas, Nevada. Bechtel SAIC Company. ACC: ENG.20080122.0003.

F2.27 *BSC 2008. *Wet Handling Facility Composite Vent Flow Diagram Non-ITS HVAC Electrical, Transportation Cask & Maintenance.* 050-M50-VCT0-00201-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0001.

F2.28 *BSC 2007. *Wet Handling Facility Composite Vent Flow Diagram Tertiary Confinement Non-ITS HVAC Supply & Exhaust System.* 050-M50-VCT0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0002.

F2.29 BSC 2008. *Wet Handling Facility Confinement ITS Battery Room Exhaust System – Train A Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00302-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0018.

F2.30 BSC 2008. *Wet Handling Facility Confinement ITS Battery Room Exhaust System – Train B Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00304-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0019.

F2.31 *BSC 2007. *Wet Handling Facility Confinement ITS Electrical Room HVAC System – Train A Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00301-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0001.

F2.32 *BSC 2007. *Wet Handling Facility Confinement ITS Electrical Room HVAC System – Train B Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00303-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0003.

F2.33 *BSC 2008. *Wet Handling Facility Confinement Maintenance Room HVAC System Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00105-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0002.

F2.34 *BSC 2008. *Wet Handling Facility Confinement Non-ITS Battery Room Exhaust System Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00203-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0017.

F2.35 *BSC 2007. *Wet Handling Facility Confinement Transportation Cask Vestibule HVAC System Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00106-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0013.

F2.36 BSC 2007. *Wet Handling Facility-Electrical Equipment Space Requirement Calculation*. 050-E2C-EE00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071214.0011.

F2.37 BSC 2007. *Wet Handling Facility Electrical Load Summary Calculation*. 050-E8C-EE00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0010.

F2.38 BSC 2007. *Wet Handling Facility General Arrangement Ground Floor Plan*. 050-P10-WH00-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0032.

F2.39 BSC 2007. *Wet Handling Facility General Arrangement Plan Below +40'-0"*. 050-P10-WH00-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0033.

F2.40 BSC 2007. *Wet Handling Facility General Arrangement Plan Below E: +93'-0"*. 050-P10-WH00-00105-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0035.

F2.41 BSC 2007. *Wet Handling Facility General Arrangement Second Floor Plan*. 050-P10-WH00-00104-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071206.0034.

F2.42 *BSC 2007. *Wet Handling Facility Hot Water System – Piping & Instrument Diagram.* 050-M60-PSH0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070924.0019.

F2.43 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System – Train A Ventilation & Instrumentation Diagram.* 050-M80-VC00-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0014.

F2.44 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System – Train B Ventilation & Instrumentation Diagram.* 050-M80-VC00-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0015.

F2.45 *BSC 2008. *Wet Handling Facility ITS Train "A" Electrical Room Equipment Layout.* 050-E4K-EEE0-00101-000 Rev 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061114.0002.

F2.46 *BSC 2008. *Wet Handling Facility ITS Train "B" Electrical Room Equipment Layout.* 050-E4K-EEE0-00201-000. Rev. 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061114.0003.

F2.47 BSC 2007. *Wet Handling Facility ITS UPS 050-EEU0-UJX-00001 Train A Single Line Diagram*. 050-E10-EEU0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0032.

F2.48 BSC 2007. *Wet Handling Facility ITS UPS 050-EEU0-UJX-00002 Train B Single Line Diagram*. 050-E10-EEU0-00201-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0033.

F2.49 *BSC 2008. *Wet Handling Facility Non-Confinement 2nd Floor Air Distribution System Ventilation & Instrumentation Diagram.* 050-M80-VNI0-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0007.

F2.50 *BSC 2008. *Wet Handling Facility Non-Confinement HVAC Supply System Ventilation & Instrumentation Diagram.* 050-M80-VNI0-00101-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0005.

F2.51 *BSC 2008. *Wet Handling Facility Non-Confinement Site Transp. Vestibule HVAC System Ventilation & Instrumentation Diagram.* 050-M80-VNI0-00104-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0008.

F2.52 *BSC 2008. *Wet Handling Facility Non-ITS Confinement Areas HEPA Exhaust System Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080109.0016.

F2.53 *BSC 2007. *Wet Handling Facility Non-ITS Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram.* 050-M80-VC00-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0004.

F2.54 *BSC 2007. *Wet Handling Facility Non-ITS Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram.* 050-M80-VCT0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0008.

F2.55 *BSC 2006. *Wet Handling Facility Normal Electrical Room Equipment Layout*. 050-E4K-EEN0-00100-000. REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061114.0004.

F2.56 BSC 2007. *Wet Handling Facility Pool Plan and Sections D, H, J*. 050-P10-WH00-00107-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ENG.20071206.0037.

F2.57 *BSC 2007. *Wet Handling Facility Pool Water Treatment and Cooling System Piping & Instrument. Diagram.* 050-M60-PW00-00101-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0006.

F2.58 *BSC 2007. *Wet Handling Facility Pool Water Treatment System Train A Piping & Instrument. Diagram.* 050-M60-PW00-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0007.

F2.59 *BSC 2007. *Wet Handling Facility Pool Water Treatment System Train B Piping & Instrument. Diagram.* 050-M60-PW00-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0008.

F2.60 *BSC 2007. *Wet Handling Facility Pool Water Treatment System Train C Piping & Instrument. Diagram.* 050-M60-PW00-00104-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0009.

F2.61 *BSC 2007. *Wet Handling Facility Transportation Cask/DPC/STC Cavity Gas Sampling System Piping & Instrument. Diagram.* 050-M60-MRE0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070328.0007.

F2.62 *BSC 2007. *Wet Handling Facility UPS 050-EEP0-UJX-00001 Single Line Diagram*. 050-E10-EEP0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071116.0031.

F2.63 *EPRI (Electric Power Research Institute) and NRC (Nuclear Regulatory Commission) 2005. *Detailed Methodology*. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI TR-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0062.

F2.64 *EPRI and NRC 2005. *Summary & Overview*. Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0061.

F2.65 *NFPA 2007. *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction, 1980-1998*. Quincy, Massachusetts: National Fire Protection Association. TIC: 259983.

F2.66 *SAIC (Science Applications International Corporation) 2002. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*. SAIC-01/2650. Abingdon, Maryland: Science Applications International Corporation, March 2002. ACC: MOL.20080115.0138.

F2.67 *Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. Ph.D. dissertation. Espoo, Finland: VTT Technical Research Centre of Finland. TIC: 259928.

F2.68 *Winkler, R. L., and Hays, W. L. 1975. *Statistics: Probability, Inference, and Decision*., Series in Quantitative Methods for Decision Making. 2nd Edition. Winkler, R.L., ed. New York, New York: Holt, Rinehart, and Winston. TIC:259976. ISBN-10: 0030140110.

F3 BOUNDARY CONDITIONS

F3.1 INTRODUCTION

The general boundary conditions used during the analysis of fire vulnerabilities and fire model development are clearly stated and documented. In general, the boundary conditions are compatible with those usually applied to fire events. The principal boundary conditions for the fire analysis are listed in the following sections:

F3.2 PLANT OPERATIONAL STATE

Initial state of the facility is normal with each system operating within its limiting condition of operation limits.

F3.3 CREDIT FOR AUTOMATIC FIRE SUPPRESSION SYSTEMS

The automatic fire suppression systems, although they will be designed to meet all requirements and standards for fire suppression systems in nuclear facilities, are considered non-(important to safety) ITS and thus no credit is taken for their operation.

F3.4 NUMBER OF FIRE EVENT TO OCCUR

The facility is analyzed to respond to one fire event at a given time. Additional fire events, as a result of independent causes or of re-ignition once a fire is extinguished, are not considered.

F3.5 IGNITION SOURCE COUNTING

Ignition sources are counted in accordance with applicable counting guidance contained in NUREG/CR-6850 (*Detailed Methodology.* Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* EPRI TR-1011989 and NUREG/CR-6850 (Ref. F2.64) and *Summary & Overview.* Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI-1011989 and NUREG/CR-6850 (Ref. F2.63)).

F3.6 FIRE CABLE AND CIRCUIT FAILURE ANALYSIS

Unlike nuclear power plants, which depend on the continued operation of equipment to prevent fuel damage, the YMP facilities cease operating on loss of power or control. Therefore, fire damage in rooms that do not contain waste cannot result in an increased level of radiological exposure. Cable and circuit analysis in these rooms is not required.

F3.7 HEATING, VENTILATION, AND AIR CONDITIONING FIRE ANALYSIS

Heating, ventilation, and air conditioning (HVAC) is not relied upon to mitigate potential releases associated with large fire event sequences. In recognition of a large amount of fire generated, non-radiological particulates could render the HVAC filters ineffective. HVAC can be credited for localized fires unless HVAC control or power circuits are present in the area of the fire.

F3.8 NO OTHER SIMULTANEOUS INITIATING EVENTS

It is standard practice to not consider the occurrence of other initiating events (i.e., human-induced and naturally occurring) during the time span of an event sequence because 1) the probability of two simultaneous initiating events within the time span is small and 2) each initiating event will cease operations of the waste handling facility, which further reduces the conditional probability of the occurrence of a second initiating event, given the first has occurred.

F3.9 DATA COLLECTION SCOPE

The fire ignition data collection and analysis are performed for locations relevant to waste handling in the facilities.

F3.10 COMPONENT FAILURE MODES

The failure mode of a structure, system, or component, affected by a fire, is the most severe with respect to consequences. For example, the failure mode for a canister could be the overpressurization of a reduced strength canister.

F3.11 COMPONENT FAILURE PROBABILITY

Fires large enough to fail waste containment components will be large enough to fail all active components in the same room. Active components fail in a de-energized state for such fires.

F3.12 INTERNAL EVENTS PCSA MODEL

To implement the systems analysis guidance contained herein, the fire PCSA team uses the internal events PCSA model, which is developed concurrently with the fire PCSA. This internal events PCSA is used as the basis for the fire PCSA. The internal events PCSA is in general conformance with the American Society of Mechanical Engineers Probabilistic Risk Assessment standard (Ref. F2.3).

F4 ANALYSIS METHOD

F4.1 INTRODUCTION

Nuclear power plant fire risk assessment techniques, as discussed in the following sections, have limited applicability to facilities such as the Wet Handling Facility (WHF) or other facilities in the geologic repository operations area (GROA). The general methodological basis of this analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*, (Ref. F2.66) which are similar to those in the GROA in that these facilities are handling and disposal facilities for highly hazardous materials. This is a "data based" approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the YMP waste handling facilities. To the extent applicable to a non-reactor facility, NUREG/CR-6850, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.64 and Ref. F2.63) is also considered in the development of this analysis method. The method complies with the applicable requirements of the American Nuclear Society (ANS) fire PRA standard (Ref. F2.2) that is relevant to a non-reactor facility. Many of the definitions, modeling approximations, and requirements of these documents were used to develop this document.

F4.2 IDENTIFICATION OF INITIATING EVENTS

Current techniques in fire risk assessment for nuclear power plants focus on fire that can damage electrical and control circuits or impact other equipment that can compromise process and safety systems. This type of approach is not generally applicable to YMP because loss of electric power is a safe state except for the need for HVAC after a release of radionuclides. In general, when systems are affected by fire, they cease to function. While at a nuclear power plant this is of concern, at YMP this means that fuel handling stops and initiating events capable of producing elevated levels of radioactivity are essentially unrealizable. While it is theoretically possible that a fire could inadvertently result in a drop of a cask or canister, it is difficult (if not impossible) to identify any mechanisms by which this would occur due to fire that would not be much more likely to occur by other means. Of much greater concern at YMP is the potential for a fire to directly affect the waste containers and cause a breach that would result in a release. The fire analysis, therefore, focused on the potential for a fire to directly affect the waste containers and cause a breach that would result in a release, rather than analyzing fires that would remove power from fuel handling systems. After a release of radionuclides, the HVAC system, with its high-efficiency particulate air (HEPA) filtration, aids in the abatement of radioactivity that is released from buildings. However, the occurrence of fires tends to significantly reduce the effectiveness of HEPA filtration and the fire event sequence analysis, therefore, does not rely on this system Consideration is given both to fires that start in rooms

containing waste and fires that start in other rooms and propagate to where the waste is located. The steps of this process are as follows:

F4.2.1 Identify Fire-Rated Barriers and Designate Fire Zones

The facility is broken into fire zones based on the location of fire-rated barriers. The rating of the barriers is not significant to the methodology, so all rated barriers are considered. In order for a fire zone to exist, the penetrations, doorways, and ducts must also be limited to the perimeter of the zone. Note that a floor is always considered to be a fire barrier as long as it is solid. Zones are identified by a number, determined by the analyst, and will consist of one or more rooms.

F4.2.2 Identify the Rooms Where Waste can be Present

Each room where waste can be present, even if only for a brief time, is listed. The first set of fire initiating events to be considered in the PCSA is fires that affect each of these rooms, but do not affect other rooms that could contain waste.

F4.2.3 Define Local Initiating Events

Fire ignition occurrences are identified for each room within a fire zone. The total occurrences of a fire within a room containing a waste form is composed of the occurrences of ignitions in that room plus the occurrences of ignitions in surrounding rooms, within the fire zone, which propagate across room boundaries to the room containing the waste form. The locations of fire initiating events were identified in the master logic diagrams.

F4.2.4 Define Large Fire Initiating Events

Traditional fire risk studies for nuclear power plants have tended to ignore large fires, arguing that the fire barriers in place will prevent such occurrences. However, actual observed historical data shows that large fires in buildings occur. Large fires are defined for this study as those that spread to encompass the entire building. This is recognized in the latest fire risk guidance from Nuclear Regulatory Commission (NRC) and Electrical Power Research Institute (EPRI).[1] There, potential large fire initiating events are identified. The general approach is as follows:

In the YMP facilities, waste forms, except during the short time they are being lifted by a canister transfer machine (CTM), are on the ground floor. Continuing with the focus on rooms that contain waste forms, large fires may be divided two ways. One is associated with fires that start on the ground floor and spread to the entire building. The other is a fire that starts anywhere else in the building and spreads to the entire building.

As a practical analysis technique, any fire that spreads out of a fire area is considered a large fire.

[1] See, for example, Ref. F2.63 and F2.64, Volume 2, Section 11.5.4.

F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY

The quantification of initiating event frequency involves three steps. First, the overall frequency of fire ignition for the facility is determined, then that frequency is allocated to the individual room in the facility based on the number and types of ignition sources in the rooms. Types of ignition sources are characterized in general terms such as mechanical, electrical, combustible liquid. Finally, propagation probabilities are applied to determine the overall frequency that a fire reaches the area of the waste. Quantification uses data from the following sources for equipment ignition frequencies and conditional probabilities of propagation:

Summary & Overview. Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* (Ref. F2.64)

Detailed Methodology. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* (Ref. F2.63)

Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Facilities: 1988 - 1997 Unallocated Annual Averages and Narratives. (Ref. F2.1)

Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction, 1980-1998. (Ref. F2.65)

Chemical Agent Disposal Facility Fire Hazard Assessment Methodology. (Ref. F2.66)

Utilisation of Statistics to Assess Fire Risks in Buildings. (Ref. F2.67)

F4.3.1 Determine the Overall Facility Fire Frequency

There is insufficient data available regarding the total frequency of fires in facilities comparable to YMP. NUREG/CR-6850 [Ref. F2.64 and Ref. F2.63] provides an overall frequency for a typical nuclear power plant, but these are much larger and complex than the YMP facilities. Therefore, it has been decided to use a more generic fire ignition frequency approach that relates building size to total fire frequency for various broad categories of facilities [Ref. F2.67]. This approach applies the following equation to overall fire ignition frequency.

Determine the Fire Frequency per Unit Area – The frequency per unit area is expressed by the following equation:

$$f_m(A) = c_1 A^r + c_2 A^s \qquad \text{(Eq. F-1)}$$

where:

f_m is the fire ignition frequency per m^2 / yr

A is the floor area (in m^2)

c_1, c_2, r, and s are coefficients that were determined from historical data observations for different types of facilities.

For industrial buildings, the parameter values are as follows:

$$c_1 = 3 \times 10^{-4}; c_2 = 5 \times 10^{-6}; r = -0.61; \text{ and } s = -0.05$$

Equation F-1 relates the frequency per unit area to the total area of the facility. This correlation was determined from the historical data, which showed that total fire frequency was not linearly related to the size of the facility. Rather, the frequency per unit area was affected by the size of the facility, and the larger the facility the lower the frequency per unit area.

Determine the Total Fire Frequency for the Facility – The total frequency of fire ignition for the building is thus represented by the following equation:

$$f_{\text{fire}} = f_{\text{m}}(A) * A \qquad \text{(Eq. F-2)}$$

F4.3.2 Determine the Fire Ignition Frequency in Each Room

The approach to allocating the fire ignition frequency is based on the two approaches used in References F2.62, F2.63, and F2.66. Both of these approaches determine the fraction of the total facility ignition frequency associated with various categories of equipment (i.e., ignition source category), then determine a facility-specific ignition frequency for each piece of equipment in each category, and then determine the total ignition frequency in the room based on the ignition source population in the room.

F4.3.2.1 Fraction of Fire Ignition Frequency Associated with Each Ignition Source Category

References F2.62 and F2.63 have data for these fractions for nuclear power plants, and Reference F2.66 has data for these frequencies for chemical process plants. Neither of these data sets is the best for the facilities at YMP. Therefore, the National Fire Protection Association (NFPA) was requested to provide an analysis (Ref. F2.65) of the data in their proprietary database on the distribution of fires by equipment type in all nuclear facilities of non-combustible construction. NFPA distinguishes between a large number of equipment types that can cause ignition of a fire. There is an insufficient amount of data to justify retaining this number of equipment types, so the equipment types were consolidated into a set of ignition source categories. These categories are defined in Appendix F.I.

Using the data by category, an analysis is performed to determine the fraction of fires that are caused by each category. That analysis is documented in Appendix F.II.

The total fire ignition frequency from Section F4.3.1 is multiplied by each of these factors to determine the total fire ignition frequency due to each equipment type. For example, the total ignition frequency due to electrical equipment for a given facility is:

$$f_{\text{elec-all}} = f_{\text{fire}} * 0.086 \qquad \text{(Eq. F-3)}$$

F4.3.2.2 Individual Ignition Source Fire Ignition Frequency

The next step is to determine the fire ignition frequency from each piece of equipment in each category. As is done in References F2.62 and F2.63, and F2.66, divide the frequency contribution for each equipment type by the total number of pieces of equipment in the facility. For example, take the case following from the above example for the frequency of fire ignition from electrical equipment. If there are 50 pieces of electrical equipment in the facility, the ignition frequency for each piece of equipment is:

$$f_{\text{elec-each}} = f_{\text{elec-all}} / 50 \qquad \text{(Eq. F-4)}$$

For the case of the category "no equipment involved" the ignition frequency is per unit area, so the total for this category is divided by the total floor area of the facility (which was already determined in Section F4.3.1).

F4.3.2.3 Allocation of Fire Ignition Frequency to Each Room

The final step is to use the per equipment values to allocate fire frequency to each room. This is done by counting the number of ignition sources of each type contained in each room, multiplying by the ignition frequency for each ignition source type, and summing across all types. For example, if Room 1 has six pieces of electrical equipment, then the ignition frequency in that room due to electrical equipment is:

$$f_{\text{elec-1}} = f_{\text{elec-each}} \times 6 \qquad \text{(Eq. F-5)}$$

Doing this for each ignition source type (including multiplying the "no equipment involved" per unit area by the floor area of the room) and summing them together yields the total fire ignition frequency for the room.

$$f_1 = f_{\text{elec-1}} + f_{\text{hvac-1}} + f_{\ldots\text{-1}} \qquad \text{(Eq. F-6)}$$

F4.4 DETERMINE INITIATING EVENT FREQUENCY

The definition of each initiating event includes the implicit condition that the fire actually threatens a target that contains radioactive material. Therefore, for each initiating event, the initiating event frequency considers two aspects; the fraction of time there is a waste container in the room, and the probability a fire propagates to that waste container.

F4.4.1 Probability of Presence of a Target

The probability of the presence of a target waste form is the fraction of time that the waste form(s) is in the area affected by the fire (e.g., for a room fire it is the fraction of time a waste form is in the room). For use in initiating event frequency equations, the probability is represented as follows:

P_{wri} = probability that a particular waste form is in room i during the preclosure period

P_{wz} = probability that a particular waste form is in zone i during the preclosure period

P_{wfi} = probability that a particular waste form is on floor i during the preclosure period

P_{wb} = probability that a particular waste form is in the building during the preclosure period.

The specific phrasing should be noted. This probability pertains to each individual waste form (i.e., one of the approximately 11,000 waste forms that will be handled at YMP). For example, if each waste form that passes through the WHF spends 60 minutes in the Cask Preparation Area, the probability that it is present when a fire occurs is 60 min/(50 yrs × 8760 hrs/yr × 60 min/hr). This is used to correct the final initiating event frequency for fires (normally expressed as per year) to be per operation over the preclosure period so that it is equivalent to the other internal initiating events (e.g., drops) and can be multiplied by the number of operations in same manner.

F4.4.2 Probability of Propagation to a Target

Of key interest for assessing the fire risk, is the extent to which fires that start in a "benign" area can spread to sensitive areas (i.e., areas where nuclear waste is present). The likelihood of fire propagation within the building is strongly dependent on the building construction and the presence of automatic fire suppression systems.

Both probabilities of exceedance and conditional probabilities were determined. The probabilities of exceedance are the probabilities that a fire propagates up to a specified limit or beyond. The conditional probabilities are probabilities that a fire spreads to a specified limit.

Probabilities of exceedance are not independent, but rather represent the total probability that a fire spreads up to the specified limit or beyond. These values are provided because, for many fire sequences, there is only be one case of interest, (i.e., there is only one target of concern, and once the fire reaches that target, the fact that the fire may propagate even further does not change the outcome of the sequence in terms of release). For example, this value could be applied to a case where a fire that spreads throughout a room affects the waste form in that room, and there are no additional waste forms in adjacent rooms or fire zones.

Conditional probabilities are independent, as they represent the probability that a fire spreads to precisely the specified limit. These values are provided to address those cases where the extent of propagation will define the number of targets involved in the fire. For example, these values would be applied when a fire that spreads throughout a room affects a waste form in that room; if it spreads to adjacent rooms, however, additional forms would be involved.

There are two types of propagation that are considered: propagation within a room and propagation between rooms.

F4.4.2.1 Fire Propagation Within Rooms

An important consideration in the fire risk assessment is propagation within a given room. This scenario is referred to as "in-room propagation." Propagation within the room is important for fires initiated in a room where waste is present. In this case, the question is whether the fire, which can ignite wherever there is an ignition source in the room, reaches the area within the room in which the waste is located.

This section provides a table with the in-room propagation values for the cases with and without automatic fire suppression systems functioning. To use this table to determine whether the fire spreads sufficiently to threaten waste forms, it is necessary to consider where the fire occurs in the room of interest. The steps in this process are as follows:

- Determine the distribution of the ignition sources (identified under Section F4.3.2.3) within the room by counting the total number of potential ignition sources that are "at," "near," or "far from" the target waste form.[2]

- Calculate the fraction of ignition sources "at," "near," and "far from" the target waste form by dividing the number at each location by the total in the room.

- Calculate the frequency of the fire reaching the waste form using the following equation:

$$f_{ier\text{-}i} = P_{wri}\,[f_i\,(FR_a + (FR_n \times (P_{pc} + P_{rc})) + (FR_f \times P_{rc}))] \qquad \text{(Eq.F-7)}$$

where:

f_i = frequency of ignition, i-th room

FR_a = fraction of ignition sources at the waste form

FR_n = fraction of ignition sources near the waste form

P_{pc} = conditional probability for fire confined to part of room of origin

FR_f = fraction of ignition sources far from the waste form

P_{rc} = conditional probability for confined to room of origin.

The values for P in the previous equation were developed from the analysis performed by NFPA (Ref. F2.65). The derivation of the values is provided in Appendix F.II for two cases (i.e., automatic fire suppression available and automatic fire suppression unavailable). The frequency f_i is the sum of frequencies of ignition of all ignition sources in the room. The fraction of ignition sources at, near, and far from the waste form was developed from equipment layout drawings such as the following:

Wet Handling Facility Normal Electrical Room Equipment Layout. (Ref. F2.55)

Wet Handling Facility General Arrangement Ground Floor Plan. (Ref. F2.38)

F4.4.2.2 Fire Propagation Beyond Rooms

This section provides propagation probabilities for fires spreading beyond the room in which they start. This type of propagation will be referred to as "ex-room propagation."

---

[2] In the context of this method, an ignition source within a few feet of the waste source would be "at" the source, whereas an ignition source beyond this distance, but within a few yards of the waste source would be "near" the source. Ignition sources more that a few yards distant would be "far from" the waste source. This definition coordinates with the fire response model given in Attachment D.

This section provides a table with the ex-room propagation values for the cases with and without automatic fire suppression systems functioning. To use this table to determine whether the fire spreads sufficiently to threaten waste forms, it is necessary to consider the various rooms where the fire could start and spread to the extent defined by the initiating event. The steps in this process are as follows:

- For each initiating event, identify all of the rooms within the area defined by the initiating event. For example, for a fire involving a specific fire zone, list all the rooms in that zone. For a fire involving the entire floor, list all the rooms on the floor. For a fire involving the entire building, list all the rooms in the building.

- For each room, calculate the probability that a fire that starts within the room is not confined to the next smaller fire initiating event but is confined to less than the definition of the next largest initiating event by multiplying the ignition frequency for the room by the conditional probability (or sum of conditional probabilities) that the fire spreads at least as far as defined, but no further. For example, for a fire involving a floor where there is also an initiating event for a fire involving a zone on the floor and an initiating event involving the entire building (multiple floors or beyond), the equation is:

$$f_{ief\text{-}fj\text{-}ri} = f_i \times P_{fc} \qquad \text{(Eq. F-8)}$$

where:

$f_{ief\text{-}fj\text{-}ri}$ = frequency of fire in zone j starting in room *i*

f_i = frequency of ignition, *i-th* room

P_{fc} = conditional probability for fire confined to the floor of origin.

Similarly, for a fire involving a floor where there is an initiating event for a fire in a zone on the floor and no specific initiating event for a fire involving the entire building the equation is:

$$f_{ief+\text{-}ri} = f_i \times (P_{fc} + P_{bc} + P_{b+c}) \qquad \text{(Eq. F-9)}$$

where:

$f_{ief+\text{-}ri}$ = frequency of fire involving an entire floor or greater starting in room i

f_i = frequency of ignition, *i-th* room

P_{fc} = conditional probability for fire confined to floor of origin

P_{bc} = conditional probability for fire confined to building of origin

P_{b+c} = conditional probability for fire extending beyond building of origin[3].

[3] Note that the definition of a fire extending beyond the building of origin does not imply that the fire crosses some distance to affect other buildings or objects, but rather that the fire (i.e., flame damage) affects the outside surfaces of the building and items attached thereto.

The total fire frequency of the defined severity is the sum across all rooms relevant to the initiating event, as discussed above.

F4.4.3 Initiating Event Frequency

The final initiating event frequency is determined by multiplying the frequency of the fire reaching the waste form (in occurrences per year) times the probability that a waste form is present (fraction of time per waste form) times 50 (years in the preclosure period). This multiplication yields the initiating event frequency for a fire of a specific severity affecting a waste form, per waste form handled, over the preclosure period.

F5 ANALYSIS

F5.1 INTRODUCTION

Fire initiating event frequencies have been calculated for each initiating event identified for the WHF. This section details the analysis performed to determine these frequencies, using the methodology documented in Section F4. The discussion of the analysis below presupposes that the reader has developed a thorough understanding of the details of that methodology, as those details are not repeated in this section. Note that the tables presented in this section, unless otherwise noted, are images of the actual spreadsheets used to perform the calculations. Therefore, there are no typographical errors in the translation of the results of the calculations into this report. The spreadsheet cells are color-coded to aid the analyst. Green numbers indicate values that are input by the analyst specific to the facility. Black numbers result from "off-line" calculations performed for this study. That is, they are facility-specific parameters whose values were determined as part of this analysis, but are not directly linked to the cell (i.e., they needed to be entered by the analyst). The source for these values is indicated in the text description of the spreadsheet. Orange numbers are values based on the analysis of operational experience (e.g., NFPA data), and should generally not be changed unless the analysis of operational experience changes or is updated. Red numbers are calculated values and should never be changed by the analyst. Green shaded cells are parameters that are assigned distributions that are used for the Crystal Ball Monte Carlo simulation runs discussed in Section F5.8. The aqua shaded cells are the final initiating event frequencies. The values shown in the cells are the baseline, point estimate values. The Monte Carlo simulation runs convert these values into distributions for use in the event sequence quantification.

F5.2 INITIATING EVENT FREQUENCIES

Fire ignition frequencies are based upon the total floor area of the building. Thus, the assessment of the area of each room of the WHF is the first step in obtaining initiating event frequencies. Table F5.2-1 shows the calculations that were performed to identify individual room areas, total ignition frequency, and uncertainty distributions.

F5.2.1 Room Area

Dimensions for room area calculations were obtained from the following WHF general layout drawings:

Wet Handling Facility General Arrangement Ground Floor Plan. (Ref. F2.38)

Wet Handling Facility General Arrangement Plan Below +40'-0". (Ref. F2.39)

Wet Handling Facility General Arrangement Plan Below E: +93'-0". (Ref. F2.40)

Wet Handling Facility General Arrangement Second Floor Plan. (Ref. F2.41)

Wet Handling Facility Pool Plan and Sections D, H, J. (Ref. F2.56)

In some cases, the dimension intervals shown on the general arrangement drawings matched the boundaries of the rooms. Where this was the case, these values were used to define the dimensions of the rooms. In cases where the dimension intervals did not accurately represent a room, the drawing scale and a straightedge was utilized to determine the dimensions. The length and width figures obtained were entered into the L1 (ft) and L2 (ft) columns of Table F5.2-1 and multiplied to produce the area in square feet. Rooms 1001, 1016, 1028, 1036, 2004, and 2025 occupy two floors of building space. The area obtained for these rooms was doubled to account for this. Rooms 1001, 10032, 1218A, 2005A, 2034, and 2203 are not of a standard rectangular shape whose area can be calculated by a single length and width. Thus, these rooms were divided into two to three rectangles, each with a determined length and width. Addition of the area of these rectangles provides the total room area. Rooms 1002, 1009, 1013, 1018, 1019, and 2012 contain smaller room(s) within themselves. To account for this, the red text indicates a reference to the cells that contain the dimensions of the smaller room(s), the area of which is subtracted from the area of the room containing it. All areas calculated in square feet were multiplied by 0.093 to obtain the area in square meters, because Equation F-1 is based in square meters.

F5.2.2 Building Ignition Frequency

Ignition frequency calculations are presented at the bottom of Table F5.2-1, and begin with the total area calculation. This is obtained by summing the areas (in square meters) of all rooms in the building. The ignition frequency per square meter per year line implements Equation F-1. The ignition frequency per year line implements Equation F-2. The ignition frequency over the 50 year period is obtained by multiplying the latter value by 50. As can be seen from the table, the expected number of ignition events over the preclosure period is approximately four.

The values shown are the baseline mean values for ignition frequency. An uncertainty analysis was performed on the results of Equation F-1 for the use of Crystal Ball software to run Monte Carlo simulations to obtain fire initiating event frequency distributions. The geometric mean and 97.5% values of the resulting distribution for Equation F-1 are shown on the table. Refer to Appendix F.III for the calculations performed to develop the uncertainty distribution.

F5.3 IGNITION SOURCE FREQUENCY

As discussed in Section F4.3.2.1, an industrial building fire can begin as the result of numerous types of ignition sources, which have been grouped into nine categories:

- Electrical
- HVAC
- Mechanical equipment
- Heat generating equipment
- Torches, welders, and burners
- Internal combustion engines
- Office/kitchen equipment
- Portable equipment
- No equipment involved.

Each category has a fraction representing the probability that, given an ignition, that category is the source of the ignition. The mean values of these fractions are shown in the column labeled ”category fraction” in Table F5.3-1. The derivation of these values is discussed in Appendix F.II. The column labeled “category frequency” implements the generic form of Equation F-3 to determine the mean ignition frequency associated with each ignition source. The next column, category population, contains the total number of ignition sources in each category in the facility. This is either the actual count of sources, a weighted point score of sources, or (for the case of “no equipment involved”) the total floor area of the facility. The source of the count or score is presented in the next section. The floor area is taken from Table F5.2-1, fourth row from the bottom. The fifth column uses the previous two columns to implement Equation F-4 to determine the frequency per ignition source unit (i.e., per ignition source, per ignition source weighted point, or per square meter of floor area). These values are used in the next section to allocate fire ignition frequency to each room in the facility.

As stated previously, these values are mean values. The right hand group of columns is used by Crystal Ball to apply an uncertainty distribution to each of the category fraction values for the purpose of developing uncertainty distributions on initiating event frequency. The mean fraction, 97.5% value, and 97.5^{th} percentile add columns show the parameters of these distributions. The development of all of the values is detailed in Appendix F.II. When Crystal Ball is run, it creates a sampled value for each fraction in the sampled value column. The spreadsheet then determines a normalized value by first assuring that each sampled value is not negative (minimum value of zero) and then normalizing the values so that the sum is always equal to one. The normalized value for each trial then replaces the category fraction value in the calculation. These probabilities must always add to one, as the groupings include all possible sources of ignition.

F5.4 IGNITION SOURCE DISTRIBUTION (EQUIPMENT LIST)

Compiling an initiating event frequency for the WHF is dependant on identifying many characteristics of the building, to include ignition sources. Ignition sources are defined as items that exist in the rooms of the building that have the potential to contribute to the initiation and/or propagation of a fire. These sources are grouped into the following categories:

- Electrical equipment
- HVAC equipment
- Mechanical process equipment
- Heat-generating process equipment
- Torches, welders, and burners
- Internal combustion engines
- Office and kitchen equipment
- Portable and special equipment.

Once the grouping for a source is determined, it is assigned a count (points)–a number which specifies the significance of the source by its contribution to fire ignition. Counts are integral to the calculations, as the total count for each category and room are multiplied by the ignition source frequency and summed to obtain the room ignition frequency. Table F5.4-1 shows the results of the ignition source distribution assessment for the WHF. The red numbers on this table highlight the actual count used, so as to make identification of the equipment count values easy to pick out from the other equipment identification information provided. Pieces of equipment that are in the room in question, but they do not count as ignition sources per the counting rules are shown in grey text. The following sections describe how the equipment was identified, categorized, and counted for the building.

F5.4.1 Electrical Equipment

Information regarding electrical equipment was gathered solely from the following single line diagrams and electrical room layout drawings.

Wet Handling Facility 480V Load Center 050-EEN0-LC-00001 Single Line Diagram. (Ref. F2.7)

Wet Handling Facility 480V Load Center 050-EEN0-LC-00002 Single Line Diagram. (Ref. F2.8)

Wet Handling Facility 480V Load Center 050-EEN0-LC-00003 Single Line Diagram. (Ref. F2.9)

Wet Handling Facility 480V ITS Load Center 050-EEE0-LC-00001 Train A Single Line Diagram. (Ref. F2.10)

Wet Handling Facility 480V Load Center 050-EEN0-LC-00002 Single Line Diagram. (Ref. F2.11)

Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00001 Train A Single Line Diagram. (Ref. F2.12)

Wet Handling Facility 480V ITS MCC 050-EEE0-MCC-00002 Train B Single Line Diagram. (Ref. F2.13)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00001 Single Line Diagram. (Ref. F2.14)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00002 Single Line Diagram. (Ref. F2.15)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00003 Single Line Diagram. (Ref. F2.16)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00004 Single Line Diagram. (Ref. F2.17)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00005 Single Line Diagram. (Ref. F2.18)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00006 Single Line Diagram. (Ref. F2.19)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00007 Single Line Diagram. (Ref. F2.20)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00008 Single Line Diagram. (Ref. F2.21)

Wet Handling Facility 480V MCC 050-EEN0-MCC-00009 Single Line Diagram. (Ref. F2.22)

Wet Handling Facility-Electrical Equipment Space Requirement Calculation. (Ref. F2.36)

Wet Handling Facility ITS Train A Electrical Room Equipment Layout. (Ref. F2.45)

Wet Handling Facility ITS Train B Electrical Room Equipment Layout. (Ref. F2.46)

Wet Handling Facility ITS UPS 050-EEU0-UJX-00001 Train A Single Line Diagram. (Ref. F2.47)

Wet Handling Facility ITS UPS 050-EEU0-UJX-00002 Train B Single Line Diagram. (Ref. F2.48)

Wet Handling Facility Normal Electrical Room Equipment Layout. (Ref. F2.55)

Wet Handling Facility UPS 050-EEP0-UJX-00001 Single Line Diagram. (Ref. F2.62)

The electrical equipment category consists of computers, equipment racks, load centers, motor control centers (MCCs), uninterruptable power supply, transformers, lighting panels, digital control and management information system, programmable logic controller panels, batteries, and electrical panels. In general, each piece of electrical equipment constitutes a single ignition source and, therefore, has a count of one. However, MCCs, load centers, and equipment racks are assigned a count based on the total number of active vertical cabinets making up the overall unit. Every vertical cabinet in an equipment rack is treated as active. In the case of MCCs and load centers, a cabinet is considered active if the single line diagram shows that a load is attached (i.e., unused circuit breakers are not counted).

F5.4.2 HVAC Equipment

HVAC equipment locations and horsepower were obtained from the following facility general layout drawings and HVAC equipment lists.

Wet Handling Facility Composite Vent Flow Diagram HVAC Electrical & Battery Rooms. (Ref. F2.24)

Wet Handling Facility Composite Vent Flow Diagram HVAC Supply & ITS Exhaust. (Ref. F2.25)

Wet Handling Facility Composite Vent Flow Diagram Non-Confinement HVAC Trans Vest & Support Areas. (Ref. F2.26)

Wet Handling Facility Composite Vent Flow Diagram Non- ITS HVAC Electrical, Transportation Cask & Maintenance. (Ref. F2.27)

Wet Handling Facility Composite Vent Flow Diagram Tertiary Confinement Non- ITS HVAC Supply & Exhaust System. (Ref. F2.28)

Wet Handling Facility Confinement ITS Battery Room Exhaust System – Train A Ventilation & Instrumentation Diagram. (Ref. F2.29)

Wet Handling Facility Confinement ITS Battery Room Exhaust System – Train B Ventilation & Instrumentation Diagram. (Ref. F2.30)

Wet Handling Facility Confinement ITS Electrical Room HVAC System – Train A Ventilation & Instrumentation Diagram. (Ref. F2.31)

Wet Handling Facility Confinement ITS Electrical Room HVAC System – Train B Ventilation & Instrumentation Diagram. (Ref. F2.32)

Wet Handling Facility Confinement Maintenance Room HVAC System Ventilation & Instrumentation Diagram. (Ref. F2.33)

Wet Handling Facility Confinement Non-ITS Battery Room Exhaust System Ventilation & Instrumentation Diagram. (Ref. F2.34)

Wet Handling Facility Confinement Transportation Cask Vestibule HVAC System Ventilation & Instrumentation Diagram. (Ref. F2.35)

Wet Handling Facility ITS Confinement Areas HEPA Exhaust System – Train A Ventilation & Instrumentation Diagram. (Ref. F2.43)

Wet Handling Facility ITS Confinement Areas HEPA Exhaust System – Train B Ventilation & Instrumentation Diagram. (Ref. F2.44)

Wet Handling Facility Non-Confinement 2nd Floor Air Distribution System Ventilation & Instrumentation Diagram. (Ref. F2.49)

Wet Handling Facility Non-Confinement HVAC Supply System Ventilation & Instrumentation Diagram. (Ref. F2.50)

Wet Handling Facility Non-Confinement Site Transp. Vestibule HVAC System Ventilation & Instrumentation Diagram. (Ref. F2.51)

Wet Handling Facility Non-ITS Confinement Areas HEPA Exhaust System Ventilation & Instrumentation Diagram. (Ref. F2.52)

Wet Handling Facility Non-ITS Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram. (Ref. F2.53)

Wet Handling Facility Non-ITS Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram. (Ref. F2.54)

HVAC equipment consists of HEPA filters, exhaust fans, air handling units, fan coil units, and sump pumps. Because any motor with a horse power rating of five or more is considered to be an initiator, the number of motors and the horsepower of each motor is determined for all applicable HVAC equipment identified. A piece of equipment containing motors is assigned a count based on the number of motors with a horsepower of five or more. Because HEPA filter units are not applicable to this process, a count of one is assigned for each.

F5.4.3 Mechanical Process Equipment

Information regarding mechanical process equipment locations and horsepower were obtained from the following facility general layout drawings, mechanical equipment lists, and equipment piping and instrument diagram drawings.

CRCF, RF, WHF, and IHF Cask Transfer Trolley Process and Instrumentation Diagram. (Ref. F2.4)

Equipment Motor Horsepower and Electrical Requirements Analysis. (Ref. F2.5)

Wet Handling Facility Chilled Water System Piping & Instrument. Diagram. (Ref. F2.23)

Wet Handling Facility Electrical Load Summary Calculation. (Ref. F2.37)

Wet Handling Facility General Arrangement Ground Floor Plan. (Ref. F2.38)

Wet Handling Facility General Arrangement Plan Below +40'-0". (Ref. F2.39)

Wet Handling Facility General Arrangement Plan Below E: +93'-0". (Ref. F2.40)

Wet Handling Facility General Arrangement Second Floor Plan. (Ref. F2.41)

Wet Handling Facility Hot Water System – Piping & Instrument Diagram. (Ref. F2.42)

Wet Handling Facility Pool Water Treatment and Cooling System Piping & Instrument. Diagram. (Ref. F2.57)

Wet Handling Facility Pool Water Treatment System Train A Piping & Instrument. Diagram. (Ref. F2.58)

Wet Handling Facility Pool Water Treatment System Train B Piping & Instrument. Diagram. (Ref. F2.59)

Wet Handling Facility Pool Water Treatment System Train C Piping & Instrument. Diagram. (Ref. F2.60)

Wet Handling Facility Transportation Cask/DPC/STC Cavity Gas Sampling System Piping & Instrument. Diagram. (Ref. F2.61)

Mechanical process equipment includes most of the motorized equipment that includes cranes, trolleys, doors, and platforms. These pieces of equipment are counted in the method described in Section F5.4.2 (i.e., each motor of 5 horsepower or more contributes a count of one). Because some of the equipment in this category is mobile, and counts are done for each room individually, it was necessary to consider the counts for equipment which can occupy more than one room. To accomplish this task, the amount of time a piece of equipment spends in each room was identified using the process throughput Gantt charts (Ref. F2.6). The cask transfer trolley (CTT) was identified as the only piece of mobile equipment that occupies more than one room.

The total time the CTT spends in the Cask Unloading Room (1008) is calculated from the following procedures (in parentheses) identified in the process throughput:

- Move TAD Canister STC into Cask Unloading Room – 20 minutes (1.5.9)
- Move TAD Canister to Aging Overpack – 138 minutes (5.1)
- Export TAD Canister in Aging Overpack – 299 minutes (1.6)
- Install TAD Canister STC Lid – 20 minutes (1.7.1)
- Open Move TAD Canister STC to Preparation Station #1 – 20 minutes (1.7.2).

The total time the CTT spends in the Cask Preparation Area (1016) is calculated by subtracting the total amount of time the CTT will be in Room 1008 from the total time of the procedure (18,195 minutes).

The time a mobile equipment item spends in each room is utilized to determine the percentage of time the equipment occupies a room, which directly corresponds to the percentage of the total count assigned to that room. This is represented on the equipment list as the residence weighting factor (RWF).

F5.4.4 Heat Generating Process Equipment

This equipment refers to such things as furnaces, dryers and other such equipment except for those associated with the HVAC, which are counted separately as discussed above. There is no equipment for any of the facilities that falls under this category.

F5.4.5 Torches, Welders, and Burners

Welding operations are the only contributors to this category. The assignment of residency in this case is based on the estimated number of hours per year that welding operations are expected to occur in the area. This determination provides a suitable relative weight for apportioning fire ignition caused by welding operations. Portable welding receptacles are provided in various areas of the facility for the purpose of occasional welding of stationary equipment that may show signs of cracking. These receptacles are provided for convenience, and are not expected to see significant use. Each station is estimated to see on the order of five hours of use per year, and so is assigned a score of five points each. The primary maintenance area also contains a welding receptacle (the "primary welding station"), intended to perform all of the maintenance related welding for repair and fabrication that does not require direct work on a stationary piece of equipment (including on components of stationary pieces of equipment that are easily removed). The primary welding station is estimated to be used about 8 hours per week, and so it is assigned a score of 400 points. The WHF also has the transportation, aging, and disposal (TAD) canister welding machine, which has weld end effectors. The number of hours of operation per year for the weld end effectors on the TAD canister welding machine is estimated based on the throughput time-and-motion study and the number of TAD canisters expected to be handled, as follows: (1) The period for preclosure operation of the WHF is 50 years; (2) The welding machine actually operates for 15 hours per TAD canister; (3) The WHF will process 1165 TAD canisters. $1165 \times 15/50$ is 350 hours per year (a score of 350).

The locations of portable welding receptacles were determined as an engineering judgment on the part of the design team based on preliminary electrical and general layout drawings. The resultant fire initiating event frequencies are insensitive to the precise distribution of the portable welding receptacles, so a more rigorous analysis of the distribution is not required.

F5.4.6 Internal Combustion Engines

There are two transporters that utilize internal combustion engines in the WHF, which provide the entire contribution of fire ignition to the internal combustion engines category. The site transporter and site prime mover are assigned a total of 100 points each. The points are allocated to the rooms where these vehicles could be located by use of a RWF, as discussed in section F5.4.3.

The site transporter occupies rooms 1007 (Loading Room) and 1023 (Site Transporter Vestibule). The times necessary to determine the percentage of time the site transporter spends

in each room are given in Sections 1.5, 5.1, and 1.6 of the WHF process throughput diagram (Ref. F2.6). A total of 28 minutes is assigned to both rooms because the doors between them are open. Resultant times are 392 minutes in the Site Transporter Vestibule (1023) and 605 minutes in the Loading Room (1007).

The site prime mover/tractor occupies rooms 1016 (Cask Preparation Area) and 1001 (Transportation Cask Vestibule). The times necessary to determine the percentage of time the prime mover/tractor spends in each room are given in section 1.1 of the WHF process throughput diagram. There are 12 total minutes that are assigned to both rooms because the doors between them are open. Resultant times are 24 minutes in the Transportation Cask Vestibule (1001) and 85 minutes in the Cask Preparation Area (1016).

The times internal combustion engines spend in each room is utilized to determine the percentage of time the engine occupies a room, which directly corresponds to the percentage of the total count assigned to that room. This is represented on the equipment list as the RWF.

Locations of the internal combustion engines were determined solely from the general layout drawings.

F5.4.7 Office/Kitchen Equipment

This category consists of miscellaneous office and kitchen equipment such as shredders, vending machines, microwaves, computers, radios and printers. The location and quantity of such equipment was inferred by the description and layout of the rooms to come up with a reasonable distribution of such equipment in the facility. Work rooms, break rooms, briefing rooms, and offices were considered to possess such equipment. A judgment was made by the analysis team based on the function and size of the room as to how much of such equipment might reside in these rooms. Points were assigned to each room expected to contain office or kitchen equipment based on this judgment (one point per room). The resultant fire initiating event frequencies are quite insensitive to the precise distribution of this equipment, so a more rigorous analysis of the distribution is not required.

Locations of the office and kitchen equipment were determined solely from the general layout drawings.

F5.4.8 Portable and Special Equipment

This category consists of portable hand tools, monitoring devices, portable heaters, diagnostic equipment and the like. Rooms where there were significant amounts of equipment that would expect to be maintained on a regular basis or where monitoring would take place were considered to possess such equipment. Determinations for the portable and special equipment category were inferred from the description and layout of the rooms, as described in Section F5.4.7. Each room containing such equipment was assigned four to eight points, depending on the quantity expected in that room. The resultant fire initiating event frequencies are quite insensitive to the precise distribution of this equipment, so a more rigorous analysis of the distribution is not required.

F5.5 ROOM IGNITION FREQUENCY

Ignition frequencies for each room are determined as a function of the number of units of ignition sources in the room, and the area of the room. The spreadsheet used to determine these frequencies is displayed as Table F5.5-1.

The major input to the spreadsheet is the number of units per category for each room (green text). These values are taken from the equipment list Table (F5.4-1), which is formulated from equipment lists and equipment and general layout drawings (Section F5.4). The total number of units in each category is the result of a sum across all rooms, and can be found in the bottom total row. It is this value that is used in Table F5.3-1 in the column entitled "Category Population" for all categories except "no equipment involved," as explained in Section F5.3.

The "no equipment involved" column of Table F5.5-1 is the area of the rooms, as a unit in this category is represented by a single square meter. These values are taken from Table F5.2-1, in the column entitled "A (sq-m)."

The final column on Table F5.5-1, entitled "Room Ignition Frequency," implements the generic forms of equations F-5 and F-6. It calculates the room ignition frequency, which uses the frequency per unit from Section F5.3. It takes the required per unit ignition frequencies directly from the spreadsheet represented by Table F5.3-1, the column entitled "Frequency per Unit". Per Equation F-5, the number of units in each category (green text) is multiplied by the corresponding frequency per unit for that category. Per Equation F-6, summing these multiplications across a row provides the room ignition frequency for that room. The sum of all rooms is the building ignition frequency. This value is shown in the lower right hand column of the table. Note that this value does not match the value shown at the bottom of Table F5.2-1. That value, which is based only on building area, pre-supposes that the ignition sources in the building cover each of entire ignition source categories used in the analysis. However, the WHF does not have any equipment that fits the definition of heat generating equipment (welders have their own category), so this contribution does not apply to WHF.

F5.6 PROPAGATION PROBABILITIES

Propagation probabilities are used in this analysis to define the probability of a fire spreading to various defined points. The first two columns of Table F5.6-1 define the maximum extent of propagation, and the conditional probability column is the probability associated with that extent of propagation. The remaining columns in Table F5.6-1 are used in the uncertainty distribution for the conditional probability. The structure of this spreadsheet is analogous to Table F5.3-1. The right hand group of columns is used by Crystal Ball to apply an uncertainty distribution to each of the propagation probability values for the purpose of developing uncertainty distributions on initiating event frequency. The mean fraction, 97.5% value, and 97.5th percentile add columns show the parameters of these distributions. The development of all of the values is detailed in Appendix F.II. When Crystal Ball is run, it creates a sampled value for each fraction in the sampled value column. The spreadsheet then determines a normalized value by first ensuring that each sampled value is not negative (minimum value of zero) and then normalizing the values so that the sum is always equal to one. The normalized value for each trial then

replaces the category fraction value in the calculation. These probabilities must always add to one, as the groupings include all possible propagation outcomes.

F5.7 INITIATING EVENT FREQUENCIES

Initiating event frequencies are the final results of the fire hazard analysis, and are a factor of all of the previously discussed data and residence fractions. The following sections shall describe the culmination of this data to conclude with initiating event frequencies.

F5.7.1 Residence Fractions

Residence fractions have been developed from process throughputs to determine the length of time a waste form will be vulnerable in a particular area of the building and in a particular configuration. The source for all of the times related to TAD canisters, dual-purpose canisters (DPCs), and spent nuclear fuel (SNF) is the WHF throughput study (Ref. F2.6). Table F5.7-1 shows the vulnerabilities for all waste forms at the WHF, and the times that contribute to the overall time of vulnerability. The column labeled block flow diagram "BFD Task" refers to the task number from the process block flow diagram that was used in the throughput study. These numbers appear directly on the Gantt charts and provide a reference for the task that was considered. The total shows the total number of minutes that the waste form was in the specified configuration in the specified location. The fraction column implements the approach discussed in Section F4.4.1 to calculate the fraction of time that a specific waste form spends in the particular configuration and location over the 50-year period of preclosure operations in WHF.

F5.7.2 Localized Fires

Initiating event frequencies have been divided into two types of calculations: localized and large fires. Table F5.7-2 contains all of the calculations contributing to the localized fire initiating event frequencies.

F5.7.2.1 Room Groupings

The first column of Table F5.7-2 identifies the room(s) of origin. If the vulnerability is expected to occur in a single room with no gates or doors open and that is surrounded by qualified fire barriers (i.e., it is a single room fire area), this room is listed as the only room of origin. However, there are several cases in which the vulnerability takes place as the waste form moves between multiple rooms, or the room where the vulnerability occurs has open doors or gates with other rooms, or it shares a qualified fire area with other rooms. Table F5.7-3 lists all of the vulnerabilities that have more than one room of origin, and the justification for the multiple room listing. Whenever such a condition exists, the quantification of the localized fire considers not only fires that start in the room where the waste form resides, but also the contribution of other rooms that could directly communicate with that room through non-qualified or open fire barriers. Rooms within the same fire area of a room of origin are listed under each vulnerability in the column labeled "Propagation From Rooms in Fire Zone" heading.

For rooms of origin, the Frequency per Unit column is populated by the results in Section F5.3. This is discussed further in Section F5.7.2.2. Propagation rooms populate the Frequency per

Unit column with the total ignition frequency for that room, as calculated and reviewed in Section F4.4 (Room Ignition Frequency).

F5.7.2.2 Ignition Source Distribution Within a Room

Per the methodology discussion in Section F4.4.2.1, the locations of the ignition sources within a room are identified relative to the target and assigned a location at the target, near the target, or away from the target. These locations are shown in their respective columns in Table F5.7-2, and must sum to the "Number In Room" column entry. These columns are designators of where the ignition sources are in relation to the vulnerable waste form.

For all categories except "no equipment involved," the distribution is determined by analysis of the room layout to determine whether the ignition source unit is at a distance within about three meters (at target), between about 3 and 7 meters (near target), or further (away from target) of the vulnerable waste form. For vulnerable waste forms in motion (e.g., in the railcar), ignition sources within the aforementioned distances of any portion of the path of motion are counted in the class representing its closest point to the waste form.

The ignition source units for the "no equipment involved" category are the area of the room (square meters). For vulnerabilities that are not waste forms in motion, the numbers for at target and near target are 30 and 120, respectively (i.e., a floor area of approximately 30 m^2 is considered at the target and the next 120 m^2 is considered near the target). The remaining area is entered as away from target. For vulnerable waste forms in motion, the "at target" value is the total area covered by the full range of motion plus a 3-m ring. Similarly, the number near target is figured to be a 7-m ring around the at target area. The remaining area is entered as away from target.

The distribution of ignition sources is used to determine how far a fire must spread before it reaches the vulnerable waste form. The propagation values are taken from Table F5.6-1 for the "no suppression" case, per the boundary conditions, in accordance with the guidance discussed in Section F4.4.2 (in particular, F4.4.2.1). The "frequency per (ignition source) unit" column is taken from Table F5.3-1, the column labeled Frequency per Unit. The target exposure time fraction, which is the probability that there is a waste form in the room, is taken from Table F5.7-1. The column labeled "Contribution to IE Frequency" implements Equation F-7 to provide the total initiating event frequency contribution from fire that start in the room where the waste form resides.

There is also a section of Table F5.7-2 that addresses the contribution from nearby rooms in the same fire area (i.e., that are separated from the room by walls or doors, but those barriers are not qualified fire barriers). In this case, the location of the ignition sources within these rooms is not important, only the probability that the fire spreads beyond the room within the same fire area matters as to whether the fire reaches the target. In this case, the Frequency per Unit column refers to the overall frequency of ignition in the room, which comes from the last column in Table F5.5-1. In this case, the appropriate propagation value for spread of a fire beyond the room is taken from Table F5.6-1, again for the no suppression case, as discussed in Section F4.4.2 (in particular, F4.4.2.2). For these rooms, the "Contribution to IE Frequency"

column implements the generic form of Equation F-8, as applied to a fire throughout a fire area (zone) where the next largest fire is a floor fire.

The overall fire initiating event frequency, provided in a shaded cell for each defined initiating event shown in bold, is the sum of all the individual contributors.

F5.7.3 Large Fires

Calculation of the Initiating Event Frequencies is completed similarly to the localized fire contributions from other rooms. Table F5.7-4 provides the analysis. In this case, the fire can start in any room in the facility and become a large fire. Since the fire can start in any room, and the methodology applies the same probability of fire propagation to each room, the starting point is the total ignition frequency from all rooms, taken from Table F5.6-1. The propagation probability is applied as discussed in Section F4.4.2 (in particular, Section F4.4.2.2) to implement Equation F-9. The target exposure time (fraction) is once again taken from Table F5.7-1. Large fires always propagate beyond the fire area of the room of origin.

F5.7.4 Contribution to Initiating Event Frequency

The probability of a fire reaching the vulnerable waste form and the target exposure time (residence fractions; refer to section F5.7.1) contribute to the final calculation of the contribution to initiating event frequency (cells highlighted in blue on Tables F5.7-2 and F5.7-4). Section F4.4 details the calculations performed to arrive at the initiating event frequency.

F5.8 MONTE CARLO SIMULATION/UNCERTAINTY DISTRIBUTIONS.

F5.8.1 Uncertainty Distributions

Uncertainty distributions are used in the contribution to initiating event frequency calculations to account for the potential of variance in the data. For example, the ignition frequency presented in Table F5.2-1, Section F5.1 is the result of a calculation based on room area. The equation used to perform this calculation was derived from data collected on building fires. While the data collected and the equation developed to fit the data have a good R-squared (percentage of variability accounted for in the equation) value (90), an uncertainty distribution is necessary to account for the natural variability of the frequency of ignition.

The uncertainty distributions used for this analysis are primarily normal, with the exception of the ignition frequency distribution, which is lognormal (skewed bell curve shape, with the median value at the top of the curve). Lognormal distributions can be accurately represented by a median (50%) and a 97.5% value. The 97.5% value is a figure that represents a point at which only 2.5% of all possible outcomes will vary from the mean more significantly.

Three uncertainty distributions were developed for this analysis: ignition frequency, category fraction, and conditional probability. The distribution for ignition frequency is discussed in detail in Appendix F.III. The distributions for category fraction and conditional probability are discussed in Appendix F.II.

F5.8.2 Monte Carlo Simulation

Monte Carlo simulations are performed to determine the mean, standard deviation, variance, minimum, and maximum values of each of the initiating event frequencies based on the variance of the contributing data. To accomplish this task, the Microsoft Excel add-on package Crystal Ball was used. This software requires input of the necessary uncertainty distribution figures (in this case, median (50%) and 97.5% values) and the figures that the simulation will produce results for (initiating event frequencies). Crystal Ball software uses the mean and 97.5% values to calculate the equation that represents the distribution. The software then randomly selects a value from the possibilities defined by the distribution. The software is set to iterate 10,000 times to ensure accurate results.

F5.9 RESULTS

The results of the analysis are the fire initiating event frequencies and their associated distributions. The initiating event frequencies represent the probability, over the length of the preclosure period, that a fire will threaten the stated waste form during the stated vulnerability. Because data used to obtain these results are based on existing fire data, it was necessary to determine the uncertainty distribution for each initiating event. Figure F5.7-1 displays the Crystal Ball results for a localized fire threatening a TAD canister in an aging overpack in the lid bolting area.

These results provide a statistical reference for the variance of each initiating event frequency. As seen in Section F5.7.2, Table F5.7-2, the baseline initiating event frequency for this case is 3.7×10^{-7}. The Crystal Ball results give insight into this, showing that given the variability of the inputs, the true result could lie anywhere between 4.8×10^{-8} and 1.7×10^{-6}, with a mean of 3.5×10^{-7}, a standard deviation of 1.8×10^{-7}, and a lognormal shape. Crystal Ball was run for all of the initiating events. A summary of the results, giving the distribution parameters of each distribution, is shown in Table F5.7-5. The 97.5 percentile values in Table F5.7-5 are not provided in the Crystal Ball full report. Instead, these values were obtained by using the "extract data" option, which allows the analyst to specify the percentile values necessary. Also not included in the Crystal Ball report are the error factors, which were calculated from the mean and median as discussed in Appendix F.V. It was determined via methods described in Appendix F.IV that all of the resultant distributions are lognormal. The complete output from Crystal Ball and the 97.5 percentile values are provided in Appendix F.VI. In addition to showing the initiating event frequency distribution, Appendix F.VI also shows the input distribution for the parameters that were varied, which match the distributions developed and documented in Appendices F.II and F.III.

Table F5.2-1. Room Areas and Total Ignition Frequency

Room	L1(ft)	L2(ft)	A(sq-ft)	A(sq-m)	L3(ft)	L4(ft)	L5(ft)	L6(ft)	L7(ft)	L8(ft)	
B001	41	18	738	69							
B002	39	18	702	65							
B003	23	18	414	38							
B004	23	32	736	68							
B005	19	20	380	35							
B006	6	5	30	3							
B007	6	12	72	7							
B008	39	17	663	62							
B009	41	17	697	65							
P001(incl in 1016)	0	0	0	0							
1001	53	50	17540	1630	60	102	*Area multiplied by two - Room extends two floors				
1002	54	43	1997	186	13	25					
1003	13	25	325	30							
1004	54	43	2322	216							
1005	11	9	99	9							
1006	40	43	1720	160							
1007	37	53	1961	182							
1008	27	53	1431	133							
1009	54	53	2457	228	15	27					
1010	15	27	405	38							
1011A	10	55	550	51							
1011B	148	10	1480	137							
1012A	10	53	530	49							
1012B	108	10	1080	100							
1013	50	68	3392	315	18	11	10	19			
1014	18	11	198	18							
1015	7	9	63	6							
1016	212	104	44096	4097	*Area multiplied by two - Room extends two floors						
1017	46	63	2898	269							
1018	33	104	222	21	46	63	13	12	13	12	
1018A	13	12	156	14							
1018B	13	12	156	14							
1019	54	43	1997	186	25	13					
1020	25	13	325	30							
1021	54	43	2322	216							

Table F5.2-1. Room Areas and Total Ignition Frequency (Continued)

Room	L1(ft)	L2(ft)	A(sq-ft)	A(sq-m)	L3(ft)	L4(ft)	L5(ft)	L6(ft)	L7(ft)
1022	7	9	63	6					
1023	64	73	4672	434					
1024	18	12	216	20					
1025	26	12	312	29					
1026	12	28	336	31					
1027	12	28	336	31					
1028	20	15	600	56	*Area multiplied by two - Room extends two floors				
1029	20	15	300	28					
1030	12	15	180	17					
1031	22	15	330	31					
1032	34	6	288	27	6	14			
1032A	20	12	240	22					
1033	29	12	348	32					
1034	26	12	312	29					
1035	12	15	180	17					
1036	7	13	182	17	*Area multiplied by two - Room extends two floors				
1037	6	13	78	7					
1038	5	14	70	7					
1039	5	14	70	7					
1042A	13	16	208	19					
1042B	13	16	208	19					
1042C	13	16	208	19					
1043A	13	25	325	30					
1043B	13	25	325	30					
1043C	13	25	325	30					
1044A	13	21	273	25					
1044B	13	21	273	25					
1044C	13	21	273	25					
1045A	40	9	360	33					
1045B	40	9	360	33					
1045C	54	20	1080	100					
1045D	13	82	1066	99					
1046	46	37	1702	158					
1201	10	9	90	8					

Table F5.2-1. Room Areas and Total Ignition Frequency (Continued)

Room	L1(ft)	L2(ft)	A(sq-ft)	A(sq-m)	L3(ft)	L4(ft)	L5(ft)	L6(ft)	L7(ft)
1202	14	16	224	21					
1203	23	16	368	34					
1204	27	16	432	40					
1205	17	28	476	44					
1206	16	8	128	12					
1207	16	34	544	51					
1208	12	8	96	9					
1209	12	35	420	39					
1210	17	14	238	22					
1211	16	8	128	12					
1212	16	14	224	21					
1213	16	10	160	15					
1214	16	10	160	15					
1215	30	25	750	70					
1216	15	18	270	25					
1217	15	18	270	25					
1218A	97	6	648	60	11	6			
1218B	6	53	318	30					
1218C	104	6	624	58					
M001	51	100	5100	474					
2001	54	28	1512	140					
2001A	50	10	500	46					
2002	54	43	2322	216					
2003	40	36	1440	134					
2004	114	48	10944	1017	*Area multiplied by two - Room extends two floors				
2005A	157	9	1533	142	10	12			
2005B	108	9	972	90					
2006	146	10	1460	136					
2007A	10	56	560	52			868.4576		
2007B	212	10	2120	197					
2008	54	104	5616	522					
2010	54	43	2322	216					
2011A	54	19	1026	95					
2011B	54	24	1296	120					

Table F5.2-1. Room Areas and Total Ignition Frequency (Continued)

Room	L1(ft)	L2(ft)	A(sq-ft)	A(sq-m)	L4(ft)	L5(ft)	L6(ft)	L7(ft)	L8(ft)
2012	64	43	2596	241	12	13			
2013	12	13	156	14					
2024	18	11	198	18					
					*Area multiplied by two - Room extends				
2025	22	11	484	45	two floors				
2026	12	28	336	31					
2027	12	28	336	31					
2029	10	18	180	17					
2030	10	15	150	14					
2032	17	6	102	9					
2033	21	6	126	12					
2034	24	6	312	29	7	24			
2201	13	16	208	19					
2202	20	16	320	30					
2203	40	12	560	52	5	16			
2204	9	14	126	12					
2205	10	14	140	13					
2206	6	14	84	8					

Total Area (sq-m)	15046		50% Value	97.5% Value
Ignition Frequency (per sq-m/yr)	3.94E-06	3.94E-06	3.94E-06	9.40E-06
Ignition Frequency (per yr)	5.93E-02			
Ignition Frequency (50 years - preclosure period)	2.96E+00			

Source: Original

Table F5.3-1. Ignition Frequency by Ignition Source

Category	Category Fraction	Category Frequency (50 years)	Category Population	Frequency per Unit (50 years)			Sampled Value	Mean Fraction	97.5% Value	97.5th percentile add
Electrical	0.086	2.54E-01	185	1.37E-03		0.086	0.086	0.086	1.26E-01	4.05E-02
HVAC	0.080	2.38E-01	50	4.76E-03		0.080	0.080	0.080	1.20E-01	3.93E-02
Mechanical Equipment	0.139	4.13E-01	64	6.45E-03		0.139	0.139	0.139	1.89E-01	5.01E-02
Heat Generating Equipment	0.155	4.60E-01	0	0.00E+00		0.155	0.155	0.155	2.07E-01	5.24E-02
Torches, welders, burners	0.219	6.50E-01	810	8.03E-04		0.219	0.219	0.219	2.79E-01	5.99E-02
Internal combustion engines	0.021	6.23E-02	200	3.12E-04		0.021	0.021	0.021	4.23E-02	2.09E-02
Office/kitchen equipment	0.064	1.90E-01	20	9.50E-03		0.064	0.064	0.064	9.97E-02	3.55E-02
Portable Equipment	0.102	3.03E-01	52	5.82E-03		0.102	0.102	0.102	1.45E-01	4.37E-02
No equipment involved	0.134	3.98E-01	15087	2.64E-05		0.134	0.134	0.134	1.83E-01	4.93E-02
	1.000					1.000				

NOTE: HVAC = heating, ventilation, and air conditioning.

Source: Original

Table F5.4-1. Ignition Source Population by Room

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
B001 (Access Stair/Leak Detection Sump Area)			**Leak Detection Sump Pump 1** 050-PW00-P-00003-A **0.5 hp**					
B002 (Storage Tank Area)			**1 MP Liquid LLW Sampling Pump** 050-MWL0-P-00001 • **5 hp** **1 MP Liquid LLW Sump Pump** 050-MWL0-P-00002 • **5 hp**					
B003 (Unassigned)								
B004 (Unassigned)								
B005 (Decon Collection Tank Area)								
B006 (Elevator Lobby)								
B007 (Elevator)								
B008 (Storage Tank Area)								
B009 (Access Stair/Leak Detection Sump Area)			**Leak Detection Sump Pump 2** 050-PW00-P-00003-B • **0.5 hp**					
P001 (Pool)			**4 Pool Treatment Filter Pumps** 050-PW00-SKD-00001-A 050-PW00-SKD-00001-B 050-PW00-SKD-00001-C 050-PW00-SKD-00001-D • **15 hp**					
1001 (Transport Cask Vestibule)		**4 Fan coil units** 050-VCT0-FCU-00009 050-VCT0-FCU-00010 050-VCT0-FCU-00011 050-VCT0-FCU-00012 • **20 HP (ea.)**	**Entrance Vest. Crane** 050-HMC0-CRN-00001 • **2+1 motors @ 45, 2, & 5 hp** **Overhead Door** • **1 motor @ 5hp**		**2 Portable Welding Receptacles – WWF = 10 points**	**22% Shared w/ room 1016 Site Prime Mover (Railcar)** • **22 units**		
1002	**480V Load Center**	**2 Fan coil units**			**Portable Welding**			**Assume 7.7% of all such**

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
(Electrical Room)	050-EEE0-LC-00001 • **2 cabs** **480V MCC** 050-EEE0-MCC-00001 • **10 cabs** **1 45 kVA Dist. XFMR** 050-EEE0-XFMR-00003 **1 40 kVA Maint. Bypass XFMR** 050-EEU0-XFMR-00001 **1 UPS** 050-EEU0-UJX-00001 **1 208/120V Dist. Panel** 050-EEE0-PL-00003 **1 120 V UPS Panel** 050-EEU0-PL-00001 **1 Lighting Panel** 050-EUL0-PL-00001-A **2 DCMIS** **2 PLC Panels**	050-VCT0-FCU-00001 050-VCT0-FCU-00002 • **15 HP (ea.)**			**Receptacle – WWF = 5 points**			**eq.** • **4 points**
1003 (Battery Room)	**1 125V Battery** 050-EEE0-BTRY-00001	**2 Exhaust Fans** 050-VCT0-EXH-00004 050-VCT0-EXH-00005 • **5 HP (ea.)** **2 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00010 050-VCT0-FLT-00011						
1004 (HVAC Room)		**1 Exhaust Fan** 050-VCS0-EXH-00001 • **200 HP** **3 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00001 050-VCT0-FLT-00002 050-VCT0-FLT-00003			**Portable Welding Receptacle – WWF = 5 points**			**Assume 7.7% of all such eq.** • **4 points**
1005 (Vestibule)								
1006 (HVAC Room)		**3 Exhaust Fans** 050-VCT0-EXH-00001 050-VCT0-EXH-00002 050-VCT0-EXH-00003 • **50 HP (ea.)** **3 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00016 050-VCT0-FLT-00017 050-VCT0-FLT-00018						**Assume 7.7% of all such eq.** • **4 points**
1007 (Loading Room)						**61% Site Transporter 1023** • **61 units**		
1008 (Cask Unloading Room)			**3% Cask Transfer Trolley** 050-HM00-TRLY-00001 1016 • **1 power drive**					**Assume 4% of all such eq.** • **2 points**

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
			• X 3% = **0.03**					
1009 (CTM Maint. Rm.)					**Portable Welding Receptacle – WWF = 5 points**			
1010 (Gas Sampling Room)			**Cask Cavity Gas Sample Sys.** 050-MRE0-VACP-00001 050-MRE0-DET-00001 • **1 motor** • **1 hp**					
1011A (Corridor)								
1011B (Corridor)								
1012A (Corridor)								
1012B (Corridor)								
1013 (LLW Staging Area)			**Overhead Door** • **1 motor @ 5hp**		**Portable Welding Receptacle – WWF = 5 points**			
1014 (Chemical Lab)								
1015 (Elevator Machine Room)								
1016 (Cask Preparation Area)			**Cask Handling Crane** 050-HM00-CRN-00001 • **4 motors @ 90, 45, 7.5, & 30 hp** • **120 hp** **Auxiliary Pool Crane** 050-HMH0-CRN-00001 • **2+1 motors @ 25, 1.5, & 7.5 hp** **DPC Cutting Jib Crane** 050-HD00-CRN-00001 • **1+2 motors @ 15, 1.5, &1.5 hp** **Spent Fuel Transfer Machine** 050-HTF0-FHM-00001 • **2+1 motors @ 30, 5, & 1.5 hp** **DPC Cutting Machine** 050-HD00-TOOL-00001 • **1 motor @ 20 hp** **DPC Cutting Station** 050-HD00-PLAT-00001		**TAD Canister Welding Machine** 050-HC00-TOOL-00001 • **350 points (15*1165/50)** **3 Portable Welding Receptacles – WWF = 15 points**	**78% Shared w/ room 1001** **Site Prime Mover (Railcar)** • **78 units**		**Assume 15% of all such eq.** • **8 points**

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
			• **2 motors @ 5 hp** **TAD Closure Station** 050-HC00-PLAT-00001 • **2 motors @ 5hp each** **TAD Closure Jib Crane** 050-HC00-CRN-00001 • **1+2 motors @ 15, 1.5, &1.5 hp** **DPC Unloading Bay Gate** 050-WH00-DR-00002 • **1 motor @ 5 hp** **Mobile Access Platform** 050-HMC0-PLAT-00001 • **6+4 motors: 4@1hp, 4@5hp, & 2@10hp** **Pool Equipment Crane** 050-PW00-CRN-00001 • **1+2 motors @ 20, 1, & 3 hp** **Preparation Stations #1 & 2** 000-HMH0-PLAT-00001 • **2 motors @ 5hp each** 050-HMH0-PLAT-00002 • **2 motors @ 5hp each** **Prep Station Jib Cranes** 050-HMH0-CRN-00002 • **1+2 motors @ 15, 1.5, &1.5 hp** 050-HMH0-CRN-00003 • **1+2 motors @ 15, 1.5, &1.5 hp** **97% Cask Transfer Trolley** 050-HM00-TRLY-00001 **1008** • **1 power drive** • X 97% = **0.97** **TAD Canister Welding Machine** 050-HC00-TOOL-00001 • **1 motor** • **5 hp** **Shield Door** 050-WH00-DR-00001 • **1 motor** • **5 hp** **Shield Door** 050-WH00-DR-00003 • **1 motor** • **15 hp**				

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
1017 (Air Compressor Room)	**480V Load Center** 050-EEN0-LC-00003 • **5 cabs**		**2 Chilled Water Pumps** 050-PSC0-P-00001A 050-PSC0-P-00001B • **1 motor (ea.)** • **75 HP (ea.)** **2 Hot Water Pumps** 050-PSH0-P-00001A 050-PSH0-P-00001B • **1 motor (ea.)** • **20 HP (ea.)**					
1018 (Maintenance Room)		**2 Fan coil units** 050-VCT0-FCU-00007 050-VCT0-FCU-00008 • **20 HP (ea.)**			**Primary Welding Station** • **400 points**			
1018A (Vestibule)								
1018B (Vestibule)								
1019 (Electrical Room)	**480V Load Center** 050-EEE0-LC-00002 • **2 cabs** **480V MCC** 050-EEE0-MCC-00002 • **10 cabs** **1 40 kVA Maint. Bypass XFMR** 050-EEU0-XFMR-00002 **1 480V XFMR** 050-EEE0-XFMR-00002 **1 45 kVA Distribution XFMR** 050-EEE0-XFMR-00004 **1 UPS** 050-EEU0-UJX-00002 **1 120V UPS Panel** 050-EEU0-PL-00002 **1 208/120V Distribution Panel** 050-EEE0-PL-00004 **1 277V Lighting Panel** 050-EUL0-PL-00001-B **2 DCMIS** **2 PLC Panels**	**2 Fan coil units** 050-VCT0-FCU-00003 050-VCT0-FCU-00004 • **15 HP (ea.)**			**Portable Welding Receptacle – WWF = 5 points**			**Assume 7.7% of all such eq.** • **4 points**
1020 (Battery Room)	**1 125V Battery** 050-EEE0-BTRY-00002	**2 Exhaust Fans** 050-VCT0-EXH-00006 050-VCT0-EXH-00007 • **5 HP (ea.)** **2 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00012 050-VCT0-FLT-00013						

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
1021 (HVAC Room)		**1 Exhaust Fan** 050-VCS0-EXH-00002 • **200 HP** **3 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00005 050-VCT0-FLT-00006 050-VCT0-FLT-00007						**Assume 7.7% of all such eq.** • **4 points**
1022 (Vestibule)								
1023 (Site Transport Vestibule)		**3 Fan coil units** 050-VNI0-FCU-00001 050-VNI0-FCU-00002 050-VNI0-FCU-00003 • **7.5 HP (ea.)**	**Aging Overpack Access Plat.** 050-HAC0-PLAT-00001 • **2 motors @ 5hp each** **Shield Door** 050-WH00-DR-00004 • **1 motor** • **15 hp** **Overhead Door** • **1 motor**			**39% Site Transporter 1007** • **39 units**		
1024 (Stair #1)								
1025 (Stair #2)								
1026 (Stair #3)								
1027 (Stair #4)								
1028 (Freight Elevator)			**Elevator** • **1 motor** • **50 hp**					
1029 (Elevator Lobby)								
1030 (Elevator Equipment Room)								
1031 (Corridor)								
1032 (Corridor)								
1032A (Storage Room)								
1033 (Corridor)								
1034 (Fire Water Riser								

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
Valve R1)								
1035 (Fire Water Riser Valve R2)								
1036 (Elevator)			**Elevator** • **1 motor** • **50 hp**					
1037 (Elevator Machine Room)								
1038 (Condenser Area N)								
1039 (Condenser Area S)								
1042A (Pool Pump Room A)			**1 Pool Treatment Pump A 050-PW00-P-00001-A** • **40 hp**					
1042B (Pool Pump Room B)			**1 Pool Treatment Pump B 050-PW00-P-00001-B** **40 hp**					
1042C (Pool Pump Room C)			**1 Pool Treatment Pump C 050-PW00-P-00001-C** **40 hp**					
1043A (Pool Filter Room A)								
1043B (Pool Filter Room B)								
1043C (Pool Filter Room C)								
1044A (Pool Ion Exchanger Room)								
1044B (Pool Ion Exchanger Room)								
1044C (Pool Ion Exchanger Room)								

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
1045A (Corridor)								
1045B (Corridor)								
1045C (Corridor)			**Overhead Door** • **1 motor @ 5hp**					
1045D (Corridor)								
1046 (Electrical Room)	**480V Load Center** 050-EEN0-LC-00002 • **4 cabs** **480V MCC** 050-EEN0-MCC-00005 • **12 cabs** **480V MCC** 050-EEN0-MCC-00006 • **14 cabs** **480V MCC** 050-EEN0-MCC-00007 • **14 cabs** **480V MCC** 050-EEN0-MCC-00008 • **11 cabs** **480V MCC** 050-EEN0-MCC-00009 • **29 cabs** **1 480 V Distribution XFMR** 050-EEN0-XFMR-00006 **1 Distribution Panel** 050-EEN0-PL-00006 **2 277V Lighting Panels** 050-EUL0-PL-00004 050-EUL0-PL-00005 **2 DCMIS** **2 PLC Panels**							
1201 (Entry/Exit Vestibule)								
1202 (Briefing Room)							**Assume 5% of all such equipment** • **1 point**	
1203 (Mens Room)								
1204 (Womens Room)								
1205 (RP Control Point)							**Assume 5% of all such equipment** **1 point**	
1206								

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
(Controlled Exit)								
1207 (Vestibule Out)								
1208 (Vestibule In)								
1209 (RP Gear Supply Room)							**Assume 5% of all such equipment** • **1 point**	
1210 (Decon)							**Assume 5% of all such equipment** • **1 point**	
1211 (Respirator Room)							**Assume 5% of all such equipment** • **1 point**	
1212 (RP Equipment Room)							**Assume 5% of all such equipment** • **1 point**	
1213 (Change Room 2)								
1214 (Change Room 1)								
1215 (RP Instrument Room)							**Assume 5% of all such equipment** • **1 point**	
1216 (RP Lab/Sample Prep. Room)							**Assume 5% of all such equipment** • **1 point**	
1217 (RP Lab/Count Room)							**Assume 5% of all such equipment** • **1 point**	
1218A (Corridor)								
1218B (Corridor)								
1218C (Corridor)								
M001 (HVAC/Pool Equipment Room)		**3 Air Handling Units** 050-VC00-AHU-00001 050-VC00-AHU-00002 050-VC00-AHU-00003 • **40 HP (ea.)**						**Assume 7.7% of all such eq.** • **4 points**
2001 (Electrical	**480V Load Center** 050-EEN0-LC-00001 • **4 cabs**							**Assume 7.7% of all such eq.** • **4 points**

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
Room)	**480V MCC** 050-EEN0-MCC-00001 • **9 cabs** **480V MCC** 050-EEN0-MCC-00002 • **14 cabs** **480V MCC** 050-EEN0-MCC-00003 • **13 cabs** **480V MCC** 050-EEN0-MCC-00004 • **11 cabs** **3 480V Distribution XFMRS** 050-EEN0-XFMR-00003 050-EEN0-XFMR-00004 050-EEN0-XFMR-00005 **1 480V Bypass XFMR** 050-EEP0-XFMR-00001 **3 480 V Distribution Panels** 050-EEN0-PL-00003 050-EEN0-PL-00004 050-EEN0-PL-00005 **1 208/120 V UPS Distribution Panel** 050-EEP0-PL-00001 **1 UPS** 050-EEP0-UJX-00001 **3 277V Lighting Panels** 050-EUL0-PL-00001 050-EUL0-PL-00002 050-EUL0-PL-00003 **2 DCMIS** **1 PLC Panel**							
2001A (Battery Room)	**1 125V Battery** 050-EEP0-BTRY-00001	**2 Exhaust Fans** 050-VCT0-EXH-00008 050-VCT0-EXH-00009 • **5 HP (ea.)** **2 HEPA Filter Units** (HP n/a) 050-VCT0-FLT-00014 050-VCT0-FLT-00015						
2002 (HVAC Room)		**2 Air Handling Units** 050-VCT0-AHU-00001 050-VCT0-AHU-00002 • **100 HP (ea.)**						**Assume 7.7% of all such eq.** • **4 points**
2003 (HVAC Room)		**1 Air Handling Unit** 050-VCT0-AHU-00003 • **100 HP (ea.)**						**Assume 7.7% of all such eq.** • **4 points**
2004 (Canister Transfer Room)			**CTM Maintenance Crane** 050-HTC0-CRN-00001 • **2+1 motors @ 35, 2, & 7.5 hp**		**Portable Welding Receptacle – WWF = 5 points**			**Assume 4% of all such eq.** • **2 points**

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
			Canister Transfer Machine 050-HTC0-FHM-00001 • **5+1 motors @ 45, 3, 7.5, 7.5, 60, & 5 hp** **2 Port Slide Gates** 050-HTC0-HTCH-00001 050-HTC0-HTCH-00002 • **2 motors each @ 0.5 hp each**					
2005A (Corridor)								
2005B (Corridor)								
2006 (Corridor)								
2007A (Corridor)								
2007B (Corridor)								
2008 (Crane Maint. Area)					**Portable Welding Receptacle – WWF = 5 points**			
2010 (HVAC Room S)		**2 Air Handling Units, 4 motors** 050-VNI0-AHU-00001 050-VNI0-AHU-00002 • **60 HP (supply)** • **25 HP (return)**						**Assume 7.7% of all such eq.** • **4 points**
2011A (Back-up Central Comm. Room)							**Assume 10% of all such equipment** • **2 points**	
2011B (Back-up Central Comm. Room)							**Assume 10% of all such equipment** • **2 points**	
2012 (Operations Room)	**6 Control Consoles**						**Assume 10% of all such equipment** • **2 points**	
2013 (Operations Supervisor Room)								
2024 (Stair #1)								
2025 (Stair #2)								
2026 (Stair								

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source / Room Number	Electrical Equipment	Mechanical/ Electrical HVAC Equipment	Mechanical Process Equipment	Heat Generating Process Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable and Special Equipment
#3)								
2027 (Stair #4)								
2029 (Elevator Lobby)								
2030 (Elevator Machine Room)								
2032 (Corridor)								
2033 (Elevator Lobby)								
2034 (Corridor)								
2201 (Briefing Room)							**Assume 5% of all such equipment** • **1 point**	
2202 (RP Staff Work Room)							**Assume 5% of all such equipment** • **1 point**	
2203 (Break/ Vending Room)							**Assume 15% of all such equipment** • **3 points**	
2204 (Women's Restroom)								
2205 (Men's Restroom)								
2206 (Janitor Room)								

NOTE: [1] Room weighting factor (RWF) is for equipment that can be in multiple rooms. Factor represents the percent of exposure (i.e., waste residence) time that the piece of equipment spends in the particular room. For the office/kitchen equipment and for the portable/process equipment, these were distributed across various locations of the building where such equipment is likely to be used. The results of the analysis are largely insensitive to this distribution. For the other types of major equipment used in the facility to move waste forms around, the residence fraction is based on the facility throughput analysis.
[2] Welding weighting factor (WWF) represents the relative number of total welding activity (hours/year) that occurs in each location where welding is performed. The number of hours for maintenance-related welding is based on about 8 hours/week in the primary maintenance welding location and 5 hours per year in each satellite welding location (for repairs that must be performed locally). Waste Package Closure Room welding is estimated based in the IHF throughput Gantt chart and the total number of waste packages expected to be handled, as follows: (1) the preclosure period is 50 years; (2) the welding machine actually operates for about 15 hours per TAD canister; (3) the WHF will produce 1165 TAD canisters; 1165x15/50 = 350 hours per year. Note that for any given WP being processed, the total welding score is "at" the WP.
[3] Power ratings are for each motor unless otherwise noted.
CTM = canister transfer machine; HVAC = heating, ventilation, and air-conditioning; LLW = low level radioactive waste; TAD = transportation, aging, and disposal canister; RP = radiation protection; WP = waste package. Cabs = cabinets; decon = decontamination; exchngr = exchanger; maint = maintenance; xfmr = transformer.

Source: Original

Table F5.5-1. Fire Ignition Frequencies by Room

	Ignition Source Category and Room-by-Room Population									
Room	Electrical	HVAC	Mechanical Equipment	Heat-Generating Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/ Kitchen Equipment	Portable Equipment	No Equipment Involved	Room Ignition Frequency
B001									69	1.81E-03
B002			2						65	1.46E-02
B003									38	1.01E-03
B004									68	1.80E-03
B005									35	9.32E-04
B006									3	7.35E-05
B007									7	1.77E-04
B008									62	1.63E-03
B009									65	1.71E-03
P001 (incl. in 1016)									0	0.00E+00
1001		4	3		10	22			1630	9.66E-02
1002	22	2			5			4	186	6.76E-02
1003	1	4							30	2.14E-02
1004		4			5			4	216	5.23E-02
1005									9	2.43E-04
1006		6						4	160	5.66E-02
1007						61			182	2.38E-02
1008			0.03					2	133	1.53E-02
1009					5				228	1.00E-02
1010									38	9.93E-04
1011A									51	1.35E-03
1011B									137	3.63E-03
1012A									49	1.30E-03
1012B									100	2.65E-03
1013			1		5				315	1.88E-02
1014									18	4.85E-04
1015									6	1.54E-04
1016			36.97		365	78		8	4097	7.09E-01
1017	5		4						269	3.87E-02
1018		2			400				21	3.31E-01
1018A									14	3.82E-04
1018B									14	3.82E-04

Table F5.5-1. Fire Ignition Frequencies by Room (Continued)

	Ignition Source Category and Room-by-Room Population									
Room	Electrical	HVAC	Mechanical Equipment	Heat-Generating Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/ Kitchen Equipment	Portable Equipment	No Equipment Involved	Room Ignition Frequency
1019	23	2			5			4	186	6.87E-02
1020	1	4							30	2.14E-02
1021		4						4	216	4.83E-02
1022									6	1.54E-04
1023		3	4			39			434	6.39E-02
1024									20	5.30E-04
1025									29	7.65E-04
1026									31	8.24E-04
1027									31	8.24E-04
1028			1						56	7.91E-03
1029									28	7.35E-04
1030									17	4.41E-04
1031									31	8.09E-04
1032									27	7.06E-04
1032A									22	5.88E-04
1033									32	8.53E-04
1034									29	7.65E-04
1035									17	4.41E-04
1036			1						17	6.88E-03
1037									7	1.91E-04
1038									7	6.61E-03
1039									7	1.72E-04
1042A			1						19	6.95E-03
1042B			1						19	6.95E-03
1042C			1						19	6.95E-03
1043A									30	7.97E-04
1043B									30	7.97E-04
1043C									30	7.97E-04
1044A									25	6.69E-04
1044B									25	6.69E-04
1044C									25	6.69E-04

Table F5.5-1. Fire Ignition Frequencies by Room (Continued)

	Ignition Source Category and Room-by-Room Population									
Room	Electrical	HVAC	Mechanical Equipment	Heat-Generating Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/ Kitchen Equipment	Portable Equipment	No Equipment Involved	Room Ignition Frequency
1045A									33	8.83E-04
1045B									33	8.83E-04
1045C			1						100	9.08E-03
1045D									99	2.61E-03
1046	92								158	1.12E-01
1201									8	2.21E-04
1202							1		21	1.00E-02
1203									34	9.02E-04
1204									40	1.06E-03
1205							1		44	1.06E-02
1206									12	3.14E-04
1207									51	1.33E-03
1208									9	2.35E-04
1209							1		39	1.05E-02
1210							1		22	1.01E-02
1211							1		12	9.80E-03
1212							1		21	1.00E-02
1213									15	3.92E-04
1214									15	3.92E-04
1215							1		70	1.13E-02
1216							1		25	1.01E-02
1217							1		25	1.01E-02
1218A									60	1.59E-03
1218B									30	7.80E-04
1218C									58	1.53E-03
M001		3						4	474	5.03E-02
2001	66							4	140	1.04E-01
2001A	1	4							46	2.18E-02
2002		2						4	216	3.86E-02
2003		1						4	134	3.16E-02
2004			7		5			2	1017	8.75E-02

Table F5.5-1. Fire Ignition Frequencies by Room (Continued)

	Ignition Source Category and Room-by-Room Population									
Room	Electrical	HVAC	Mechanical Equipment	Heat-Generating Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/ Kitchen Equipment	Portable Equipment	No Equipment Involved	Room Ignition Frequency
2005A									142	3.76E-03
2005B									90	2.38E-03
2006									136	3.58E-03
2007A									52	1.37E-03
2007B									197	5.20E-03
2008					5				522	1.78E-02
2010		4						4	216	4.83E-02
2011A							2		95	2.15E-02
2011B							2		120	2.21E-02
2012	6						2		241	3.23E-02
2013									14	3.82E-04
2024									18	4.85E-04
2025									45	1.19E-03
2026									31	8.24E-04
2027									31	8.24E-04
2029									17	4.41E-04
2030									14	3.68E-04
2032									9	2.50E-04
2033									12	3.09E-04
2034									29	7.65E-04
2201							1		19	9.99E-03
2202							1		30	1.03E-02
2203							3		52	2.98E-02
2204									12	3.09E-04
2205									13	3.43E-04
2206									8	2.06E-04
TOTAL	217	49	64	0	810	200	20	52		2.51E+00

Source: Original

Table F5.6-1. Fire Propagation Probabilities

	Conditional Probability			Sampled Value	Mean Fraction	97.5% Value	97.5th percentile add
Alternative Definition							
No Propagation	0.551		0.551	0.551	0.551	0.667	0.117
Spreads Through Part of Room of Origin	0.317		0.317	0.317	0.317	0.426	0.109
Spreads Throughout Room of Origin	0.028		0.028	0.028	0.028	0.066	0.038
Spreads Throughout Fire-Rated Area of Origin	0.005		0.005	0.005	0.005	0.020	0.016
Spreads Throughout Floor of Origin	0.069		0.069	0.069	0.069	0.128	0.059
Spreads Throughout Building	0.028		0.028	0.028	0.028	0.055	0.028
Breaches Building Boundary	0.005		0.005	0.005	0.005	0.020	0.016
	1.000		1.000				
Alternative Definition							
No Propagation	0.621		0.621	0.621	0.621	0.725	0.104
Spreads Through Part of Room of Origin	0.149		0.149	0.149	0.149	0.226	0.076
Spreads Throughout Room of Origin	0.004		0.004	0.004	0.004	0.017	0.013
Spreads Throughout Fire-Rated Area of Origin	0.057		0.057	0.057	0.057	0.107	0.050
Spreads Throughout Floor of Origin	0.004		0.004	0.004	0.004	0.017	0.013
Spreads Throughout Building	0.161		0.161	0.161	0.161	0.240	0.079
Breaches Building Boundary	0.004		0.004	0.004	0.004	0.017	0.013
	1.000		1.000				

Source: Original

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions

WHF Residence Times and Fractions														
Section I - Localized Fires														
BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction	
TC/SNF on Truck Trailer in Receipt Area w/Tractor (Diesel Present)					**TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/Tractor/SPM (Diesel Present)**					**TC/DPC on Truck Trailer in Receipt Area w/Tractor (Diesel Present)**				
1.1.1		44			1.1.1		44			1.1.1	Steps 1-4	44		
Total		**44**	**1.7E-06**		**Total**		**44**	**1.7E-06**		**Total**		**44**	**1.7E-06**	
TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel)					**TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel)**					**TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel)**				
1.1.2		15			1.1.2		15			1.1.1	Step 5	75		
1.1.10		160			Not in BFD		170			1.1.2		15		
Not in BFD	Prepare CHC	15			1.1.3		90			1.1.10		206		
1.1.11		60			1.1.4	Prepare CHC	80			Not in BFD	Prepare CHC	15		
1.1.12		15			1.1.5		220			1.1.11		60		
1.1.13	Step 1	5			1.1.6		95			1.1.12		30		
Total		**270**	**1.0E-05**		1.1.7		40			1.1.24		20		
					Not in BFD	Prepare CHC	25			1.1.26	Step 1	5		
					1.1.8		15			**Total**		**426**	**1.6E-05**	
					1.1.9		40							
					1.1.24		20							
					1.1.26	Step 1	5							
					Total		**815**	**3.1E-05**						
TC/SNF in Preparation Station (Dry Cavity)					**TC/DPC (TTC) on CTT in Preparation Station**					**TC/DPC on CTT in Preparation Station**				
1.1.13	Steps 2-4	50			1.1.26	Steps 2-4	35			(Same as TTC)				
Not in BFD	Remove/Store Platform	15			1.1.27		200							
1.1.15	Steps 1-8	38			1.1.28		202							
Total		**103**	**3.9E-06**		1.1.29		30							
					1.1.30		20							
TC/SNF in Preparation Station (Wet Cavity)					1.1.31		40							
1.1.15	Steps 9-13	46			1.1.32		40							
1.1.16		36			1.1.33		40							
1.1.17		45			1.1.34		20							
Not in BFD	Prepare CHC	20			**Total**		**627**	**2.4E-05**						
1.1.18	Steps 1-6	55												
Total	38	**202**	**7.7E-06**											

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
					TC/DPC (TTC) on CTT in Unloading Room					**TC/DPC on CTT in Unloading Room**			
					1.1.34	again	20			(Same as TTC)			
					5.2.11		5						
					5.2.12		2						
					5.2.13		25						
					Total		**52**	**2.0E-06**					
					DPC (TTC) in CTM in Transfer Room					**DPC in CTM in Transfer Room**			
					5.2.13	Step 3 (again)	10			(Same as TTC)			
					5.2.14		2						
					5.2.15		5						
					5.2.27		5						
					5.2.28		2						
					5.2.29	Step 1	5						
					Total		**29**	**1.1E-06**					
					STC/DPC (TTC) on CTT in Unloading Room					**STC/DPC on CTT in Unloading Room**			
					5.2.29	again	35			(Same as TTC)			
					5.2.30		2						
					5.2.31		75						
					5.2.32		20						
					Total		**132**	**5.0E-06**					
					STC/DPC (TTC) on CTT in Preparation Station					**STC/DPC on CTT in Preparation Station**			
					5.2.32	Again	20			(Same as TTC)			
					5.2.33		35						
					5.2.34		40						
					5.2.35		69						
					5.2.36		40						
					5.2.37		75						
					5.2.38		270						
					5.2.39		220						
					5.2.40	Steps 1-6	35						
					Total		**804**	**3.1E-05**					
					STC/DPC (TTC) in DPC Cutting Station (Dry Cavity, Dry Annulus)					**STC/DPC in DPC Cutting Station (Dry Cavity, Dry Annulus)**			
					5.2.40	Steps 7-12	55			(Same as TTC)			
					3.1.1		105						
					Total		**160**	**6.1E-06**					

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
					STC/DPC (TTC) in DPC Cutting Station (Dry Cavity, Wet Annulus)					**STC/DPC in DPC Cutting Station (Dry Cavity, Wet Annulus)**			
					3.1.2		5			(Same as TTC)			
					3.1.3		12						
					3.1.4		65						
					3.1.5		40						
					3.1.6		30						
					3.1.7		10						
					3.1.8		75						
					3.1.9		250						
					3.1.10		160						
					3.1.11		10						
					3.1.12		30						
					3.1.13		250						
					3.1.14		55						
					3.1.15		60						
					3.1.16		40						
					Total		**1092**	**4.2E-05**					
					STC/DPC (TTC) in DPC Cutting Station (Wet Cavity, Wet Annulus)					**STC/DPC in DPC Cutting Station (Wet Cavity, Wet Annulus)**			
					3.1.17		5			(Same as TTC)			
					3.1.21		480						
					3.1.22		30						
					3.1.23		15						
					3.1.24		10						
					3.1.25		30						
					3.1.26		25						
					3.1.27		15						
					3.1.28		40						
					3.1.29		55						
					3.1.30		101						
					3.1.31		5						
					Not in BFD	Prepare CHC	20						
					3.1.32	Steps 1-6	55						
					Total		**886**	**3.4E-05**					

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
STC/TAD in TAD Closure Station (Wet Cavity)					**STC/TAD in TAD Closure Station (Wet Cavity)**					**STC/TAD in TAD Closure Station (Wet Cavity)**			
4.1.8	Step 4	15			(Same)					(Same)			
4.1.9		30											
4.1.10		20											
Not in BFD	Clean up CHC	25											
Not in BFD	PPE/Temp Shielding	90											
4.1.11		34											
4.1.12		12											
4.1.13		35											
4.1.14		35											
4.1.15		32											
4.1.16		15											
4.1.17		50											
4.1.18		440											
Not in BFD	Inspect weld	200											
4.1.19		34											
Total		**1067**	**4.1E-05**										
STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus)					**STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus)**					**STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus)**			
4.1.20		325			(Same)					(Same)			
4.1.21		200											
Not in BFD	Inspect weld	140											
4.1.22		35											
4.1.23		45											
4.1.24		65											
4.1.25		440											
Not in BFD	Inspect weld	200											
4.1.26		35											
4.1.27		35											
4.1.28		40											
4.1.29		240											
4.1.30		6											
4.1.31		38											
Total		**1844**	**7.0E-05**										
STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus)					**STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus)**					**STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus)**			
4.1.32		110			(Same)					(Same)			
Not in BFD	Close STC Drain Port	11											
1.5.6	Prepare CHC	45											
1.5.7		200											
1.5.8		12											
1.5.9		32											
Total		**410**	**1.6E-05**										

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
STC/TAD on CTT in Unloading Room					**STC/TAD on CTT in Unloading Room**					**STC/TAD on CTT in Unloading Room**			
1.5.9	Steps 2-4 (again)	20			**(Same as TC/SNF from here down)**					**(Same as TC/SNF from here down)**			
5.1.1		30											
5.1.2		5											
5.1.3		30											
5.1.4		2											
5.1.5		25											
Total		**112**	**4.3E-06**										
TAD in CTM in Transfer Room													
5.1.5	Step 3 (again)	10											
5.1.6		2											
5.1.7		5											
5.1.8		2											
5.1.9	Step 1	5											
Total		**24**	**9.1E-07**										
TAD in AO in Loading Room													
5.1.9	Again	35											
5.1.10		2											
1.6.1		45											
1.6.2		14											
Total		**96**	**3.7E-06**										
TAD in AO in Bolting Room													
1.6.2	Again	14											
1.6.3		240											
Total		**254**	**9.7E-06**										
Section II - Large Fire													
TC/SNF or TC/DPC (incl. TTC) w/Tractor/SPM (Diesel Present)													
1.1.1		44											
Total		**44**	**1.7E-06**										

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
TC/SNF (No Diesel)					**TC/DPC (TTC) (No Diesel)**					**TC/DPC (No Diesel)**			
1.1.2		15			1.1.2		15			1.1.1	Step 5	75	
1.1.10		160			Not in BFD		170			1.1.2		15	
Not in BFD	Prepare CHC	15			1.1.3		90			1.1.10		206	
1.1.11		60			1.1.4	Prepare CHC	80			Not in BFD	Prepare CHC	15	
1.1.12		15			1.1.5		220			1.1.11		60	
1.1.13		55			1.1.6		95			1.1.12		30	
Not in BFD	Remove/Store Platform	15			1.1.7		40			1.1.24		20	
1.1.15	Steps 1-8	38			Not in BFD	Prepare CHC	25			1.1.26		40	
Total		**373**	**1.4E-05**		1.1.8		15			1.1.27		200	
					1.1.9		40			1.1.28		202	
					1.1.24		20			1.1.29		30	
					1.1.26		40			1.1.30		20	
					1.1.27		200			1.1.31		40	
					1.1.28		202			1.1.32		20	
					1.1.29		30			1.1.26		5	
					1.1.30		20			1.1.32	again	20	
					1.1.31		40			5.2.11		5	
					1.1.32		40			5.2.12		2	
					1.1.33		40			5.2.13		25	
					1.1.34		20			**Total**		**1030**	**3.9E-05**
					5.2.11		5						
					5.2.12		2						
					5.2.13		25						
					Total		**1474**	**5.6E-05**					
					DPC (incl TTC) in CTM								
					5.2.13	Step 3 (again)	10						
					5.2.14		2						
					5.2.15		5						
					5.2.27		5						
					5.2.28		2						
					5.2.29	Step 1	5						
					Total		**29**	**1.1E-06**					

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
					STC/DPC (incl TTC)			
					5.2.29	again	35	
					5.2.30		2	
					5.2.31		75	
					5.2.32		20	
					5.2.33		35	
					5.2.34		40	
					5.2.35		69	
					5.2.36		40	
					5.2.37		75	
					5.2.38		270	
					5.2.39		220	
					5.2.40		90	
					3.1.1		105	
					Total		**1076**	**4.1E-05**
					STC/DPC (incl TTC) (Dry Cavity, Wet Annulus)			
					3.1.2		5	
					3.1.3		12	
					3.1.4		65	
					3.1.5		40	
					3.1.6		30	
					3.1.7		10	
					3.1.8		75	
					3.1.9		250	
					3.1.10		160	
					3.1.11		10	
					3.1.12		30	
					3.1.13		250	
					3.1.14		55	
					3.1.15		60	
					3.1.16		40	
					Total		**1092**	**4.2E-05**

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)	Fraction
					STC/DPC (incl TTC) (Wet Cavity, Wet Annulus)			
					3.1.17		5	
					3.1.21		480	
					3.1.22		30	
					3.1.23		15	
					3.1.24		10	
					3.1.25		30	
					3.1.26		25	
					3.1.27		15	
					3.1.28		40	
					3.1.29		55	
					3.1.30		101	
					3.1.31		5	
					Not in BFD	Prepare CHC	20	
					3.1.32	Steps 1-6	55	
					Total		**886**	**3.4E-05**
TC/SNF (Wet Cavity)								
1.1.15	Steps 9-13	46						
1.1.16		36						
1.1.17		45						
Not in BFD	Prepare CHC	20						
1.1.18	Steps 1-6	55						
Total		**202**	**7.7E-06**					

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction		BFD Task	Steps (if needed)	Time (m)
STC/TAD (Wet Cavity)					**STC/TAD**		
4.1.8	Step 4	15			TC/DPC (incl TTC) same as TC/SNF from here down)		
4.1.9		30					
4.1.10		20					
Not in BFD	Clean up CHC	25					
Not in BFD	PPE/Temp Shielding	90					
4.1.11		34					
4.1.12		12					
4.1.13		35					
4.1.14		35					
4.1.15		32					
4.1.16		15					
4.1.17		50					
4.1.18		440					
Not in BFD	Inspect weld	200					
4.1.19		34					
Total		**1067**	**4.1E-05**				
STC/TAD (Dry Cavity, Wet Annulus)							
4.1.20		325					
4.1.21		200					
Not in BFD	Inspect weld	140					
4.1.22		35					
4.1.23		45					
4.1.24		65					
4.1.25		440					
Not in BFD	Inspect weld	200					
4.1.26		35					
4.1.27		35					
4.1.28		40					
4.1.29		240					
4.1.30		6					
4.1.31		38					
Total		**1844**	**7.0E-05**				

Table F5.7-1. TAD canister, DPC, and SNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction
STC/TAD (Dry Cavity, Dry Annulus)			
4.1.32		110	
Not in BFD	Close STC Drain Port	11	
1.5.6	Prepare CHC	45	
1.5.7		200	
1.5.8		12	
1.5.9		32	
5.1.1		30	
5.1.2		5	
5.1.3		30	
5.1.4		2	
5.1.5	Steps 1-2	15	
Total		**492**	**1.9E-05**
TAD in CTM			
5.1.5	Step 3	10	
5.1.6		2	
5.1.7		5	
5.1.8		2	
5.1.9	Step 1	5	
Total		**24**	**9.1E-07**
TAD in AO			
5.1.9	Steps 2+	30	
5.1.10		2	
1.6.1		45	
1.6.2		14	
1.6.3		240	
Total		**331**	**1.3E-05**

NOTE: AO = aging overpack; BFD = block flow diagram; CHC = cask handling crane; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; PPE = personnel protective equipment; SNF = spent nuclear fuel; SPM = site prime mover; STC = shielded transfer cask; TAD = transportation, aging, and disposal canister; TC = transportation cask; TTC = a transportation cask that is upended using a tilt frame; m = minutes.

Source: Original

Table F5.7-2. Localized Fire Initiating Event Frequencies

Localized Fire Threatens Waste Form														
Contributions from Rooms Containing Waste Form														
Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
Entry represents a vulnerability due to the Railcar/Truck (Diesel Present)									TC/SNF or TC/DPC (incl. TTC)					
1001	Electrical	0	1.17E-03			0.211		0.061	1.7E-06	0.0E+00				
1016	HVAC	4	4.85E-03	4		0.211		0.061	1.7E-06	3.2E-08				
B001	Mechanical Equipment	39.97	6.44E-03	9	11.97	0.211	19	0.061	1.7E-06	1.4E-07				
B007	Heat Generating Equipment	0	0.00E+00			0.211		0.061	1.7E-06	0.0E+00				
B009	Torches, welders, burners	375	8.01E-04			0.211	375	0.061	1.7E-06	3.1E-08				
	Internal combustion engines	100	3.11E-04	100		0.211		0.061	1.7E-06	5.2E-08				
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	1.7E-06	0.0E+00				
	Portable Equipment	8	5.81E-03	1	2	0.211	5	0.061	1.7E-06	1.7E-08				
	No equipment involved	5866	2.64E-05	2808	120	0.211	2938	0.061	1.7E-06	1.3E-07				
Propagation from rooms in Fire Zone FA-00-01														
1022			1.54E-04			0.057			1.7E-06	1.5E-11				
B002			1.46E-02			0.057			1.7E-06	1.4E-09				
B003			1.01E-03			0.057			1.7E-06	9.8E-11				
B004			1.80E-03			0.057			1.7E-06	1.7E-10				
B006			7.35E-05			0.057			1.7E-06	7.1E-12				
B008			1.63E-03			0.057			1.7E-06	1.6E-10				
P001			0.00E+00			0.057			1.7E-06	0.0E+00				
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)										**4.0E-07**				

Table F5.7-2. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
Entry represents a vulnerability due to the Railcar/Truck (Diesel Present)									TC/SNF		TC/DPC (TTC)		TC/DPC	
1001	Electrical	0	1.17E-03			0.211		0.061	1.0E-05	0.0E+00	3.1E-05	0.0E+00	1.6E-05	0.0E+00
1016	HVAC	4	4.85E-03	4		0.211		0.061	1.0E-05	2.0E-07	3.1E-05	6.0E-07	1.6E-05	3.1E-07
B001	Mechanical Equipment	39.97	6.44E-03	9	11.97	0.211	19	0.061	1.0E-05	8.4E-07	3.1E-05	2.5E-06	1.6E-05	1.3E-06
B007	Heat Generating Equipment	0	0.00E+00			0.211		0.061	1.0E-05	0.0E+00	3.1E-05	0.0E+00	1.6E-05	0.0E+00
B009	Torches, welders, burners	375	8.01E-04			0.211	375	0.061	1.0E-05	1.9E-07	3.1E-05	5.7E-07	1.6E-05	3.0E-07
	Internal combustion engines	100	3.11E-04			0.211	100	0.061	1.0E-05	2.0E-08	3.1E-05	5.9E-08	1.6E-05	3.1E-08
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	1.0E-05	0.0E+00	3.1E-05	0.0E+00	1.6E-05	0.0E+00
	Portable Equipment	8	5.81E-03	1	2	0.211	5	0.061	1.0E-05	1.0E-07	3.1E-05	3.1E-07	1.6E-05	1.6E-07
	No equipment involved	5866	2.64E-05	2808	120	0.211	2938	0.061	1.0E-05	8.2E-07	3.1E-05	2.5E-06	1.6E-05	1.3E-06
Propagation from rooms in Fire Zone FA-00-01														
1022			1.54E-04			0.057			1.0E-05	9.1E-11	3.1E-05	2.8E-10	1.6E-05	1.4E-10
B002			1.46E-02			0.057			1.0E-05	8.6E-09	3.1E-05	2.6E-08	1.6E-05	1.4E-08
B003			1.01E-03			0.057			1.0E-05	6.0E-10	3.1E-05	1.8E-09	1.6E-05	9.5E-10
B004			1.80E-03			0.057			1.0E-05	1.1E-09	3.1E-05	3.2E-09	1.6E-05	1.7E-09
B006			7.35E-05			0.057			1.0E-05	4.3E-11	3.1E-05	1.3E-10	1.6E-05	6.9E-11
B008			1.63E-03			0.057			1.0E-05	9.6E-10	3.1E-05	2.9E-09	1.6E-05	1.5E-09
P001			0.00E+00			0.057			1.0E-05	0.0E+00	3.1E-05	0.0E+00	1.6E-05	0.0E+00
Localized Fire Threatens Waste Form on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)														
	Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)									**2.2E-06**				
	Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)											**6.6E-06**		
	Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)													**3.4E-06**
Entry represents a vulnerability due to the Preparation Station									TC/SNF (Dry Cavity)		TC/SNF (Wet Cavity)			
1016	Electrical	0	1.17E-03			0.211		0.061	3.9E-06	0.0E+00	7.7E-06	0.0E+00		
B001	HVAC	0	4.85E-03			0.211		0.061	3.9E-06	0.0E+00	7.7E-06	0.0E+00		
B007	Mechanical Equipment	36.97	6.44E-03	13	9	0.211	14.97	0.061	3.9E-06	4.0E-07	7.7E-06	7.8E-07		
B009	Heat Generating Equipment	0	0.00E+00			0.211		0.061	3.9E-06	0.0E+00	7.7E-06	0.0E+00		
	Torches, welders, burners	365	8.01E-04	365		0.211		0.061	3.9E-06	1.1E-06	7.7E-06	2.2E-06		
	Internal combustion engines	78	3.11E-04			0.211	78	0.061	3.9E-06	5.8E-09	7.7E-06	1.1E-08		
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	3.9E-06	0.0E+00	7.7E-06	0.0E+00		
	Portable Equipment	8	5.81E-03		3	0.211	5	0.061	3.9E-06	2.1E-08	7.7E-06	4.2E-08		
	No equipment involved	4237	2.64E-05	30	120	0.211	4087	0.061	3.9E-06	3.2E-08	7.7E-06	6.2E-08		
Propagation from rooms in Fire Zone FA-00-01														
1001			9.66E-02			0.057			3.9E-06	2.2E-08	7.7E-06	4.3E-08		
1022			1.54E-04			0.057			3.9E-06	3.5E-11	7.7E-06	6.8E-11		
B002			1.46E-02			0.057			3.9E-06	3.3E-09	7.7E-06	6.4E-09		
B003			1.01E-03			0.057			3.9E-06	2.3E-10	7.7E-06	4.5E-10		
B004			1.80E-03			0.057			3.9E-06	4.1E-10	7.7E-06	8.0E-10		
B006			7.35E-05			0.057			3.9E-06	1.7E-11	7.7E-06	3.2E-11		
B008			1.63E-03			0.057			3.9E-06	3.7E-10	7.7E-06	7.2E-10		
P001			0.00E+00			0.057			3.9E-06	0.0E+00	7.7E-06	0.0E+00		
Localized Fire Threatens TC/SNF in the Preparation Area														
	Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area									**1.6E-06**				
	Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station in the Preparation Area											**3.2E-06**		

Table F5.7-2. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
Entry represents a vulnerability due to the CTT and Preparation Station									TC/DPC		STC/DPC			
1016	Electrical	0	1.17E-03			0.211		0.061	2.4E-05	0.0E+00	3.1E-05	0.0E+00		
B001	HVAC	0	4.85E-03			0.211		0.061	2.4E-05	0.0E+00	3.1E-05	0.0E+00		
B007	Mechanical Equipment	36.97	6.44E-03	13.97	9	0.211	14	0.061	2.4E-05	2.6E-06	3.1E-05	3.3E-06		
B009	Heat Generating Equipment	0	0.00E+00			0.211		0.061	2.4E-05	0.0E+00	3.1E-05	0.0E+00		
	Torches, welders, burners	365	8.01E-04			0.211	365	0.061	2.4E-05	4.3E-07	3.1E-05	5.5E-07		
	Internal combustion engines	78	3.11E-04			0.211	78	0.061	2.4E-05	3.5E-08	3.1E-05	4.5E-08		
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	2.4E-05	0.0E+00	3.1E-05	0.0E+00		
	Portable Equipment	8	5.81E-03		3	0.211	5	0.061	2.4E-05	1.3E-07	3.1E-05	1.7E-07		
	No equipment involved	4237	2.64E-05	30	120	0.211	4087	0.061	2.4E-05	1.9E-07	3.1E-05	2.5E-07		
Propagation from rooms in Fire Zone FA-00-01														
1001			9.66E-02			0.057			2.4E-05	1.3E-07	3.1E-05	1.7E-07		
1022			1.54E-04			0.057			2.4E-05	2.1E-10	3.1E-05	2.7E-10		
B002			1.46E-02			0.057			2.4E-05	2.0E-08	3.1E-05	2.6E-08		
B003			1.01E-03			0.057			2.4E-05	1.4E-09	3.1E-05	1.8E-09		
B004			1.80E-03			0.057			2.4E-05	2.5E-09	3.1E-05	3.2E-09		
B006			7.35E-05			0.057			2.4E-05	1.0E-10	3.1E-05	1.3E-10		
B008			1.63E-03			0.057			2.4E-05	2.2E-09	3.1E-05	2.9E-09		
P001			0.00E+00			0.057			2.4E-05	0.0E+00	3.1E-05	0.0E+00		
Localized Fire Threatens TC/DPC or STC/DPC on CTT in the Preparation Station														
	Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station in the Preparation Area									**3.5E-06**				
	Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area											**4.5E-06**		
Entry represents a vulnerability due to the Cask Transfer Trolley									TC/DPC		STC/DPC		STC/TAD	
1008	Electrical	0	1.17E-03			0.211		0.061	2.0E-06	0.0E+00	5.0E-06	0.0E+00	4.3E-06	0.0E+00
2004	HVAC	0	4.85E-03			0.211		0.061	2.0E-06	0.0E+00	5.0E-06	0.0E+00	4.3E-06	0.0E+00
	Mechanical Equipment	7.98	6.44E-03	7.98	0	0.211		0.061	2.0E-06	1.0E-07	5.0E-06	2.6E-07	4.3E-06	2.2E-07
	Heat Generating Equipment	0	0.00E+00			0.211		0.061	2.0E-06	0.0E+00	5.0E-06	0.0E+00	4.3E-06	0.0E+00
	Torches, welders, burners	5	8.01E-04			0.211	5	0.061	2.0E-06	4.9E-10	5.0E-06	1.2E-09	4.3E-06	1.0E-09
	Internal combustion engines	0	3.11E-04			0.211		0.061	2.0E-06	0.0E+00	5.0E-06	0.0E+00	4.3E-06	0.0E+00
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	2.0E-06	0.0E+00	5.0E-06	0.0E+00	4.3E-06	0.0E+00
	Portable Equipment	4	5.81E-03		2	0.211	2	0.061	2.0E-06	6.3E-09	5.0E-06	1.6E-08	4.3E-06	1.3E-08
	No equipment involved	1150	2.64E-05	150	120	0.211	880	0.061	2.0E-06	1.2E-08	5.0E-06	3.0E-08	4.3E-06	2.6E-08
Propagation from rooms in Fire Zone FA-32-01														
2003			3.16E-02			0.057			2.0E-06	3.6E-09	5.0E-06	9.1E-09	4.3E-06	7.7E-09
2006			3.58E-03			0.057			2.0E-06	4.1E-10	5.0E-06	1.0E-09	4.3E-06	8.8E-10
2032			2.50E-04			0.057			2.0E-06	2.8E-11	5.0E-06	7.2E-11	4.3E-06	6.1E-11
Localized Fire Threatens Waste Form on CTT in the Unloading Room														
	Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room									**1.2E-07**				
	Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room											**3.2E-07**		
	Localized Fire Threatens STC/TAD on CTT in the Unloading Room													**2.7E-07**

Table F5.7-2. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
Entry represents a vulnerability due to the Canister Transfer Machine									DPC		TAD			
2004	Electrical	0	1.17E-03			0.211		0.061	1.1E-06	0.0E+00	9.1E-07	0.0E+00		
	HVAC	0	4.85E-03			0.211		0.061	1.1E-06	0.0E+00	9.1E-07	0.0E+00		
	Mechanical Equipment	7.95	6.44E-03	7.95		0.211		0.061	1.1E-06	5.6E-08	9.1E-07	4.7E-08		
	Heat Generating Equipment	0	0.00E+00			0.211		0.061	1.1E-06	0.0E+00	9.1E-07	0.0E+00		
	Torches, welders, burners	5	8.01E-04			0.211	5	0.061	1.1E-06	2.7E-10	9.1E-07	2.2E-10		
	Internal combustion engines	0	3.11E-04			0.211		0.061	1.1E-06	0.0E+00	9.1E-07	0.0E+00		
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	1.1E-06	0.0E+00	9.1E-07	0.0E+00		
	Portable Equipment	2	5.81E-03		1	0.211	1	0.061	1.1E-06	1.7E-09	9.1E-07	1.4E-09		
	No equipment involved	1017	2.64E-05	163	120	0.211	734	0.061	1.1E-06	6.8E-09	9.1E-07	5.6E-09		
Propagation from rooms in Fire Zone FA-32-01														
2003			3.16E-02			0.057			1.1E-06	2.0E-09	9.1E-07	1.7E-09		
2006			3.58E-03			0.057			1.1E-06	2.3E-10	9.1E-07	1.9E-10		
2032			2.50E-04			0.057			1.1E-06	1.6E-11	9.1E-07	1.3E-11		
Localized Fire Threatens DPC or TAD in the Transfer Room														
	Localized Fire Threatens DPC (all) in the Transfer Room									**6.8E-08**				
	Localized Fire Threatens TAD in the Transfer Room											**5.6E-08**		
									STC/DPC		STC/DPC (Dry Cavity,		STC/DPC (Wet Cavity,	
Entry represents a vulnerability due to the DPC Cutting Station									(Dry Cavity, Dry Annulus)		Wet Annulus)		Wet Annulus)	
1016	Electrical	0	1.17E-03			0.211		0.061	6.1E-06	0.0E+00	4.2E-05	0.0E+00	3.4E-05	0.0E+00
B001	HVAC	0	4.85E-03			0.211		0.061	6.1E-06	0.0E+00	4.2E-05	0.0E+00	3.4E-05	0.0E+00
B007	Mechanical Equipment	36.97	6.44E-03	13.97	7	0.211	16	0.061	6.1E-06	6.4E-07	4.2E-05	4.4E-06	3.4E-05	3.6E-06
B009	Heat Generating Equipment	0	0.00E+00			0.211		0.061	6.1E-06	0.0E+00	4.2E-05	0.0E+00	3.4E-05	0.0E+00
	Torches, welders, burners	365	8.01E-04		365	0.211		0.061	6.1E-06	3.8E-07	4.2E-05	2.6E-06	3.4E-05	2.1E-06
	Internal combustion engines	78	3.11E-04			0.211	78	0.061	6.1E-06	9.1E-09	4.2E-05	6.2E-08	3.4E-05	5.0E-08
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	6.1E-06	0.0E+00	4.2E-05	0.0E+00	3.4E-05	0.0E+00
	Portable Equipment	8	5.81E-03		3	0.211	5	0.061	6.1E-06	3.3E-08	4.2E-05	2.3E-07	3.4E-05	1.8E-07
	No equipment involved	4237	2.64E-05	30	120	0.211	4087	0.061	6.1E-06	4.9E-08	4.2E-05	3.4E-07	3.4E-05	2.7E-07
Propagation from rooms in Fire Zone FA-00-01														
1001			9.66E-02			0.057			6.1E-06	3.4E-08	4.2E-05	2.3E-07	3.4E-05	1.9E-07
1022			1.54E-04			0.057			6.1E-06	5.4E-11	4.2E-05	3.7E-10	3.4E-05	3.0E-10
B002			1.46E-02			0.057			6.1E-06	5.1E-09	4.2E-05	3.5E-08	3.4E-05	2.8E-08
B003			1.01E-03			0.057			6.1E-06	3.6E-10	4.2E-05	2.4E-09	3.4E-05	2.0E-09
B004			1.80E-03			0.057			6.1E-06	6.3E-10	4.2E-05	4.3E-09	3.4E-05	3.5E-09
B006			7.35E-05			0.057			6.1E-06	2.6E-11	4.2E-05	1.8E-10	3.4E-05	1.4E-10
B008			1.63E-03			0.057			6.1E-06	5.7E-10	4.2E-05	3.9E-09	3.4E-05	3.1E-09
P001			0.00E+00			0.057			6.1E-06	0.0E+00	4.2E-05	0.0E+00	3.4E-05	0.0E+00
Localized Fire Threatens STC/DPC in DPC Cutting Station in the Preparation Area														
	Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area									**1.2E-06**				
	Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area											**7.9E-06**		
	Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area													**6.4E-06**

Table F5.7-2. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
									STC/TAD (Dry Cavity, Dry Annulus)		STC/TAD (Dry Cavity, Wet		STC/TAD (Wet Cavity Annulus)	
Entry represents a vulnerability due to the TAD Closure Station														
1016	Electrical	0	1.17E-03			0.211		0.061	1.6E-05	0.0E+00	7.0E-05	0.0E+00	4.1E-05	0.0E+00
B001	HVAC	0	4.85E-03			0.211		0.061	1.6E-05	0.0E+00	7.0E-05	0.0E+00	4.1E-05	0.0E+00
B007	Mechanical Equipment	36.97	6.44E-03	14	9.97	0.211	13	0.061	1.6E-05	1.7E-06	7.0E-05	4.4E-06	4.1E-05	3.6E-06
B009	Heat Generating Equipment	0	0.00E+00			0.211		0.061	1.6E-05	0.0E+00	7.0E-05	0.0E+00	4.1E-05	0.0E+00
	Torches, welders, burners	365	8.01E-04	365		0.211		0.061	1.6E-05	4.6E-06	7.0E-05	2.6E-06	4.1E-05	2.1E-06
	Internal combustion engines	78	3.11E-04			0.211	78	0.061	1.6E-05	2.3E-08	7.0E-05	6.2E-08	4.1E-05	5.0E-08
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	1.6E-05	0.0E+00	7.0E-05	0.0E+00	4.1E-05	0.0E+00
	Portable Equipment	8	5.81E-03		3	0.211	5	0.061	1.6E-05	8.5E-08	7.0E-05	2.3E-07	4.1E-05	1.8E-07
	No equipment involved	4237	2.64E-05	30	120	0.211	4087	0.061	1.6E-05	1.3E-07	7.0E-05	3.4E-07	4.1E-05	2.7E-07
Propagation from rooms in Fire Zone FA-00-01														
1001			9.66E-02			0.057			1.6E-05	8.7E-08	7.0E-05	3.9E-07	4.1E-05	2.3E-07
1022			1.54E-04			0.057			1.6E-05	1.4E-10	7.0E-05	6.2E-10	4.1E-05	3.6E-10
B002			1.46E-02			0.057			1.6E-05	1.3E-08	7.0E-05	5.9E-08	4.1E-05	3.4E-08
B003			1.01E-03			0.057			1.6E-05	9.1E-10	7.0E-05	4.1E-09	4.1E-05	2.4E-09
B004			1.80E-03			0.057			1.6E-05	1.6E-09	7.0E-05	7.3E-09	4.1E-05	4.2E-09
B006			7.35E-05			0.057			1.6E-05	6.6E-11	7.0E-05	3.0E-10	4.1E-05	1.7E-10
B008			1.63E-03			0.057			1.6E-05	1.5E-09	7.0E-05	6.6E-09	4.1E-05	3.8E-09
Localized Fire Threatens STC/TAD in TAD Closure Station in the Preparation Area														
	Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area									**6.6E-06**				
	Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area											**8.0E-06**		
	Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area													**6.4E-06**
Entry represents a vulnerability due to the Site Transporter									TAD in AO					
1007	Electrical	0	1.17E-03			0.211		0.061	3.7E-06	0.0E+00				
2004	HVAC	0	4.85E-03			0.211		0.061	3.7E-06	0.0E+00				
	Mechanical Equipment	7	6.44E-03	5		0.211	2	0.061	3.7E-06	1.2E-07				
	Heat Generating Equipment	0	0.00E+00			0.211		0.061	3.7E-06	0.0E+00				
	Torches, welders, burners	5	8.01E-04			0.211	5	0.061	3.7E-06	9.0E-10				
	Internal combustion engines	61	3.11E-04	61		0.211		0.061	3.7E-06	6.9E-08				
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	3.7E-06	0.0E+00				
	Portable Equipment	2	5.81E-03	1		0.211	1	0.061	3.7E-06	2.3E-08				
	No equipment involved	1199	2.64E-05	182	120	0.211	897	0.061	3.7E-06	2.5E-08				
Propagation from rooms in Fire Zone FA-32-01														
2003			3.16E-02			0.057			3.7E-06	6.6E-09				
2006			3.58E-03			0.057			3.7E-06	7.5E-10				
2032			2.50E-04			0.057			3.7E-06	5.3E-11				
Localized Fire Threatens TAD in AO in Loading Room										**2.5E-07**				

Table F5.7-2. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (If Applicable)	Number in Room	Frequency per Unit (50 years)	Number at Target	Number Near Target	Propagation Probability to Target	Number Away from Target	Propagation Probability to Target	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)	Target Exposure Time (Fraction)	Contribution to IE Frequency (50 years)
Entry represents a vulnerability due to the Site Transporter									TAD in AO					
1023	Electrical	0	1.17E-03			0.211		0.061	9.7E-06	0.0E+00				
	HVAC	3	4.85E-03		3	0.211		0.061	9.7E-06	3.0E-08				
	Mechanical Equipment	4	6.44E-03	2	2	0.211		0.061	9.7E-06	1.5E-07				
	Heat Generating Equipment	0	0.00E+00			0.211		0.061	9.7E-06	0.0E+00				
	Torches, welders, burners	0	8.01E-04			0.211		0.061	9.7E-06	0.0E+00				
	Internal combustion engines	39	3.11E-04	39		0.211		0.061	9.7E-06	1.2E-07				
	Office/kitchen equipment	0	9.48E-03			0.211		0.061	9.7E-06	0.0E+00				
	Portable Equipment	0	5.81E-03			0.211		0.061	9.7E-06	0.0E+00				
	No equipment involved	434	2.64E-05	280	120	0.211	34	0.061	9.7E-06	7.8E-08				
Localized Fire Threatens TAD in AO in Bolting Room										**3.8E-07**				

Source: Original

Table F5.7-3. Localized Fire Initiating Events with Multiple Rooms of Origin

Rooms	Vulnerability	Justification
1001	Railcar/Truck (Diesel)	Rooms 1001 and 1016 are open to each other due to open doors as the Railcar/Truck moves from 1001 to 1016. Room 1016 is open to rooms B001, B007, and B009.
1016		
B001		
B007		
B009		
1016	Railcar/Truck (Diesel) Preparation Station DPC Cutting Station Cask Transfer Trolley	Room 1016 is open to rooms B001, B007, and B009 at all times.
B001		
B007		
B009		
1008	Cask Transfer Trolley	Rooms open to each other through the port slide gates as the cask is accessed from room 2004
2004		

Source: Original

Table F5.7-4. Large Fire Initiating Event Frequencies

Large Fire Threatens Waste Form In Fire Zones Containing Vulnerable Waste Forms										
Large fires are those that spread beyond the boundaries of a fire area, up through those that breach the building boundary.										
					Total Ignition Frequency	Propagation Probability Beyond Fire -rated Area			Target Exposure Time (Fraction)	Contribution to IE Frequency
Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present)					2.51E+00	0.169			1.7E-06	7.1E-07
Large Fire Threatens TC/SNF (No Diesel)					2.51E+00	0.169			1.4E-05	6.0E-06
Large Fire Threatens TC/DPC (TTC) (No Diesel)					2.51E+00	0.169			5.6E-05	2.4E-05
Large Fire Threatens TC/DPC (No Diesel)					2.51E+00	0.169			3.9E-05	1.7E-05
Large Fire Threatens DPC (all) in CTM					2.51E+00	0.169			1.1E-06	4.7E-07
Large Fire Threatens STC/DPC (all)					2.51E+00	0.169			4.1E-05	1.7E-05
Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus)					2.51E+00	0.169			4.2E-05	1.8E-05
Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus)					2.51E+00	0.169			3.4E-05	1.4E-05
Large Fire Threatens TC/SNF (Wet Cavity)					2.51E+00	0.169			7.7E-06	3.3E-06
Large Fire Threatens STC/TAD (Wet Cavity, Wet Annulus)					2.51E+00	0.169			4.1E-05	1.7E-05
Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus)					2.51E+00	0.169			7.0E-05	3.0E-05
Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus)					2.51E+00	0.169			1.9E-05	7.9E-06
Large Fire Threatens TAD in CTM					2.51E+00	0.169			9.1E-07	3.9E-07
Large Fire Threatens TAD in AO					2.51E+00	0.169			1.3E-05	5.3E-06

Source: Original

Table F5.7-5. Fire Initiating Events Results Summary

Initiating Event	Equipment	Mean	Median	97.5% Value	Error Factor	Type
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	**Railcar/Truck**					
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w /Tractor (Diesel Present)		4.7E-07	4.2E-07	1.1E-06	2.2E+00	Lognormal
Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)	**Railcar/Truck**					
Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w /o Tractor (No Diesel Present)		2.5E-06	2.3E-06	5.7E-06	2.2E+00	Lognormal
Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w /o Tractor/SPM (No Diesel Present)		7.6E-06	6.8E-06	1.7E-05	2.2E+00	Lognormal
Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w /o Tractor (No Diesel Present)		4.0E-06	3.6E-06	9.0E-06	2.2E+00	Lognormal
Localized Fire Threatens TC/SNF in the Preparation Area	**Preparation Station**					
Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area		1.9E-06	1.7E-06	4.2E-06	2.1E+00	Lognormal
Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station in the Preparation Area		3.6E-06	3.3E-06	8.2E-06	2.1E+00	Lognormal
Localized Fire Threatens TC/DPC or STC/DPC on CTT in the Preparation Station	**Cask Transfer Trolley**					
Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station in the Preparation Area		4.2E-06	3.8E-06	9.8E-06	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area		5.4E-06	4.8E-06	1.3E-05	2.2E+00	Lognormal
Localized Fire Threatens Waste Form on CTT in the Unloading Room	**Cask Transfer Trolley**					
Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room		1.5E-07	1.4E-07	3.5E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room		3.9E-07	3.5E-07	8.9E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD on CTT in the Unloading Room		3.3E-07	3.0E-07	7.6E-07	2.2E+00	Lognormal
Localized Fire Threatens DPC or TAD in the Transfer Room	**Canister Transfer Machine**					
Localized Fire Threatens DPC (all) in the Transfer Room		8.3E-08	7.4E-08	1.9E-07	2.2E+00	Lognormal
Localized Fire Threatens TAD in the Transfer Room		6.9E-08	6.2E-08	1.6E-07	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC in DPC Cutting Station in the Preparation Area	**DPC Cutting Station**					
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area		1.2E-06	1.1E-06	2.8E-06	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area		8.3E-06	7.4E-06	1.9E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area		6.8E-06	6.0E-06	1.5E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station in the Preparation Area	**TAD Closure Station**					
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area		7.5E-06	6.8E-06	1.7E-05	2.1E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area		8.6E-06	7.6E-06	2.0E-05	2.2E+00	Lognormal
Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area		6.8E-06	6.1E-06	1.6E-05	2.2E+00	Lognormal
Localized Fire Threatens TAD in AO in Loading Room	**Site Transporter**					
Localized Fire Threatens TAD in AO in Loading Room		2.9E-07	2.6E-07	6.8E-07	2.2E+00	Lognormal
Localized Fire Threatens TAD in AO in Bolting Room	**Site Transporter**					
Localized Fire Threatens TAD in AO in Bolting Room		3.5E-07	3.1E-07	8.3E-07	2.2E+00	Lognormal

Table F5.7-5. Fire Initiating Events Results Summary (Continued)

Initiating Event	Mean	Median	97.5% Value	Error Factor	Type
Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present)	7.9E-07	7.0E-07	1.8E-06	2.2E+00	Lognormal
Large Fire Threatens TC/SNF (No Diesel)	6.7E-06	5.9E-06	1.6E-05	2.2E+00	Lognormal
Large Fire Threatens TC/DPC (TTC) (No Diesel)	2.6E-05	2.3E-05	6.1E-05	2.2E+00	Lognormal
Large Fire Threatens TC/DPC (No Diesel)	1.8E-05	1.6E-05	4.3E-05	2.2E+00	Lognormal
Large Fire Threatens DPC (all) in CTM	5.2E-07	4.6E-07	1.2E-06	2.3E+00	Lognormal
Large Fire Threatens STC/DPC (all)	1.9E-05	1.7E-05	4.5E-05	2.1E+00	Lognormal
Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus)	2.0E-05	1.7E-05	4.6E-05	2.4E+00	Lognormal
Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus)	1.6E-05	1.4E-05	3.7E-05	2.3E+00	Lognormal
Large Fire Threatens TC/SNF (Wet Cavity)	3.6E-06	3.2E-06	8.4E-06	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Wet Cavity, Wet Annulus)	1.9E-05	1.7E-05	4.4E-05	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus)	3.3E-05	2.9E-05	7.7E-05	2.2E+00	Lognormal
Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus)	8.8E-06	7.8E-06	2.1E-05	2.2E+00	Lognormal
Large Fire Threatens TAD in CTM	4.3E-07	3.8E-07	1.0E-06	2.2E+00	Lognormal
Large Fire Threatens TAD in AO	5.9E-06	5.3E-06	1.4E-05	2.2E+00	Lognormal

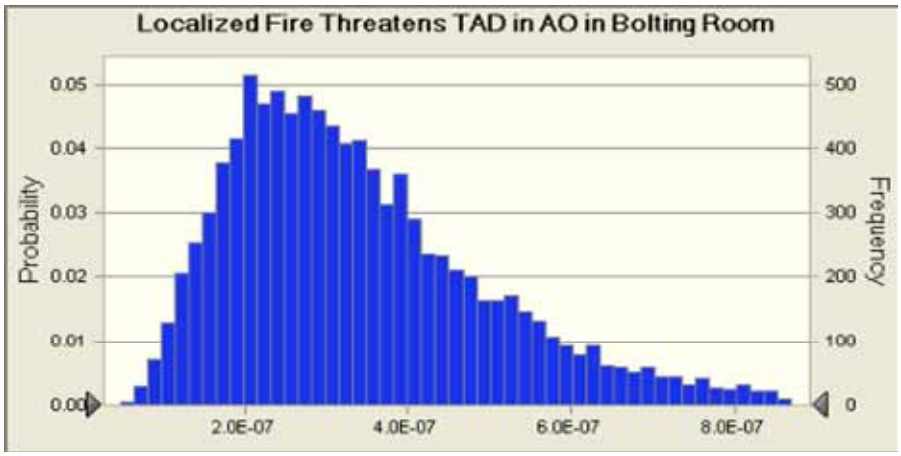
Source: Original

Figure F5.7-1. Example of Crystal Ball Output for a Fire Initiating Event

Forecast: Localized Fire Threatens TAD in AO in Bolting Room **Cell: K213**

Summary:

Entire range is from 4.8E-08 to 1.7E-06
Base case is 3.1E-07
After 10,000 trials, the std. error of the mean is 1.8E-09



Statistics:	Forecast values
Trials	10,000
Mean	3.5E-07
Median	3.1E-07
Mode	---
Standard Deviation	1.8E-07
Variance	3.4E-14
Skewness	1.57
Kurtosis	6.98
Coeff. of Variability	0.5229
Minimum	4.8E-08
Maximum	1.7E-06
Range Width	1.7E-06
Mean Std. Error	1.8E-09

Forecast: Localized Fire Threatens TAD in AO in Bolting Room (cont'd) **Cell: K213**

Percentiles:	Forecast values
0%	4.8E-08
10%	1.7E-07
20%	2.1E-07
30%	2.4E-07
40%	2.8E-07
50%	3.1E-07
60%	3.5E-07
70%	4.0E-07
80%	4.7E-07
90%	5.8E-07
100%	1.7E-06

APPENDIX F.I
DEFINITION OF IGNITION SOURCE CATEGORY

Table F.I-1. Ignition Source Categories

Ignition Source Category	NFPA Equipment Categories Included
Electrical Equipment	**Fixed wiring**; **transformer, associated over current or disconnect equipment**; **meter, meter box**; power switch gear, over current protection devices; switch, receptacle, outlet; lighting fixture, lamp holder, ballast, sign; cord, plug; lamp, light bulb; unclassified or **unknown-type electrical distribution equipment**; electronic equipment; rectifier, charger
Mechanical and Electrical HVAC Equipment	**Central heating unit**; water heater; **fixed, stationary local heating unit**; central air conditioning, refrigeration equipment; water cooling device, tower; **fixed, stationary local refrigeration unit**; fixed, stationary local air conditioning unit; chimney, gas vent flue; chimney connector, vent connector; **heat transfer system**; unclassified heating systems; **other HVAC equipment;** and unclassified air conditioning, refrigeration systems
Mechanical Equipment	Chemical process equipment; **waste recovery equipment**; **working, shaping machine**; coating machine; painting machine; unclassified process equipment; **separate motor or generator**; separate pump or compressor; conveyor, and **unknown mechanical equipment**
Fixed Heat-Generating Process Equipment	**Casting, molding, or forging equipment**; heat treating equipment; **dryers; furnaces; and incinerators**.
Torches/Welders	**Torches, welders, and burners**
Internal Combustion Engines	**Internal combustion engines**
Office and Kitchen Equipment	**Television, radio, stereo; fixed food warming appliance; fixed or stationary oven;** and all other categories
Portable and Special Equipment	**Portable local heating unit**; **hand tools**; portable appliance designed to produce controlled heat; **portable appliance designed not to produce heat; unclassified special equipment; unclassified service or maintenance equipment; biomedical equipment or device**
No Equipment Involved	**No equipment**

NOTE: The entries shown in bold in the table were those that had caused fires in the data set. The other entries were included in the data set retrieval, but no fires were attributed to them. Given that there were only a total of 188 fires in the entire data set, the fact that certain items had not been associated with an observed fire cannot be taken to mean that they can be eliminated as potential ignition sources.

Source: Ref F2.65

APPENDIX F.II
DERIVATION OF IGNITION SOURCE DISTRIBUTION AND FIRE PROPAGATION PROBABILITIES

Three independent data sets concerning fires in radioactive material working facilities (Tables F.II-1 through F.II-3) have been analyzed for statistical confidence. The data sets are in the format of a tally; each sample (fire) is placed in the appropriate category (e.g., equipment type, extent of flame damage), and the reported figure for each category is the number of fires that pertained to the category. All of these data sets reflect the operating history of nuclear facilities of non-combustible construction as defined by the National Fire Protection Association (NFPA). The NFPA data is taken from *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction* (Ref. F2.65).

The first data set provides a distribution of fire ignition as a function of the ignition source category, as defined in Appendix .FI. Table F.II -1 provides a summary of that data.

Table F.II-1 Fires in Radioactive Material Working Facilities by Originating Equipment

Ignition Source Category	Fires	
Electrical	16	9%
Mechanical/Electrical HVAC	15	8%
Mechanical	26	14%
Heat Generating	29	16%
Torches/Welders	41	22%
Internal Combustion	4	2%
Offices/Kitchen Equipment	12	6%
Portable Equipment	19	10%
No Equipment	25	13%
Total	187	100%

NOTE: HVAC = heating, ventilation, and air conditioning.

Source: Ref F2.65.

Table F.II-2 Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate

Extent of Flame Damage	Fires	
Confined to object of origin	54	63%
Confined to part of room/area of origin	13	15%
Confined to room of origin	0	0
Confined to fire-rated compartment of origin	5	6%
Confined to floor of origin	0	0
Confined to structure of origin	14	16%
Extended beyond structure of origin	0	0
Total	86	100%

Source: Ref F2.65.

Table F.II-3 Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly

Extent of Flame Damage	Fires	
Confined to object of origin	40	56%
Confined to part of room/area of origin	23	32%
Confined to room of origin	2	3%
Confined to fire-rated compartment of origin	0	0%
Confined to floor of origin	5	7%
Confined to structure of origin	2	3%
Extended beyond structure of origin	0	0
Total	72	100%

Source: Ref F2.65.

The method chosen for calculating the confidence interval of the data is the margin of error calculation:

$$ME = \sqrt{\frac{p(1-p)}{n}} \times t \qquad \text{(Eq. F.II-1)}$$

Where:

ME = Margin of Error

p = Event Probability

n = Number of Samples

t = t-distribution value (see Table F.II-4)

The Event Probabilities are in the second "fire" column of Tables F.II -1 through F.II -3, and are converted to decimal format (divided by 100) for the calculations. Values for t are obtained from a standard t-distribution table, the necessary excerpt from which is provided in Table F.II-4.

Table F.II-4. t-Distribution

t-distribution

		α	
		0.025	0.005
v	60	2.000	2.660
	120	1.980	2.617

Source: Ref F2.68.

Where:

α = One minus the confidence interval divided by two (example: a 95% confidence interval corresponds to an α of 0.025)

v = Degrees of freedom (number of samples minus one)

For the data sets analyzed, confidence intervals of 95% and 99% were analyzed. This is done because, while 95% is an accepted and commonly used confidence interval, 99% is an extremely conservative confidence interval.

Completed calculations and the ranges based on the margins of error are provided in Tables F.II-5 through F.II-10 below. To demonstrate the calculations performed in Tables F.II-5 through F.II-10, an example will be completed from Table F.II-5, row 1. The event probability (p) is determined by dividing the number of occurrences (16) for that event by the total number of fires (187). Thus, 0.0856 is the event probability for an electrically originated fire. The margin of error is then calculated using Equation 1 above, obtaining t from Table F.II-4. For this example, t is 1.98 because the degrees of freedom (v = n-1 = 186) is greater than 120, and the confidence interval is 95%, making α = 0.025. The margin of error obtained, ±0.0405, when subtracted from and added to the event probability provides a percentile range (probability range column). It can be said with 95% confidence that the true event probability lies within this range. The final column is an occurrences range, which is calculated by converting the percentages of the preceding row to decimal format (dividing by 100), and multiplying them by the total number of fires (187). It can be said with 95% confidence that the true number of occurrences for any set of 187 fires is within this range. The calculations throughout Tables F.II 5 through F.II-10 are performed in the same manner, with the value of t depending on the number of samples (fires) and the confidence intervals.

Table F.II-5. Margin of Error Results at 95% Confidence Interval for Fires in Radioactive Material Working Facilities by Originating Equipment

Equipment Type	Occurances	Probability		Margin of Error (95% confidence)		Probability range based on Margin of Error (%)				Occurances range based on Margin of Error		
Electrical	16	8.56E-02	±	4.05E-02		4.51	≤ p ≤	12.61		8.43	≤ O ≤	23.58
Mechanical/Electrical HVAC	15	8.02E-02	±	3.93E-02		4.09	≤ p ≤	11.95		7.65	≤ O ≤	22.35
Mechanical	26	1.39E-01	±	5.01E-02		8.89	≤ p ≤	18.91		16.62	≤ O ≤	35.36
Heat Generating	29	1.55E-01	±	5.24E-02		10.27	≤ p ≤	20.75		19.20	≤ O ≤	38.80
Torches/Welders	41	2.19E-01	±	5.99E-02		15.93	≤ p ≤	27.92		29.79	≤ O ≤	52.21
Internal Combustion	4	2.14E-02	±	2.09E-02		0.04	≤ p ≤	4.23		0.07	≤ O ≤	7.91
Offices/Kitchen Equipment	12	6.42E-02	±	3.55E-02		2.87	≤ p ≤	9.97		5.37	≤ O ≤	18.64
Portable Equipment	19	1.02E-01	±	4.37E-02		5.79	≤ p ≤	14.53		10.83	≤ O ≤	27.17
No Equipment	25	1.34E-01	±	4.93E-02		8.44	≤ p ≤	18.3		15.78	≤ O ≤	34.22
Total	187	1										

Source: Original

Table F.II-6. Margin of Error Results at 99% Confidence Interval for Fires in Radioactive Material Working Facilities by Originating Equipment

Equipment Type	Occurances	Probability		Margin of Error (99% confidence)		Probability range based on Margin of Error (%)				Occurances range based on Margin of Error		
Electrical	16	8.56E-02	±	5.35E-02		3.2	≤ p ≤	13.91		5.98	≤ O ≤	26.01
Mechanical/Electrical HVAC	15	8.02E-02	±	5.20E-02		2.82	≤ p ≤	13.22		5.27	≤ O ≤	24.72
Mechanical	26	1.39E-01	±	6.62E-02		7.28	≤ p ≤	20.53		13.61	≤ O ≤	38.39
Heat Generating	29	1.55E-01	±	6.93E-02		8.58	≤ p ≤	22.44		16.04	≤ O ≤	41.96
Torches/Welders	41	2.19E-01	±	7.92E-02		14.01	≤ p ≤	29.84		26.20	≤ O ≤	55.80
Internal Combustion	4	2.14E-02	±	2.77E-02		-0.63	≤ p ≤	4.91		0.00	≤ O ≤	9.18
Offices/Kitchen Equipment	12	6.42E-02	±	4.69E-02		1.73	≤ p ≤	11.11		3.24	≤ O ≤	20.78
Portable Equipment	19	1.02E-01	±	5.78E-02		4.38	≤ p ≤	15.94		8.19	≤ O ≤	29.81
No Equipment	25	1.34E-01	±	6.51E-02		6.86	≤ p ≤	19.88		12.83	≤ O ≤	37.18
Total	187	1										

Source: Original

Table F.II-7. Margin of Error Results at 95% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate

Extent of Flame Damage	Occurances	Probability		Margin of Error (95% confidence)			Probability range based on Margin of Error (%)				Occurances range based on Margin of Error		
Confined to object of origin	54	6.21E-01		±	1.04E-01		51.67	≤ p ≤	72.48		44.78	≤ O ≤	62.81
Confined to part of room/area of origin	13	1.49E-01		±	7.65E-02		7.3	≤ p ≤	22.59		6.33	≤ O ≤	19.58
Confined to room of origin	0.33	3.79E-03		±	1.32E-02		0	≤ p ≤	1.7		0	≤ O ≤	1.47
Confined to fire-rated compartment of origin	5	5.75E-02		±	4.99E-02		0.76	≤ p ≤	10.74		0.66	≤ O ≤	9.31
Confined to floor of origin	0.33	3.79E-03		±	1.32E-02		0	≤ p ≤	1.7		0	≤ O ≤	1.47
Confined to structure of origin	14	1.61E-01		±	7.88E-02		8.21	≤ p ≤	23.97		7.11	≤ O ≤	20.77
Extended beyond structure of origin	0.33	3.79E-03		±	1.32E-02		0	≤ p ≤	1.7		0	≤ O ≤	1.47
Total	86.99	1											

Source: Original

Table F.II-8. Margin of Error Results at 99% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate

Extent of Flame Damage	Occurances	Probability	Margin of Error (99% confidence)		Probability range based on Margin of Error (%)			Occurances range based on Margin of Error		
Confined to object of origin	54	6.21E-01	±	1.38E-01	48.24	≤ p ≤	75.91	41.8	≤ O ≤	65.78
Confined to part of room/area of origin	13	1.49E-01	±	1.02E-01	4.78	≤ p ≤	25.11	4.14	≤ O ≤	21.76
Confined to room of origin	0.33	3.79E-03	±	1.75E-02	0	≤ p ≤	2.13	0	≤ O ≤	1.85
Confined to fire-rated compartment of origin	5	5.75E-02	±	6.64E-02	0	≤ p ≤	12.39	0	≤ O ≤	10.74
Confined to floor of origin	0.33	3.79E-03	±	1.75E-02	0	≤ p ≤	2.13	0	≤ O ≤	1.85
Confined to structure of origin	14	1.61E-01	±	1.05E-01	5.61	≤ p ≤	26.57	4.86	≤ O ≤	23.03
Extended beyond structure of origin	0.33	3.79E-03	±	1.75E-02	0	≤ p ≤	2.13	0	≤ O ≤	1.85
Total	86.99	1								

Source: Original

Table F.II-9. Margin of Error Results at 95% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly

Extent of Flame Damage	Occurances	Probability	Margin of Error (95% confidence)		Probability range based on Margin of Error (%)			Occurances range based on Margin of Error		
Confined to object of origin	40	5.51E-01	±	1.17E-01	43.38	≤ p ≤	66.72	31.52	≤ O ≤	48.48
Confined to part of room/area of origin	23	3.17E-01	±	1.09E-01	20.74	≤ p ≤	42.57	15.07	≤ O ≤	30.93
Confined to room of origin	2	2.75E-02	±	3.84E-02	0	≤ p ≤	6.59	0	≤ O ≤	4.79
Confined to fire-rated compartment of origin	0.33	4.54E-03	±	1.58E-02	0	≤ p ≤	2.03	0	≤ O ≤	1.47
Confined to floor of origin	5	6.88E-02	±	5.94E-02	0.94	≤ p ≤	12.82	0.68	≤ O ≤	9.32
Confined to structure of origin	2	2.75E-02	±	3.84E-02	0	≤ p ≤	6.59	0	≤ O ≤	4.79
Extended beyond structure of origin	0.33	4.54E-03	±	1.58E-02	0	≤ p ≤	2.03	0	≤ O ≤	1.47
Total	72.66	1								

Source: Original

Table F.II-10. Margin of Error Results at 99% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction and in which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly

Extent of Flame Damage	Occurances	Probability		Margin of Error (99% confidence)			Probability range based on Margin of Error (%)				Occurances range based on Margin of Error		
Confined to object of origin	40	5.51E-01		±	1.55E-01		39.53	≤ p ≤	70.57		28.72	≤ O ≤	51.28
Confined to part of room/area of origin	23	3.17E-01		±	1.45E-01		17.14	≤ p ≤	46.17		12.45	≤ O ≤	33.55
Confined to room of origin	2	2.75E-02		±	5.11E-02		0	≤ p ≤	7.86		0	≤ O ≤	5.71
Confined to fire-rated compartment of origin	0.33	4.54E-03		±	2.10E-02		0	≤ p ≤	2.55		0	≤ O ≤	1.85
Confined to floor of origin	5	6.88E-02		±	7.90E-02		0	≤ p ≤	14.78		0	≤ O ≤	10.74
Confined to structure of origin	2	2.75E-02		±	5.11E-02		0	≤ p ≤	7.86		0	≤ O ≤	5.71
Extended beyond structure of origin	0.33	4.54E-03		±	2.10E-02		0	≤ p ≤	2.55		0	≤ O ≤	1.85
Total	72.66	1											

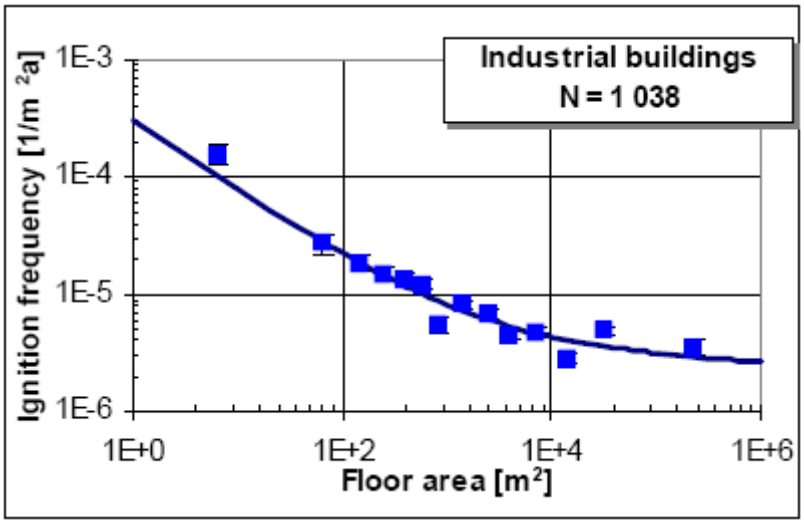
Source: Original

APPENDIX F.III
DERIVATION OF IGNITION FREQUENCY DISTRIBUTION

For proper consideration of the fire frequency analysis of the CRCF, WHF, IHF, and RF, it was necessary to develop an uncertainty distribution for the industrial building fire frequency. *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. F2.67) is used to develop these frequencies. It presents an equation with floor area as an input to determine frequency. The following equation is developed based on sample data collected:

$$f_m''(A) \quad c_1 A^r + c_2 A^s \qquad \text{(Eq. F.III-1)}$$

Where f_m'' is the annual fire frequency per square meter of floor area, A is the floor area, and the values c_1, c_2, r, and s are constants determined by the line of best fit derived from the data. For industrial buildings, the values for the constants are as follows: $c_1 = 3 \times 10^{-4}$, $c_2 = 5 \times 10^{-6}$, $r = -0.61$, and $s = -0.05$. The data for industrial buildings and the resulting line of best fit are presented in Figure F.III-1.

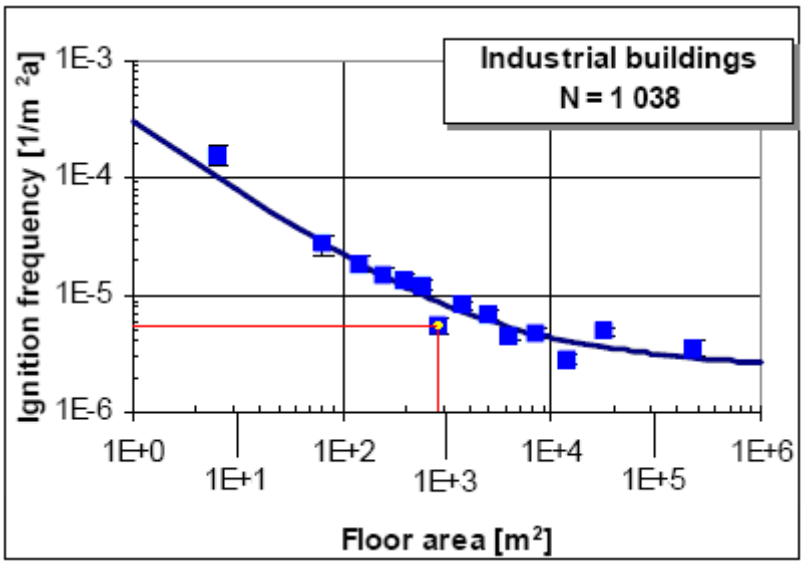


Source: Ref. F2.67

Figure F.III.1. Ignition Frequency Observations

Each data point in the graph represents the average of many data points. The individual data points and the average values were not provided in the reference. Because the data were only presented graphically, it was necessary to estimate the data for the purposes of this analysis. To do so, the center of each data point was found, and x-axis values were added such that the powers increased by a unit of one. Horizontal and vertical lines were drawn from each data point to the x and y axes. The ignition frequency and floor area were then estimated based on the relative distances between these lines and the major axis values. For the example shown in Figure F.III-2, the distance from the 1E+2 label to the red vertical line is divided by the distance from the 1E+2 to 1E+3 labels. In this case, the result is 0.925. Thus, the floor area for the data point is $10^{2.925}$. The ignition frequency is determined in an identical manner. The ignition

frequency and floor area obtained in this manner are displayed in Table F.III-1. The ignition frequency predicted based on Equation F.III-1 is also provided in the table.



Source: Original

Figure F.III-2. Data Point Determination

Table F.III-1. Ignition Frequency Data from Figure F.III-1 and Equation F.III-1

Graphically Determined Data Points		From Equation F.III-1
Floor Area (m^2)	Ignition Frequency (1/yr m^2)	Predicted Frequency (1/yr m^2)
7	1.6×10^{-4}	9.6×10^{-5}
65	2.8×10^{-5}	2.8×10^{-5}
150	1.9×10^{-5}	1.8×10^{-5}
240	1.5×10^{-5}	1.4×10^{-5}
380	1.4×10^{-5}	1.2×10^{-5}
570	1.2×10^{-5}	9.9×10^{-6}
840	5.6×10^{-6}	8.5×10^{-6}
1,400	8.9×10^{-6}	7.1×10^{-6}
2,500	7.0×10^{-6}	5.9×10^{-6}
4,100	4.6×10^{-6}	5.2×10^{-6}
7,100	4.8×10^{-6}	4.5×10^{-6}
14,000	2.9×10^{-6}	4.0×10^{-6}
33,000	5.1×10^{-6}	3.5×10^{-6}
230,000	3.6×10^{-6}	2.9×10^{-6}

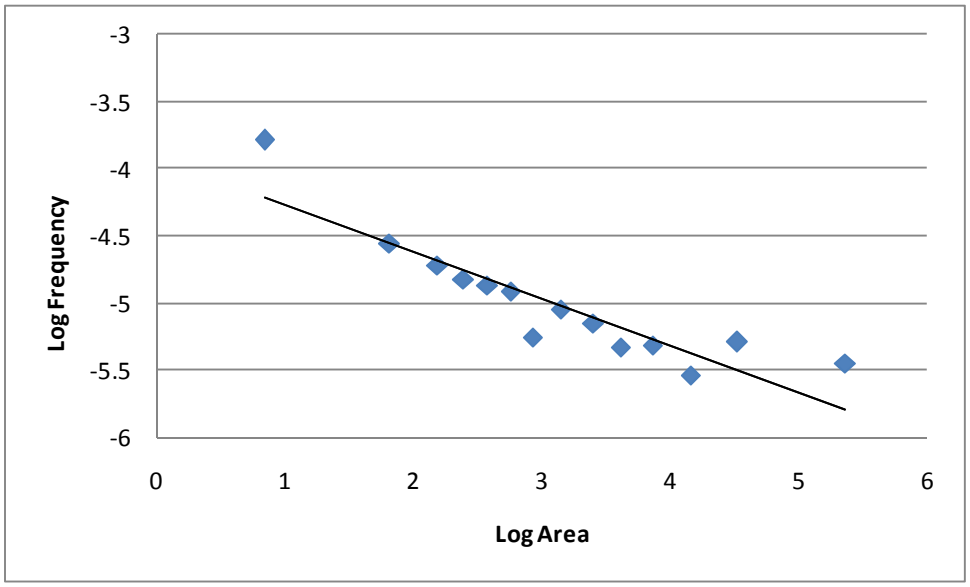
Source: Original

Because the ignition frequency is determined based on the line of best fit, the uncertainty distribution for the calculated ignition frequency can be determined by estimating the uncertainty

in the ability of the best fit equation to predict the ignition frequency of any industrial building not included in the database. This is accomplished using the methodology presented below.

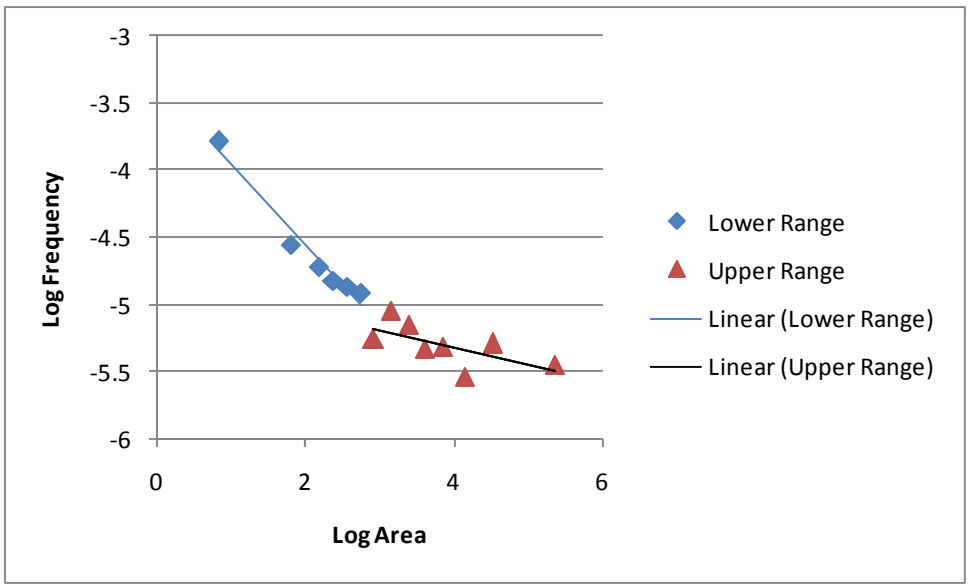
Statistics: Probability, Inference, and Decision (Ref. F2.68) outlines a procedure to determine the confidence limits for a value predicted based on a linear regression equation. Though the ignition frequency and floor area are not linearly related, as illustrated by the figure and by Equation F.III-1, the relationship between the log of the ignition frequency and the log of the floor area is approximately linear. This is illustrated in Figure F.III-3.

As shown in Figures F.III-1 and F.III-3, the portion of the curve for buildings less than 1,000m^2 has a steeper slope than the portion of the curve for buildings larger than 1,000m^2. For that reason, the data were divided into two ranges as shown in Figure F.III-4. Because all of the YMP facilities have floor areas larger than 1,000m^2, the remaining analysis focused on the upper end of the floor area range.



Source: Original

Figure F.III-3. Plot of Log(Ignition Frequency) as a Function of Log(Floor Area)



Source: Original

Figure F.III-4. Plot of Log(Ignition Frequency) as a Function of Log(Floor Area) Divided into Two Floor Area Ranges

To arrive at the confidence interval for the log of the ignition frequency, the follow equations are used:

$$\hat{y} \pm a \frac{s_{xy}}{\sqrt{n-2}} \sqrt{n+1+\frac{(x-m_x)^2}{s_x^2}} \qquad \text{(Eq. F.III-2)}$$

$$s_{xy} = \sqrt{s_y^2 (1-r_{xy}^2)} \qquad \text{(Eq. F.III-3)}$$

$$r_{xy} = \frac{\sum_{i=0}^{i=n} (x_i - m_x)(y - m_y)}{n s_x s_y} \qquad \text{(Eq. F.III-4)}$$

Where:

$\hat{y}$ = the predicted value for the log of the ignition frequency using Equation F-III.1

x = the log of the corresponding floor area value

n = number of data points used in the linear regression analysis (8 for the upper floor area range)

a = the 1-(α/2) fractile of the t-distribution with n-2 degrees of freedom (for a 95% confidence interval, α is 5% and the value for a is 2.447)

x_i = the x data values (log of floor area)

y_i = the y data values (log of ignition frequency)

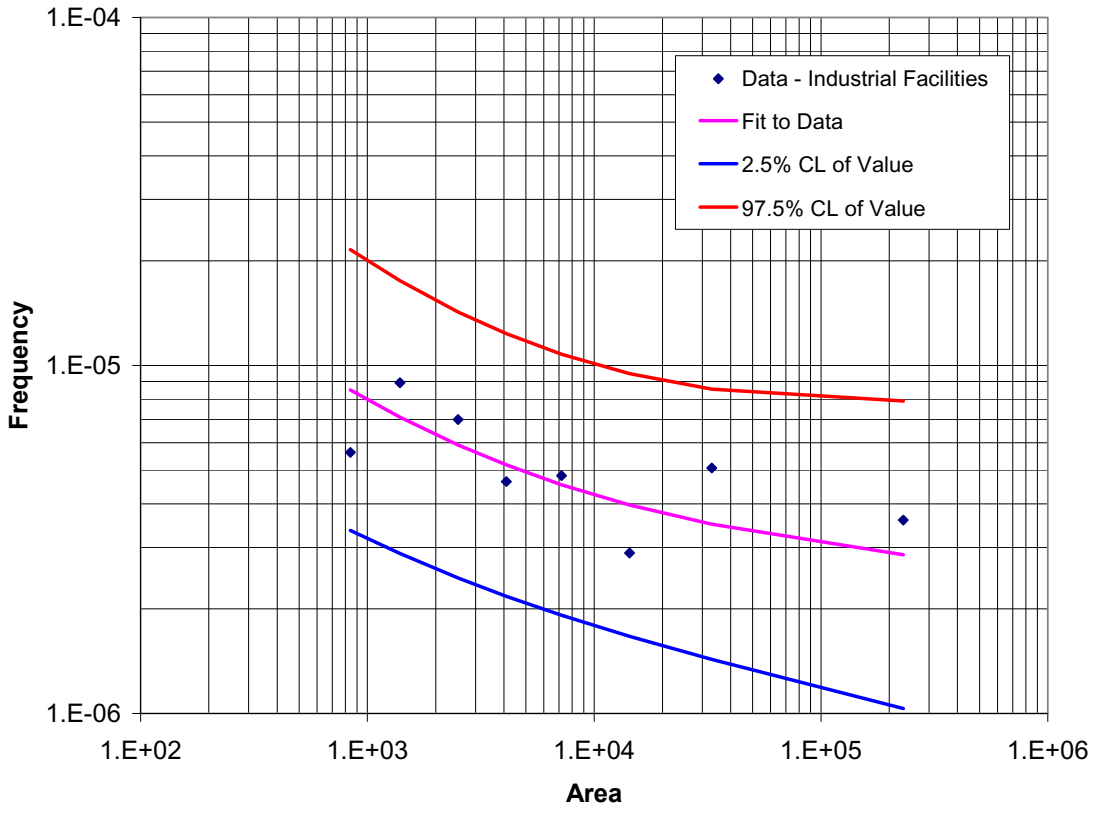
m_x = the mean of the x data values

m_y = the mean of the y data values

s_x = the standard deviation of the x data values

s_y = the standard deviation of the y data values.

The upper and lower confidence limits (i.e., the 97.5% and 2.5% values) for any predicted value of the ignition frequency can be determined from Equations F.III-2 through F.III-4 using the x-y data for the upper end of the floor area range. The upper and lower confidence limits for the ignition frequency were then determined by taking the anti-log of the predicted y values. Figure F.III-5 is a plot showing the original data, the predicted values using Equation F.III-1, and the upper and lower confidence limits for the predicted values. The same approach can be used to determine the upper and lower confidence limits for the ignition frequency calculated for each of the YMP facilities. Those results are provided in Table F.III-2.



NOTE: CL = confidence limit.

Source: Original

Figure F.III-5. Plot of the Ignition Frequency Data, the Predicted Ignition Frequency, and Confidence Limits for the Predicted Value

Table F.III-2. Calculated Mean and Confidence Limits for the YMP Facility Ignition Frequency

Facility	Ignition Frequency (Ignitions per sq-m per year)		
	Median	**2.5% LCL**	**97.5% UCL**
CRCF	3.78×10^{-6}	1.58×10^{-6}	9.08×10^{-6}
IHF	4.79×10^{-6}	2.02×10^{-6}	1.14×10^{-5}
RF	4.05×10^{-6}	1.70×10^{-6}	9.64×10^{-6}
WHF	3.93×10^{-6}	1.65×10^{-6}	9.39×10^{-6}

NOTE: LCL = lower confidence limit; UCL = upper confidence limit;

Source: Original

APPENDIX F.IV
PROOF OF LOGNORMAL DISTRIBUTION

The fire initiating event frequencies presented throughout this document are the result of a series of calculations performed using inputs in the form of three different probability distributions. Two of the input distributions (see Appendix F.II) are normally distributed, and the third (see Appendix F.III) is lognormally distributed. After the calculations were performed, it was necessary to determine what type of distribution best represented the results. The Crystal Ball output (see Appendix E.VI) shows the calculated distributions at ten percentile intervals. Crystal Ball also provides the mean and the median of the distributions.

Microsoft Excel (*WHF Fire Frequency_No Suppression.xls*) has a function, LOGNORMDIST, which can be used to calculate intervals for a lognormal distribution. The Excel function requires that the log mean (μ) and log standard deviation (σ) be provided. To perform this analysis, it was necessary to calculate μ and σ using Equations F.IV-1 and F.IV-2, where the mean and median in these equations are provided in the Crystal Ball results.

$$\mu \quad \ln(median) \qquad \text{(Eq. F.IV-1)}$$

$$\sigma \quad \sqrt{2\ln\left(\frac{mean}{median}\right)} \qquad \text{(Eq. F.IV-2)}$$

A comparison between the Crystal Ball and Excel percentile intervals reveals whether the data is a satisfactory fit to a lognormal distribution. Table F.IV-1 shows the result of this analysis. The table shows that the difference between the Excel calculated values and the Crystal Ball percentile values never exceeds 1%. Thus, it is concluded that the fire initiating events are lognormally distributed.

Table F.IV-1 Comparison Between Crystal Ball and Excel Percentile Intervals

Forecast Values	Excel Calculated Percentiles	Crystal Ball Percentiles	Difference
1.10E-08	0.003	0	0.00
4.04E-08	10.042	10	0.04
5.0E-08	19.93	20	0.07
5.8E-08	30.58	30	0.58
6.6E-08	40.23	40	0.23
7.4E-08	50.00	50	0.00
8.4E-08	59.75	60	0.25
9.5E-08	69.67	70	0.33
1.1E-07	79.85	80	0.15
1.4E-07	90.01	90	0.01
4.3E-07	99.99	100	0.01
Mu	-16.4149	Mean	8.33E-08
Sigma	0.4771	Median	7.43E-08

Source: Original

APPENDIX F.V
DERIVATION OF ERROR FACTORS

It was necessary to provide an error factor for each initiating event frequency, which was calculated using data provided by Crystal Ball. The software output in Appendix F.VI provides the mean and median necessary to determine the error factor. Equation F.V-1 is utilized to calculate the log standard deviation (σ), and equation F.V-2 provides a method for calculating the error factor from the log standard deviation.

$$\sigma \quad \sqrt{2\ln\left(\frac{mean}{median}\right)} \qquad \text{(Eq. F.V-1)}$$

$$\text{EF} = e^{\sigma \times 1.645} \qquad \text{(Eq. F.V-2)}$$

The resultant error factors for each initiating event frequency are displayed in Table F5.7-5, as well as the mean and median utilized to calculate the error factor.

Several of the initiating event frequencies were not utilized as originally anticipated, many were summed for the purpose of developing split fractions. It was necessary to develop error factors for these summed figures as well. This was accomplished by directly summing the figures, then defining the summation as a Crystal Ball forecast value. The Crystal Ball results (Table F.5.7-5) provided a mean and median by which the error factor can be calculated using equations F.V-1 and F.V-2.

APPENDIX F.VI
CRYSTAL BALL FULL RESULTS

Percentiles	Mean	97.5%
Large Fire Threatens DPC (all) in CTM	5.2E-07	1.2E-06
Large Fire Threatens STC/DPC (all)	1.9E-05	4.5E-05
Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus)	2.0E-05	4.6E-05
Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus)	1.6E-05	3.7E-05
Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus)	8.8E-06	2.1E-05
Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus)	3.3E-05	7.7E-05
Large Fire Threatens STC/TAD (Wet Cavity, Wet Annulus)	1.9E-05	4.4E-05
Large Fire Threatens TAD in AO	5.9E-06	1.4E-05
Large Fire Threatens TAD in CTM	4.3E-07	1.0E-06
Large Fire Threatens TC/DPC (No Diesel)	1.8E-05	4.3E-05
Large Fire Threatens TC/DPC (TTC) (No Diesel)	2.6E-05	6.1E-05
Large Fire Threatens TC/SNF (No Diesel)	6.7E-06	1.6E-05
Large Fire Threatens TC/SNF (Wet Cavity)	3.6E-06	8.4E-06
Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present)	7.9E-07	1.8E-06
Localized Fire Threatens DPC (all) in the Transfer Room	8.3E-08	1.9E-07
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area	1.2E-06	2.8E-06
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area	8.3E-06	1.9E-05
Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area	6.8E-06	1.5E-05
Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area	5.4E-06	1.3E-05
Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room	3.9E-07	8.9E-07
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area	7.5E-06	1.7E-05
Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area	8.6E-06	2.0E-05
Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area	6.8E-06	1.6E-05
Localized Fire Threatens STC/TAD on CTT in the Unloading Room	3.3E-07	7.6E-07
Localized Fire Threatens TAD in AO in Bolting Room	3.5E-07	8.3E-07
Localized Fire Threatens TAD in AO in Loading Room	2.9E-07	6.8E-07
Localized Fire Threatens TAD in the Transfer Room	6.9E-08	1.6E-07
Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station in the Preparation Area	4.2E-06	9.8E-06
Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room	1.5E-07	3.5E-07
Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present)	7.6E-06	1.7E-05
Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)	4.0E-06	9.0E-06
Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area	1.9E-06	4.2E-06
Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station in the Preparation Area	3.6E-06	8.2E-06
Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present)	2.5E-06	5.7E-06
Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present)	4.7E-07	1.1E-06

The Crystal Ball report *WHF CB Report.xls*, forecast worksheets, and "assumptions" follow. The term "assumptions" is used by Crystal Ball to denote the probability distributions of the inputs, and does not refer to assumptions as defined by the calculations and analysis procedure.

Crystal Ball Report - Full
Simulation started on 12/31/2007 at 13:26:08
Simulation stopped on 12/31/2007 at 13:27:24

Run preferences:

Number of trials run	10,000
Monte Carlo	
Random seed	

Run statistics:

Total running time (sec)	76.07
Trials/second (average)	131
Random numbers per sec	2,235

Crystal Ball data:

Assumptions	17
Correlations	0
Correlated groups	0
Decision variables	0
Forecasts	35

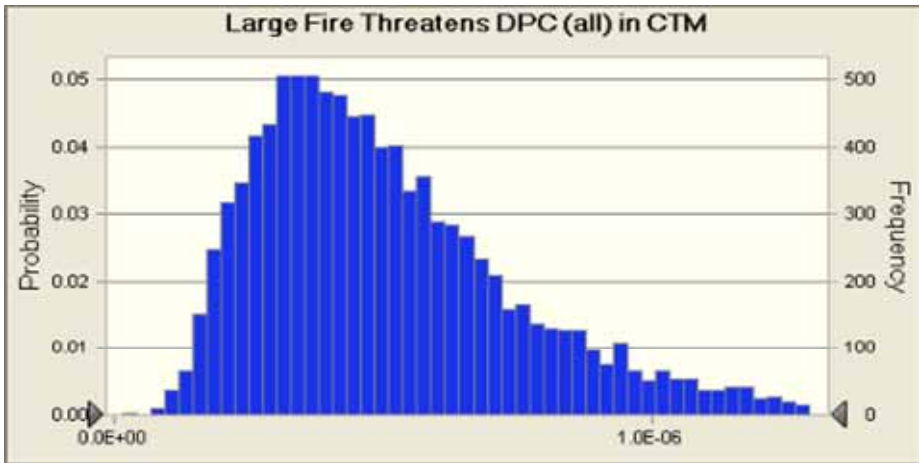
Forecasts

Worksheet: [WHF Fire Frequency_No Suppression.xls]Initiating Event Frequency

Forecast: Large Fire Threatens DPC (all) in CTM **Cell: K225**

Summary:

Entire range is from 1.5E-08 to 3.6E-06
Base case is 4.7E-07
After 10,000 trials, the std. error of the mean is 2.8E-09



Statistics:	Forecast values
Trials	10,000
Mean	5.2E-07
Median	4.6E-07
Mode	---
Standard Deviation	2.8E-07
Variance	7.6E-14
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	1.5E-08
Maximum	3.6E-06
Range Width	3.6E-06
Mean Std. Error	2.8E-09

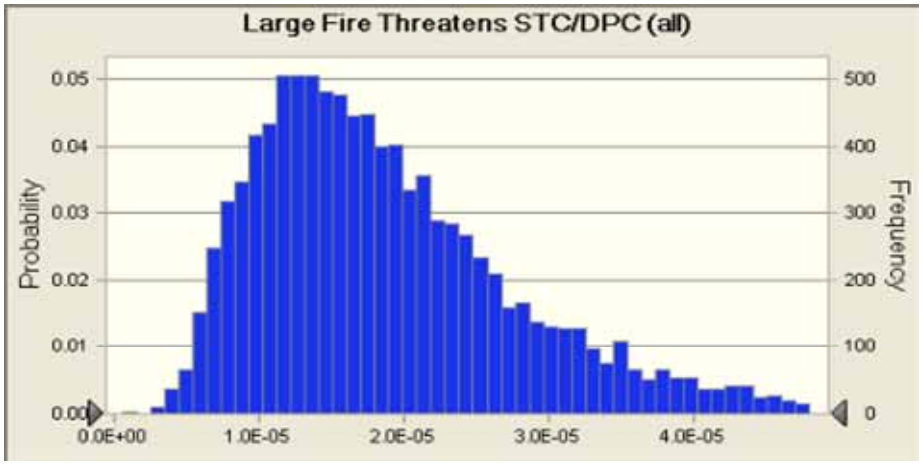
Forecast: Large Fire Threatens DPC (all) in CTM (cont'd) **Cell: K225**

Percentiles:	Forecast values
0%	1.5E-08
10%	2.4E-07
20%	3.0E-07
30%	3.5E-07
40%	4.0E-07
50%	4.6E-07
60%	5.2E-07
70%	6.0E-07
80%	7.0E-07
90%	8.7E-07
100%	3.6E-06

Forecast: Large Fire Threatens STC/DPC (all) **Cell: K226**

Summary:

Entire range is from 5.5E-07 to 1.3E-04
Base case is 1.7E-05
After 10,000 trials, the std. error of the mean is 1.0E-07



Statistics:	Forecast values
Trials	10,000
Mean	1.9E-05
Median	1.7E-05
Mode	---
Standard Deviation	1.0E-05
Variance	1.0E-10
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	5.5E-07
Maximum	1.3E-04
Range Width	1.3E-04
Mean Std. Error	1.0E-07

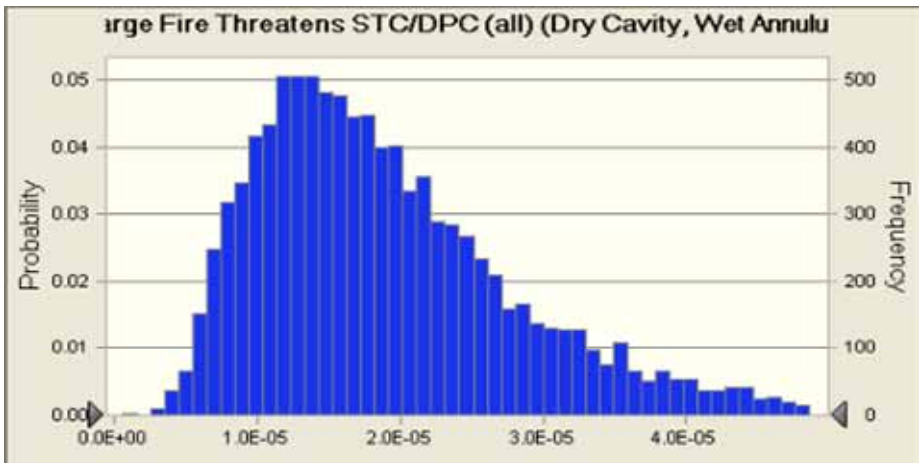
Forecast: Large Fire Threatens STC/DPC (all) (cont'd) **Cell: K226**

Percentiles:	Forecast values
0%	5.5E-07
10%	8.8E-06
20%	1.1E-05
30%	1.3E-05
40%	1.5E-05
50%	1.7E-05
60%	1.9E-05
70%	2.2E-05
80%	2.6E-05
90%	3.2E-05
100%	1.3E-04

Forecast: Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus) Cell: K227

Summary:

Entire range is from 5.5E-07 to 1.3E-04
Base case is 1.8E-05
After 10,000 trials, the std. error of the mean is 1.0E-07



Statistics:	Forecast values
Trials	10,000
Mean	2.0E-05
Median	1.7E-05
Mode	---
Standard Deviation	1.0E-05
Variance	1.1E-10
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	5.5E-07
Maximum	1.3E-04
Range Width	1.3E-04
Mean Std. Error	1.0E-07

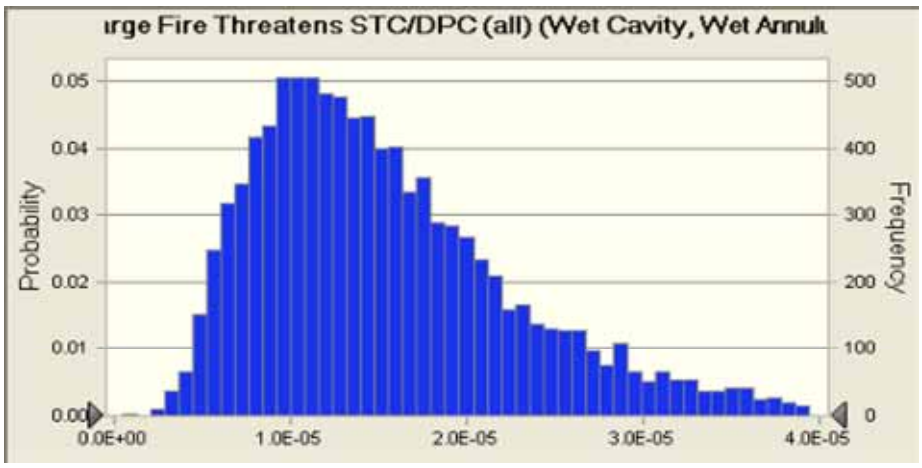
Forecast: Large Fire Threatens STC/DPC (all) (Dry Cavity, Wet Annulus) (cont'd) Cell: K227

Percentiles:	Forecast values
0%	5.5E-07
10%	8.9E-06
20%	1.1E-05
30%	1.3E-05
40%	1.5E-05
50%	1.7E-05
60%	2.0E-05
70%	2.3E-05
80%	2.6E-05
90%	3.3E-05
100%	1.3E-04

Forecast: Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus) Cell: K228

Summary:

Entire range is from 4.5E-07 to 1.1E-04
Base case is 1.4E-05
After 10,000 trials, the std. error of the mean is 8.4E-08



Statistics:	Forecast values
Trials	10,000
Mean	1.6E-05
Median	1.4E-05
Mode	---
Standard Deviation	8.4E-06
Variance	7.1E-11
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	4.5E-07
Maximum	1.1E-04
Range Width	1.1E-04
Mean Std. Error	8.4E-08

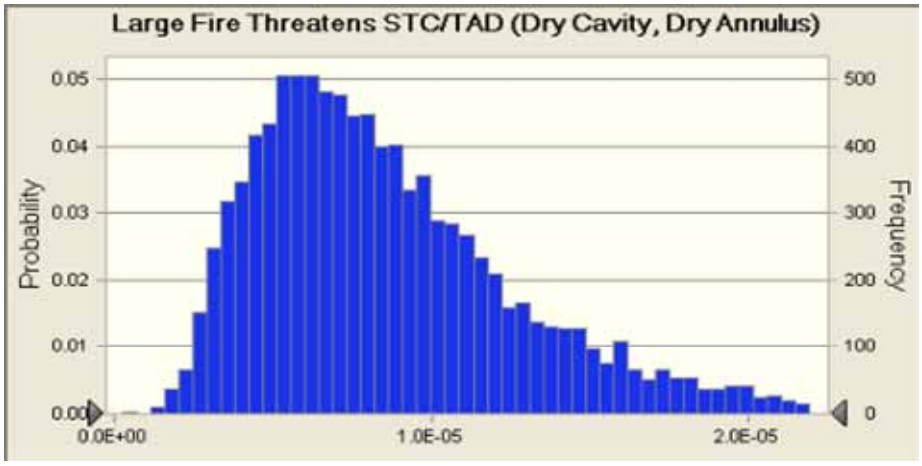
Forecast: Large Fire Threatens STC/DPC (all) (Wet Cavity, Wet Annulus) (cont'd) Cell: K228

Percentiles:	Forecast values
0%	4.5E-07
10%	7.2E-06
20%	9.2E-06
30%	1.1E-05
40%	1.2E-05
50%	1.4E-05
60%	1.6E-05
70%	1.8E-05
80%	2.1E-05
90%	2.7E-05
100%	1.1E-04

Forecast: Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus) **Cell: K232**

Summary:

Entire range is from 2.5E-07 to 6.1E-05
Base case is 7.9E-06
After 10,000 trials, the std. error of the mean is 4.7E-08



Statistics:	Forecast values
Trials	10,000
Mean	8.8E-06
Median	7.8E-06
Mode	---
Standard Deviation	4.7E-06
Variance	2.2E-11
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	2.5E-07
Maximum	6.1E-05
Range Width	6.0E-05
Mean Std. Error	4.7E-08

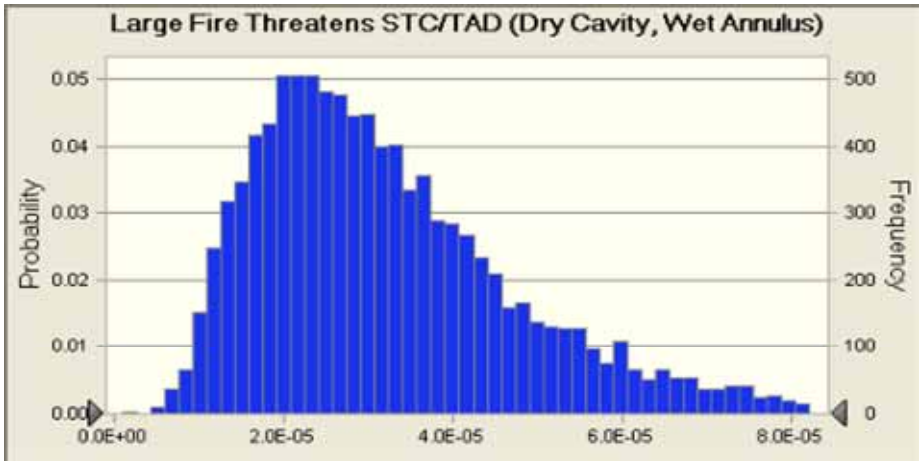
Forecast: Large Fire Threatens STC/TAD (Dry Cavity, Dry Annulus) (cont'd) **Cell: K232**

Percentiles:	Forecast values
0%	2.5E-07
10%	4.0E-06
20%	5.1E-06
30%	6.0E-06
40%	6.9E-06
50%	7.8E-06
60%	8.9E-06
70%	1.0E-05
80%	1.2E-05
90%	1.5E-05
100%	6.1E-05

Forecast: Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus) **Cell: K231**

Summary:

Entire range is from 9.3E-07 to 2.3E-04
Base case is 3.0E-05
After 10,000 trials, the std. error of the mean is 1.8E-07



Statistics:	Forecast values
Trials	10,000
Mean	3.3E-05
Median	2.9E-05
Mode	---
Standard Deviation	1.8E-05
Variance	3.1E-10
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	9.3E-07
Maximum	2.3E-04
Range Width	2.3E-04
Mean Std. Error	1.8E-07

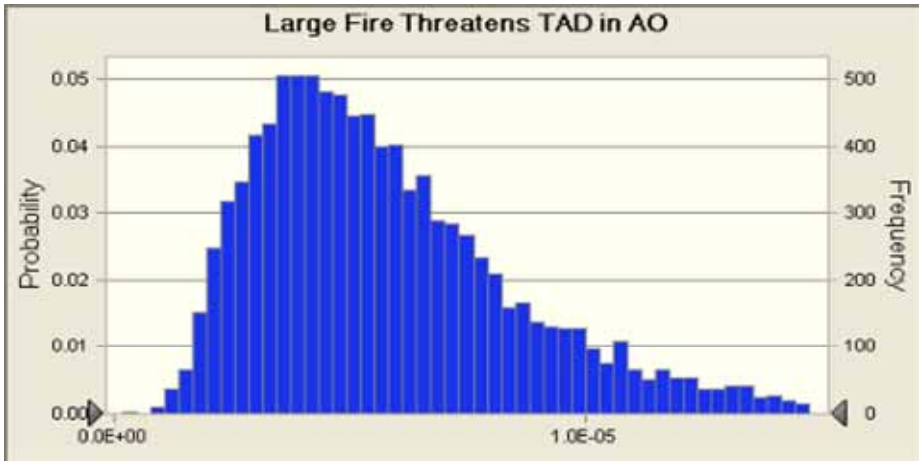
Forecast: Large Fire Threatens STC/TAD (Dry Cavity, Wet Annulus) (cont'd) **Cell: K231**

Percentiles:	Forecast values
0%	9.3E-07
10%	1.5E-05
20%	1.9E-05
30%	2.2E-05
40%	2.6E-05
50%	2.9E-05
60%	3.3E-05
70%	3.8E-05
80%	4.4E-05
90%	5.5E-05
100%	2.3E-04

Forecast: Large Fire Threatens TAD in AO **Cell: K234**

Summary:

Entire range is from 1.7E-07 to 4.1E-05
Base case is 5.3E-06
After 10,000 trials, the std. error of the mean is 3.1E-08



Statistics:	Forecast values
Trials	10,000
Mean	5.9E-06
Median	5.3E-06
Mode	---
Standard Deviation	3.1E-06
Variance	9.9E-12
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	1.7E-07
Maximum	4.1E-05
Range Width	4.1E-05
Mean Std. Error	3.1E-08

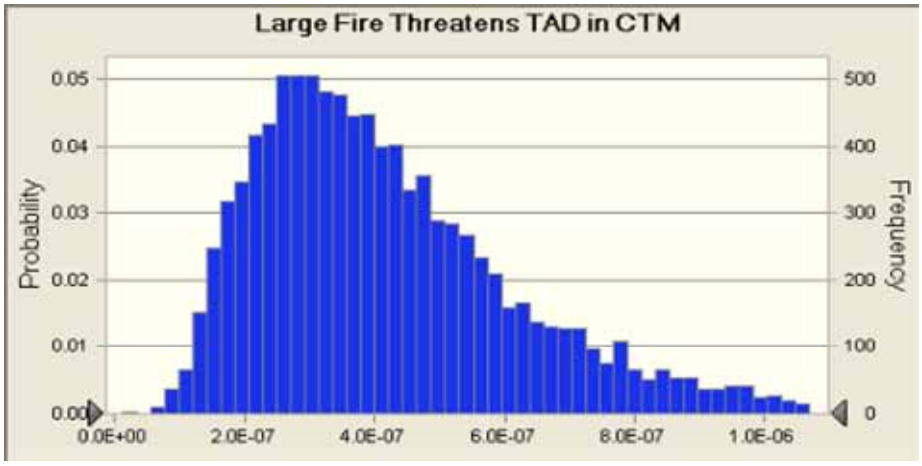
Forecast: Large Fire Threatens TAD in AO (cont'd) **Cell: K234**

Percentiles:	Forecast values
0%	1.7E-07
10%	2.7E-06
20%	3.4E-06
30%	4.0E-06
40%	4.6E-06
50%	5.3E-06
60%	6.0E-06
70%	6.8E-06
80%	8.0E-06
90%	1.0E-05
100%	4.1E-05

Forecast: Large Fire Threatens TAD in CTM **Cell: K233**

Summary:

Entire range is from 1.2E-08 to 3.0E-06
Base case is 3.9E-07
After 10,000 trials, the std. error of the mean is 2.3E-09



Statistics:	Forecast values
Trials	10,000
Mean	4.3E-07
Median	3.8E-07
Mode	---
Standard Deviation	2.3E-07
Variance	5.2E-14
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	1.2E-08
Maximum	3.0E-06
Range Width	2.9E-06
Mean Std. Error	2.3E-09

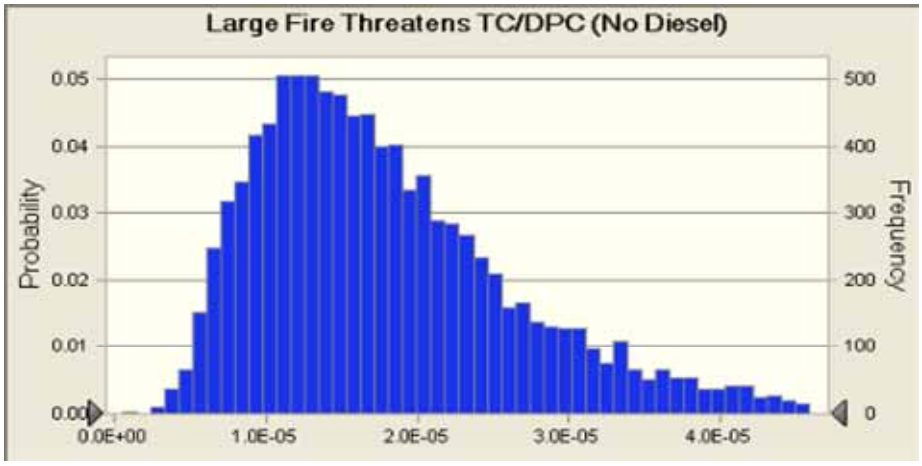
Forecast: Large Fire Threatens TAD in CTM (cont'd) **Cell: K233**

Percentiles:	Forecast values
0%	1.2E-08
10%	2.0E-07
20%	2.5E-07
30%	2.9E-07
40%	3.3E-07
50%	3.8E-07
60%	4.3E-07
70%	4.9E-07
80%	5.8E-07
90%	7.2E-07
100%	3.0E-06

Forecast: Large Fire Threatens TC/DPC (No Diesel) **Cell: K224**

Summary:

Entire range is from 5.2E-07 to 1.3E-04
Base case is 1.7E-05
After 10,000 trials, the std. error of the mean is 9.8E-08



Statistics:	Forecast values
Trials	10,000
Mean	1.8E-05
Median	1.6E-05
Mode	---
Standard Deviation	9.8E-06
Variance	9.6E-11
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	5.2E-07
Maximum	1.3E-04
Range Width	1.3E-04
Mean Std. Error	9.8E-08

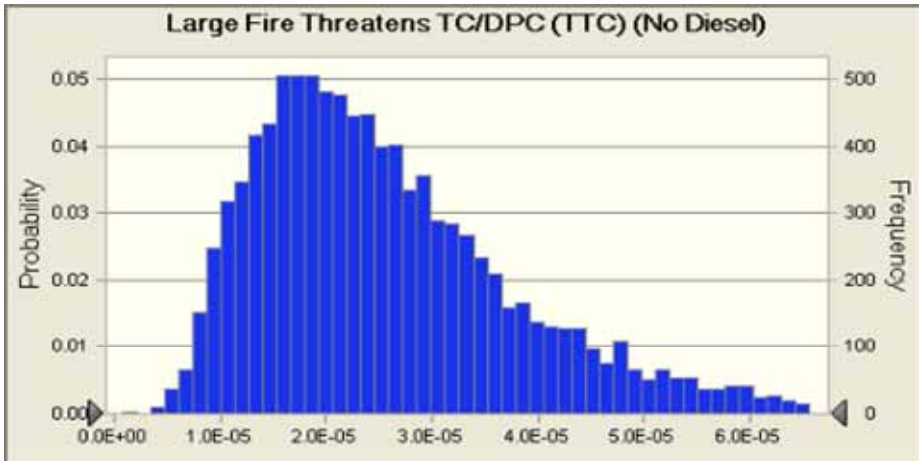
Forecast: Large Fire Threatens TC/DPC (No Diesel) (cont'd) **Cell: K224**

Percentiles:	Forecast values
0%	5.2E-07
10%	8.4E-06
20%	1.1E-05
30%	1.3E-05
40%	1.4E-05
50%	1.6E-05
60%	1.9E-05
70%	2.1E-05
80%	2.5E-05
90%	3.1E-05
100%	1.3E-04

Forecast: Large Fire Threatens TC/DPC (TTC) (No Diesel) **Cell: K223**

Summary:

Entire range is from 7.5E-07 to 1.8E-04
Base case is 2.4E-05
After 10,000 trials, the std. error of the mean is 1.4E-07



Statistics:	Forecast values
Trials	10,000
Mean	2.6E-05
Median	2.3E-05
Mode	---
Standard Deviation	1.4E-05
Variance	2.0E-10
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	7.5E-07
Maximum	1.8E-04
Range Width	1.8E-04
Mean Std. Error	1.4E-07

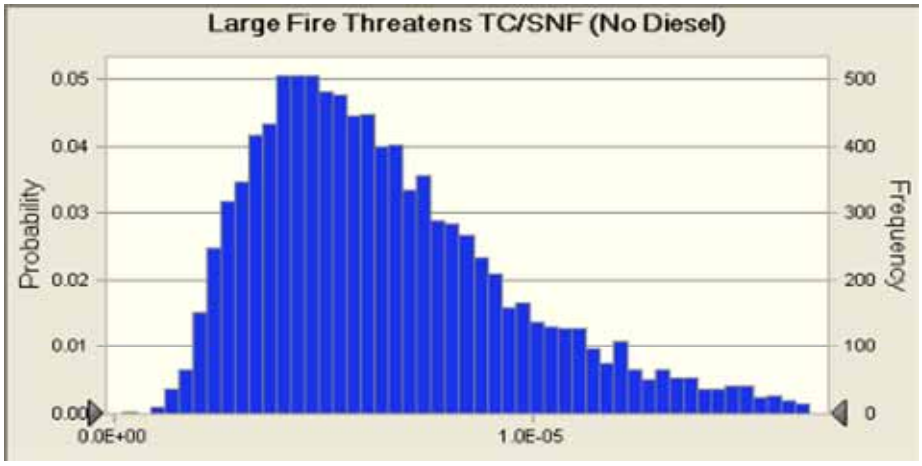
Forecast: Large Fire Threatens TC/DPC (TTC) (No Diesel) (cont'd) **Cell: K223**

Percentiles:	Forecast values
0%	7.5E-07
10%	1.2E-05
20%	1.5E-05
30%	1.8E-05
40%	2.1E-05
50%	2.3E-05
60%	2.7E-05
70%	3.0E-05
80%	3.5E-05
90%	4.4E-05
100%	1.8E-04

Forecast: Large Fire Threatens TC/SNF (No Diesel) **Cell: K222**

Summary:

Entire range is from 1.9E-07 to 4.6E-05
Base case is 6.0E-06
After 10,000 trials, the std. error of the mean is 3.5E-08



Statistics:	Forecast values
Trials	10,000
Mean	6.7E-06
Median	5.9E-06
Mode	---
Standard Deviation	3.5E-06
Variance	1.3E-11
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	1.9E-07
Maximum	4.6E-05
Range Width	4.6E-05
Mean Std. Error	3.5E-08

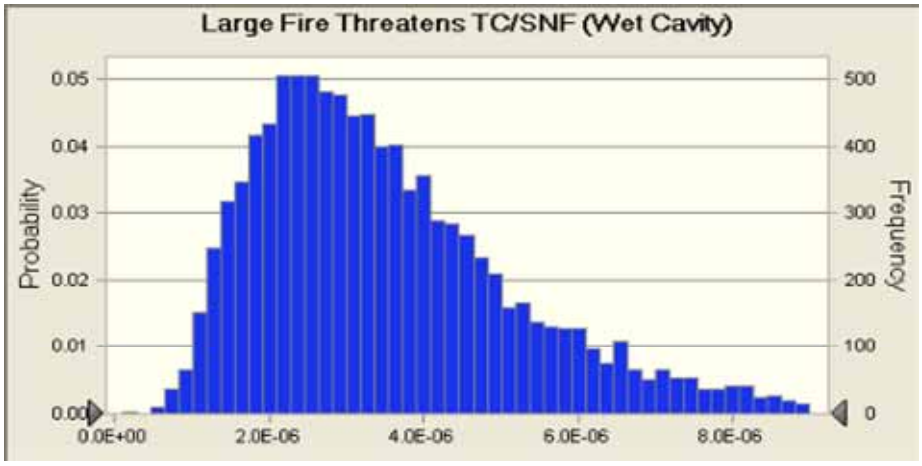
Forecast: Large Fire Threatens TC/SNF (No Diesel) (cont'd) **Cell: K222**

Percentiles:	Forecast values
0%	1.9E-07
10%	3.1E-06
20%	3.9E-06
30%	4.5E-06
40%	5.2E-06
50%	5.9E-06
60%	6.7E-06
70%	7.7E-06
80%	9.0E-06
90%	1.1E-05
100%	4.6E-05

Forecast: Large Fire Threatens TC/SNF (Wet Cavity) **Cell: K229**

Summary:

Entire range is from 1.0E-07 to 2.5E-05
Base case is 3.2E-06
After 10,000 trials, the std. error of the mean is 1.9E-08



Statistics:	Forecast values
Trials	10,000
Mean	3.6E-06
Median	3.2E-06
Mode	---
Standard Deviation	1.9E-06
Variance	3.7E-12
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	1.0E-07
Maximum	2.5E-05
Range Width	2.5E-05
Mean Std. Error	1.9E-08

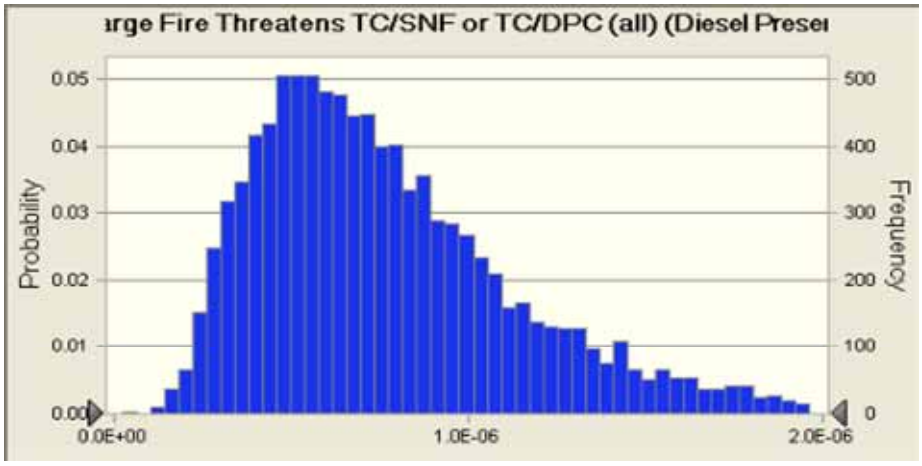
Forecast: Large Fire Threatens TC/SNF (Wet Cavity) (cont'd) **Cell: K229**

Percentiles:	Forecast values
0%	1.0E-07
10%	1.7E-06
20%	2.1E-06
30%	2.5E-06
40%	2.8E-06
50%	3.2E-06
60%	3.6E-06
70%	4.2E-06
80%	4.9E-06
90%	6.1E-06
100%	2.5E-05

Forecast: Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present) Cell: K221

Summary:

Entire range is from 2.2E-08 to 5.4E-06
Base case is 7.1E-07
After 10,000 trials, the std. error of the mean is 4.2E-09



Statistics:	Forecast values
Trials	10,000
Mean	7.9E-07
Median	7.0E-07
Mode	---
Standard Deviation	4.2E-07
Variance	1.8E-13
Skewness	1.66
Kurtosis	8.45
Coeff. of Variability	0.5314
Minimum	2.2E-08
Maximum	5.4E-06
Range Width	5.4E-06
Mean Std. Error	4.2E-09

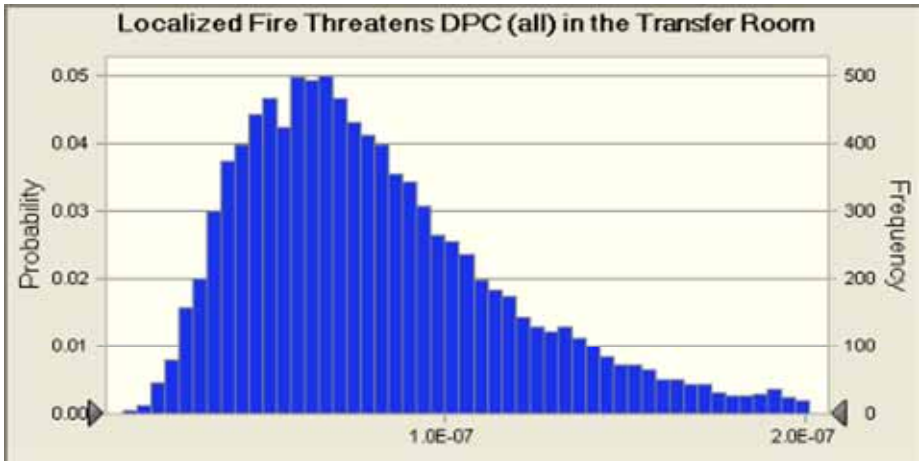
Forecast: Large Fire Threatens TC/SNF or TC/DPC (all) (Diesel Present) (cont'd) Cell: K221

Percentiles:	Forecast values
0%	2.2E-08
10%	3.6E-07
20%	4.6E-07
30%	5.3E-07
40%	6.1E-07
50%	7.0E-07
60%	7.9E-07
70%	9.1E-07
80%	1.1E-06
90%	1.3E-06
100%	5.4E-06

Forecast: Localized Fire Threatens DPC (all) in the Transfer Room **Cell: K130**

Summary:

Entire range is from 1.1E-08 to 4.3E-07
Base case is 7.5E-08
After 10,000 trials, the std. error of the mean is 4.2E-10



Statistics:	Forecast values
Trials	10,000
Mean	8.3E-08
Median	7.4E-08
Mode	---
Standard Deviation	4.2E-08
Variance	1.8E-15
Skewness	1.59
Kurtosis	7.38
Coeff. of Variability	0.5045
Minimum	1.1E-08
Maximum	4.3E-07
Range Width	4.2E-07
Mean Std. Error	4.2E-10

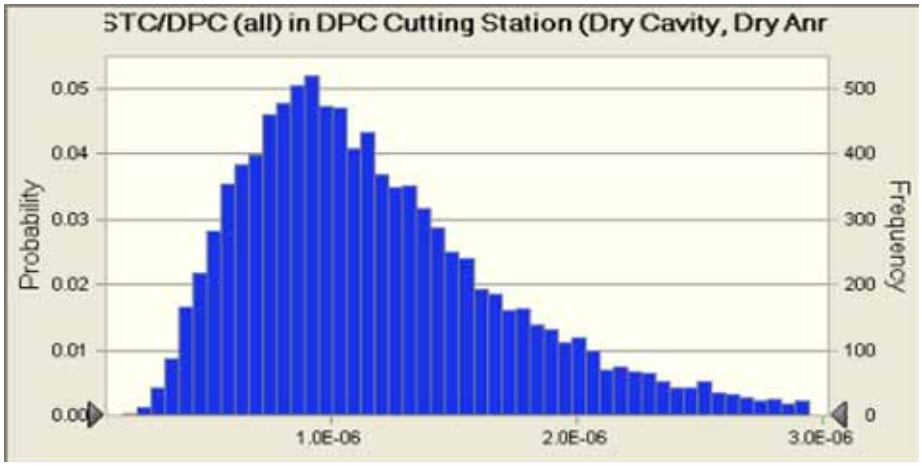
Forecast: Localized Fire Threatens DPC (all) in the Transfer Room (cont'd) **Cell: K130**

Percentiles:	Forecast values
0%	1.1E-08
10%	4.0E-08
20%	5.0E-08
30%	5.8E-08
40%	6.6E-08
50%	7.4E-08
60%	8.4E-08
70%	9.5E-08
80%	1.1E-07
90%	1.4E-07
100%	4.3E-07

Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area **Cell: K154**

Summary:

Entire range is from 1.6E-07 to 6.2E-06
Base case is 1.1E-06
After 10,000 trials, the std. error of the mean is 6.2E-09



Statistics:	Forecast values
Trials	10,000
Mean	1.2E-06
Median	1.1E-06
Mode	---
Standard Deviation	6.2E-07
Variance	3.8E-13
Skewness	1.60
Kurtosis	7.39
Coeff. of Variability	0.5047
Minimum	1.6E-07
Maximum	6.2E-06
Range Width	6.0E-06
Mean Std. Error	6.2E-09

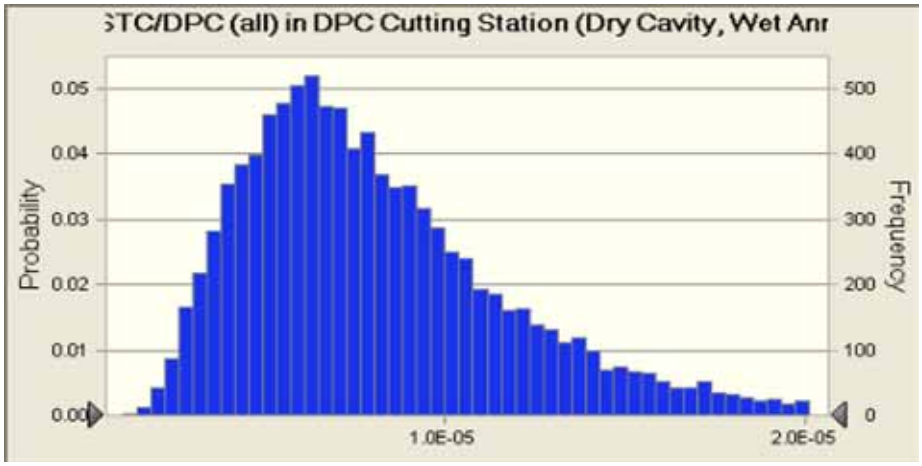
Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Dry Annulus) in the Preparation Area (cont'd) **Cell: K154**

Percentiles:	Forecast values
0%	1.6E-07
10%	5.9E-07
20%	7.3E-07
30%	8.5E-07
40%	9.6E-07
50%	1.1E-06
60%	1.2E-06
70%	1.4E-06
80%	1.6E-06
90%	2.0E-06
100%	6.2E-06

Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area **Cell: M155**

Summary:

Entire range is from 1.1E-06 to 4.2E-05
Base case is 7.5E-06
After 10,000 trials, the std. error of the mean is 4.2E-08



Statistics:	Forecast values
Trials	10,000
Mean	8.3E-06
Median	7.4E-06
Mode	---
Standard Deviation	4.2E-06
Variance	1.8E-11
Skewness	1.60
Kurtosis	7.39
Coeff. of Variability	0.5047
Minimum	1.1E-06
Maximum	4.2E-05
Range Width	4.1E-05
Mean Std. Error	4.2E-08

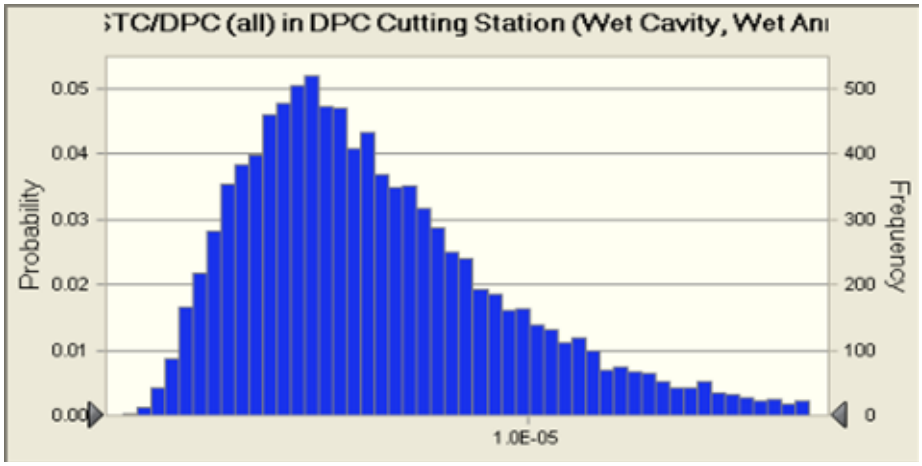
Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Dry Cavity, Wet Annulus) in the Preparation Area (cont'd) **Cell: M155**

Percentiles:	Forecast values
0%	1.1E-06
10%	4.0E-06
20%	5.0E-06
30%	5.8E-06
40%	6.6E-06
50%	7.4E-06
60%	8.4E-06
70%	9.5E-06
80%	1.1E-05
90%	1.4E-05
100%	4.2E-05

Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area **Cell: O156**

Summary:

Entire range is from 8.8E-07 to 3.4E-05
Base case is 6.1E-06
After 10,000 trials, the std. error of the mean is 3.4E-08



Statistics:	Forecast values
Trials	10,000
Mean	6.8E-06
Median	6.0E-06
Mode	---
Standard Deviation	3.4E-06
Variance	1.2E-11
Skewness	1.60
Kurtosis	7.39
Coeff. of Variability	0.5047
Minimum	8.8E-07
Maximum	3.4E-05
Range Width	3.3E-05
Mean Std. Error	3.4E-08

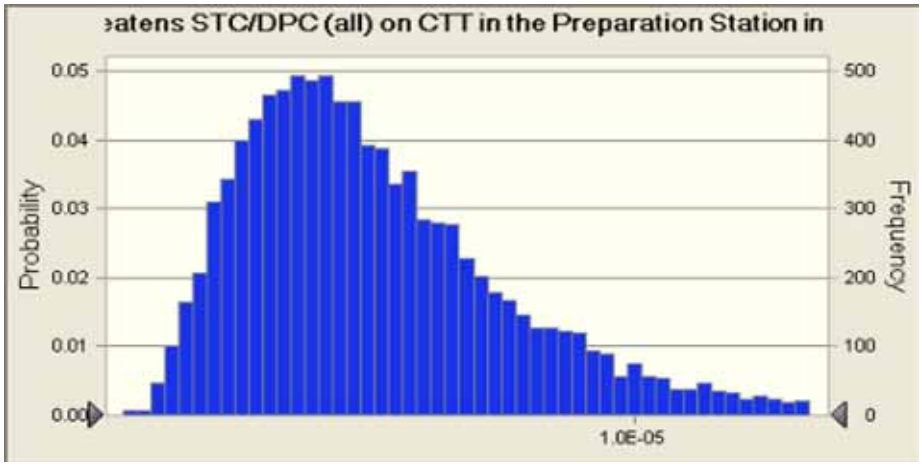
Forecast: Localized Fire Threatens STC/DPC (all) in DPC Cutting Station (Wet Cavity, Wet Annulus) in the Preparation Area (cont'd) **Cell: O156**

Percentiles:	Forecast values
0%	8.8E-07
10%	3.3E-06
20%	4.1E-06
30%	4.7E-06
40%	5.3E-06
50%	6.0E-06
60%	6.8E-06
70%	7.7E-06
80%	9.0E-06
90%	1.1E-05
100%	3.4E-05

Forecast: Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area **Cell: M94**

Summary:

Entire range is from 6.8E-07 to 2.7E-05
Base case is 4.9E-06
After 10,000 trials, the std. error of the mean is 2.8E-08



Statistics:	Forecast values
Trials	10,000
Mean	5.4E-06
Median	4.8E-06
Mode	---
Standard Deviation	2.8E-06
Variance	7.7E-12
Skewness	1.61
Kurtosis	7.43
Coeff. of Variability	0.5117
Minimum	6.8E-07
Maximum	2.7E-05
Range Width	2.7E-05
Mean Std. Error	2.8E-08

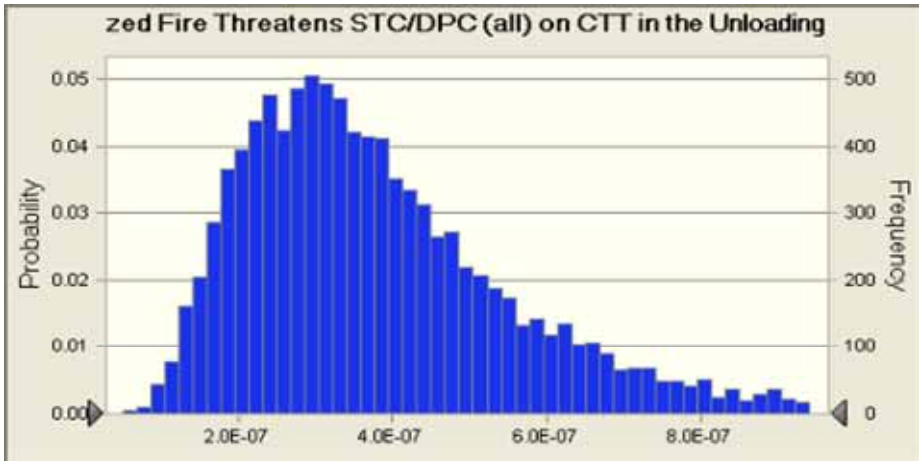
Forecast: Localized Fire Threatens STC/DPC (all) on CTT in the Preparation Station in the Preparation Area (cont'd) **Cell: M94**

Percentiles:	Forecast values
0%	6.8E-07
10%	2.6E-06
20%	3.2E-06
30%	3.8E-06
40%	4.3E-06
50%	4.8E-06
60%	5.4E-06
70%	6.2E-06
80%	7.2E-06
90%	9.0E-06
100%	2.7E-05

Forecast: Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room Cell: M112

Summary:

Entire range is from 5.1E-08 to 2.0E-06
Base case is 3.5E-07
After 10,000 trials, the std. error of the mean is 2.0E-09



Statistics:	Forecast values
Trials	10,000
Mean	3.9E-07
Median	3.5E-07
Mode	---
Standard Deviation	2.0E-07
Variance	3.9E-14
Skewness	1.59
Kurtosis	7.36
Coeff. of Variability	0.5035
Minimum	5.1E-08
Maximum	2.0E-06
Range Width	1.9E-06
Mean Std. Error	2.0E-09

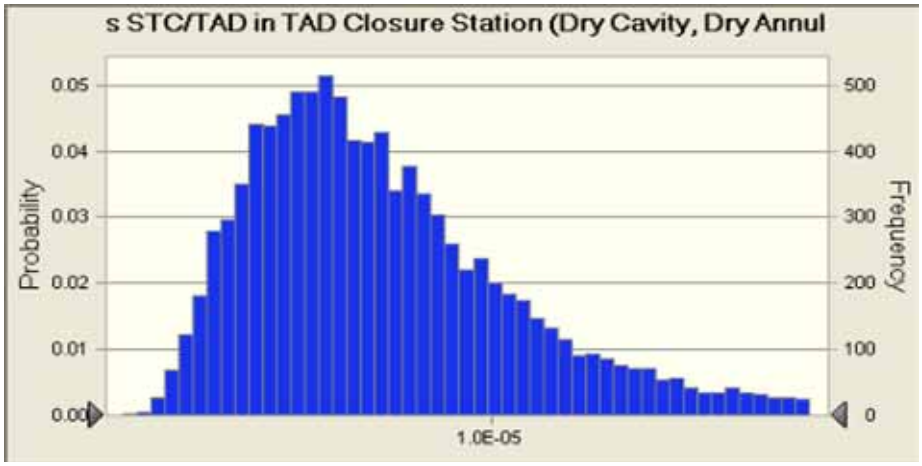
Forecast: Localized Fire Threatens STC/DPC (all) on CTT in the Unloading Room (cont'd) **Cell: M112**

Percentiles:	Forecast values
0%	5.1E-08
10%	1.9E-07
20%	2.3E-07
30%	2.7E-07
40%	3.1E-07
50%	3.5E-07
60%	3.9E-07
70%	4.5E-07
80%	5.2E-07
90%	6.4E-07
100%	2.0E-06

Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area **Cell: K182**

Summary:

Entire range is from 9.8E-07 to 3.8E-05
Base case is 6.8E-06
After 10,000 trials, the std. error of the mean is 3.7E-08



Statistics:	Forecast values
Trials	10,000
Mean	7.5E-06
Median	6.8E-06
Mode	---
Standard Deviation	3.7E-06
Variance	1.3E-11
Skewness	1.54
Kurtosis	7.03
Coeff. of Variability	0.4872
Minimum	9.8E-07
Maximum	3.8E-05
Range Width	3.7E-05
Mean Std. Error	3.7E-08

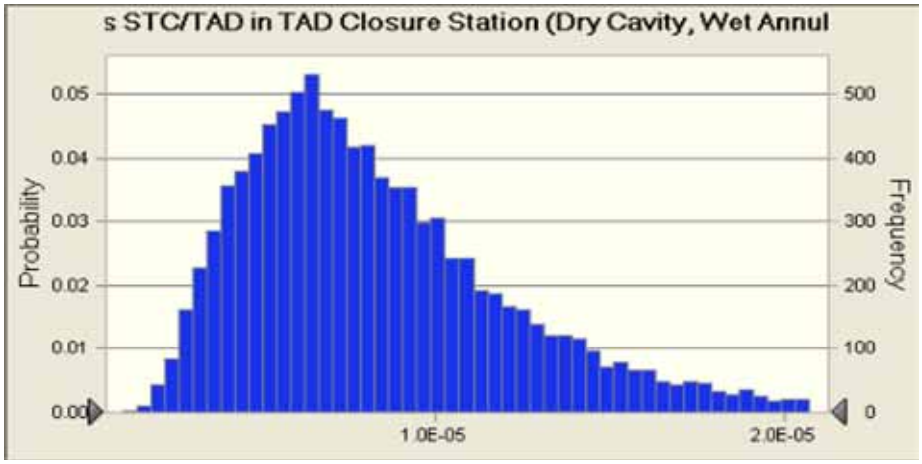
Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Dry Annulus) in the Preparation Area (cont'd) **Cell: K182**

Percentiles:	Forecast values
0%	9.8E-07
10%	3.7E-06
20%	4.6E-06
30%	5.3E-06
40%	6.0E-06
50%	6.8E-06
60%	7.6E-06
70%	8.6E-06
80%	9.9E-06
90%	1.2E-05
100%	3.8E-05

Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area **Cell: M183**

Summary:

Entire range is from 1.1E-06 to 4.3E-05
Base case is 7.7E-06
After 10,000 trials, the std. error of the mean is 4.3E-08



Statistics:	Forecast values
Trials	10,000
Mean	8.6E-06
Median	7.6E-06
Mode	---
Standard Deviation	4.3E-06
Variance	1.9E-11
Skewness	1.61
Kurtosis	7.41
Coeff. of Variability	0.5060
Minimum	1.1E-06
Maximum	4.3E-05
Range Width	4.2E-05
Mean Std. Error	4.3E-08

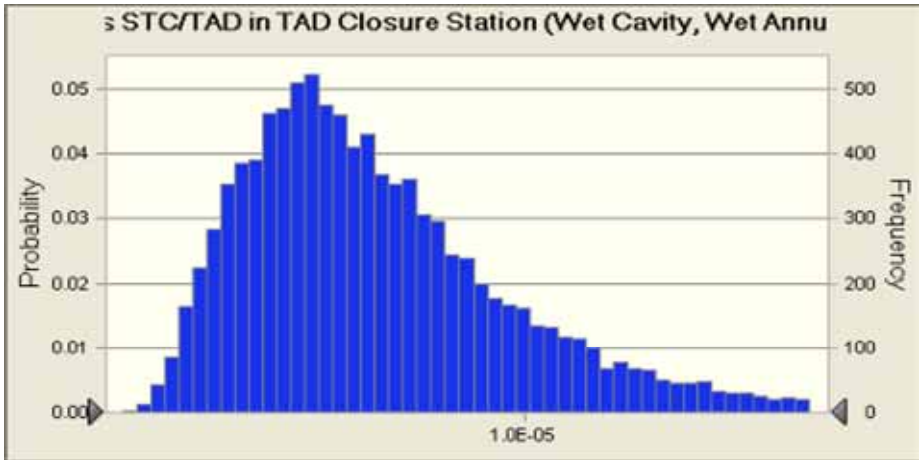
Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Dry Cavity, Wet Annulus) in the Preparation Area (cont'd) **Cell: M183**

Percentiles:	Forecast values
0%	1.1E-06
10%	4.1E-06
20%	5.1E-06
30%	6.0E-06
40%	6.7E-06
50%	7.6E-06
60%	8.6E-06
70%	9.8E-06
80%	1.1E-05
90%	1.4E-05
100%	4.3E-05

Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area **Cell: O184**

Summary:

Entire range is from 8.8E-07 to 3.4E-05
Base case is 6.1E-06
After 10,000 trials, the std. error of the mean is 3.4E-08



Statistics:	Forecast values
Trials	10,000
Mean	6.8E-06
Median	6.1E-06
Mode	---
Standard Deviation	3.4E-06
Variance	1.2E-11
Skewness	1.61
Kurtosis	7.40
Coeff. of Variability	0.5050
Minimum	8.8E-07
Maximum	3.4E-05
Range Width	3.4E-05
Mean Std. Error	3.4E-08

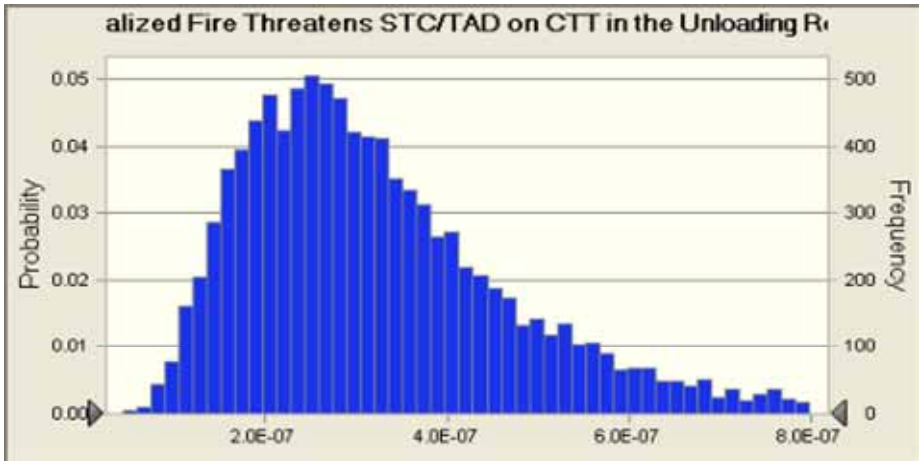
Forecast: Localized Fire Threatens STC/TAD in TAD Closure Station (Wet Cavity, Wet Annulus) in the Preparation Area (cont'd) **Cell: O184**

Percentiles:	Forecast values
0%	8.8E-07
10%	3.3E-06
20%	4.1E-06
30%	4.8E-06
40%	5.4E-06
50%	6.1E-06
60%	6.9E-06
70%	7.8E-06
80%	9.1E-06
90%	1.1E-05
100%	3.4E-05

Forecast: Localized Fire Threatens STC/TAD on CTT in the Unloading Room Cell: O113

Summary:

Entire range is from 4.4E-08 to 1.7E-06
Base case is 3.0E-07
After 10,000 trials, the std. error of the mean is 1.7E-09



Statistics:	Forecast values
Trials	10,000
Mean	3.3E-07
Median	3.0E-07
Mode	---
Standard Deviation	1.7E-07
Variance	2.8E-14
Skewness	1.59
Kurtosis	7.36
Coeff. of Variability	0.5035
Minimum	4.4E-08
Maximum	1.7E-06
Range Width	1.6E-06
Mean Std. Error	1.7E-09

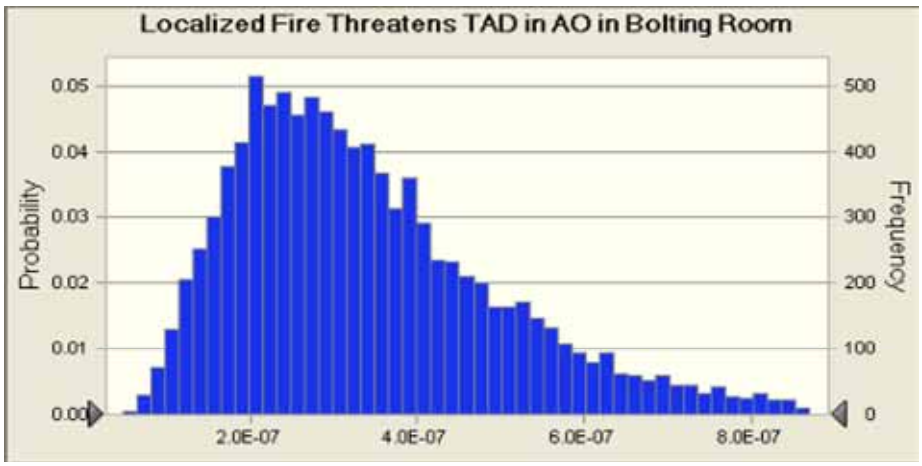
Forecast: Localized Fire Threatens STC/TAD on CTT in the Unloading Room (cont'd) Cell: O113

Percentiles:	Forecast values
0%	4.4E-08
10%	1.6E-07
20%	2.0E-07
30%	2.3E-07
40%	2.6E-07
50%	3.0E-07
60%	3.3E-07
70%	3.8E-07
80%	4.4E-07
90%	5.4E-07
100%	1.7E-06

Forecast: Localized Fire Threatens TAD in AO in Bolting Room **Cell: K213**

Summary:

Entire range is from 4.8E-08 to 1.7E-06
Base case is 3.1E-07
After 10,000 trials, the std. error of the mean is 1.8E-09



Statistics:	Forecast values
Trials	10,000
Mean	3.5E-07
Median	3.1E-07
Mode	---
Standard Deviation	1.8E-07
Variance	3.4E-14
Skewness	1.57
Kurtosis	6.98
Coeff. of Variability	0.5229
Minimum	4.8E-08
Maximum	1.7E-06
Range Width	1.7E-06
Mean Std. Error	1.8E-09

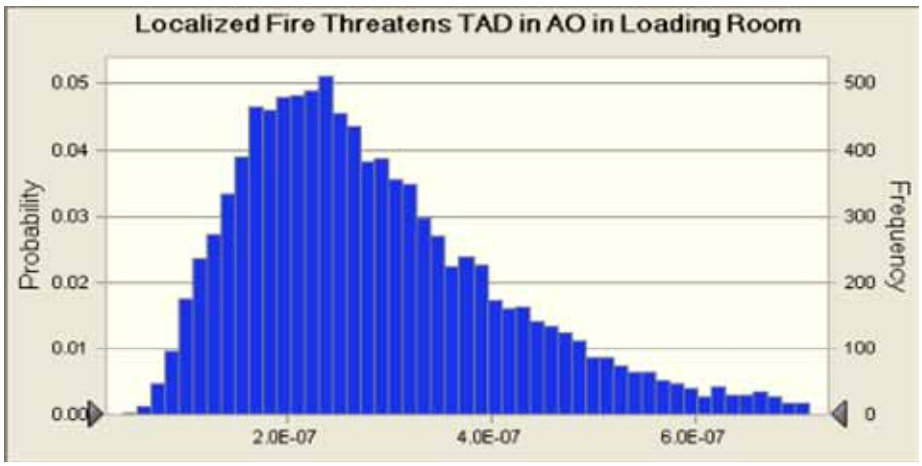
Forecast: Localized Fire Threatens TAD in AO in Bolting Room (cont'd) **Cell: K213**

Percentiles:	Forecast values
0%	4.8E-08
10%	1.7E-07
20%	2.1E-07
30%	2.4E-07
40%	2.8E-07
50%	3.1E-07
60%	3.5E-07
70%	4.0E-07
80%	4.7E-07
90%	5.8E-07
100%	1.7E-06

Forecast: Localized Fire Threatens TAD in AO in Loading Room **Cell: K201**

Summary:

Entire range is from 3.9E-08 to 1.4E-06
Base case is 2.6E-07
After 10,000 trials, the std. error of the mean is 1.5E-09



Statistics:	Forecast values
Trials	10,000
Mean	2.9E-07
Median	2.6E-07
Mode	---
Standard Deviation	1.5E-07
Variance	2.2E-14
Skewness	1.56
Kurtosis	7.05
Coeff. of Variability	0.5074
Minimum	3.9E-08
Maximum	1.4E-06
Range Width	1.4E-06
Mean Std. Error	1.5E-09

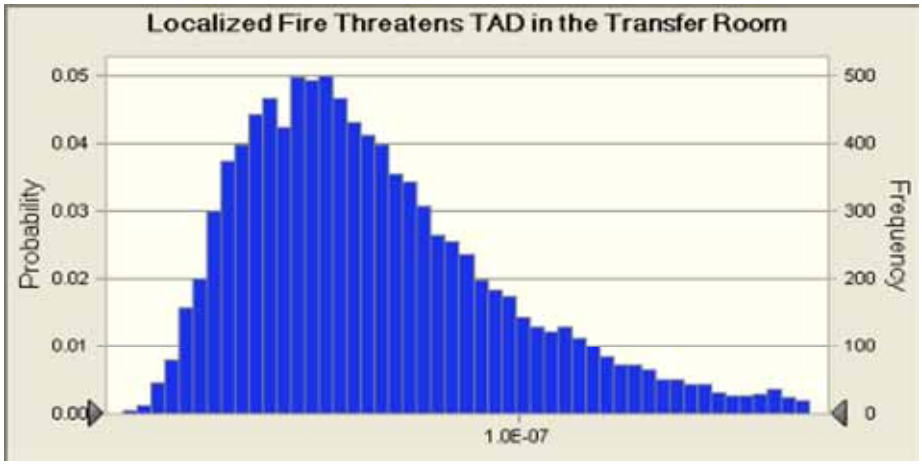
Forecast: Localized Fire Threatens TAD in AO in Loading Room (cont'd) **Cell: K201**

Percentiles:	Forecast values
0%	3.9E-08
10%	1.4E-07
20%	1.7E-07
30%	2.0E-07
40%	2.3E-07
50%	2.6E-07
60%	3.0E-07
70%	3.4E-07
80%	3.9E-07
90%	4.8E-07
100%	1.4E-06

Forecast: Localized Fire Threatens TAD in the Transfer Room **Cell: M131**

Summary:

Entire range is from 9.1E-09 to 3.5E-07
Base case is 6.2E-08
After 10,000 trials, the std. error of the mean is 3.5E-10



Statistics:	Forecast values
Trials	10,000
Mean	6.9E-08
Median	6.2E-08
Mode	---
Standard Deviation	3.5E-08
Variance	1.2E-15
Skewness	1.59
Kurtosis	7.38
Coeff. of Variability	0.5045
Minimum	9.1E-09
Maximum	3.5E-07
Range Width	3.5E-07
Mean Std. Error	3.5E-10

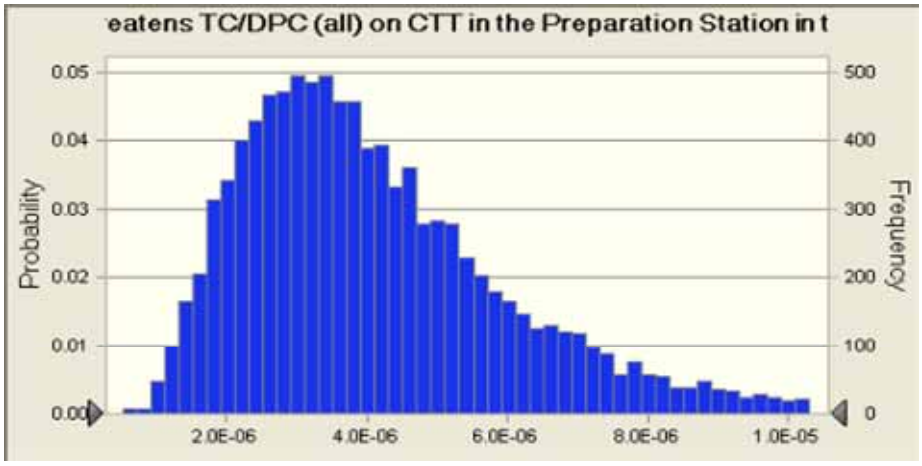
Forecast: Localized Fire Threatens TAD in the Transfer Room (cont'd) **Cell: M131**

Percentiles:	Forecast values
0%	9.1E-09
10%	3.3E-08
20%	4.1E-08
30%	4.8E-08
40%	5.5E-08
50%	6.2E-08
60%	6.9E-08
70%	7.9E-08
80%	9.2E-08
90%	1.1E-07
100%	3.5E-07

Forecast: Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station Cell: K93

Summary:

Entire range is from 5.3E-07 to 2.1E-05
Base case is 3.8E-06
After 10,000 trials, the std. error of the mean is 2.2E-08



Statistics:	Forecast values
Trials	10,000
Mean	4.2E-06
Median	3.8E-06
Mode	---
Standard Deviation	2.2E-06
Variance	4.7E-12
Skewness	1.61
Kurtosis	7.43
Coeff. of Variability	0.5118
Minimum	5.3E-07
Maximum	2.1E-05
Range Width	2.1E-05
Mean Std. Error	2.2E-08

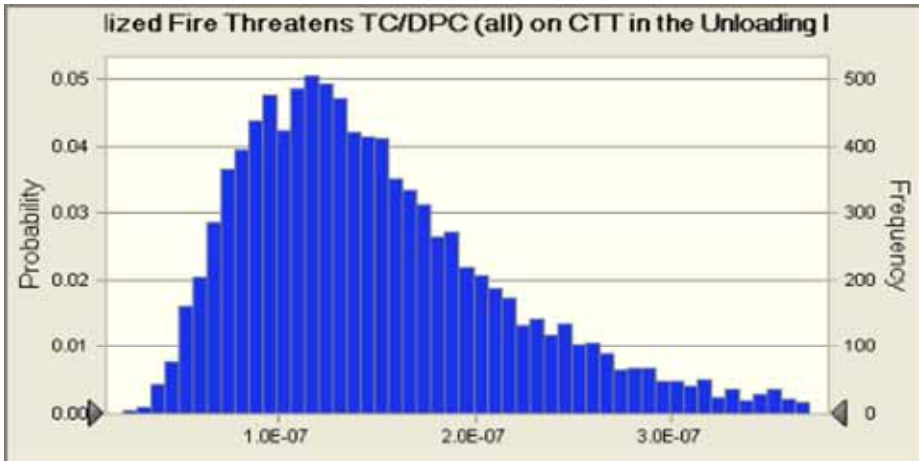
Forecast: Localized Fire Threatens TC/DPC (all) on CTT in the Preparation Station Cell: K93

Percentiles:	Forecast values
0%	5.3E-07
10%	2.0E-06
20%	2.5E-06
30%	2.9E-06
40%	3.3E-06
50%	3.8E-06
60%	4.3E-06
70%	4.8E-06
80%	5.6E-06
90%	7.0E-06
100%	2.1E-05

Forecast: Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room Cell: K111

Summary:

Entire range is from 2.0E-08 to 7.8E-07
Base case is 1.4E-07
After 10,000 trials, the std. error of the mean is 7.7E-10



Statistics:	Forecast values
Trials	10,000
Mean	1.5E-07
Median	1.4E-07
Mode	---
Standard Deviation	7.7E-08
Variance	6.0E-15
Skewness	1.59
Kurtosis	7.36
Coeff. of Variability	0.5035
Minimum	2.0E-08
Maximum	7.8E-07
Range Width	7.6E-07
Mean Std. Error	7.7E-10

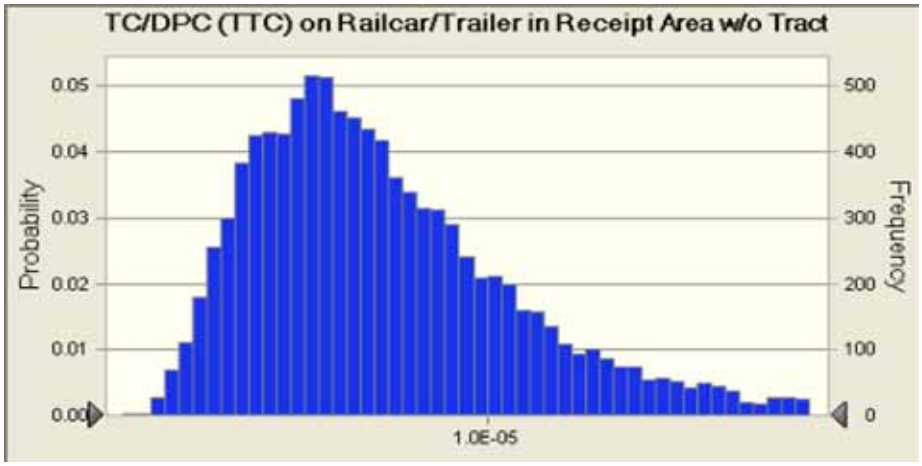
Forecast: Localized Fire Threatens TC/DPC (all) on CTT in the Unloading Room (cC Cell: K111

Percentiles:	Forecast values
0%	2.0E-08
10%	7.5E-08
20%	9.2E-08
30%	1.1E-07
40%	1.2E-07
50%	1.4E-07
60%	1.5E-07
70%	1.8E-07
80%	2.0E-07
90%	2.5E-07
100%	7.8E-07

Forecast: Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present) **Cell: M47**

Summary:

Entire range is from 8.9E-07 to 3.6E-05
Base case is 6.8E-06
After 10,000 trials, the std. error of the mean is 3.7E-08



Statistics:	Forecast values
Trials	10,000
Mean	7.6E-06
Median	6.8E-06
Mode	---
Standard Deviation	3.7E-06
Variance	1.4E-11
Skewness	1.53
Kurtosis	6.87
Coeff. of Variability	0.4918
Minimum	8.9E-07
Maximum	3.6E-05
Range Width	3.5E-05
Mean Std. Error	3.7E-08

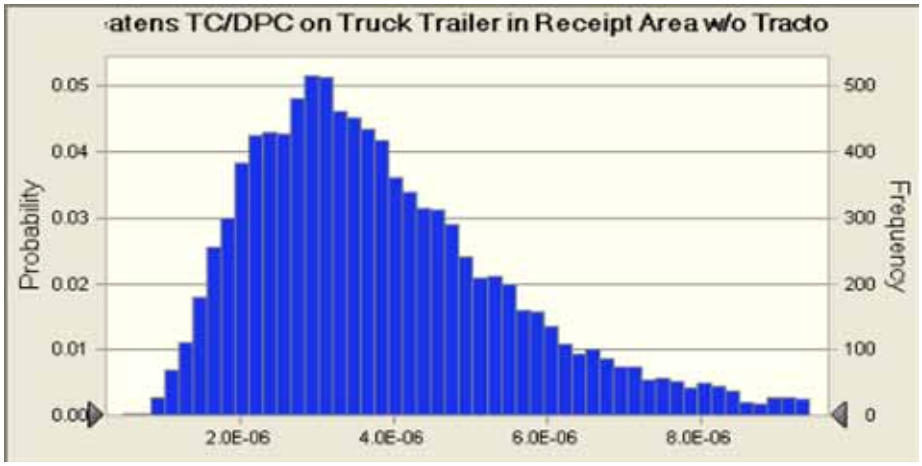
Forecast: Localized Fire Threatens TC/DPC (TTC) on Railcar/Trailer in Receipt Area w/o Tractor/SPM (No Diesel Present) (cont'd) **Cell: M47**

Percentiles:	Forecast values
0%	8.9E-07
10%	3.7E-06
20%	4.6E-06
30%	5.4E-06
40%	6.0E-06
50%	6.8E-06
60%	7.6E-06
70%	8.7E-06
80%	1.0E-05
90%	1.2E-05
100%	3.6E-05

Forecast: Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present) **Cell: O48**

Summary:

Entire range is from 4.7E-07 to 1.9E-05
Base case is 3.6E-06
After 10,000 trials, the std. error of the mean is 1.9E-08



Statistics:	Forecast values
Trials	10,000
Mean	4.0E-06
Median	3.6E-06
Mode	---
Standard Deviation	1.9E-06
Variance	3.8E-12
Skewness	1.53
Kurtosis	6.87
Coeff. of Variability	0.4918
Minimum	4.7E-07
Maximum	1.9E-05
Range Width	1.8E-05
Mean Std. Error	1.9E-08

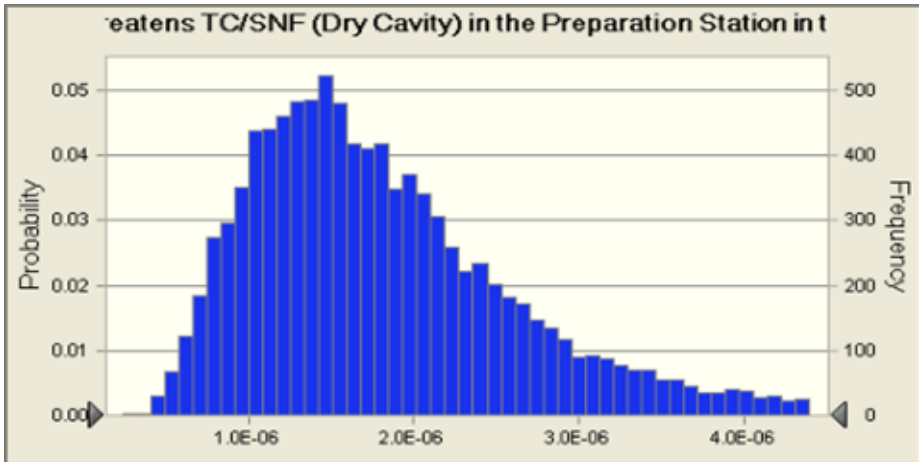
Forecast: Localized Fire Threatens TC/DPC on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present) (cont'd) **Cell: O48**

Percentiles:	Forecast values
0%	4.7E-07
10%	2.0E-06
20%	2.4E-06
30%	2.8E-06
40%	3.2E-06
50%	3.6E-06
60%	4.0E-06
70%	4.5E-06
80%	5.2E-06
90%	6.5E-06
100%	1.9E-05

Forecast: Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area **Cell: K70**

Summary:

Entire range is from 2.4E-07 to 9.3E-06
Base case is 1.7E-06
After 10,000 trials, the std. error of the mean is 9.1E-09



Statistics:	Forecast values
Trials	10,000
Mean	1.9E-06
Median	1.7E-06
Mode	---
Standard Deviation	9.1E-07
Variance	8.2E-13
Skewness	1.54
Kurtosis	7.03
Coeff. of Variability	0.4874
Minimum	2.4E-07
Maximum	9.3E-06
Range Width	9.1E-06
Mean Std. Error	9.1E-09

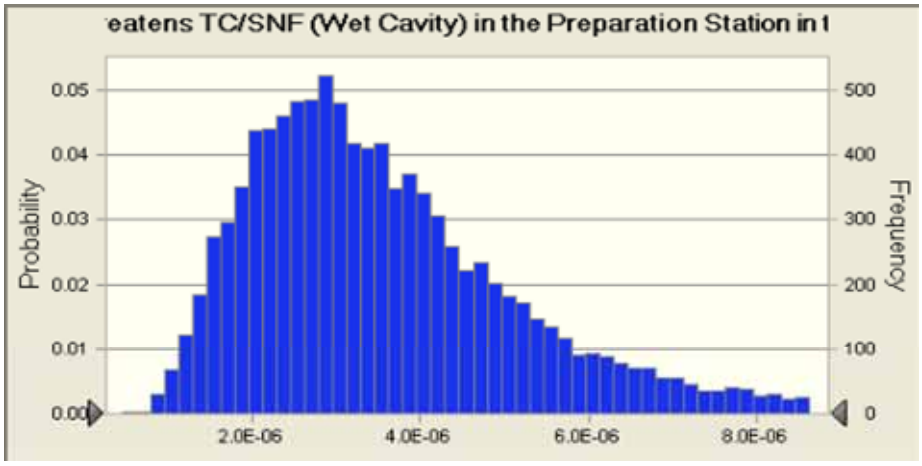
Forecast: Localized Fire Threatens TC/SNF (Dry Cavity) in the Preparation Station in the Preparation Area (cont'd) **Cell: K70**

Percentiles:	Forecast values
0%	2.4E-07
10%	9.2E-07
20%	1.1E-06
30%	1.3E-06
40%	1.5E-06
50%	1.7E-06
60%	1.9E-06
70%	2.1E-06
80%	2.5E-06
90%	3.0E-06
100%	9.3E-06

Forecast: Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station Cell: M71

Summary:

Entire range is from 4.7E-07 to 1.8E-05
Base case is 3.3E-06
After 10,000 trials, the std. error of the mean is 1.8E-08



Statistics:	Forecast values
Trials	10,000
Mean	3.6E-06
Median	3.3E-06
Mode	---
Standard Deviation	1.8E-06
Variance	3.2E-12
Skewness	1.54
Kurtosis	7.03
Coeff. of Variability	0.4874
Minimum	4.7E-07
Maximum	1.8E-05
Range Width	1.8E-05
Mean Std. Error	1.8E-08

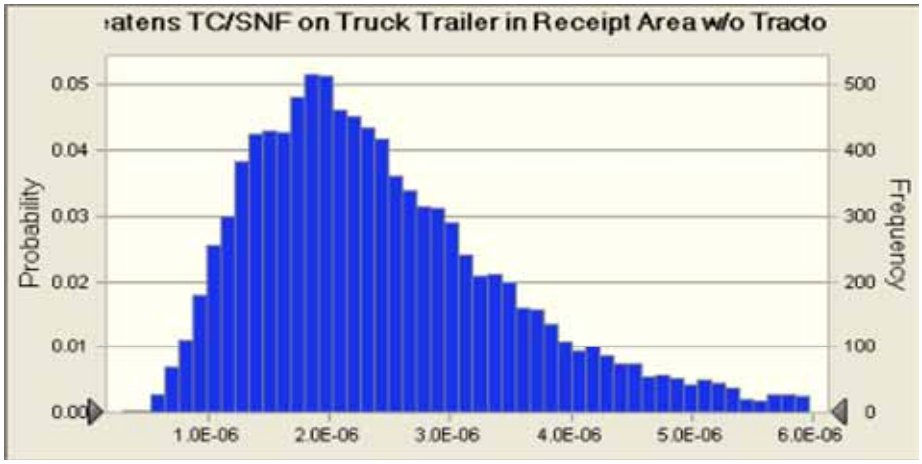
Forecast: Localized Fire Threatens TC/SNF (Wet Cavity) in the Preparation Station Cell: M71

Percentiles:	Forecast values
0%	4.7E-07
10%	1.8E-06
20%	2.2E-06
30%	2.6E-06
40%	2.9E-06
50%	3.3E-06
60%	3.7E-06
70%	4.2E-06
80%	4.8E-06
90%	5.9E-06
100%	1.8E-05

Forecast: Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present) **Cell: K46**

Summary:

Entire range is from 3.0E-07 to 1.2E-05
Base case is 2.3E-06
After 10,000 trials, the std. error of the mean is 1.2E-08



Statistics:	Forecast values
Trials	10,000
Mean	2.5E-06
Median	2.3E-06
Mode	---
Standard Deviation	1.2E-06
Variance	1.5E-12
Skewness	1.53
Kurtosis	6.87
Coeff. of Variability	0.4918
Minimum	3.0E-07
Maximum	1.2E-05
Range Width	1.1E-05
Mean Std. Error	1.2E-08

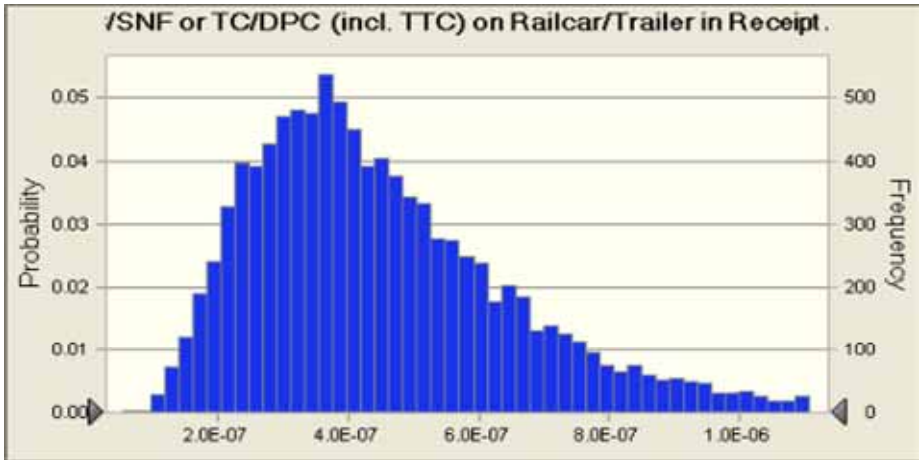
Forecast: Localized Fire Threatens TC/SNF on Truck Trailer in Receipt Area w/o Tractor (No Diesel Present) (cont'd) **Cell: K46**

Percentiles:	Forecast values
0%	3.0E-07
10%	1.2E-06
20%	1.5E-06
30%	1.8E-06
40%	2.0E-06
50%	2.3E-06
60%	2.5E-06
70%	2.9E-06
80%	3.3E-06
90%	4.1E-06
100%	1.2E-05

Forecast: Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present) **Cell: K24**

Summary:

Entire range is from 5.7E-08 to 2.2E-06
Base case is 4.2E-07
After 10,000 trials, the std. error of the mean is 2.3E-09



Statistics:	Forecast values
Trials	10,000
Mean	4.7E-07
Median	4.2E-07
Mode	---
Standard Deviation	2.3E-07
Variance	5.2E-14
Skewness	1.53
Kurtosis	6.80
Coeff. of Variability	0.4920
Minimum	5.7E-08
Maximum	2.2E-06
Range Width	2.1E-06
Mean Std. Error	2.3E-09

Forecast: Localized Fire Threatens TC/SNF or TC/DPC (incl. TTC) on Railcar/Trailer in Receipt Area w/Tractor (Diesel Present) (cont'd) **Cell: K24**

Percentiles:	Forecast values
0%	5.7E-08
10%	2.3E-07
20%	2.8E-07
30%	3.3E-07
40%	3.7E-07
50%	4.2E-07
60%	4.7E-07
70%	5.3E-07
80%	6.2E-07
90%	7.5E-07
100%	2.2E-06

End of Forecasts

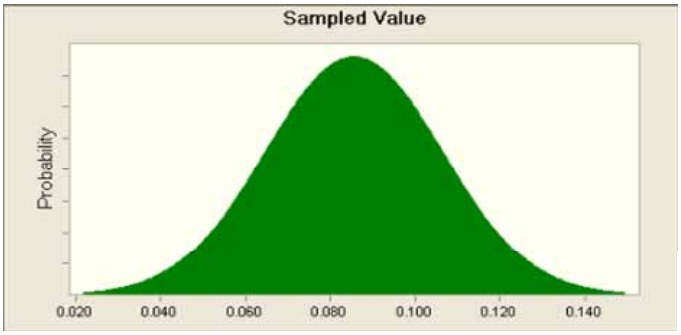
Assumptions

Worksheet: [WHF Fire Frequency_No Suppression.xls]Ignition Source Frequency

Assumption: Sampled Value **Cell: H2**

Normal distribution with parameters:

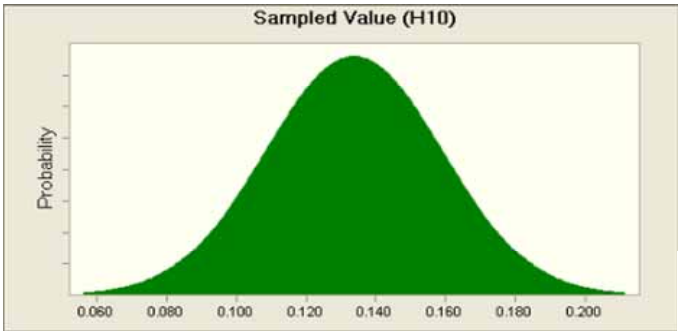
Mean	0.086	(=I2)
97.5%	0.126	(=J2)



Assumption: Sampled Value (H10) **Cell: H10**

Normal distribution with parameters:

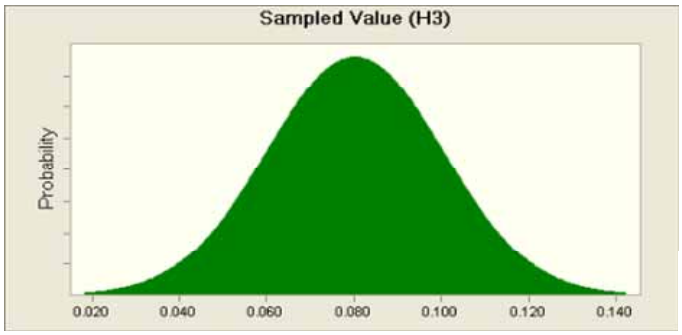
Mean	0.134	(=I10)
97.5%	0.183	(=J10)



Assumption: Sampled Value (H3) **Cell: H3**

Normal distribution with parameters:

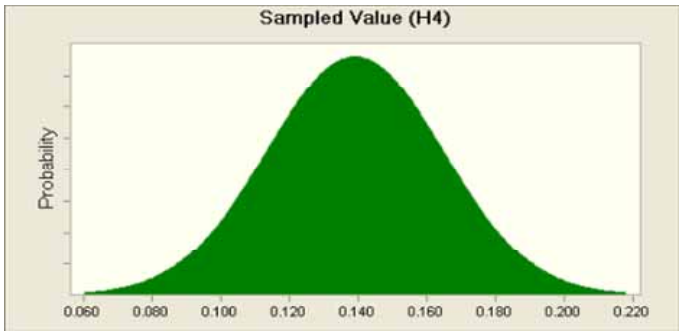
Mean	0.080	(=I3)
97.5%	0.120	(=J3)



Assumption: Sampled Value (H4) **Cell: H4**

Normal distribution with parameters:

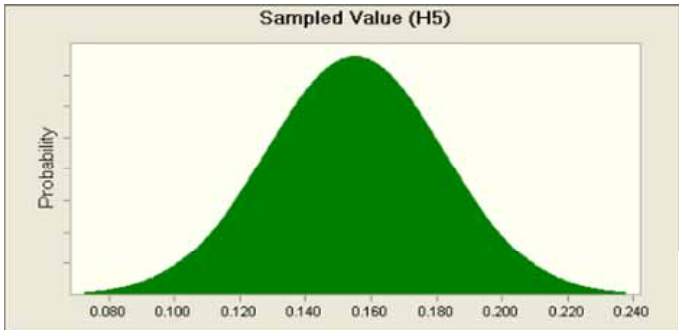
Mean	0.139	(=I4)
97.5%	0.189	(=J4)



Assumption: Sampled Value (H5) **Cell: H5**

Normal distribution with parameters:

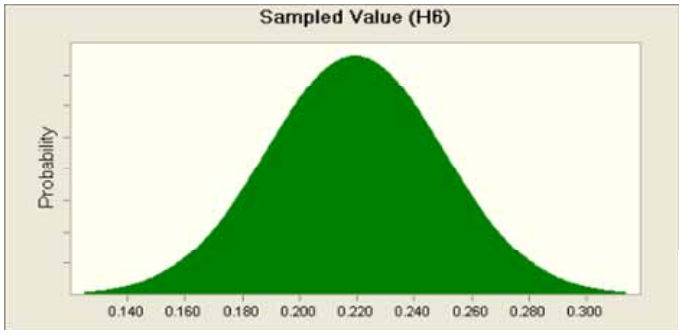
Mean	0.155	(=I5)
97.5%	0.207	(=J5)



Assumption: Sampled Value (H6) **Cell: H6**

Normal distribution with parameters:

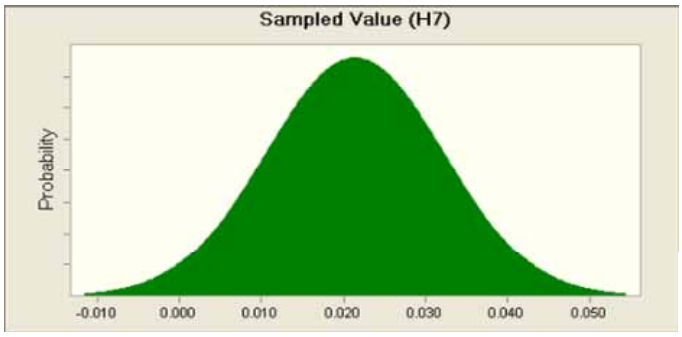
Mean	0.219	(=I6)
97.5%	0.279	(=J6)



Assumption: Sampled Value (H7) **Cell: H7**

Normal distribution with parameters:

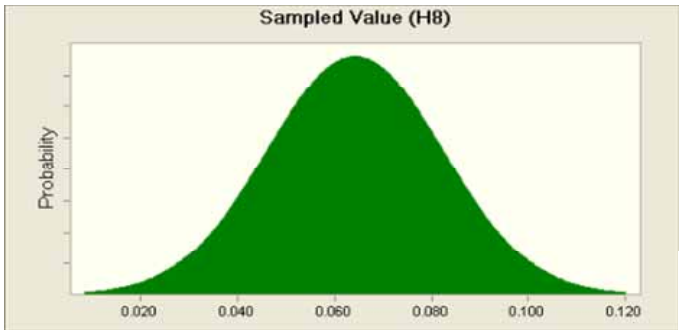
Mean	0.021	(=I7)
97.5%	0.042	(=J7)



Assumption: Sampled Value (H8) **Cell: H8**

Normal distribution with parameters:

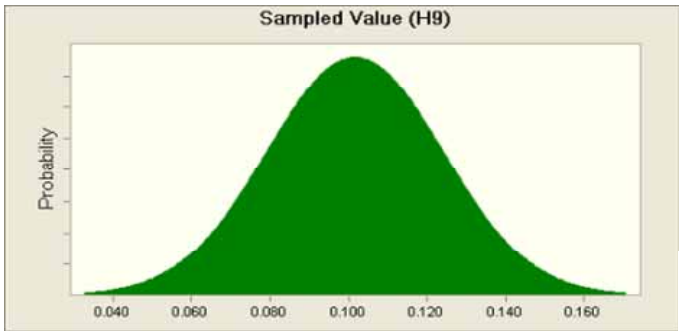
Mean	0.064	(=I8)
97.5%	0.100	(=J8)



Assumption: Sampled Value (H9) **Cell: H9**

Normal distribution with parameters:

Mean	0.102	(=I9)
97.5%	0.145	(=J9)

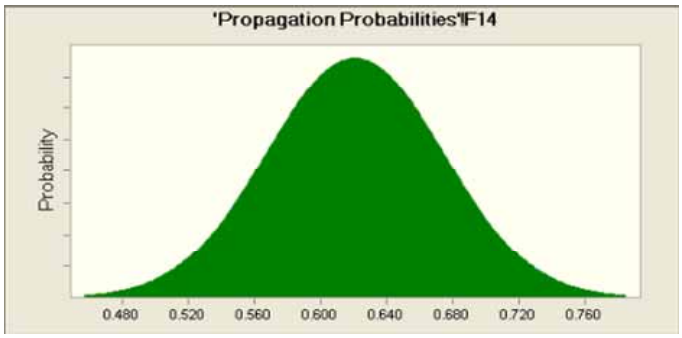


Worksheet: [WHF Fire Frequency_No Suppression.xls]Propagation Probabilities

Assumption: F14 **Cell: F14**

Normal distribution with parameters:

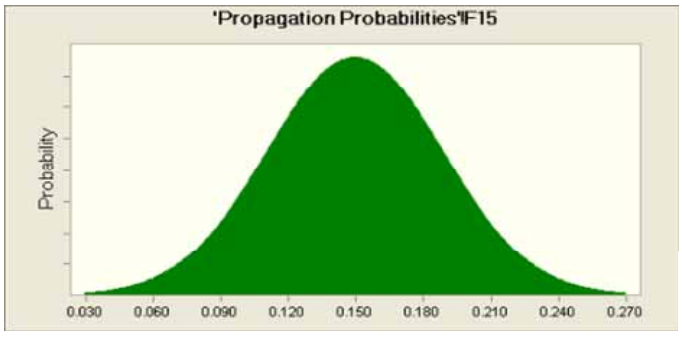
Mean	0.621	(=G14)
97.5%	0.725	(=H14)



Assumption: F15 **Cell: F15**

Normal distribution with parameters:

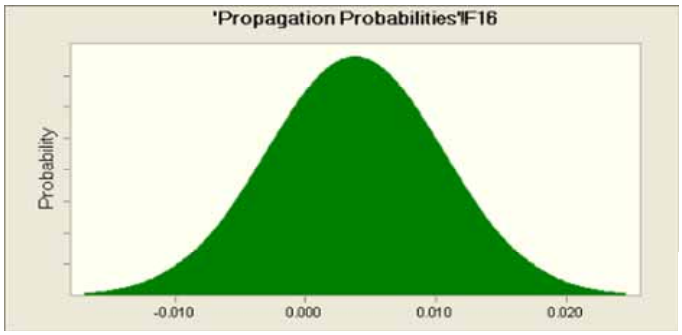
Mean	0.149	(=G15)
97.5%	0.226	(=H15)



Assumption: F16 **Cell: F16**

Normal distribution with parameters:

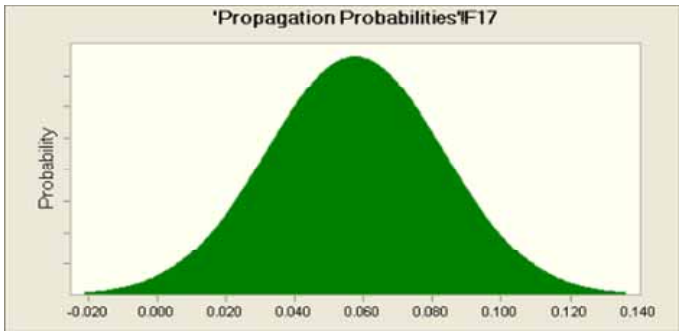
Mean	0.004	(=G16)
97.5%	0.017	(=H16)



Assumption: F17 **Cell: F17**

Normal distribution with parameters:

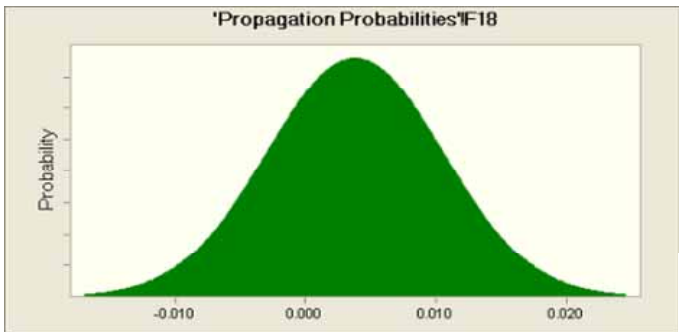
Mean	0.057	(=G17)
97.5%	0.107	(=H17)



Assumption: F18 **Cell: F18**

Normal distribution with parameters:

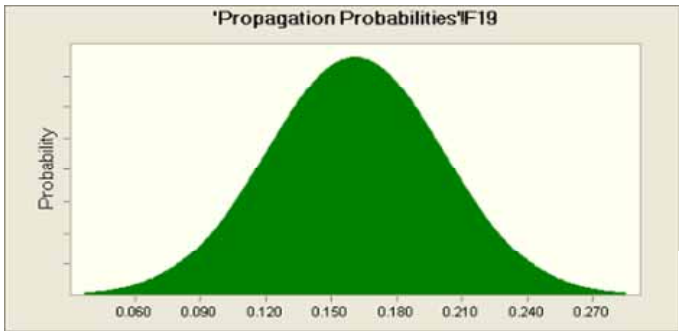
Mean	0.004	(=G18)
97.5%	0.017	(=H18)



Assumption: F19 **Cell: F19**

Normal distribution with parameters:

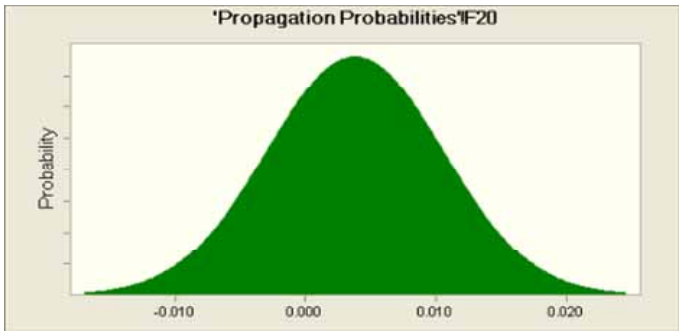
Mean	0.161	(=G19)
97.5%	0.240	(=H19)



Assumption: F20 **Cell: F20**

Normal distribution with parameters:

Mean	0.004	(=G20)
97.5%	0.017	(=H20)

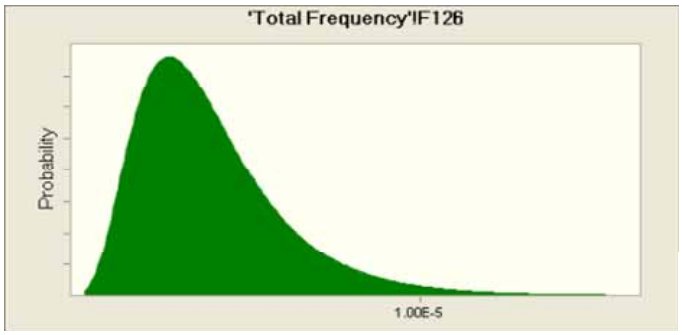


Worksheet: [WHF Fire Frequency_No Suppression.xls]Total Frequency

Assumption: F126 **Cell: F126**

Lognormal distribution with parameters:

50%	3.94E-6	
97.5%	9.40E-6	(=I126)



End of Assumptions

ATTACHMENT G
EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES

ATTACHMENT G
EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES

Attachment G contains Table G-1, *Event Sequence Quantification Summary*, referenced by Section 6.7. It also contains Table G-2, *Final Event Sequences Summary*; Table G-3, *Beyond Category 2 Final Event Sequences Summary*; and Table G-4, *Important to Criticality Final Event Sequences Summary* that are referenced in Section 6.8. Cells in these tables with 0.00E+00 indicate that the value is <E-12. This attachment can be found on the CD in Attachment H, in a file named Attachment G.doc.

This attachment can be found on the CD in Attachment H, in a file named Attachment G.doc.

ATTACHMENT H
SAPHIRE MODEL AND SUPPORTING FILES

ATTACHMENT H
SAPHIRE MODEL AND SUPPORTING FILES

This attachment is the CD containing the SAPHIRE model and supporting files. The electronic files contained on the CD are identified below.