

BSC

Design Calculation or Analysis Cover Sheet

1. QA: QA

2. Page 1

Complete only applicable items.

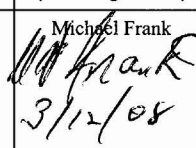
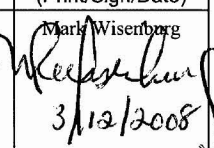
3. System Monitored Geologic Repository	4. Document Identifier 51A-PSA-IH00-00200-000-00A
5. Title Initial Handling Facility Reliability and Event Sequence Categorization Analysis	
6. Group Preclosure Safety Analyses	
7. Document Status Designation <input type="checkbox"/> Preliminary <input checked="" type="checkbox"/> Committed <input type="checkbox"/> Confirmed <input type="checkbox"/> Cancelled/Superseded	

8. Notes/Comments

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

1) CACN-001, DATED 04/06/2008

Attachments	Total Number of Pages
Attachment A. Event Trees	96
Attachment B. System/Pivotal Event Analysis – Fault Trees	238
Attachment C. Active Component Reliability Data Analysis	52
Attachment D. Passive Equipment Failure Analysis	93
Attachment E. Human Reliability Analysis	168
Attachment F. Fire Analysis	115
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	990	H-2	Guy Ragan/See page 2	See Page 3	Michael Frank  3/12/08	Mark Wisenbarg  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	Originator	Signature/Date
1	PURPOSE	Guy Ragan	<i>Guy Ragan 3/11/08</i>
2	REFERENCES	Guy Ragan	<i>Guy Ragan 3/11/08</i>
3	ASSUMPTIONS	Guy Ragan	<i>Guy Ragan 3/11/08</i>
4	METHODOLOGY	Guy Ragan	<i>Guy Ragan 3/11/08</i>
4.1	QUALITY ASSURANCE	Guy Ragan	<i>Guy Ragan 3/11/08</i>
4.2	USE OF SOFTWARE	Guy Ragan	<i>Guy Ragan 3/11/08</i>
4.3	DESCRIPTION OF ANALYSIS METHODS	Doug Orvis Erin Collins & Pierre Macheret Dan Christman David Bradley Paul Amico & Mary Presley Joe Minarick	<i>Doug Orvis 3/11/08</i> <i>Erin Collins 3/11/08</i> <i>P. Macheret 3/11/08</i> <i>Dan Christman 3/11/08</i> <i>David Bradley 3/11/08</i> <i>Paul Amico 3/11/08</i> <i>Mary Presley 3/11/08</i> <i>Joe Minarick 3/11/08</i>
5	LIST OF ATTACHMENTS	Doug Orvis	<i>Doug Orvis 3/11/08</i>
6	BODY OF CALCULATION	NA	
6.0	INITIATING EVENT SCREENING	Guy Ragan	<i>Guy Ragan 3/11/08</i>
6.1	EVENT TREE ANALYSIS	Guy Ragan	<i>Guy Ragan 3/11/08</i>
6.2	INITIATING AND PIVOTAL EVENT ANALYSIS	Daryl Keppler Bill Schwinkendorf	<i>Daryl Keppler 3/11/08</i> <i>Bill Schwinkendorf 3/11/08</i>
6.3	DATA UTILIZATION	Erin Collins Dan Christman (6.3.2.1, 6.3.2.2, 6.3.2.5) David Bradley (6.3.2.3, 6.3.2.4) Daryl Keppler Bill Schwinkendorf	<i>Erin Collins 3/11/08</i> <i>Dan Christman 3/11/08</i> <i>David Bradley 3/11/08</i> <i>Daryl Keppler 3/11/08</i> <i>Bill Schwinkendorf 3/11/08</i>
6.4	HUMAN RELIABILITY ANALYSIS	Paul Amico Mary Presley Erin Collins Doug Orvis	<i>Paul Amico 3/11/08</i> <i>Mary Presley 3/11/08</i> <i>Erin Collins 3/11/08</i> <i>Doug Orvis 3/11/08</i>
6.5	FIRE ANALYSIS	Paul Amico & Laura Plumb under supervision of Paul Amico	<i>Paul Amico 3/11/08</i> <i>Laura Plumb 3/11/08</i>
6.6	(Not used)		
6.7	EVENT SEQUENCE QUANTIFICATION	Daryl Keppler Jeff Marr Bill Schwinkendorf	<i>Daryl Keppler 3/11/08</i> <i>Jeff Marr 3/11/08</i> <i>Bill Schwinkendorf 3/11/08</i>
6.8	EVENT SEQUENCE GROUPING AND CATEGORIZATION	Daryl Keppler Jeff Marr Bill Schwinkendorf	<i>Daryl Keppler 3/11/08</i> <i>Jeff Marr 3/11/08</i> <i>Bill Schwinkendorf 3/11/08</i>
6.9	DEFINED ITS SSCs AND PROCEDURAL SAFETY CONTROLS REQUIREMENTS	Doug Orvis & Jeff Marr	<i>Doug Orvis 3/11/08</i> <i>Jeff Marr 3/11/08</i>
7	RESULTS AND CONCLUSIONS	Guy Ragan	<i>Guy Ragan 3/11/08</i>


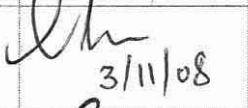
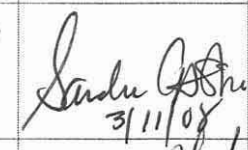
Section	Section Name	Originator	Signature/Date
Att A	EVENT TREES	Daryl Keppler Guy Ragan Bill Schwinkendorf	<i>[Handwritten signatures]</i> 3/11/08
Att B	SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES	Daryl Keppler Bill Schwinkendorf	<i>[Handwritten signatures]</i> 3/11/08
Att C	ACTIVE COMPONENT RELIABILITY DATA ANALYSIS	Erin Collins	<i>[Handwritten signature]</i> 3/11/08
Att D	PASSIVE EQUIPMENT FAILURE ANALYSIS	Dan Christman (D1 and D3) & David Bradley (D2)	<i>[Handwritten signatures]</i> 3/11/08
Att E	HUMAN RELIABILITY ANALYSIS	Paul Amico Mary Presley Erin Collins Doug Orvis	<i>[Handwritten signatures]</i> 3/11/08
Att F	FIRE ANALYSIS	Paul Amico & Laura Plumb under supervision of Paul Amico	<i>[Handwritten signatures]</i> 3/11/08
Att G	EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES	Jeff Marr	<i>[Handwritten signature]</i> 3/11/08
Att H	SAPPHIRE MODEL AND SUPPORTING FILES (CD)	Guy Ragan	<i>[Handwritten signature]</i> 3/11/08

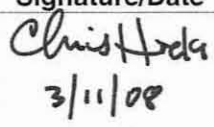
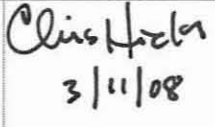
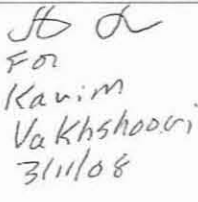
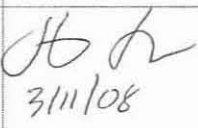
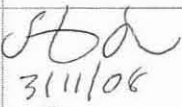
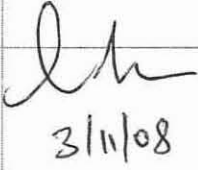
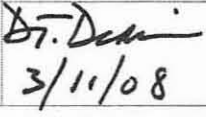
Kathy Ashley performed general coordination of document for the check copy (00Aa) and completed the Originator Checklist.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Andrew Burningham	<i>[Handwritten signature]</i> 3/11/08	Section 1-7	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.)
Amy Primmer	<i>[Handwritten signature]</i> 3/11/08	Attachments B, C, D, E, G, H		
William Chris Allen	<i>[Handwritten signature]</i> FOR 3/11/08	Attachments A and F		
Alex Deng	<i>[Handwritten signature]</i> 03/11/08	Sections 1, 3, 4, and 7	Overall approach and methodology	Check that the standard approach and methodology reflect input from industry reviewers.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Phuoc Le / Dan Gallagher	<i>Phuoc Le</i> 3/11/08 <i>Daniel W Gallagher</i> 3/11/08	Section 6.0 through 6.8 and Attachments A through H	Cut set check	Cut Set Check - Section 6.0 - 6.8 and Attachments A - H
Kathy Ashley	<i>Kathy Ashley</i> 3/11/08	Section 6.9	Specialty check	Section 6.9.
Dan Christman	<i>Dan Christman</i> 3/11/08	Section 6.5 and Attachment F	Specialty check: Fire Initiating Events	Fire Initiating Events - Section 6.5 and Attachment F
Doug Orvis	<i>Doug Orvis</i> 3/11/08	Section 6.0	Specialty check: Section 6.0	Initiating Event Screening - Section 6.0
Laura Plumb	<i>Laura Plumb</i> 3/11/08	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
M. J. Rubano for Ekachai Danupatampa	<i>May Jane Rubano</i> 3.11.08	Attachment B - System Pivotal Events Analyses - Fault Tree Analysis - Loading/Unloading Room Shield Door/Slide Gate	Design concurrency	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
Stefhan Sherman	 3/11/08	Attachment B - System Pivotal Events Analyses - Fault Tree Analysis - Cask Transfer Trolley	Design concurrency	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	 3/11/08	Attachment B - System Pivotal Events Analyses - Fault Tree Analysis - CTM System	Design concurrency	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	 for Narci Encarnacion	Attachment B - System Pivotal Events Analyses - Fault Tree Analysis - Waste Package Transfer Trolley	Design concurrency	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	 3/11/2008	Attachment B - System Pivotal Events Analyses - Fault Tree Analysis - Prime Mover	Design concurrency	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
Dan Christman	 3/4/08	Attachment C	Specialty check	Check Attachment C including the MathCad file for Bayesian update of reliability values
Doug Smith	 3/13/08	Attachment C inputs	Detailed references and numerical inputs	This check traced input data back to references for Attachment C.
Stephen Skochko for Karim Vakhshoori	 3/11/08			
Stephen Skochko	 3/11/08			
Dan Christman	 3/4/08	Attachment D	Specialty check	Check Sections D2, 6.3.2.3, and 6.3.2.4.
David Bradley	 3/4/08	Attachment D	Specialty check	Check Sections D1, D3, 6.3.2.1, 6.3.2.2, and 6.3.2.5.
Phuoc Le	 3/11/08	Attachment E - Human Reliability Analysis	Specialty check	Section 6.4 and Attachment E
Clarence Smith	 3/11/08	Attachment E - Human Reliability Analysis	Design concurrence	Check that the Basic Scenarios in Attachment E are consistent with the concept of operations.
Dan Christman	 3/4/08	Attachment F Fire Analysis	Specialty check	Check Attachment F and Section 6.5
Nasser Dehkordi	 3/11/08	Attachment F Fire Analysis	Design concurrence	Check dimensions of rooms and area computation
Stephen Skochko	 3/11/08	Attachment F - Fire Analysis	Detailed references and numerical Inputs	Check tabulation of equipment contained in each room
Sandra Castro	 3/11/08	Section 2	Detailed references and numerical Inputs	Check that all references to engineering documents are correct and up to date.
Nasser Dehkordi	 3/11/08	Main body, Attachment E Human Reliability Analysis, and Attachment F Fire Analysis	Detailed references and numerical Inputs	Reference check: Check that all references in the body of the analysis and in Attachments E and F are references to the appropriate document.
Kathryn Sheffield	 3/11/08	All sections of main body and Attachment B	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Chris Hicks	 3/11/08	Attachment A - Event Tree Analyses	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Chris Hicks	 3/11/08	Attachment C - Active Component Reliability Data Analysis	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Stephen Skochko for Karim Vakhshoori	 3/11/08	Attachment D - Passive Equipment Failure Analysis and Attachment E - Human Reliability Analysis	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Stephen Skochko	 3/11/08	Attachment F- Fire Analysis	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Stephen Skochko	 3/11/08	Attachment G - Event Sequences Quantification	Detailed references and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments
Phouc Le	 3/11/08	Attachment H - SAPHIRE Model and Supporting Files (CD)	Detailed references and numerical Inputs	Check CD has correct files and is in required format.
Dale Dexheimer	 3/11/08	Section 6.8	Specialty check	Check consistency with Preclosure Consequence Analysis

CONTENTS

	Page
ACRONYMS AND ABBREVIATIONS	12
1. PURPOSE	15
2. REFERENCES	19
2.1 PROCEDURES/DIRECTIVES	19
2.2 DESIGN INPUTS	19
2.3 DESIGN CONSTRAINTS	26
2.4 DESIGN OUTPUTS	27
2.5 ATTACHMENT REFERENCES	27
3. ASSUMPTIONS	28
3.1 ASSUMPTIONS REQUIRING VERIFICATION	28
3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION	28
4. METHODOLOGY	29
4.1 QUALITY ASSURANCE	29
4.2 USE OF SOFTWARE	30
4.3 DESCRIPTION OF ANALYSIS METHODS	31
5. LIST OF ATTACHMENTS	92
6. BODY OF ANALYSIS	93
6.0 INITIATING EVENT SCREENING	93
6.1 EVENT TREES	106
6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS	113
6.3 DATA UTILIZATION	132
6.4 HUMAN RELIABILITY ANALYSIS	172
6.5 FIRE INITIATING EVENTS	182
6.6 NOT USED	192
6.7 EVENT SEQUENCE FREQUENCY RESULTS	192
6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION	195
6.9 IMPORTANT TO SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS AND PROCEDURAL SAFETY CONTROL REQUIREMENTS	205
7. RESULTS AND CONCLUSIONS	221
ATTACHMENT A EVENT TREES	A-1
ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES	B-1
ATTACHMENT C ACTIVE COMPONENT RELIABILITY DATA ANALYSIS	C-1
ATTACHMENT D PASSIVE EQUIPMENT FAILURE ANALYSIS	D-1
ATTACHMENT E HUMAN RELIABILITY ANALYSIS	E-1
ATTACHMENT F FIRE ANALYSIS	F-1
ATTACHMENT G EVENT SEQUENCE QUANTIFICATION SUMMARY TABLE	G-1
ATTACHMENT H SAPHIRE MODEL AND SUPPORTING FILES	H-1

FIGURES

	Page
4.3-1. Event Sequence Analysis Process.....	32
4.3-2. Preclosure Safety Assessment Process	37
4.3-3. Portion of a Simplified Process Flow Diagram for a Typical Waste-Handling Facility	39
4.3-4. Event Sequence Diagram–Event Tree Relationship	40
4.3-5. Example Fault Tree.....	44
4.3-6. Concept of Uncertainty in Load and Resistance.....	47
4.3-7. Point Estimate Load Approximation Used in PCSA	49
4.3-8. Component Failure Rate “Bathtub Curve” Model.....	55
4.3-9. Incorporation of Human Reliability Analysis within the PCSA.....	65
4.3-10. Transfer from Event Tree to Fault Tree.....	77
6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population- Variability Probability Density Function (Solid Line)	135
6.4-1. Initial Handling Facility Operations	173

TABLES

	Page
4.3-1. Criticality Control Parameter Summary	87
6.0-1. Retention Decisions from External Events Screening Analysis	97
6.0-2. Bases for Screening Internal Initiating Events.....	100
6.1-1. Waste Form Throughputs for the IHF Over the Preclosure Period	110
6.1-2. Figure Locations for Initiating Event Trees and Response Trees.....	110
6.2-1. Summary of Top Event Quantification for the SPM on a per Cask Basis.....	117
6.2-2. Summary of Top Event Quantification for the CTT.....	120
6.2-3. Summary of Top Event Quantification for the Shield Doors and Slide Gate.....	122
6.2-4. Summary of Top Event Quantification for the CTM.....	126
6.2-5. Summary of Top Event Quantification for the WPTT	129
6.2-6. Probability of Spurious Sprinkler Actuation.....	130
6.3-1. Active Component Reliability Data Summary	138
6.3-2. Failure Probabilities Due to Drops and Other Impacts.....	148
6.3-3. Failure Probabilities Due to Miscellaneous Events	149
6.3-4. Failure Probabilities for Collision Events and Two-Blocking.....	151
6.3-5. Summary of Canister Failure Probabilities in Fire	154
6.3-6. Probabilities of Degradation or Loss of Shielding.....	157
6.3-7. Summary of Passive Event Failure Probabilities.....	159
6.3-8. Passive Equipment Failure Basic Events used in IHF Event Sequence Analysis.....	160
6.3-9. Fire Analysis for Wastes Types in Specific Configuration	164
6.3-10. Split Fractions for Waste Types in Various Configurations.....	165
6.3-11. Miscellaneous Data Used In the Reliability Analysis.....	166
6.4-1. Formulae for Addressing HFE Dependencies	177
6.4-2. Human Failure Event Probability Summary.....	177
6.5-1. Room Areas and Total Ignition Frequency.....	183
6.5-2. Ignition Source Category and Room-by-Room Population.....	184
6.5-3. Residence Fractions	186
6.5-4. Results from Monte Carlo Simulation of Fire Initiating Event Frequency Distributions.....	187

TABLES (Continued)

	Page
6.5-5. Basic Events Data Associated with Fire Analysis	190
6.8-1. Bounding Category 2 Event Sequences	196
6.8-2. Category 1 Final Event Sequences Summary	201
6.8-3. Category 2 Final Event Sequences Summary	202
6.9-1. Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs	206
6.9-2. Summary of Procedural Safety Controls for the IHF Facility	219
7-1. Key to Results	221
7-2. Summary of Category 2 Event Sequences.....	222

ACRONYMS AND ABBREVIATIONS

Acronyms

ATHEANA	a technique for human event analysis
BSC	Bechtel SAIC Company, LLC
CCF	common-cause failure
CDF	cumulative density function
CRCF	Canister Receipt and Closure Facility
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 content
EOC	error of commission
EOO	error of omission
EPRI	Electric Power Research Institute
ESD	event sequence diagram
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
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
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
LOSP	loss of offsite power
LOS	loss of shielding

ACRONYMS AND ABBREVIATIONS (Continued)

LS-DYNA	Livermore Software–Dynamic Finite Element Program
MCO	multicanister overpack
MLD	master logic diagram
N/A	not applicable
NARA	Nuclear Action Reliability Assessment
NFPA	National Fire Protection Association
NNPP	Naval Nuclear Propulsion Program
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
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSC	procedural safety control
PSF	performance shaping factor
QA	quality assurance
RF	Receipt Facility
SDU	steel/depleted uranium
SFTM	spent fuel transfer machine
SLS	steel/lead/steel
SNF	spent nuclear fuel
SPM	site prime mover
SPMRC	site prime mover railcar
SPMTT	site prime mover truck trailer
SRET	system response event tree
SSC	structure, system, or component
SSCs	structures, systems, and components
TAD	transportation, aging, and disposal
TEV	transport and emplacement vehicle
THERP	Technique for Human Error Rate Prediction
TYP-FM	type and failure mode combination
WHF	Wet Handling Facility
WPTT	waste package transfer trolley
YMP	Yucca Mountain Project

ACRONYMS AND ABBREVIATIONS (Continued)

Abbreviations

AC	alternating current
°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
V	volt
yr, yrs	year, years

1. PURPOSE

This document on the Initial Handling Facility (IHF) and its companion document entitled *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28) constitute a portion of the preclosure safety analysis (PCSA) that is described in its entirety in the safety analysis report that will be 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28) describes the identification of initiating events and the development of potential event sequences that emanate from them. This analysis uses the resulting event sequences 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 (Ref. 2.3.2) and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report* (Ref. 2.2.64). The PCSA, however, limits the use of PRA technology to identification and development of event sequences that might lead to the 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 should 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 should be analyzed to determine if reactivity can exceed the upper subcriticality limit.

The Naval Nuclear Propulsion Program (NNPP) performs a criticality evaluation of a series of IHF conditions that are capable of increasing the criticality potential of naval SNF. The evaluation is based on modeling rearrangement of naval SNF due to mechanical damage, neutron reflection from materials outside the naval SFC, and neutronic coupling with other fissile material in proximity to the naval SFC. Based on the event sequences in this document and established facility limits, NNPP deterministically demonstrates that the end state configurations are subcritical. In order to determine the criticality potential for waste forms 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 NNPP and PCSA criticality analyses determined the parameters that this event sequence analysis should include. 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. Situations treated in the event sequence analyses of repository facilities other than the IHF for similar reasons are multiple U.S. Department of Energy (DOE) spent nuclear fuel (SNF) canisters in the Canister Receipt and Closure Facility (CRCF) in the same general location and presence of sufficient soluble boron in the pool in the Wet Handling Facility.

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 system, 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 manufacturing 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 Part 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 an 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. 2.2.27) and *Frequency Analysis of Aircraft Hazards for License Application* (Ref. 2.2.17). Internal event identification (using a master logic diagram and hazard and operability evaluation), event sequence development and grouping, and related facility details are provided in *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28), which also documents the methodology and process employed and initiates the analysis that is completed here.

This document uses event trees from *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28) 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 (Ref. 2.2.28) 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 for the main report are listed in this section and the Design Inputs for Attachments B through F are 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 *ANSI/ANS-58.23-2007. 2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.
- 2.2.4 *Apostolakis, G. and Kaplan, S. 1981. "Pitfalls in Risk Calculations." *Reliability Engineering*, 2, 135-145. Barking, England: Applied Science Publishers. TIC: 253648.

- 2.2.5 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.
- 2.2.6 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.
- 2.2.7 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.
- 2.2.8 ASME (American Society of Mechanical Engineers) 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 ANSI/AISC N690-1994. 1994. *American National Standard Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities*. Chicago, Illinois: American Institute of Steel Construction. TIC: 252734.
- 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 (Bechtel SAIC Company) 2004. *BSC Engineering Study, Waste Package Closure Welding Process Characteristics*. 000-30R-HW00-00300-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20041119.0001.
- 2.2.14 BSC 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.
- 2.2.15 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.

- 2.2.16 *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.
- 2.2.17 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.
- 2.2.18 BSC 2007. *GROA External Dose Rate Calculation*. 000-PSA-MGR0-01300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071023.0003.
- 2.2.19 *BSC 2007. *Initial Handling Facility Electrical Room Equipment Layout*. 51A-E40-EEN0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070521.0003.
- 2.2.20 BSC 2007. *Initial Handling Facility General Arrangement Ground Floor Plan*. 51A-P10-IH00-00102-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0017.
- 2.2.21 *BSC 2007. *Liquid Low-Level Waste Collection Calculation (C2 and C3 Contamination Zones)*. 000-M0C-MWL0-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ENG.20071101.0013.
- 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. *Mechanical Handling Design Report - Waste Package Transfer Trolley*. 000-30R-WHS0-01200-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0001.
- 2.2.24 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.
- 2.2.25 BSC 2007. *Receipt Facility Fire Hazard Analysis*. 200-M0A-FP00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070823.0001.
- 2.2.26 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 2008. *External Events Hazards Screening Analysis*. 000-00C-MGR0-00500-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080219.0001.
- 2.2.28 BSC 2008. *Initial Handling Facility Event Sequence Development Analysis*. 51A-PSA-IH00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070207.0005.

- 2.2.29 *BSC 2008. *Initial Handling Facility Fire Hazard Analysis*. 51A-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0007.
- 2.2.30 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.
- 2.2.31 BSC 2008. *Preclosure Consequence Analyses*. 000-00C-MGR0-00900-000-00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080129.0006.
- 2.2.32 BSC 2008. *Preclosure Criticality Safety Analysis*. TDR-MGR-NU-000002 REV 01. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0007.
- 2.2.33 BSC 2008. *Seismic and Structural Container Analyses for the PCSA*. 000-PSA-MGR0-02100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ENG.20080220.0003.
- 2.2.34 *BSC 2008. *Wet Handling Facility Fire Hazard Analysis*. 050-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080213.0001.
- 2.2.35 *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.
- 2.2.36 *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.
- 2.2.37 DOE (U.S. Department of Energy) 2007. *Software Independent Verification and Validation Change in Operating System Version Report for: SAPHIRE v7.26*. Document ID: 10325-COER-7.26-01. Las Vegas, Nevada: U.S. Department of Energy, Office of Repository Development. ACC: MOL.20070607.0263. (DIRS 184933)
- 2.2.38 *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.
- 2.2.39 *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.

- 2.2.40 *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.
- 2.2.41 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.
- 2.2.42 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.
- 2.2.43 *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
- 2.2.44 *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.
- 2.2.45 *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.
- 2.2.46 *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.
- 2.2.47 *Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-042848-7.
- 2.2.48 *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.
- 2.2.49 *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* Vol. 83, 311-321. New York, New York: Elsevier. TIC: 259380.

- 2.2.50 *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.
- 2.2.51 *Martz, H.F. and Waller, R.A. 1991. *Bayesian Reliability Analysis*. Malabar, Florida: Krieger Publishing Company. TIC: 252996. ISBN: 0-89464-395-9.
- 2.2.52 *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.
- 2.2.53 *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.
- 2.2.54 *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.
- 2.2.55 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.
- 2.2.56 *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.
- 2.2.57 *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.
- 2.2.58 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.
- 2.2.59 *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.
- 2.2.60 NRC 1997. *Standard Review Plan for Dry Cask Storage Systems*. Final Report. NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.

- 2.2.61 NRC 2000. *Standard Review Plan for Transportation Packages for Spent Nuclear Fuel*. NUREG-1617. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249470.
- 2.2.62 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.
- 2.2.63 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.
- 2.2.64 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.
- 2.2.65 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071211.0230.
- 2.2.66 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.
- 2.2.67 *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.
- 2.2.68 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.
- 2.2.69 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.
- 2.2.70 SAPHIRE V. 7.26. 2007. VMware/WINDOWS XP. STN: 10325-7.26-01. (DIRS 183846)
- 2.2.71 SFPE (Society of Fire Protection Engineers) 2002. *SFPE Handbook of Fire Protection Engineering*. 3rd Edition. Quincy, Massachusetts: National Fire Protection Association. TIC: 255463. ISBN: 0-87765-451-4.
- 2.2.72 *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.

- 2.2.73 *Smith, C. 2007. *Master Logic Diagram*. Bethesda, Maryland: Futron Corporation. ACC: MOL.20071105.0153; MOL.20071105.0154.
- 2.2.74 *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. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0062.
- 2.2.75 *Snow, S.D. and Morton, D.K. 2007. *Qualitative Analysis of the Standardized DOE SNF Canister Specific Canister-on-Canister Drop Events at the Repository*. EDF-NSNF-087, Rev. 0. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0063.
- 2.2.76 *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.
- 2.2.77 *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.
- 2.2.78 *Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. PhD Dissertation. Espoo, Finland: VTT Technical Research Centre of Finland. TIC: 259928. ISBN: 951-38-6392-1.
- 2.2.79 *Tooker, D. W. 2007. "Estimated Quantities of Wet Piping in the Nuclear Facility Buildings (CRCF, RF, WHF, and IHF)." Interoffice Memorandum from D. W. Tooker (BSC) to Distribution, November 29, 2007, D.I. 1129072284. ACC: CCU.20071130.0012.
- 2.2.80 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.
- 2.2.81 *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.
- 2.2.82 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 50. Energy: Domestic Licensing of Production and Utilization Facilities. U.S. Nuclear Regulatory Commission.

- 2.3.2 10 CFR 63. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. U.S. Nuclear Regulatory Commission.
- 2.3.3 10 CFR 71. Energy: Packaging and Transportation of Radioactive Material. U.S. Nuclear Regulatory Commission.
- 2.3.4 10 CFR 72. Energy: Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste. U.S. Nuclear Regulatory Commission.

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.
- 2.5.3 Attachment C: Design Input references are listed in Section C5.
- 2.5.4 Attachment D: Design Input references are listed in Section D4.1.
- 2.5.5 Attachment E: Design Input references are listed in Section E8.1.
- 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 the 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 inputs 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, Section 3.2.2 and 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 “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 memoranda: Due to the early nature of the design of some systems, the only available sources for the information used are interoffice memoranda. These sources provide conservative estimates and are 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 V. 7.26 STN 10325-7.26-01 (Ref. 2.2.70) 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. 2.2.37). 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 version 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.

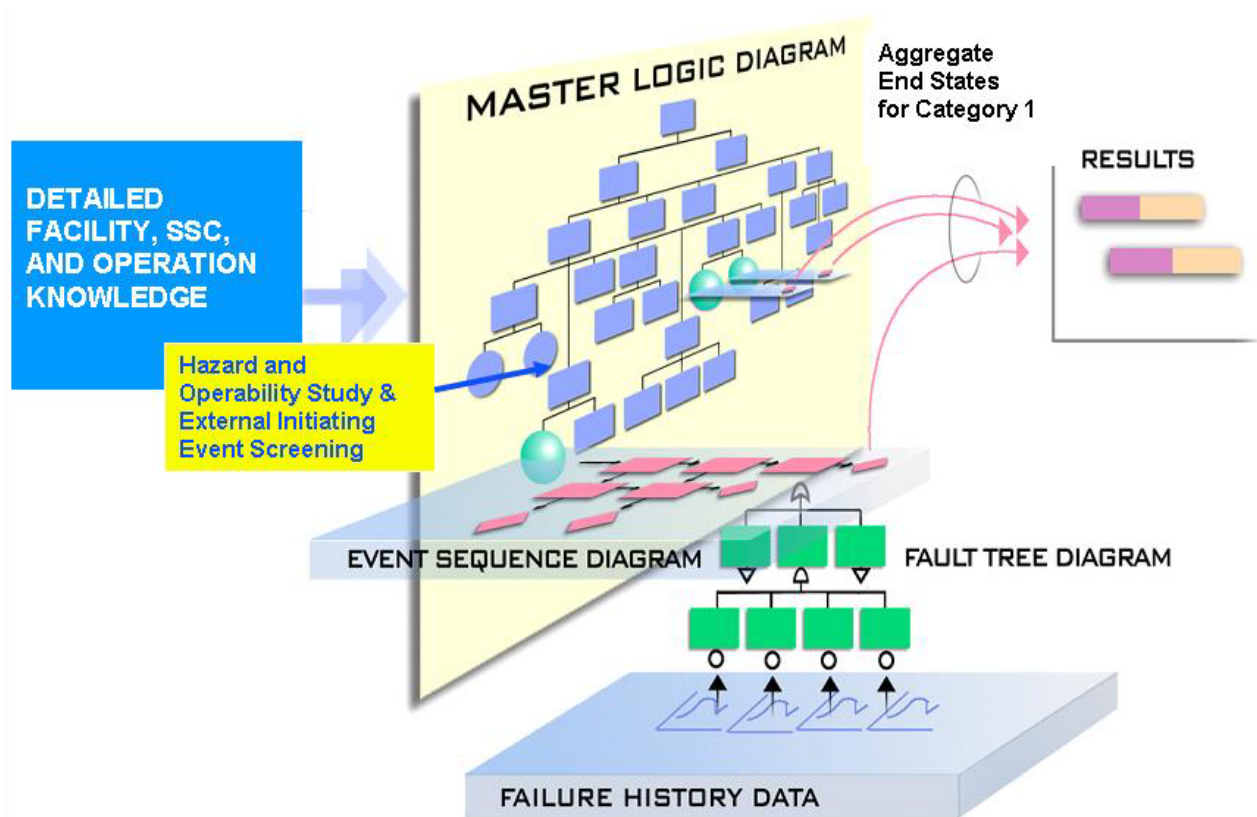
4.3 DESCRIPTION OF ANALYSIS METHODS

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 IHF. Specific features of the IHF and its operations are not discussed until Section 6, where the

methods described here are applied to the IHF. The PCSA uses the technology of PRA as described in references such as *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6). 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 the 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. 2.2.73)

Figure 4.3-1. Event Sequence Analysis Process

The PCSA starts with analysts obtaining sufficient knowledge of the designs and operations of facility, equipment, and SSCs to understand how the YMP waste handling is conducted. This is largely performed and documented in the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28). An understanding of how a facility should operate 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 master logic diagram (MLD) development, cross-checked with an evaluation based on applied hazard and operability (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 Wet Handling Facility 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. 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. The NNPP performs a criticality evaluation of a series of IHF conditions that are capable of increasing the criticality potential of naval SNF. The evaluation is based on modeling rearrangement of naval SNF due to mechanical damage, neutron reflection from materials outside the naval SFC, and neutronic coupling with other fissile material in proximity to the naval SFC. Based on the event sequences in this document and established facility limits, NNPP deterministically demonstrates that the end state configurations are subcritical. In order to determine the criticality potential for other waste forms 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. 2.2.36) and *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations*. NUREG/CR-4639 (Ref. 2.2.46)), 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* unreliabilities, 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.

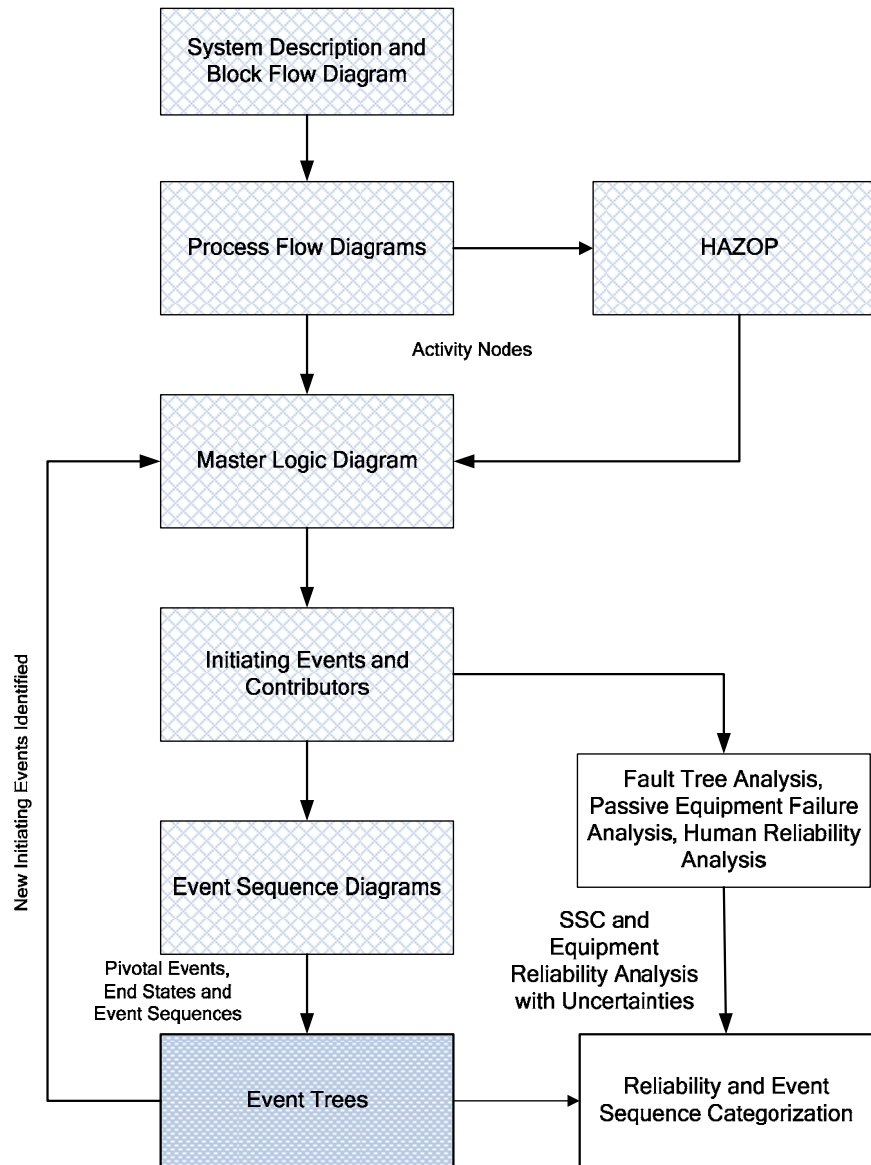
The PCSA is described above as a system simulation. This is important in that any simulation or model is an approximate representation of reality. Approximations may lead to uncertainties regarding the frequencies of event sequences. The event sequence quantification presented in this document propagates 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28).
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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28). 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; SSC = structure, system, or component

Source: Modified from *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28, Figure 2).

Figure 4.3-2. Preclosure Safety Assessment Process

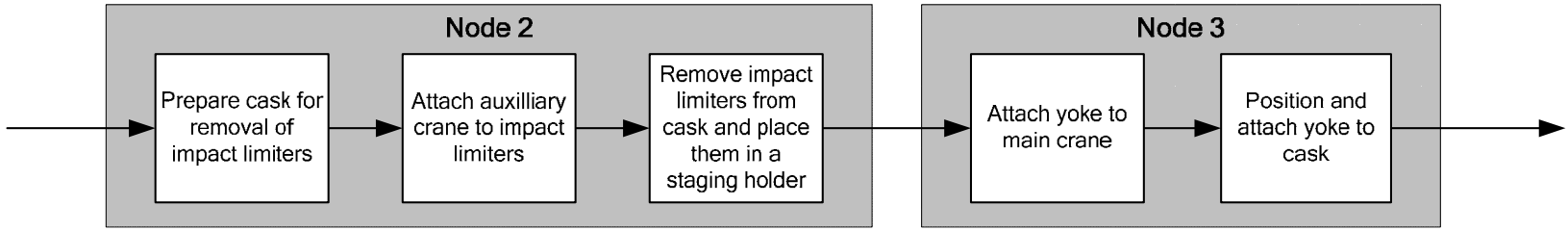
The event sequences that are categorized in the present analysis can be more fully understood by consulting the event sequence development analysis (Ref. 2.2.28). The remainder of this subsection presents a refresher of the event sequence development process

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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28, 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) 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28, 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

The initiating events that are represented in the MLD are transferred to events depicted as “little bubbles” (Figure 4.3-4, 1,2,3) 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. 2.2.37), 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. 2.2.59, 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. 2.2.59). 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 (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. 2.2.15, 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

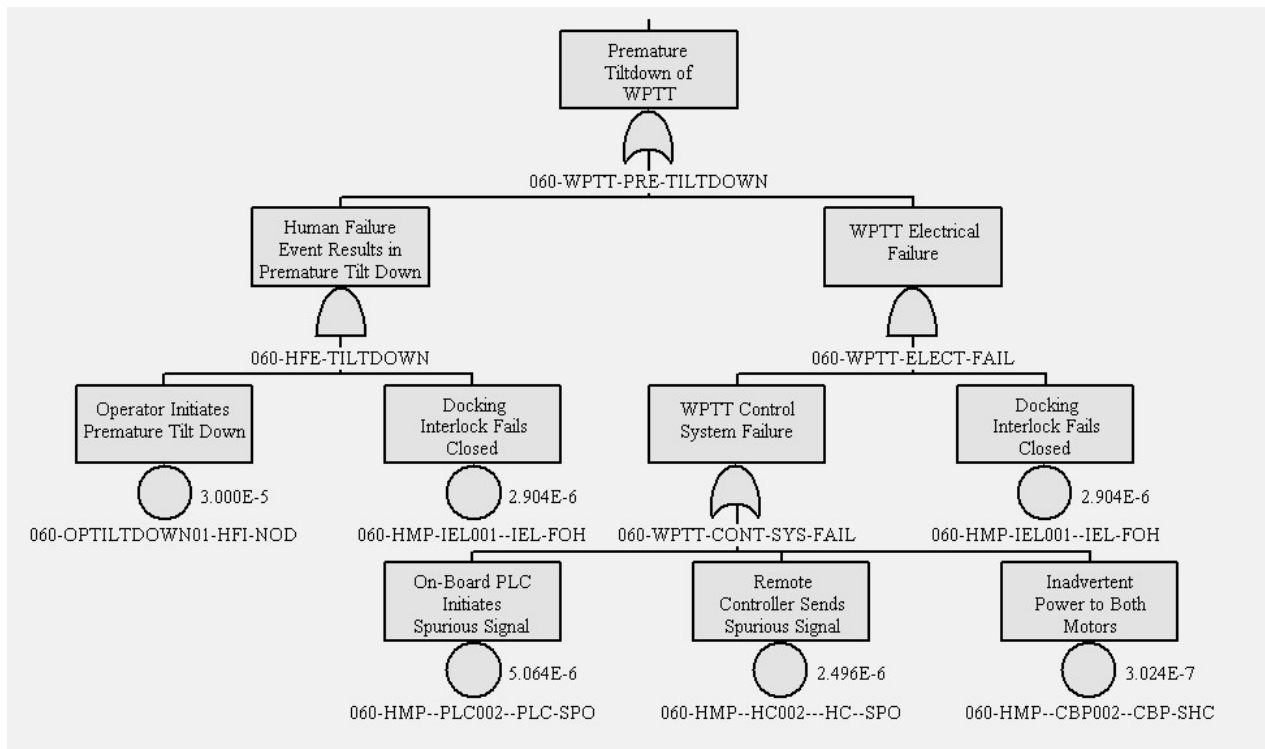
than or equal to one, the resulting product is not greater than the number of occurrences of the event sequence before multiplication by the probability. The number of occurrences of an event sequence is calculated for a given waste form type, without adjustment for the probability of presence of other 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 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 each other up, 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 bubbles beneath them indicating a *basic event*. Basic events are associated with frequencies from industry-wide active equipment reliability information, passive equipment failure analysis, or human reliability analysis.

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. 2.2.80). 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. 2.2.5) and Section III, Subsection NCA of *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 Section III, Subsection NCA of the *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).

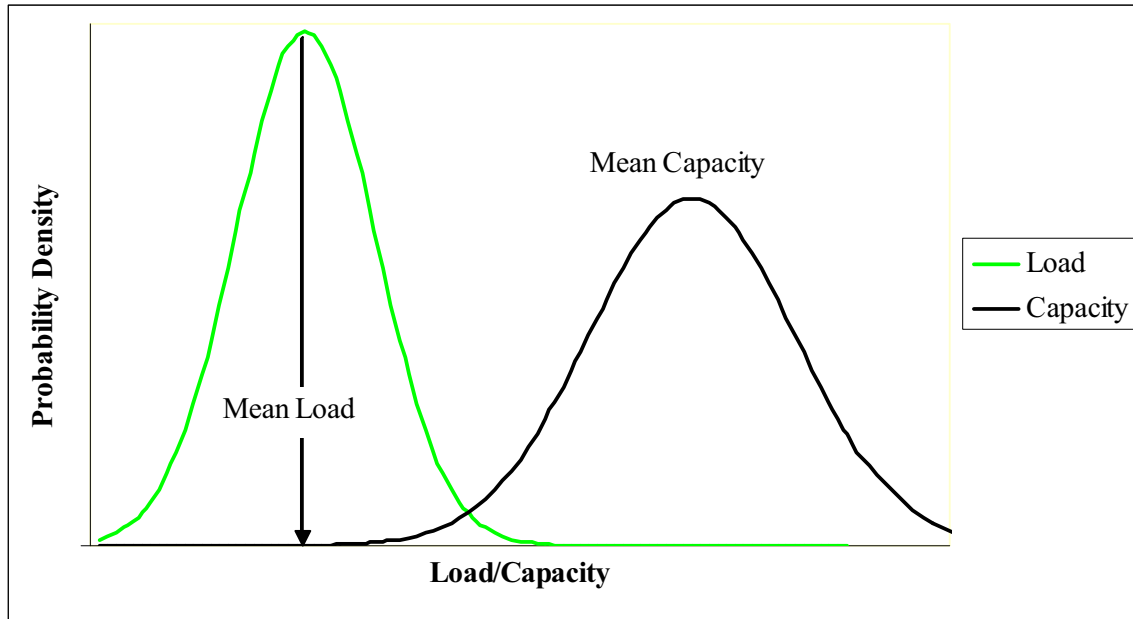
The development of code requirements for minimum design loads in buildings and other structures in the late 1970s considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures* (Ref. 2.2.40). 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:

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

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:

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

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. 2.2.5), 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.

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

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, \bar{L} and \bar{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 $V_L = \sigma_L/\bar{L}$ and $V_R = \sigma_R/\bar{R}$ 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. 2.2.33). 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.

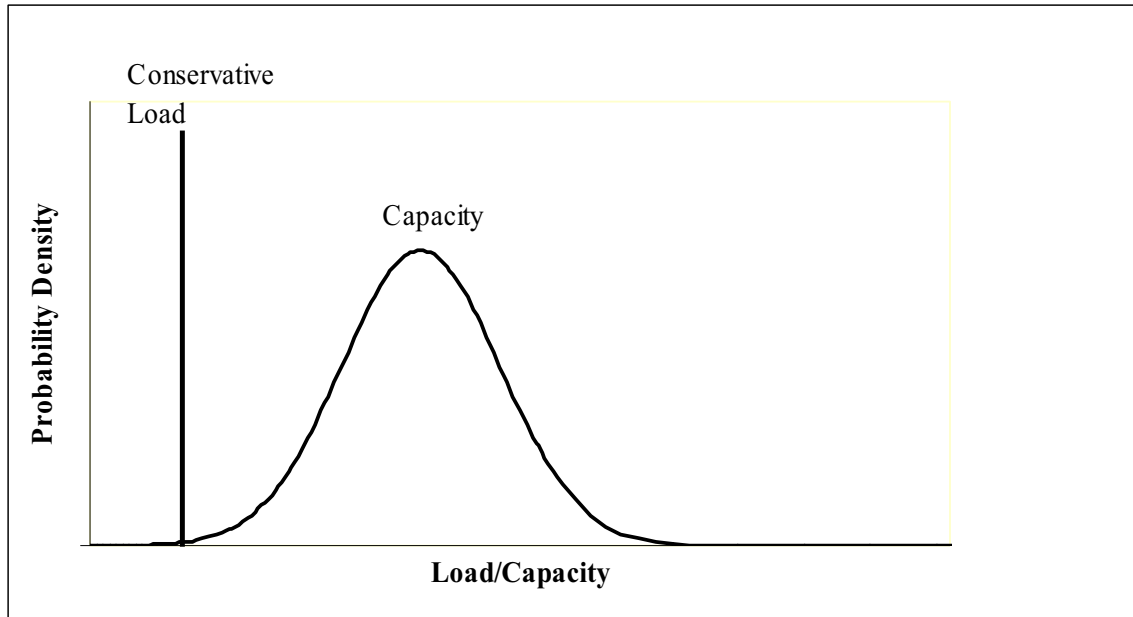
Impact Events Associated with Containment Breach

A simplification of Equation 3, consistent with *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.66), and shown in Equation 4 is used in the PCSA. It is illustrated in Figure 4.3-7.

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

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. 2.2.33). 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 PEFAs 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 trolley, 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 industry-wide transportation casks types for transportation accidents as reported in NUREG/CR-6672 (Ref. 2.2.76). 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 (SDU) 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 miles per hour (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.

NUREG/CR-6672 (Ref. 2.2.76) 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 IHF.

Principal insights reported in NUREG/CR-6672 (Ref. 2.2.76) 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. 2.2.43) 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. 2.2.76) 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 industry-wide 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. 2.2.78)
- *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report. NUREG/CR-4680* (Ref. 2.2.56)
- *Quantitative Data on the Fire Behavior of Combustible Material in Nuclear Power Plants: A Literature Review. NUREG/CR-4679* (Ref. 2.2.57).

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. 2.2.71, p. 2-56). Fires within a 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. 2.2.71, Section 2, Chapter 2) with information about liquid hydrocarbon pool fires. 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, Hypothetical Accident Conditions (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:

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

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 ($\text{W/m}^2 \text{K}^4$)
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 4.3.7) 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:

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

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. 2.2.76) 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. 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.

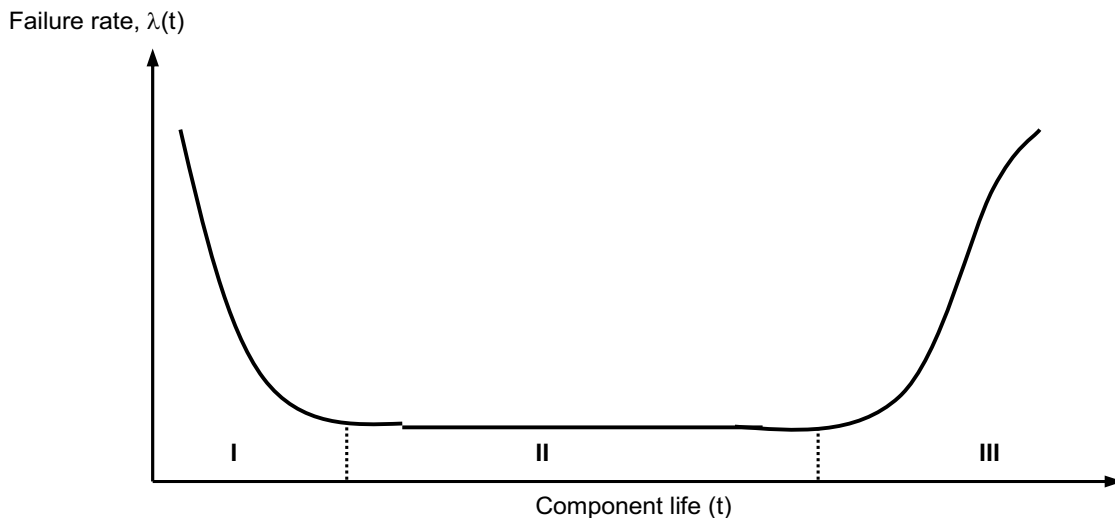
The analysis of loss of building cooling on containment integrity takes a similar, conservative, analytical approach. A bounding set of conditions and configurations are postulated, and then using the ANSYS code (Ref. 2.2.14), the maximum steady state temperature is compared to the temperature at which 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. 2.2.80, 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. 2.2.80, 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:

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

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. It is assumed that 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. 2.2.66) 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. 2.2.51, Ref. 2.2.10, and Ref. 2.2.59). Furthermore, *HLWRS-ISG-02* includes the use of engineering judgment, supported by sufficient technical basis, as a means of justifying reliability estimates for certain SSCs (Ref. 2.2.66).

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:

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

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. 2.2.72, 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 or 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. 2.2.72, 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. 2.2.72, Section 4.4) and (Ref. 2.2.49, 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. 2.2.49, 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. 2.2.72, p. 99). The validity of this can be 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 Appendix 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 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 in Equation 11:

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

where $\text{Binom}(x, r, n)$ 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. 2.2.72, 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. 2.2.72, 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. 2.2.49, 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 *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. 2.2.45, 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. 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 the NUREG/CR-6823 (Ref. 2.2.10, Section A.7.3), the median is calculated as $\exp(v)$, where v 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 NUREG/CR-6823 (Ref. 2.2.10, 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 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 Jeffreys' noninformative prior distribution as indicated in NUREG/CR-6823 (Ref. 2.2.10, Section 6.2.2.5.2). This noninformative 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. 2.2.27 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 which is described later in this section, in Section 6.4 and in Attachment E. The results of the human reliability analysis (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. 2.2.44,

Ref. 2.2.54, and Ref. 2.2.50). 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: the Beta Factor method (Ref. 2.2.44), the Multiple Greek Letter method (Ref. 2.2.53), which is an extension of the Beta Factor method, and the Alpha Factor method (Ref. 2.2.54). These methods do not require an explicit knowledge of the dependence failure mode.

The PCSA uses the Alpha Factor method (Ref. 2.2.54), 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. 2.2.52). 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:

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

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

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

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

Industry-wide alpha factors used in the PCSA are taken from NUREG/CR-5801 (Ref. 2.2.52). 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. 2.2.6) and incorporates the guidance in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. 2.2.65). 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 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.

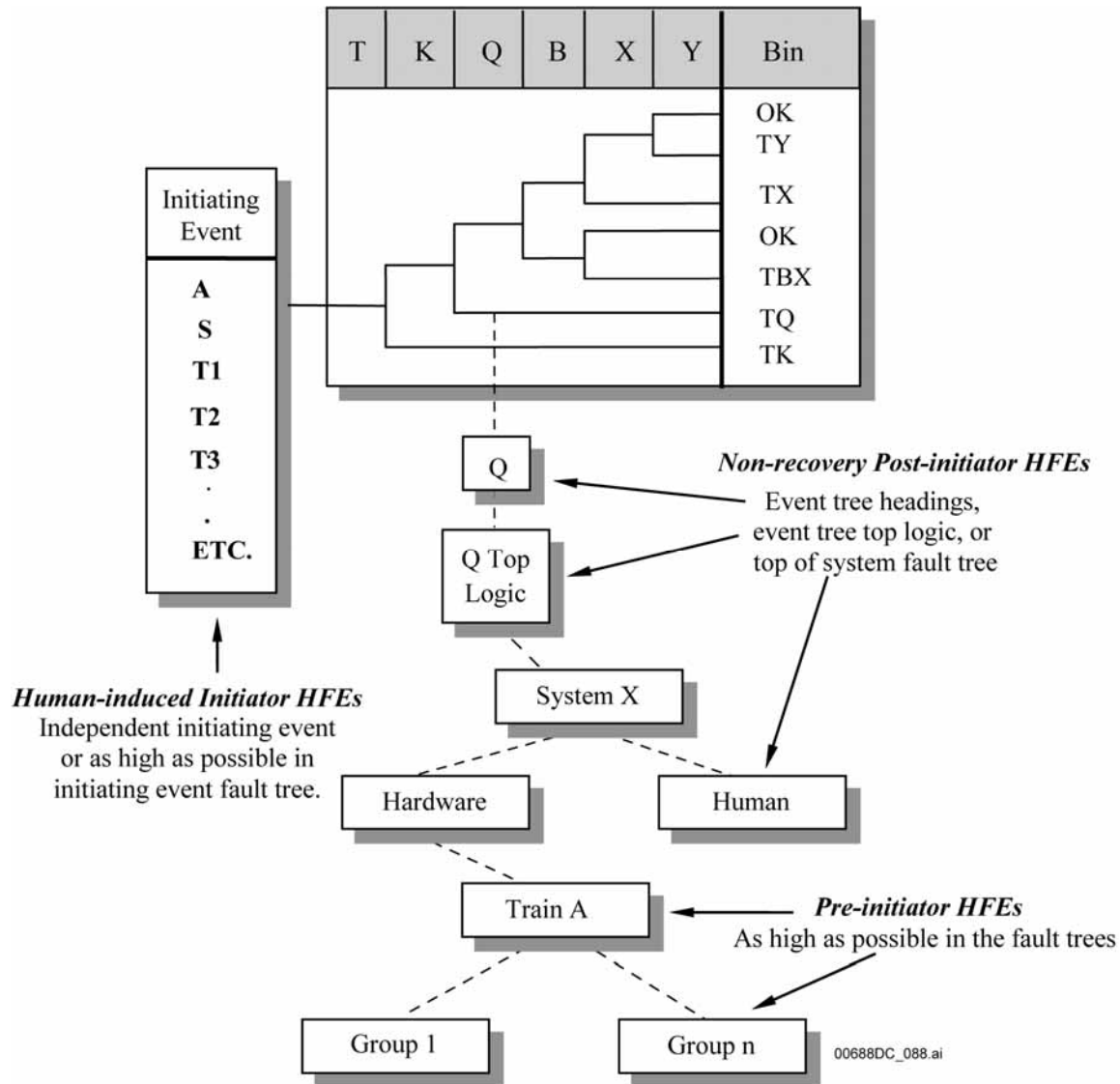
3. Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include SNF handling at reactor sites having independent spent fuel storages, 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 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. 2.2.6) and the process guidance provided in *Technical Basis and Implementation Guidelines for Technique for Human Event Analysis (ATHEANA)* NUREG-1624 (Ref. 2.2.62). 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. 2.2.62). Section 10.3 of *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)* NUREG-1624 (Ref. 2.2.62) 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 PSCA

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. 2.2.62), 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 industry-wide, 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 CFR 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. 2.2.47)
2. Human Error Assessment and Reduction Technique (HEART) (Ref. 2.2.81)—
Nuclear Action Reliability Assessment (NARA) (Ref. 2.2.35)

3. Technique for Human Error Rate Prediction (THERP) with some modifications (Ref. 2.2.77).

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. 2.2.62).

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. 2.2.62) 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 NUREG-1624 (Ref. 2.2.62) 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28). Quantification of fire event trees is conducted exactly like quantification of any other event tree and is described in Section 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. 2.2.42).
- 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 IHF 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. 2.2.69). 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, NUREG/CR-6850: Volumes 1 and 2 (Ref. 2.2.41 and Ref. 2.2.42) are also considered in the development of this analysis method. The method complies with the applicable requirements of *Fire PRA Methodology* (Ref. 2.2.3) 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 the 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. 2.2.28, Attachment D).
 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. 2.2.42 and Ref. 2.2.41, Section 11.5.4) 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. *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. 2.2.78)
 2. *Detailed Methodology. Volume 2 of EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI TR-1011989 and NUREG/CR-6850. (Ref. 2.2.42)
 3. *Summary & Overview. Volume 1 of EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.* EPRI-1011989 and NUREG/CR-6850. (Ref. 2.2.41)

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. 2.2.69).
- 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:

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

where

f_{ier-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) *Initial Handling Facility Electrical Room Equipment Layout* (Ref. 2.2.19)

- b) *Initial Handling Facility General Arrangement Ground Floor Plan*
(Ref. 2.2.20)
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:

$$f_{ief-jj-ri} = f_i \times P_{jc} \quad (\text{Eq. 16})$$

where

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

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

P_{jc} = 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:

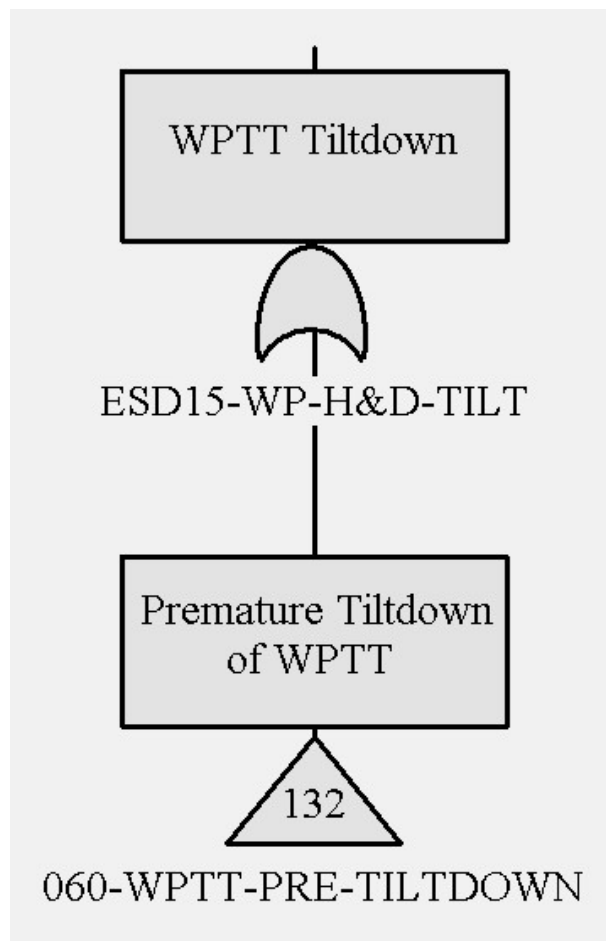
1. The number of demands (sometimes called trials) or the time exposure interval of the operation or activity that gives rise to the event sequence. For example, this could be the total number of transfers of a cask in a facility preparation area.
2. The frequency of occurrence per demand or per time 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 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 (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 number 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 has produced 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 not 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 because all potential criticality initiators are associated with a radiological release (i.e., end state RR-UNFILTERED-ITC) and will be shown to be beyond Category 2 for the IHF.

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. 2.2.31). 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). 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. 2.2.32) 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.

The NNPP performs a criticality evaluation of a series of IHF conditions that are capable of increasing the criticality potential of naval SNF. The evaluation is based on modeling rearrangement of naval SNF due to mechanical damage, neutron reflection from materials outside the naval SFC, and neutronic coupling with other fissile material in proximity to the naval SFC. Based on the event sequences in this document and established facility limits, NNPP

deterministically demonstrates that the end state configurations are subcritical. To determine the criticality potential for other waste forms 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. The 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. 2.2.32). 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

- NOTES: ^a The *Preclosure Criticality Safety Analysis* (Ref. 2.2.32) considers bounding waste form characteristics. Therefore, there is no potential for a waste form misload.
^b The *Preclosure Criticality Safety Analysis* (Ref. 2.2.32) 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 needs to be controlled.
^f Needs to be controlled only if moderator is present.
^g Needs to be controlled only if the soluble boron concentration in the pool and transportation cask/dual purpose canister 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 % ¹⁰B.

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. 2.2.32, 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 such as 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 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 Part 50 (Ref. 2.3.1) facilities (e.g., Regulatory Guide 1.174 (Ref. 2.2.68) and *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear*

Power Plants. NUREG-0800 (Ref. 2.2.63, 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. 2.2.51, Ref. 2.2.4, Ref. 2.2.10, and Ref. 2.2.59).

The NRC issued *HLWRS-ISG-02* (Ref. 2.2.66) 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, *HLWRS-ISG-02* (Ref. 2.2.66) 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. 2.2.66).

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 and pressures, 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 quality assurance 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 IHF 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 *HLWRS-ISG-02* (Ref. 2.2.66), 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. 2.2.67). 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	96
Attachment B System/Pivotal Event Analysis – Fault Trees	238
Attachment C Active Component Reliability Data Analysis	52
Attachment D Passive Equipment Failure Analysis	93
Attachment E Human Reliability Analysis	168
Attachment F Fire Analysis	115
Attachment G Event Sequence Quantification Summary Tables	2
Attachment H SAPHIRE Model and Supporting Files	2 + CD

6. BODY OF ANALYSIS

The *Initial Handling Facility Event Sequence Development Analysis*, which describes the IHF, its equipment, and its operations (Ref. 2.2.28, 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 interim staff guidance for its evaluation of the level of information and reliability estimation related to the Yucca Mountain repository, *Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.66, p. 3), states that there are multiple approaches that could be used 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 consideration. 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 (Ref. 2.3.2) (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 provide reasonable assurance that the health and safety of the public are 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 boundary condition is reasonable 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 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. 2.2.61) 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. 2.2.61, 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-1567 (Ref. 2.2.82, Section 9.5.4.1) and NUREG-1536 (Ref. 2.2.60, Chapter 8, Section V), refer to a vacuum drying procedure to ensure casks and canisters are free of water. The following statement is cited as providing adequate drying (Ref. 2.2.82, Section 9.5.4.1):

The vacuum drying procedure involves a vacuum test to demonstrate that there is no water in the cask or fuel. A cask that is evacuated to less than 3 torr and, after sealing, does not have a cask pressure which increases by 1 torr over 30 minutes is considered to be free of water.

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. 2.2.60). Indeed, there is no after-the-fact water or error detection method in NUREG-1536 or the regulation. Therefore, some unknown number of canisters may arrive in 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 the inside of 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. **Criticality.** GROA operating processes are similar to those of nuclear power plant sites with respect to the use of cranes, and there are no processes or conditions that would exacerbate adverse effects associated with abnormal amounts of water retention. Event sequences involving the drop and breach of a naval canister are Beyond Category 2 as shown in Section 6.8. To receive a license to transport SNF, 10 CFR 71.55 (Ref. 2.3.3) requires the licensee to demonstrate subcriticality given that “the fissile material is in the most reactive credible configuration consistent with the damaged condition of the package and the chemical and physical form of the contents” under the hypothetical accident conditions specified in 10 CFR 71.73 (Ref. 2.3.3). Drop events, which are unlikely to breach the canister, are also unlikely to impart sufficient energy to the fuel to reconfigure it so dramatically that criticality would be possible even if water is present. It is concluded that existing regulations that apply to the canister and transportation cask for transportation to the repository provide reasonable assurance that a criticality event sequence that depends on the presence of residual water inside the canister and reconfiguration of the fuel would not occur under conditions that could reasonably be achieved during handling at the repository.
2. **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 or explosion 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, an unlikely event during handling, 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 screened from further consideration on the judgment that they contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.

3. **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 in the GROA are similar to those that would be encountered by the canister while it is on the supplier's site and during transportation to the GROA. If there is not enough water to cause overpressurization before the canister reaches the GROA, then overpressurization would not occur in the GROA. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable for loaded canisters that are received from off-site.

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. 2.2.27) 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 $10^{-6}/\text{yr}$, 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 $10^{-6}/\text{yr}$, 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 $10^{-6}/\text{yr}$, 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 6.0.2.2.

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

External Event Category ^a	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 includes: 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. 2.2.27, Sections 6 and 7).

6.0.2.2 Screening of Loss of Electrical Power as an Initiating Event

The IHF does not rely on ITS AC power or ITS HVAC to prevent or mitigate event sequences, however, the loss of electrical power is considered as an initiating event with respect to mechanical handling equipment. Loss of electrical power, whether caused by onsite or offsite failures, is expected to occur during the preclosure period. Conveyances, cranes, and canister transfer machines (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 loss of offsite power in order to continue operation of the ITS HVAC confinement system.

The 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 loss of offsite power 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. 2.2.38, Table 3-8), with a failure to recover power within 24 hours of 1.8E-02 (Ref. 2.2.38, 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:

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

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

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

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 event sequences are 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. 2.2.38). 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. 2.2.7)).

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:

$$\begin{aligned} & \text{LOSP-IE} \times \text{Holding brake fails} \times \text{Emergency brake fails} = \\ & = 3.2\text{E-}02 \times (8.4\text{E-}06 \times 720) \times (4.4\text{E-}06 \times 720) \\ & = 6.1\text{E-}07 \end{aligned}$$

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, take 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28) 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. 2.2.28; 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 #)	Initiating Event Description	Screening Basis
IHF-ESD-01-HLW (#3) (Figure A5-2)	Rollover of a truck trailer carrying a transportation cask in the Cask Preparation Area	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. It is 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 Cask Preparation Area 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.
IHF-ESD-05-HLW (#2) (Figure A5-10) IHF-ESD-05-NVL (#2) (Figure A5-12)	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 platform, and therefore cannot be impacted. Therefore, event sequences associated with these initiating events are considered to be physically unrealizable.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
IHF-ESD-07-HLW(#2) (Figure A5-16)	Drop of a heavy object onto an HLW canister	The waste package inner lid and the transportation cask lid are the only pertinent heavy objects (except for another canister) whose drop onto an HLW canister could jeopardize the canister's structural integrity. (Drop of one HLW canister onto another is not screened out.) Divider plates in the codisposal waste package extend higher than the canisters inside. Therefore, a dropped waste package lid would not impact the canisters. Transportation casks containing HLW canisters are designed such that a lid drop would not impact the canisters inside. Thus, a drop of a heavy load does not have an adverse effect on the integrity of HLW canisters and can be screened from further consideration.
IHF-ESD-07-HLW(#6) (Figure A5-16) IHF-ESD-07-NVL(#6) (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. In addition, the motors on the slide gates have insufficient power to significantly damage a canister.
IHF-ESD-09-HLW(#2) (Figure A5-21) IHF-ESD-09-NVL(#2) (Figure A5-23)	Welding of the waste package lid causes canister breach	No plausible scenarios have been identified whereby the gas tungsten arc welding process could cause burn through of the waste package and canister (Ref. 2.2.13). Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.
IHF-ESD-11-HLW(#2) (Figure A5-27) IHF-ESD-11-NVL(#2) (Figure A5-28)	TEV collision with stationary waste package	The TEV is parked in the Waste Package Loadout Room when the waste package enters via the WPTT, and cannot collide with the waste package. The WPTT is on rails so its path is well defined. The TEV is separated from the WPTT by the docking station. Even a TEV and/or WPTT derailment cannot cause a collision between the two vehicles because of the extremely low speed of these vehicles. Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened from further analysis in Section 6.0.4.
No applicable event trees	Canister dropped into the Cask Unloading Room or Waste Package Positioning Room with no waste package present	Dropping a canister through a port without a staged waste package below would require a series of human failures and mechanical failures that makes the initiating event unlikely. The design incorporates an interlock to prevent the opening of the waste package port slide gate when the WPTT and waste package shield ring are not present (Ref. 2.2.30). The combination of (a) failure to stage the waste package, (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.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
No applicable event trees	Tipover of CTT	The CTT is designed to prevent tipover (Ref. 2.2.22, Section 3.2). The size, weight, low center of gravity, and low speed of the CTT ensure that no tipover can occur. During cask preparation activities, the CTT is set on the floor inside the cask preparation platform. 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, 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 is 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 (Ref. 2.4.4).
No applicable event trees	Conveyance carrying a waste form 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.
IHF-ESD-08-HLW(#3) (Figure A5-18) IHF-ESD-08-NVL(#3) (Figure A5-20) IHF-ESD-10-HLW(#3) (Figure A5-24) IHF-ESD-10-NVL(#3) (Figure A5-26)	Tilt-down of WPTT at uncontrolled speed	The main feature of the WPTT is the shielded enclosure, which holds the waste package, the waste package pallet, the waste package transfer carriage, and the waste package pedestal (Ref. 2.2.23, Section 2.1.1). The enclosure pivots between vertical and horizontal orientations to position the waste package for loading and unloading. There are two sets of redundant tipping motor-and-gear systems, each of which is designed to withstand the maximum possible torque without failure. If one motor-and-gear system were to fail, the shielded enclosure would still be supported. The center of gravity of the shielded enclosure is positioned such that the vertical position is the most stable position (Ref. 2.2.23, Section 3.3.2). Therefore, even in the unlikely event that both motor-and-gear systems fail catastrophically, the shielded enclosure would not undergo tilt-down at uncontrolled speed.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
No applicable event trees	Operator drops cask during cask preparation activities	<p>The cask preparation crane, rather than the cask handling crane, is used in the lid-removal operation for the naval cask. Because the cask is not intentionally lifted in this step, dropping the cask would require a series of extraordinary human failures. The HLW-cask lid is not removed during preparation activities.</p> <p>For naval casks, 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 cask preparation 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.</p> <p>For HLW 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 HLW casks, is considered to be unrealizable.</p>
IHF-ESD-07-HLW(#8) (Figure A5-16) IHF-ESD-07-NVL(#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.
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.
No applicable event trees	Neutronic interaction involving more than two naval canisters.	<p>The <i>Preclosure Criticality Safety Analysis</i>, (Ref. 2.2.32, Section 2.3.2.5) indicates that interaction must be controlled for highly enriched DOE SNF. Similarly, because NNPP SNF is highly enriched and is expected to have similar neutronic characteristics, interaction between naval canisters also needs to be controlled. Interactions involving two naval canisters in close proximity are analyzed in the classified NNPP documents that contain a bounding criticality calculation for interaction involving naval canisters. However, interactions involving more than two canisters have not been evaluated for criticality. The following screening argument demonstrates that placing more than two naval canisters in close proximity in the IHF is not reasonably achievable.</p> <p>Given the mechanical handling-capabilities of the IHF as described in <i>Initial Handling Facility Event Sequence Development Analysis</i> (Ref. 2.2.28, Section 6.1, Attachment A, and Attachment B), reasonably achievable configurations involving two naval casks or canisters can be imagined. However, in each case, as demonstrated below, adding a third cask or canister is not achievable.</p>

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
		<p>(1) Normal handling operations for naval casks allow a single cask to be present in the Cask Preparation Area. A conceivable human error could result in receipt of a second naval cask on a railcar while the first cask is still in the CTT in the Cask Preparation Area. Once this has been done, operators could conceivably be unaware that a cask is already present in the CTT and attempt to use the cask handling crane to load the second cask into the CTT. The error would become inescapably obvious when operators attempt to load the second cask into the CTT, which is already occupied by the first cask. At this point, two casks may be side by side in close proximity. The design of the facility does not admit the possibility of bringing in a third cask because the crane is already occupied with the second cask.</p> <p>(2) Two naval canisters may conceivably be brought end to end as follows. Suppose that a canister has been loaded into the CTM. Given a series of human errors, it is conceivable that the presence of the canister in the CTM could be forgotten. Then, another naval cask could be brought in, loaded into the CTT, and then transferred into the Cask Unloading Room underneath the first canister in the CTM. At this point, the slide gates could be opened and the canister in the CTM could be brought into end-to-end contact with the canister in the cask. The facility is not capable of bringing a third canister into close proximity because the CTT is already occupied.</p> <p>(3) A similar end-to-end configuration could conceivably be achieved after a canister has been loaded into the waste package in the Waste Package Loading Room. In this case, the presence of the canister in the waste package has been forgotten and a second canister is erroneously loaded into the CTM. Operators attempt to load the second canister into the waste package, which already contains a canister. The facility is not capable of bringing a third canister into close proximity because the CTM and WPTT are already occupied with canisters.</p>

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
		(4) An end-to-end configuration involving loaded, sealed waste packages is also conceivable. In this case, the operators have placed a waste package into the TEV and forgotten that it is there. Another waste package is brought into the Waste Package Loadout Room on the WPTT. The TEV doors are opened and the WPTT transfer carriage carries the second waste package end to end with the first. The facility is not capable of bringing a third waste package into close proximity because the WPTT and TEV are already occupied with waste packages.

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 "#". CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HLW = high-level radioactive waste; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

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. Transportation casks are elevated as all times at least five feet above the floor by railcar, truck, or canister transfer trolley. Waste packages are similarly elevated on the waste package transfer trolley. Inside the TEV, the waste package is elevated approximately 1 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 in which 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.

Now consider the possibility of inadvertent direct exposure of workers due to internal flooding. 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, cask preparation platforms, concrete floors and walls, the CTM shield bell or shield skirt, the WPTT, canister transfer trolley, shield doors, or the shield compartment of the TEV. Loss of electrical power to any of these simply stops operation, if any, 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 prevents such inadvertent motion. Therefore, internal flooding cannot initiate an event sequence that causes increased levels of radiological exposure to workers.

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

6.1 EVENT TREES

The event trees that are quantified in this analysis were developed from ESDs in the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28, 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), HRA (Section 6.4 and Attachment E), and PEFA (Section 6.3 and Attachment D). 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 NNPP for placement in waste packages destined for emplacement in the repository emplacement drifts.

3. The Wet Handling Facility (WHF) accepts DPCs and transportation casks containing uncanistered commercial SNF, 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 Naval Nuclear Propulsion Program (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 IHF and CRCF and, by means of rail, transports them and deposits them into designated locations 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 IHF has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container. As described in the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28), 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 mutually exclusive end states:

1. OK
2. Direct Exposure, Degraded Shielding
3. Direct Exposure, Loss of Shielding
4. Radionuclide Release, Filtered (HVAC is represented in the event sequences despite the fact that it is not relied upon for the IHF for prevention or mitigation of event sequences.)
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 (not applicable to the IHF)

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. The SAPHIRE 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. 2.2.28, Attachment F). An example is IHF-ESD-06-NVL, which is shown in Figure A5-17 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 the challenge is equal to the number of transportation casks containing naval canisters that are handled over the preclosure period. 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. 2.2.28, 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, IHF-ESD-01-HLW, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, IHF-RESP-TC1, 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 HLW canisters 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 waste packages) to be handled over the life of the IHF. 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 IHF Over the Preclosure Period

Waste Form Unit	IHF Throughput	Comment
Transportation casks containing a naval canister	400	
Transportation casks containing HLW canisters	600	100 rail-based transportation casks containing 5 HLW canisters and 500 truck-based transportation casks contain 1 HLW canister
Naval canisters	400	
HLW canisters	1000	
Waste packages containing a naval canister	400	
Waste packages containing HLW canisters	200	5 canisters per waste package

NOTE: IHF = Initial Handling Facility; HLW = high-level radioactive waste;

Source: 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. 2.2.28, 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
IHF-ESD-01	Event Sequences for Activities Associated with Receipt of Naval or HLW TC on RC or TT in Cask Preparation Area and Upending and Transfer of Naval TC to CTT	ESD-01-HLW ESD-01-NVL	Figure A5-2 Figure A5-4	IHF-RESP-TC1 IHF-RESP-TC1	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
IHF-ESD-02	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending and Transfer of HLW Cask to CTT and Removal of Impact Limiters from Naval TC	ESD-02-HLW ESD-02-NVL	Figure A5-5 Figure A5-6	IHF-RESP-TC1 IHF-RESP-TC1	Figure A5-3 Figure A5-3
IHF-ESD-03	Event Sequences for Activities Associated with Cask Preparation Activities Associated with Unbolting and Lid Adapter Installation for the HLW Cask	ESD-03-HLW	Figure A5-7	IHF-RESP-TC1	Figure A5-3
IHF-ESD-04	Event Sequences for Activities Associated with Removal of the Naval Cask Lid and Installing the Naval Canister Lifting Adapter	ESD-04-NVL	Figure A5-8	IHF-RESP-CAN1	Figure A5-9
IHF-ESD-05	Event Sequences for Activities Associated with Transfer of a Cask on CTT from Cask Preparation Area to Cask Unloading Room	ESD-05-HLW ESD-05-NVL	Figure A5-10 Figure A5-12	IHF-RESP-CAN2-HLW IHF-RESP-CAN2-NVL	Figure A5-11, Figure A5-13
IHF-ESD-06	Event Sequences for Activities Associated with Collision of CTT with Cask Unloading Room Shield Door	ESD-06-HLW ESD-06-NVL	Figure A5-14 Figure A5-15	N/A N/A	N/A N/A
IHF-ESD-07	Event Sequences for Activities Associated with the Transfer of a Canister from a TC to a WP with CTM	ESD-07-HLW ESD-07-NVL	Figure A5-16 Figure A5-17	IHF-RESP-CAN1 IHF-RESP-CAN1	Figure A5-9 Figure A5-9

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
IHF-ESD-08	Event Sequences for Activities Associated with WP Transfer from WP Loading Room to Closing Position in WP Positioning Room below WP Closure Room	ESD-08-HLW ESD-08-NVL	Figure A5-18 Figure A5-20	IHF-RESP-WP1 IHF-RESP-WP1	Figure A5-19 Figure A5-19
IHF-ESD-09	Event Sequences for Activities Associated with Assembly and Closure of the WP	ESD-09-HLW ESD-09-NVL	Figure A5-21 Figure A5-23	IHF-RESP-WP2 IHF-RESP-WP2	Figure A5-22 Figure A5-22
IHF-ESD-10	Event Sequences for Activities Associated with the Transfer of the WP from the WP Positioning Room to the WPTT Docking Station	ESD-10-HLW ESD-10-NVL	Figure A5-24 Figure A5-26	IHF-RESP-WP3 IHF-RESP-WP3	Figure A5-25 Figure A5-25
IHF-ESD-11	Event Sequences for Activities Associated with Exporting a WP	ESD-11-HLW ESD-11-NVL	Figure A5-27 Figure A5-28	IHF-RESP-WP3 IHF-RESP-WP3	Figure A5-25 Figure A5-25
IHF-ESD-12	Event Sequences for Activities Associated with Direct Exposure During Various Activities	ESD-12A-HLW ESD-12A-NVL ESD-12B-HLW ESD-12B-NVL ESD-12C-HLW ESD-12C-NVL	Figure A5-29 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34	N/A N/A N/A N/A N/A N/A	
IHF-ESD-13	Event Sequences Associated with Fires Occurring in the IHF	ESD-13-HLW-CAN ESD-13-HLW-CSK ESD-13-HLW-WP ESD-13-NVL	Figure A5-35 Figure A5-37 Figure A5-38 Figure A5-39	IHF-RESP-FIRE IHF-RESP-FIRE IHF-RESP-FIRE IHF-RESP-FIRE	Figure A5-36 Figure A5-36 Figure A5-36 Figure A5-36

NOTE: CAN = canister; CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HLW = high-level radioactive waste; IHF = Initial Handling Facility; NVL = naval; RC = railcar; RESP = response; TC = transportation cask; TT = transfer trolley; WP = waste package; WPTT = waste package transfer trolley.

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 fault tree analysis (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 IHF is also used in other surface facilities and Intra-Site Operations. Furthermore, a given system, such as the waste package transfer trolley, may affect the event sequences for several operational nodes of the same facility or several kinds of waste forms, as it does for the IHF. 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 to B5, presents the system fault trees. The present section describes the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B6, presents the linking fault trees used in the IHF 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 ITS success criteria for a given SSC fails to be achieved. At least one success criterion is defined for each system. Multiple success criteria are defined for systems that perform multiple safety functions in the IHF.

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 for 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, however, developed directly. 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.

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 is to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (e.g., electrical, mechanical) 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
- Support systems and subsystems such as transporters (site prime mover, cask transfer trolley), 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 site prime mover (SPM).

6.2.2.1.1 Physical Description

The 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 and within the IHF. A speed limiter is used on the SPM to ensure the maximum speed does not exceed 9 miles per hour. Movement of the SPM with railcars (termed site prime mover railcar (SPMRC)) or SPM with truck trailers (termed site prime mover truck trailer (SPMTT)) within the IHF is limited to the Cask Preparation Area. 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 SPM is electrically driven via an umbilical cord (or remote control) from the facility 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 IHF. The site prime mover diesel engine is shut down and the outer door 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 Cask Preparation Area.

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 block diagram of the functional components on the SPMRC/truck trailer is shown in Attachment B, Section 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 derailments
- Prevent SPMTT rollovers.

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 IHF, 0.04 miles, and industry data derailment rate of 1.18E-05 per mile 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. SPM collides with IHF structures for naval and HLW transportation casks.
2. SPMRC derails for both naval and HLW rail transportation casks.
3. SPMTT rollover for only HLW truck 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 on a per Cask Basis

Top Event	Mean Probability	Standard Deviation
SPM collides with IHF structures (NVL or HLW on RC or TT)	4.6E-03	1.4E-02
SPMRC derailment (NVL or HLW on RC)	4.7E-07	7.4E-9
SPMTT rollover (HLW on TT)	0.0E+00	0.0E+00

NOTE: IHF = Initial Handling Facility; NVL = naval; HLW = high-level radioactive waste; RC = railcar; SPM = site prime mover; TT = truck trailer.

Source: Attachment B, Figures B1.4-1, B1.4-6, B1.4-12 and B1.4-15

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 will be used to transport various vertically oriented transportation casks from the Cask Preparation Area to the Canister Transfer Area. 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 subcomponent 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 Area 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 maximum speed of the drives, 10 feet per minute (ft/min), 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 provide a proportional control signal to the air valve that produces a speed range of 0 to 10 ft/min. 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.

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 Cask Unloading Room. Guides bolted to the floor ensure 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 Cask Unloading 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 – The operator presses both handles simultaneously to allow air to flow to the CTT system to allow the CTT to levitate or move horizontally.
- Emergency stop button – The operator presses the emergency stop button on the pendant control to stop the CTT (Section B2.2.2).

- 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 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 use 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 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 Area while loading a cask onto the CTT

2. Spurious movement in the Cask Preparation Area during unbolting and lid adapter installation
3. Spurious movement in 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 Cask Unloading 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	9.9E-4	1.3E-3
Spurious movement during canister transfer	2.8E-14	1.3E-13

NOTE: CTT = cask transfer trolley.

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

6.2.2.3 Slide Gate and Shield Door Fault Tree Analysis

The IHF Cask Unloading Room and Waste Package Loading Room have a port slide gate providing access to the Canister Transfer Area. There is a shield door between the Cask Preparation Area and the Cask Unloading Room, between the Waste Package Loading Room and the Waste Package Positioning Room, and between the Waste Package Positioning Room and the Waste Package Loadout Room. The shield doors and port slide gates provide shielding during canister 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 equipment shield doors and slide gates.

6.2.2.3.1 Physical Description

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 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 port 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 port slide gate consists of two gates that close together between the loading/unloading rooms and the Canister Transfer Area. 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 port 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 the CTT to enter the room. Once the CTT 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 cask port slide gate may be opened to allow the canister transfer machine (CTM) to perform cask unloading operations. Waste package loading operations in the Waste Package Loading Room are analogous to cask unloading operations. The waste package port slide gate may be opened to allow waste package loading access if the shield doors are closed. Once loading is complete and the slide gate is closed, the shield doors may be opened to allow the WPTT to carry the waste package into the Waste Package Positioning Room.

6.2.2.3.3 Control System

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

- 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 port 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 hardwired interlocks to prevent one 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 shield door closing on conveyance.

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 was 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 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-6	2.0E-8
Inadvertent Opening of the Slide Gate	3.5E-9	1.2E-8
Shield Door Closes on Conveyance	1.8E-5	2.5E-5

Source: Attachment B, 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 CTM is located and operated in the Canister Transfer Area of the IHF. The CTM is used to transfer waste canisters from a cask on the CTT to a waste package supported by the WPTT. The ports in the floor of the Canister Transfer Area provide access to the Cask Unloading Room and Waste Package Loading Room.

The CTM is an overhead 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 CTM slide gate, when closed, provides bottom shielding for 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

The CTM transfers waste canisters from the transportation cask to the waste package. For this operation, a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. In the case of the naval SNF canister, the lifting fixture has been affixed to the canister and it is ready to be grappled to the CTM. In the case of the HLW cask, the cask lid is in place but unbolted. Similarly, an empty waste package secured by the WPTT is positioned under the adjacent transfer port in the Waste Package Loading Room.

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 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 canister lifting feature. The 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 waste package. The waste package loading operations are essentially the reverse of the cask unloading.

The CTM canister grapple is used for handling naval canisters. Other grapples are used to access the smaller diameter HLW canisters. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Area 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 (also referred to in this document as the control 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 stop and the hoist holding brake engages. Operations are 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 CTM shield skirt is lowered
- Prevent raising the shield bell skirt when the port slide gate is open
- Prevent hoist movement unless the grapple is fully engaged or disengaged
- Stop the hoist and erase the lift command when a canister clears the CTM slide gate
- Stop a lift before upper lift height limits are reached (two interlocks are provided for this function)
- Prevent opening of the port slide gate unless the CTM shield skirt is lowered and in position
- Prevent hoist movement unless the CTM shield skirt is lowered
- Prevent lifting of a load that exceeds the operational weight 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 CTM shield skirt position and the position of the port 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.

Many 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 lifting, lateral movement, and lowering portions of the canister transfer

- Prevent a collision between the canister and the shield bell or Canister Transfer Area floor from any cause during the lifting, 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 IHF.

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 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 CTM slide gate has been closed and drops through a Canister Transfer Area port to the loading or unloading room that can occur before the CMT 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 IHF 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 five 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 below the design basis height	2.1E-4	2.6E-4
CTM high drops from two blocking events	2.8E-8	1.4E-7
Drop of object onto cask	1.0E-3	1.2E-3
CTM collision results in an impact to canister	7.9E-6	9.7E-6
CTM Shear	2.8E-5	3.5E-5

NOTE: CTM = canister transfer machine.

Source: Attachment B, Figures B4.4-1, B4.4-15, B4.4-20, B4.4-34, and B4.4-41

6.2.2.5 Waste Package Transfer Trolley Fault Tree Analysis

The FTA for the WPTT is detailed in Attachment B, Section B5. 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 WPTT.

6.2.2.5.1 Physical Description and Functions

The waste package transfer trolley (WPTT) is an electrically powered machine used to transport the waste package containing various waste canisters from the Waste Package Loading Room to the Waste Package Positioning Room and then to the waste package transfer carriage docking station in the Waste Package Loadout Room. The WPTT consists of a shielded enclosure that holds the waste package, waste package pallet, waste package transfer carriage, and pedestal. The shielded enclosure acts as a radiation shield to minimize radiation to the surroundings. The enclosure pivots between a vertical and horizontal position for waste package loading and unloading.

The WPTT travels on rails between the Waste Package Loading Room and the docking station. The crane rails supporting the WPTT are gapped in multiple locations. Power is supplied to the motor by a third rail system and the maximum speed is less than 20 ft/min, as required by ASME NOG-1-2004 (Ref. 2.2.7) and established by the size of the drive motor and the gear drive system. The WPTT includes seismic rail clamps and rails anchored to the floor to ensure the stability of the WPTT during a seismic event.

The rotation of the shielded enclosure from vertical to horizontal is driven by worm gear mechanisms and is also powered by the third rail system. Each of the rotation mechanisms is sized to rotate the full design load (no greater than 178,200 lbs) on its own and at a speed no faster than 18-degrees per minute. The worm gear mechanism has the inherent property to self lock to prevent uncontrolled tilt down.

The waste package transfer carriage is a wheeled platform which carries the waste package pallet and waste package. The transfer carriage is moved by a mechanical screw-driven carriage retrieval assembly that places an empty waste package in the shielded enclosure and retrieves the loaded and sealed waste package from the shielded enclosure for interfacing with the TEV.

6.2.2.5.2 Operation

The waste package loadout operation begins with an empty waste package being loaded into the WPTT. The WPTT is locked into the waste package transfer carriage docking station and rotated to the horizontal position. The transfer carriage with an empty waste package and pallet is moved into the shielded enclosure of the WPTT via the waste package transfer carriage docking station's waste package retrieval assembly. The shielded enclosure is rotated into the vertical position and the shield ring is lowered and locked into position on top of the shielded enclosure by the waste package handling crane.

The WPTT is unlocked from the waste package transfer carriage docking station and is remotely driven into the Waste Package Loading Room. The WPTT is situated so that the empty waste package is directly beneath the center of the port slide gate that separates the Waste Package Loading Room from the Canister Transfer Area.

The WPTT is positioned in the Waste Package Loading Room and the port slide gate is opened to allow the waste canister(s) to be lowered into the empty waste package using the CTM.

After the waste package is loaded, the inner lid is placed onto the waste package, and the port slide gate closed, the WPTT moves to the Waste Package Positioning Room. At this station, the inner lid is welded in place, and the weld is inspected. The air within the waste package is replaced by helium with a helium purging operation. After the inner lid is inspected for leakage, the outer lid is positioned and welded in place. The welds of the outer lid are inspected to ensure the waste package is properly sealed.

After the waste package is sealed, the WPTT is moved into the Waste Package Loadout Room where it is locked into the waste package transfer carriage docking station. The shield ring is remotely removed with the waste package handling crane and the shielded enclosure is rotated into the horizontal position. The waste package carriage retrieval assembly is then retracted to pull the carriage and waste package out of the shielded enclosure to a position where the TEV is able to lift the waste package and pallet off the carriage.

6.2.2.5.3 Control System

Interlocks prevent translational or rotational motion of the WPTT while a canister is being loaded into the waste package (i.e., when the waste package slide gate is open) or while the waste package is being withdrawn from the shielded enclosure on the transfer carriage. The shielded enclosure is not able to rotate in either direction unless the WPTT is locked into the waste package transfer carriage docking station and the waste package carriage retrieval assembly is completely extended or retracted. Interlocks also prevent over-travel of the trolley and travel through portals when the shield doors are closed. Manually actuated, hardwired emergency stop buttons are available at all control locations to allow power to be removed from the drive motors.

6.2.2.5.4 System/Pivotal Event Success Criteria

Success criteria for the WPTT are the following:

- Ensure the WPTT in the Waste Package Loading Room remains stationary with no movement while loading a canister onto the shielded enclosure.
- Ensure the WPTT travels at a speed no greater than 40 ft/min and that the operator is in control and able to stop the WPTT as required.
- Ensure the WPTT does not derail during the transport process.
- Prevent premature tilt-down of the shielded enclosure during transfer.
- Prevent premature tilt-up or WPTT departure during loadout 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 WPTT.

6.2.2.5.5 Mission Times

A conservative mission time of one hour per canister was used for canister and waste package transfers through the process for each fault tree.

6.2.2.5.6 Fault Tree Results

The WPTT fault tree analysis is detailed in Attachment B, Section B5.

There are five fault trees associated with the WPTT that represent potential initiating events:

1. Spurious movement in the Waste Package Loading Room while loading a canister into the waste package.
2. Impact of the WPTT with a structure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
3. Derailment of the WPTT while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
4. Premature tilt-down of the shielded enclosure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
5. WPTT or carriage malfunctions while extracting the carriage and waste package from the shielded enclosure at the Waste Package Loadout Room.

The results of the analysis are summarized in Table 6.2-5.

Table 6.2-5. Summary of Top Event Quantification for the WPTT

Top Event	Mean Probability	Standard Deviation
Spurious movement of the WPTT in the loading area while loading the WP with canisters	2.8E-12	3.7E-11
Impact of the WPTT with a structure	3.0E-3	3.5E-3
Derailment of the WPTT	4.7E-7	7.4E-9
Premature tilt-down of the shielded enclosure	2.7E-5	3.3E-5
Malfunction of WPTT or WP transfer carriage	1.0E-3	1.3E-3

NOTE: WP = waste package; WPTT = waste package transfer trolley.

Source: Attachment B, Figures B5.4-1, B5.4-7, B5.4-11, B5.4-14 and B5.4-17

6.2.2.6 Site Transporter Fault Tree Analysis

The site transporter is not used in the IHF.

6.2.2.7 HVAC Fault Tree Analysis

The HVAC in the IHF is not designated as ITS equipment and therefore does not provide confinement capability in the event of a release.

6.2.2.8 AC Power Fault Tree Analysis

There are no ITS AC power requirements for the IHF.

6.2.2.9 Potential Moderator Sources

6.2.2.9.1 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. 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, 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. 2.2.16, Ref. 2.2.29, Ref. 2.2.25, and Ref. 2.2.34). 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 (1st quarter following annual test).

The probability 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 ft² based on NFPA 13 (Ref. 2.2.55, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2.21). For example, the area of CRCF Waste Package Loadout Room 1015 is listed as 7,470 ft² in *Liquid Low-Level Waste Collection Calculation (C2 and C3 Contamination Zone)* (Ref. 2.2.21). At 130 ft²/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 hr/yr × 720 h) × (8.1E-7/hr × 720 h) = 8E-11/sprinkler head. The second cut set is more significant: 0.025 (human error screening value) × (1.6E-6/yr × 1/8760 hr/yr × 720 h) = 3E-9/sprinkler head.

Applying the sum of these values, 3E-9/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 6.2-6.

Table 6.2-6. 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: Ref. 2.2.21 for area.

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. For the IHF, approximately 6,800 feet of piping runs no closer than 60 feet of the cask unbolting area

(Ref. 2.2.79). Even the length of piping in the IHF has little impact post-breach, as the probability of a pipe crack or rupture in a 30 day period following a potential breach is $1.4E-03$. (Due to the early nature of the design, the only available reference for the length of pipe is this interoffice memorandum. Due to the conservatism used to determine the length of pipe, this information does not require verification.)

The probability of a pipe crack in a 30 day period was 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. 2.2.39, 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 of the conditioning applied to the fluids in the systems will be that typical of the commercial nuclear power plant:

External leak small (1 to 50 gallon/min): Leak rate = $2.5E-10 \text{ hr}^{-1}\text{ft}^{-1}$

External leak large (> 50 gallon/min): Leak rate = $2.5E-11 \text{ hr}^{-1}\text{ft}^{-1}$

Multiplying the sum of the small and large crack frequencies ($2.8E-10 \text{ hr}^{-1}\text{ft}^{-1}$) 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:

$$\text{CRCF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 100 \text{ ft} \times 720 \text{ h} = 2.0E-05$$

$$\text{IHF} < 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 6800 \text{ ft} \times 720 \text{ h} = 1.4E-03$$

$$\text{WHF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 75 \text{ ft} \times 720 \text{ h} = 1.5E-05$$

$$\text{RF} = 2.8E-10 \text{ hr}^{-1}\text{ft}^{-1} \times 0 \text{ ft} \times 720 \text{ h} = 0.$$

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 which neither accounts for the CTT or WPTT enclosures that surround the overpack nor the elevated position of the canisters with respect to a fire on the floor. The frequency of containment breach due to fire is significantly overestimated because of this conservative approach.

6.2.2.9.2 Lubricating Fluid

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a gearbox with a leak pan below it capable of capturing the entire gearbox fluid inventory. An estimate of the leakage rate through the gearbox and drip pan is found by multiplying the all-modes gearbox, motor failure frequency of $0.88E-06$ per hour

(Ref. 2.2.36, p. 2-104 and Section 6.3) over 50 years by 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 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. 2.2.36, p. 2-213). Using an exposure interval of 50 years (which represents the operating life of the surface facilities), the conditional probability of lubricating fluid entering a breached canister would be less than:

$$0.88\text{E-}06/\text{hr} \times 50 \text{ yrs} \times 8760 \text{ hr/yr} \times 0.34\text{E-}06/\text{hr} \times 720 \text{ hr} = 9.4\text{E-}05 \text{ over the preclosure period.}$$

This probability is conservatively 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.

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-kind facility and has no operating history, it was necessary to develop the required data from the experience of other nuclear and nonnuclear 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 can be 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 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, waste package maneuvering cranes and the spent fuel transfer machine (SFTM). The SFTM is not used in the IHF; however it is being discussed in this section for completeness. 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 component type and failure mode combination (TYP-FM), although 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 TYP-FM. Ultimately, 53 percent of the TYP-FMs are quantified with one data source, 8 percent with two data sources, 8 percent with three data sources, and 31 percent 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:

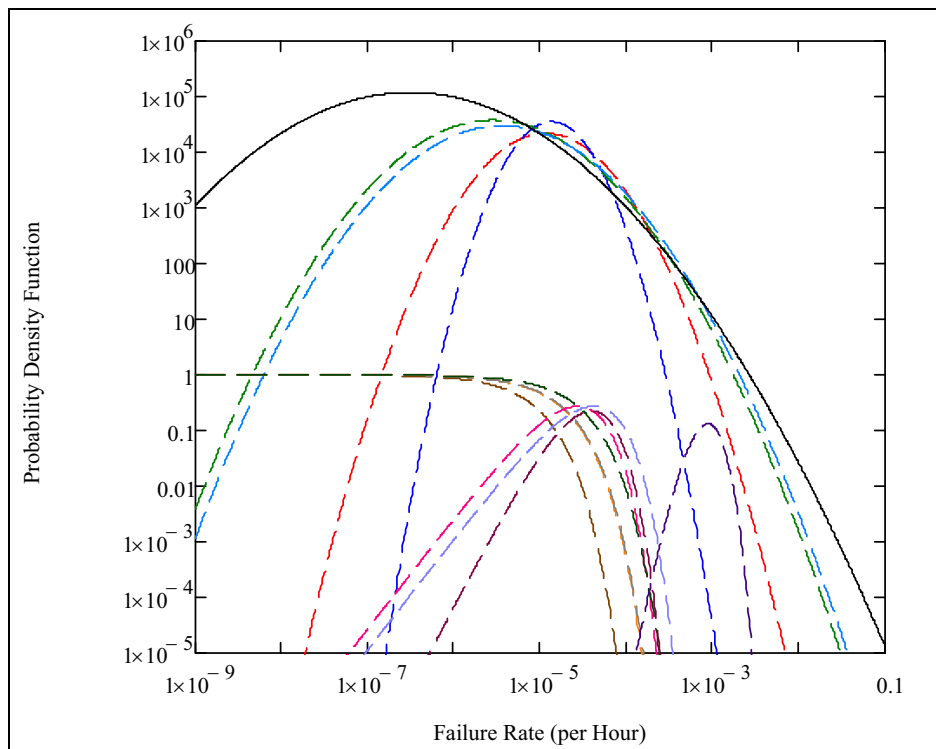
1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, 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.

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. 2.2.49, 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, ν and τ , respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating ν 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 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 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. 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 noninformative 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.

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 (Ref. 2.2.44), the Multiple Greek Letter method (Ref. 2.2.53), which is an extension of the Beta Factor method, and the Alpha Factor method (Ref. 2.2.54). 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 (Ref. 2.2.54) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in ANUREG/CR-5485 (Ref. 2.2.54) 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 NUREG/CR-5485 (Ref. 2.2.54, 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:

- .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 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 275 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 IHF Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the IHF 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 ^a	Mission Time (Hours)
51A-##ZS0133-#ZS-SPO	Limit Switch Failure Spurious Operation	1.28E-06	1.28E-06	
51A-CR---IEL001--IEL-FOD	Interlock A from Slide Gate Fails	2.75E-05		
51A-CR---IEL00A--IEL-FOD	Interlock A from Slide Gate Fails	2.75E-05		
51A-CR---IEL00B--IEL-FOD	Interlock B from Slide Gate Fails	2.75E-05		
51A-CR---IELCCF--IEL-CCF	Common Cause Failure of Interlocks from Slide Gate	1.29E-06	1.29E-06	1
51A-CR---PLC001--PLC-SPO	Inadvertent Signal Sent Due to PLC Failure	3.65E-07	3.65E-07	1
51A-CR-IEL001-IEL-FOD	Interlock B from Slide Gate Fails	2.75E-05		
51A-CR-IEL002-IEL-FOD	Interlock B from Slide Gate Fails	2.75E-05		
51A-CR-IELCCF-IEL-FOD	Common Cause Failure of Interlocks from Slide Gate	1.29E-06		
51A-CR-PLC001-PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3.65E-07	3.65E-07	
51A-CRN-BRIDGMTR-MOE-FSO	Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	6.74E-07	6.74E-07	
51A-CRN-HSTTRLMO-MOE-FSO	Crane Hoist Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	
51A-CRN-PLC0101--PLC-SPO	Crane Bridge Motor PLC Spurious Operation	3.65E-07	3.65E-07	
51A-CRN3-2-BLOCK-CRN-TBK	300-Ton Crane 2-Block Drop	4.41E-07		
51A-CRN3-2BLKDON-CRN-TBK	300-Ton Crane 2-Block Crane Drop on	4.41E-07		
51A-CRN3-DROPHLW-CRN-DRP	300-Ton Crane - Drop of HLW	3.21E-05		
51A-CRN3-DROPNVL-CRN-DRP	300-Ton Crane - Drop of Naval Cask	3.21E-05		
51A-CRN3-DROPON--CRN-DRP	300-Ton Crane Drop	3.21E-05		

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-CTM-##Z10133-ALM-SPO	CTM Bell.Grap	4.74E-07	4.74E-07	
51A-CTM-##ZE0133-ECP-FOH	CTM Bell	1.43E-05	1.79E-06	8
51A-CTM-##Z10133-ALM-SPO	Bell Grapple Alarm/Annunciator Spurious Operation	4.74E-07	4.74E-07	1
51A-CTM-##ZS0133-#ZS-SPO	CTM Bell	1.28E-06	1.28E-06	
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield Skirt Position Switch 0112 Fails	5.78E-05	7.23E-06	8
51A-CTM-#ZSH0112-ZS-FOH	Shield Skirt Position Switch Fails	5.78E-05	7.23E-06	8
51A-CTM--121122-ZS--CCF	CCF CTM Upper Limit Postion Switches	1.38E-05		1
51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.93E-04		
51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.93E-04		
51A-CTM--CBL0001-CBL-FOD	CTM Hoist Wire Rope Breaks	2.00E-06		
51A-CTM--CBL0001-WNE-BRK	Wire Rope Breaks	2.00E-06		
51A-CTM--CBL0002-CBL-FOD	CTM Hoist Wire Rope Breaks	2.00E-06		
51A-CTM--CBL0002-WNE-BRK	Wire Rope Breaks	2.00E-06		
51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist Wire ropes	9.40E-08	9.40E-08	
51A-CTM--DRTRN-CT--FOD	CTM Drive Train Protection and Fail Detection Controller Failure	4.00E-06		
51A-CTM--DRUM001-DM--FOD	Hoisting Drum Structural Failure	4.00E-08		
51A-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	5.02E-05		
51A-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure to Hold	2.01E-04	8.38E-06	24
51A-CTM--EQL-SHV-BLK-FOD	Equalizer Sheaves Structural Failure	1.15E-06		
51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1.15E-06		
51A-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	6.50E-06	6.50E-06	
51A-CTM--HOLDBRK-BRK-FOD	Brake Failure on Demand	1.46E-06		
51A-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Fails to Hold	3.52E-05	4.40E-06	8
51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	2.75E-05		

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Structural Failure	1.15E-06		
51A-CTM--MISSPOOL-DM-MSP	CTM Miss-Spool Event	6.86E-07	6.86E-07	
51A-CTM--OVERSP--ZS--FOD	CTM Hoist Motor Speed Limit Switch Failure on Demand	2.93E-04		
51A-CTM--OVERSP--ZS-FOD	Hoist Motor Speed Limit Switch Fails	2.93E-04		
51A-CTM--PORTGT1-MOE-SPO	Spurious Port Gate 1 Motor Operation	6.74E-07	6.74E-07	
51A-CTM--PORTGT1-PLC-SPO	Programmable Logic Controller Spurious Operation	3.65E-07	3.65E-07	1
51A-CTM--PORTGT2-MOE-SPO	Spurious Port Gate 2 Motor Operation	6.74E-07	6.74E-07	
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3.65E-07	3.65E-07	1
51A-CTM--TROLLY-MOE-SPO	Trolley Motor Spurious Operation	6.74E-07	6.74E-07	
51A-CTM--UPPERBL-BLK-FOD	Upper Sheaves Structural Failure	1.15E-06		
51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.99E-03		
51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	2.93E-04		360
51A-CTM--YS01129-ZS--FOD	CTM Drum Brake control circuit Limit Switch 1129 Failure	2.93E-04		
51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	1.28E-06	1.28E-06	1
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist Adjustable Speed Drive Controller Fails	2.03E-03		
51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge Motor Torque Limiter Failure	2.86E-02	8.05E-05	360
51A-CTM-BRDGPSTN-PLC-SPO	Programmable Logic Controller Spurious Operation	3.65E-07	3.65E-07	1
51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	1.95E-06	4.45E-10	4380
51A-CTM-BRIDGETR-#PR-FOH	Passive Restraint (Bumper) Failure	1.95E-06	4.45E-10	4380
51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge Motor Interlock Failure	2.74E-05		
51A-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation - Shear	6.74E-08	6.74E-07	0.1
51A-CTM-BRIDTR-CT-FOD	CTM Bridge Motor Controller Failure	4.00E-06		
51A-CTM-DRTRN-CT-FOD	CTM Drive Train Protection and Fail Detection Controller Failure	4.00E-06		

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-CTM-DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Fails on Demand	5.02E-05		
51A-CTM-HC0104##-HC-FOD	Handheld Radio Remote Controller Failure to Stop (on Demand)	1.74E-03		
51A-CTM-HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	6.50E-06	6.50E-06	
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
51A-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m-shear	6.74E-08	6.74E-07	0.1
51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist Motor Torque Limiter Failure	2.86E-02	8.05E-05	360
51A-CTM-HSTTRLLY-IEL-FOD	CTM Shield Skirt Hoist Trolley Motor Interlock Failure	2.74E-05		
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	6.74E-07	6.74E-07	
51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Controller Interlock Fails on Demand	2.75E-05		
51A-CTM-OPSENSOR-SRX-FOH	Canister Above CTM Slide Gate Optical Sensor Fails	4.70E-06	4.70E-06	1
51A-CTM-PLC0101-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3.65E-07	3.65E-07	
51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation - Shear	3.65E-08	3.65E-07	0.1
51A-CTM-PLC01021-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operations	3.65E-07	3.65E-07	
51A-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation - Shear	3.65E-08	3.65E-07	0.1
51A-CTM-PLC0103-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3.65E-07	3.65E-07	
51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation - Shear	3.65E-08	3.65E-07	0.1
51A-CTM-SBELTRLS-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operation - Shear	6.74E-08	6.74E-07	0.1
51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque Limiter Failure	2.86E-02	8.05E-05	360
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.74E-05		
51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	6.74E-07	6.74E-07	
51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt Floor Contact Sensors Fail	3.99E-03		
51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	6.74E-07	6.74E-07	

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-CTM-SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3.65E-07	3.65E-07	
51A-CTM-SLIDEGT1-IEL-FOD	CTM Slide Gate Interlock Fails	2.75E-05		
51A-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1.10E-03		
51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	1.08E-07	1.35E-08	8
51A-CTM-TROLLYTR--PR-FOH	CTM Trolley End Run Stops Failure	1.95E-06	4.45E-10	4380
51A-CTM-TROLT1-HC-FOD	Controller Failure to Stop (on Demand)	1.74E-03		
51A-CTM-WT0125-SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.99E-03		
51A-CTM-WTSW125-ZS-FOD	CTM Load Cell Limit Switch Failure on Demand	2.93E-04		
51A-CTM-YS01129-ZS-FOD	CTM Drum Brake Controller Circuit Limit Switch 1129 Fails	2.93E-04		
51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	1.28E-06	1.28E-06	1
51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.27E-05	2.27E-05	
51A-CTT--DSW000--ESC-CCF	Common Cause Failure of Deadman Switches	1.18E-05		
51A-CTT--DSW001--ESC-FOD	Deadman Switch #1 Fails Closed	2.50E-04		
51A-CTT--DSW002--ESC-FOD	Deadman Switch #2 Fails Closed	2.50E-04		
51A-CTT--HC001---HC--SPO	Handheld Controller Initiates Spurious Signal	5.23E-07	5.23E-07	
51A-CTT--HC021---HC-FOD	Remote Controller Transmits Wrong Instruction	1.74E-03		
51A-CTT--SV601---SV--FOD	Main Air Supply Valve Fails on Demand	6.28E-04		
51A-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	6.28E-04		
51A-CTT--ZS301---ZS--FOD	Pin Limit Switch #1 Fails	2.93E-04		
51A-CTT--ZS302---ZS--FOD	Pin Limit Switch #2 Fails	2.93E-04		
51A-CTT-FWDREVM1-SV-FOH	Failure of Supply Valve Providing Forward/Reverse to Motor 1	4.87E-05	4.87E-05	
51A-CTT-FWDREVM2-SV-FOH	Failure of Supply Valve Providing Forward/Reverse to Motor 2	4.87E-05	4.87E-05	
51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.38E-05		
51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.09E-07	4.09E-07	

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-CTT-SV401-SV-FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.87E-05	4.87E-05	
51A-CTT-SVROTM1-SV-FOH	Failure of Supply Valve Providing Rotation to Motor 1	4.87E-05	4.87E-05	
51A-CTT-SVROTM2-SV-FOH	Failure of Supply Valve Providing Rotation to Motor 2	4.87E-05	4.87E-05	
51A-FL---SC001---SC--FOH	Forklift Speed Control Fails	1.28E-04	1.28E-04	
51A-PMRC-DERAIL-DER-FOM	Derailment of a Railcar per Mile	1.18E-05	1.18E-05	
51A-PORTSLIDEGTE-IEL-FOD	Port Slide Gate Interlock Fails	2.75E-05		
51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.75E-05		
51A-RC---BRP001--BRP-FOD	SPMRC Brake Failure	5.02E-05		
51A-RHS-2BLKDON-CRW-TBK	RHS (Non-SFP) Crane Two Block Drop	4.49E-05		
51A-RHSCRN-DRPON-CRW-DRP	RHS (Non-SFP) Crane Drop	1.05E-04		
51A-SD---PLC001--PLC-SPO	Spurious Signal from PLC Closes Door	3.65E-07	3.65E-07	
51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.08E-02	9.62E-05	438
51A-SD---TL000---TL--CCF	Common Cause Failure of Over Torque Sensors	6.80E-04	3.78E-06	
51A-SD---TL001---TL--FOH	Motor #1 Over Torque Sensor Fails	1.44E-02	8.05E-05	
51A-SD---TL002---TL--FOH	Motor #2 Over Torque Sensor Fails	1.44E-02	8.05E-05	
51A-SGBYPASSRSTR-IEL-FOD	Failure of Interlock Bypass to Reset	2.75E-05		
51A-SLDGATE-IEL-FOD	Slide gate Interlock Fails	2.75E-05		
51A-SPMRC-BRK000-BRP-FOD	Pneumatic Brakes on SPMRC Fail on Demand	5.02E-05		
51A-SPMRC-BRP000-BRP-FOD	SPMRC Fails to Stop on Loss of Power	5.02E-05		
51A-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	9.13E-08	9.13E-08	
51A-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable Short Circuit	1.88E-08	1.88E-08	
51A-SPMRC-CPL00-CPL-FOH	SPMRC Automatic Coupler System Fails	1.91E-06	1.91E-06	
51A-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.00E-06		
51A-SPMRC-CT001--CT-SPO	Controller Spurious Operation	2.27E-05	2.27E-05	

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-SPMRC-CT001-CT-FOD	On-Board Controller Fails to Respond	4.00E-06		
51A-SPMRC-CT002--CT--FOH	Pendant Direction Controller Fails	6.88E-05	6.88E-05	
51A-SPMRC-DERAIL-DER-FOM	Derailment of SPMRC per Mile	1.18E-05	1.18E-05	
51A-SPMRC-G6500--G65-FOH	SPMRC Speed Control (Speed Limiter) Fails	1.16E-05	1.16E-05	
51A-SPMRC-HC001--HC--SPO	Spurious Command from Pendant Controller	5.23E-07	5.23E-07	
51A-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.74E-03		
51A-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.75E-05		
51A-SPMRC-MOE000-MOE-FSO	SPMRC Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	
51A-SPMRC-SC021--SC--FOH	Speed Controller on SPMRC Pendant Fails	1.28E-04	1.28E-04	
51A-SPMRC-SEL021-SEL-FOH	Speed Selector on SPMRC Pendant Fails	2.84E-06	2.84E-06	
51A-SPMRC-STU01-STU--FOH	SPMRC End Stop Fails	2.11E-04	4.81E-08	4380
51A-SPMTT-BRK000-BRP-FOD	Pneumatic Brakes on SPMTT Fail on Demand	5.02E-05		
51A-SPMTT-BRP001-BRP-FOD	Brake (Pneumatic) Failure on Demand	5.02E-05		
51A-SPMTT-CBP002-CBP-OPC	SPMTT Power Cable - Open Circuit	9.13E-08	9.13E-08	
51A-SPMTT-CBP003-CBP-SHC	SPMTT Power Cable Short Circuit	1.88E-08	1.88E-08	
51A-SPMTT-CPL00-CPL-FOH	SPMTT Automatic Coupler System Fails	1.91E-06	1.91E-06	
51A-SPMTT-CT000--CT--FOD	SPMTT Primary Stop Switch Fails	4.00E-06		
51A-SPMTT-CT001--CT--FOD	On-Board Controller Fails to Respond	4.00E-06		
51A-SPMTT-CT002--CT--FOH	Pendant Direction Controller Fails	6.88E-05	6.88E-05	
51A-SPMTT-G65000-G65-FOH	SPMTT Speed Control (Speed Limiter) Fails	1.16E-05	1.16E-05	
51A-SPMTT-HC001-HC-FOD	SPMTT Emergency Stop Switch Fails	1.74E-03		
51A-SPMTT-HC002--HC--SPO	Handheld Radio Remote Controller Spurious Operation	5.23E-07	5.23E-07	
51A-SPMTT-IEL102-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.75E-05		

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-SPMTT-MOE000-MOE-FSO	SPMTT Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	
51A-SPMTT-SC001--CT--SPO	On-Board Controller Initiates Spurious Signal	2.27E-05	2.27E-05	
51A-SPMTT-SC021--SC--FOH	Speed Controller on SPMTT Pendant Fails	1.28E-04	1.28E-04	
51A-SPMTT-SEL021-SEL-FOH	Speed Selector on SPMTT Pendant Fails	2.84E-06	2.84E-06	
51A-SPMTT-STU001-STU-FOH	SPMTT End Stops Fail	2.11E-04	4.81E-08	4380
51A-WPCRN-DROPON-CRW-DRP	WP (Non-SFP) Crane Drop	1.05E-04		
51A-WPCRN-DROPON-CRW-TBK	WP (Non-SFP) Crane Two Block Drop	4.49E-05		
51A-WPTT--CAM001-CAM-FOH	Locking Mechanism at Unload Area Fails	9.84E-07	9.84E-07	
51A-WPTT--HC001--HC--SPO	Remote Control Sends Spurious Signal	5.23E-07	5.23E-07	
51A-WPTT--ZS002--ZS--FOD	Gate Closed Limit Switch #2 Spurious Transfer	2.93E-04		
51A-WPTT-BRK401--BRK-FOD	Brakes Fail	1.46E-06		
51A-WPTT-DERAIL-DER-FOM	Probability of WPTT Derailment per Mile	1.18E-05	1.18E-05	
51A-WPTT-GRB001-GRB-SHH	Gearbox Shaft/Coupling #1 Shears	2.40E-06	2.40E-06	
51A-WPTT-GRB001-GRB-STH	Gearbox #1 Internals Teeth on Gears Strip	7.86E-08	7.86E-08	
51A-WPTT-GRB002-GRB-STH	Gearbox #2 Internals Teeth on Gears Strip	7.86E-08	7.86E-08	
51A-WPTT-GRB0021-GRB-SHH	Gearbox Shaft/Coupling #2 Shears	2.40E-06	2.40E-06	
51A-WPTT-GRBGRS-GRB-CCF	Common Cause Failure of Gearbox	3.69E-09	3.69E-09	
51A-WPTT-GRBSHFT-GRB-CCF	Common Cause Failure of Gearbox Shaft	1.13E-07	1.13E-07	
51A-WPTT-HC002---HC--SPO	Remote Controller Sends Spurious Signal	5.23E-07	5.23E-07	
51A-WPTT-HC002-HC-SPO	Remote Controller Sends	5.23E-07	5.23E-07	
51A-WPTT-IEL001-IEL-FOD	Carriage Motor Interlock Fails	2.75E-05		
51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.75E-05		
51A-WPTT-IEL003--IEL-FOD	WPTT Dock Interlock Fails to Halt Power to Trolley	2.75E-05		
51A-WPTT-IELDK3--IEL-FOD	WPTT Dock Interlock Fails	2.75E-05		

Table 6.3-1. Active Component Reliability Data Summary (Continued)

Basic Event Name	Basic Event Description	Basic Event Mean Probability ^a	Mean Failure Rate ^a	Mission Time (Hours)
51A-WPTT-IME001--IEL-FOD	Interlock Failure on Demand	2.75E-05		
51A-WPTT-MOE001-MOE-FSO	Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	
51A-WPTT-PLC001-PLC-SPO	On-Board PLC Initiated Spurious Signal	3.65E-07	3.65E-07	
51A-WPTT-PLC002--PLC-SPO	On-Board PLC Initiates Spurious Signal	3.65E-07	3.65E-07	
51A-WPTT-PLC002-PLC-SPO	On-Board PLC Initiates Spurious Signal	3.65E-07	3.65E-07	
51A-WPTT-ZS000---ZS--CCF	CCF of Gate Closed Limit Switches	1.38E-05	5.08E-05	
51A-WPTT-ZS001---ZS--FOD	Gate Closed Limit Switch #1 Spurious Transfer	2.93E-04		

NOTE: ^aAlthough 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.

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; WP = waste package; WPTT = waste package transfer trolley.

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 containment 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. 2.2.66), 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. The methodology is applicable to all of the waste containers that are processed in the IHF, as well as the other waste handling facilities, 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 IHF 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 Sections 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 such parameters. 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. Loss of containment probability analysis has been evaluated for various containers by three different studies:

- *Seismic and Structural Container Analyses for the PCSA* (Ref. 2.2.33)
- *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-Foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations* (Ref. 2.2.74) and *Qualitative Analysis of the Standardized DOE SNF Canister Specific Canister-on-Canister Drop Events at the Repository* (Ref. 2.2.75)
- *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert* (Ref. 2.2.24)

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), in *Seismic and Structural Container Analyses for the PCSA* (Ref. 2.2.33), predicts failure probabilities of $<1.0 \times 10^{-8}$ for most of the events. If a probability for the event sequence is less than 1×10^{-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 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, LS-DYNA (Ref. 2.2.33). 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.

INL calculates strains by modeling DOE SNF and multicanister overpacks (MCOs) with the static finite element code, ABAQUS (Ref. 2.2.74). The structural evaluations consider off-vertical drops. In such cases, the deformation of the waste form container is greater on the localized area of impact than for a flat-bottom drop, and will therefore yield a greater calculated probability of breach.

Probability of failure is conservatively calculated by comparing the peak strain to the cumulative distribution function derived from tensile strain to failure test data reported in the literature, representing aleatory uncertainty associated with the variability of test coupon data.

BSC FEA analysis used LS-DYNA 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

Item	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	40	1.0×10^{-5}	Flat bottomed, LLNL, adjusted
DOE Standardized 24" or 18" canister	23	1.0×10^{-5}	3 degrees from vertical, LLNL, adjusted using INL FEA
Aging overpack	3	1.0×10^{-5}	LLNL, adjusted

Table 6.3-2. Failure Probabilities Due to Drops and Other Impacts (Continued)

Item	Drop Height (ft)	Failure Probability	Note
MCO canister	23	9.0×10^{-2}	LLNL using INL FEA
HLW canister	30	6.7×10^{-2}	Bayesian interpretation of test data, 0 failures in 13 drops.
Waste package	2	1.0×10^{-5}	BSC FEA, horizontal orientation

NOTE: ^aAlso applies to shielded transfer casks used on-site and horizontal transfer casks. Although shielded transfer casks are not used in the IHF, they are mentioned here for completeness.

BSC = Bechtel SAIC; DOE = U.S. Department of Energy; FEA=finite element analysis; HLW = high-level radioactive waste; INL = Idaho National Laboratory; LLNL = Lawrence Livermore National Laboratory; MCO = multiccanister overpack.

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 Lawrence Livermore National Laboratory (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-metric-ton load onto container
Tipover	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 ft/min 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.

$$P = \int_{-\infty}^x N(t) dt \quad \text{and} \quad x = \frac{H_d/H_m - 1}{COV} \quad (\text{Eq. 17})$$

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.

Table 6.3-4. Failure Probabilities for Collision Events and Two-Blocking

Collision Scenario	Speed	Velocity (ft/sec) ^a	Equivalent Drop Height (ft) ^b	Failure Probabilities for Various Container Types				
				Transportation Cask	Canister	Waste Package	MCO	High-Level Radioactive Waste
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 ft/min	0.33	0.00	1.00E-08				
CTT	10 ft/min	0.17	0.00	1.00E-08	1.00E-08		1.00E-08	1.00E-08
ST	2.5 mph	3.67	0.21		1.00E-08		1.00E-08	1.00E-08
WPTT	40 ft/min	0.67	0.01		1.00E-08	1.00E-08	1.00E-08	1.00E-08
WP (in TEV)	1.7 mph	2.49	0.10			1.00E-08		
CTM	20 ft/min	0.33	0.00		1.00E-08		1.00E-08	1.00E-08
CTM	40 ft/min	0.67	0.01		1.00E-08		1.00E-08	1.00E-08
Two blocking				1.00E-04	1.00E-05	NA	1.00E+00	1.40E-02

NOTE: ^aConversions from the previous column are as follows. From speed in mph: multiply by 5280/3600. From speed in ft / min: divide by 60.

^bCalculated as follows based on constant acceleration due to gravity (no air resistance): $v^2 / (2 \times 32.2 \text{ ft} / \text{sec}^2)$, where v is the velocity in ft / sec. Values are rounded to the nearest hundredth of a ft. Values that are less than 0.005 are reported as 0.00.

CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; DSTD = DOE standardized canister; ft = feet; MCO = multicanister overpack; min = minutes; mph = miles per hour; sec = seconds; ST = site transporter; TAD = transportation, aging, and disposal; TEV = transport and emplacement vehicle; WP =waste package; WPTT = waste package transfer trolley.

Source: Original

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 would be 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 its probability cannot be inferred from comparison with other structural challenges to the canister.

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, characteristic of some DPCs and other waste canisters; and 1.0 inches, the anticipated thickness of TAD canisters and naval SNF canisters. 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 ^b	Failure Probability	
	Mean	Standard Deviation
Thin-Walled ^c Canister in a Waste Package ^a	3.2×10^{-4}	5.7×10^{-5}
Thick-Walled ^c Canister in a Waste Package ^a	1.0×10^{-4}	2.2×10^{-5}
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 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 the 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, so that failures for these configurations can be screened. For conservatism, a screening conditional probability of 1×10^{-6} could be used.

^c Naval SNF canisters are modeled as thick walled. Other canisters are modeled as thin walled.

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 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, 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 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 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, 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 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. 2.2.14). These calculations consider a range of decay heat levels and a loss of cooling for 30 days, which is consistent with NUREG-0800, Section 9.2.5 (Ref. 2.2.63). These analyses indicate that the canister temperature would remain well below 500°C (773°K) (Ref. 2.2.14). This temperature is hundreds of degrees below the temperature at which the canister would fail (Figure D.2.1-4 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 are summarized in Table 6.3-6. Some of the items discussed in this section and listed in Table 6.3-6 are not used in the IHF, such as aging overpacks and the TEV. However, there are included in this section at drop heights characteristic of crane operations. .

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.

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. 2.2.76), 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 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.

A WPTT that transports a waste package is considered to lose its shielding function, if it is subjected to a structural challenge sufficiently severe to cause the breach of the sealed waste package, or, when the waste package is not yet sealed, the breach of one or more canisters inside, as applicable. Conversely, if the structural challenge is not sufficiently severe to cause a canister or waste package breach, it is postulated to also be sufficiently mild to leave the shielding function intact.

Similarly, a TEV that transports a waste package is considered to lose its shielding function if it is subjected to a structural challenge sufficiently severe to cause the breach of the waste package. Conversely, if the structural challenge is not sufficiently severe to cause a waste package breach, it is postulated to also be sufficiently mild to leave the shielding function of the TEV 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. The SSC providing shielding may be, for example, a WPTT. A transportation cask containing uncanistered SNF is also considered to have lost its shielding if it has lost its containment function.

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, cask transfer trolley, waste package transfer trolley, or TEV 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 most 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 subjected to a fire are postulated to lose their shielding function with a probability of 1, 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

Event	Probability	Note
Sealed transportation cask and shielded transfer casks shielding degradation after structural challenge	1×10^{-5}	Attachment D.
Aging overpack shielding loss after structural challenge	5×10^{-6}	Attachment D.
CTM shielding loss after structural challenge	0	Structural challenges sufficiently mild to leave the shielding function intact
WPTT shielding loss after structural challenge	0	Structural challenges sufficiently mild to leave the shielding function intact
TEV shielding loss (shield end)	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 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 for 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 a fire.

NOTE: CTM = canister transfer machine; TEV = transport and emplacement vehicle; WPTT = waste package transfer trolley.

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 should be noted that Table 6.3-7 addresses 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 IHF. The probability of each basic event is based on one of the values presented in Tables 6.3-2 through 6.3-7.

6.3.3 Miscellaneous Data

Split fractions for specific fire scenarios are derived from the exposure frequencies detailed in Section 6.5 and Attachment F. Table 6.3-9 identifies the frequency associated with a waste type in a specific configuration and location with or without diesel fuel present.

Table 6.3-10 provides details on how specific residence time fractions were developed for the IHF fire event sequence analysis. The formulas use the index notation in Table 6.3-9. For example, index A1 represents the HLW waste package present in the Positioning/Closure Room over the entire preclosure period. Index A2 represents a naval waste package present in the room over the preclosure period.

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 6.3-11.

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													
Representative Canister ³ or HLW Canister in a Transportation Cask ⁶	1.0E-05	1.0E-05	1.0E-05	N/A	1.0E-05	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-05	2.0E-06	1.0E-06
T Transportation Cask with Bare Fuel	1.0E-05	1.0E-05	1.0E-05	N/A	1.0E-05	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-05	5.0E-02 ¹	6.0E-03 ²
Bare Representative Canister ³ (except DSTD) ⁶	1.0E-05	1.0E-05	1.0E-05	1.0E-05	N/A	N/A	N/A	N/A	N/A	N/A	1.0E-05	N/A	N/A
Any Waste Package ⁶	1.0E-05	N/A	N/A	N/A	1.0E-05	1.0E-08	N/A	1.0E-08	1.0E-05	N/A	No challenge	3.0E-04	1.0E-04
Bare MCO	N/A	1.0E-01	~ 1	~ 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bare DOE Standardized SNF Canister (DSTD)	1.0E-05	1.0E-05	1.0E-05	N/A	N/A	N/A	N/A	N/A	1.0E-05	1.0E-05	N/A	N/A	N/A
Bare HLW Canister	3.0E-02 ³	3.0E-02	7.0E-02	~ 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Any Canister in CTM Shield Bell ⁶	N/A	1.0E-05	N/A	N/A	N/A	1.0E-08	N/A	N/A	N/A	N/A	N/A	1.0E-04	9.0E-05
Applicable Representative Canister in Aging Overpack	1.0E-05	1.0E-05	N/A	N/A	N/A	1.0E-08	1.0E-08	1.0E-08	N/A	N/A	1.0E-05	1.0E-06	1.0E-06
Loss of Shielding													
Any Transportation Cask	1.0E-05	1.0E-05	1.0E-05	N/A	1.0E-05	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-08	1.0E-05	~ 1	~ 1
Aging Overpack	1.0E-05	5.0E-06	N/A	N/A	N/A	1.0E-05	1.0E-05	1.0E-05	1.0E-05	1.0E-05	1.0E-05	~ 0	~ 0
TEV, CTM, WPTT ⁶	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
³ Represents passive event failure probabilities for a drop of a HLW canister onto another HLW canister.
⁴ Naval SNF canisters are modeled as thick walled. Other canisters are modeled as thin walled.
⁵ SNF Canister analyzed as representative of DOE Standardized SNF Canister (DSTD), DPC, naval, and TAD Canisters.
⁶ Used in IHF event sequences.

mph = miles per hour; N/A = not applicable, no scenarios identified.

Source: Attachment D

Table 6.3-8. Passive Equipment Failure Basic Events used in IHF Event Sequence Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Condition
51A-HLW-CAN-FAIL-2BLK	Canister Fails from 2-Block Drop	1.00E+00	40-Foot Vertical Drop
51A-HLW-CAN-FAIL-COLL	Canister fails from Low Speed Collision	1.000E-08	20 Feet per minute flat side impact/collision
51A-HLW-CAN-FAIL-DERAIL	Canister Fails from Derailment	1.000E-05	2.5 mph end-to-end collision
51A-HLW-CAN-FAIL-DROP	Canister Fails from Drop	3.000E-02	Canister drop normal height
51A-HLW-CAN-FAIL-DROPIN	Canister fails from Drop inside CTM Bell	0.000E+00	Canister Drop from CTM Bell
51A-HLW-CAN-FAIL-DROPON	Canister Fails from Object dropped on Canister	3.000E-02	Canister Drops on Canister
51A-HLW-CAN-FAIL-DRPONW	Canister fails from Object dropped on WP	0.000E+00	Object Dropped on HLW Canister in WP
51A-HLW-CAN-FAIL-IMPACT	Canister Failure from Impact	1.000E+00	HLW Canister Shear
51A-HLW-CAN-FAIL-IN-WP	Canister Failure from Fire	3.000E-004	HLW in WP Fail from Fire
51A-HLW-CAN-FAIL-LID	Canister Fails from Impact by Lid During Lid Removal	0.000E+00	10-Ton Drop On Canister in TC
51A-HLW-CAN-FAIL-S-CTM	HLW Canister Failure in CTM	1.000E-04	Thin-walled canister fire
51A-HLW-CAN-FAIL-SIMP	Canister Fails from Side impact from Shield Door	1.000E+00	Canister in TC; fails if TC fails
51A-HLW-CAN-FAIL-TILT	Canister Fails from Pre-Tilt/Down	1.000E-05	Tipover
51A-HLW-CANTC-FAIL-COLL	Failure of HLW Canister in TC from Collision	1.000E-05	Canister in TC : TC lid unbolted
51A-HLW-CANTC-FAIL-IMP	Failure of HLW Canister in TC from Impact	1.000E-05	Canister in TC : TC lid unbolted
51A-HLW-CANWP-FAIL-COLL	Canister in WP Fails from Collision	1.000E+00	Canister in WP; fails if WP fails
51A-HLW-CANWP-FAIL-DERAIL	Canister in WP Fails from Derailment	1.000E+00	Canister in WP; fails if WP fails
51A-HLW-CANWP-FAIL-TILT	Canister in WP Fails from Tilt/Down	1.000E+00	Canister in WP; fails if WP fails
51A-HLW-CONT-FAIL-IMP	HLW Containment Fails from Impact with Shield Door	1.000E-08	Shield doors impact TC
51A-HLW-IMPACT-WP	WP Fails from Impact	1.00E-08	Canister in WP; fails if WP fails
51A-HLW-SHIELD-FAIL-COLL	WP Shield Fails from Low Speed Collision	0.000E+00	Loss of shielding-low speed collision; shielding provide by WPTT
51A-HLW-SHIELD-FAIL-TILT	WP Shielding fails from Pre-Tilt/Down	0.000E+00	Loss of shielding-tipover; shielding provide by WPTT
51A-HLW-SHLDWP-FAIL-COLL	WP Shield Fails from Collision	0.000E+00	WP shielding failure; shielding provide by WPTT
51A-HLW-SHLDWP-FAIL-TILT	WP Shield Fails from Tilt/Down	0.000E+00	WP shielding failure; shielding provide by WPTT
51A-HLW-TCASK-FAIL-COLL	HLW TC Failure in Low Speed Collision	1.000E-08	9 mph end-to-end collision; WP sealed
51A-HLW-TCASK-FAIL-DERAIL	HLW TC Failure in Derailment	1.000E-08	2.5 mph end-to-end collision; WP sealed

Table 6.3-8. Passive Equipment Failure Basic Events used in IHF Event Sequence Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Condition
51A-HLW-TCASK-FAIL-ROLL	HLW TC Failure in Rollover	1.000E-05	6 ft horizontal drop
51A-HLW-TC-FAIL-2BLK	Failure of HLW TC from 2-Block Drop	1.000E-05	30 ft vertical drop
51A-HLW-TC-FAIL-DROP	Failure of HLW TC from Drop	1.000E-05	15 ft vertical drop
51A-HLW-TC-FAIL-DROPON	Failure of HLW Cask from Object Dropped on Cask	1.000E-05	10 ton drop on TC
51A-HLW-TC-FAIL-SIMP	Failure of HLW Cask from Side Impact	1.000E-08	2.5 mph side impact to TC
51A-HLW-TC-FAIL-SPURMOV	Failure of HLW Cask from Spurious Movement	1.000E-08	2.5 mph side impact to TC
51A-HLW-TC-FAIL-TIPOVER	Failure of HLW Cask from Tipover	1.000E-05	TC tipover
51A-HLW-TC-TIPOVER	HLW TC Tipover	1.000E-05	TC tipover
51A-HLW-WP-FAIL-COLLIDE	WP Fails from Collision	1.000E-08	2.5 mph flat side collision of WPTT
51A-HLW-WP-FAIL-DERAIL	WP Fails from Derailment	1.000E-05	2.5 mph end-to-end collision
51A-HLW-WP-FAILS-DROPON	WP Fails from Object dropped on WP	1.000E-05	10-Ton drop on WP
51A-HLW-WP-FAIL-TILT	WP Fails from Tiltdown	0.000E+00	WP in WPTT during Tiltdown
51A-HLW-WP-FAIL-DERAIL	WP Shielding fails from WPTT Derailment	0.000E+00	WP shielding
51A-HLW-WP-FAIL-IMPACT-TEV	WP Fails from Impact	1.000E-005	Canister in WP; fails if WP fails
51A-NVL-CAN-FAIL-2BLK	Canister Fails from 2-Block Drop	1.000E-05	40-foot vertical drop
51A-NVL-CAN-FAIL-COLL	Canister Fails in Low Speed Collision	1.000E-08	2.5 mph flat side collisions; in CTM
51A-NVL-CAN-FAIL-DERAIL	Canister fails from WPTT Derailment	1.000E-05	2.5 mph end-to-end collisions
51A-NVL-CAN-FAIL-DROP	Canister Fails from Drop	1.000E-05	15-foot vertical drop
51A-NVL-CAN-FAIL-DROPIN	Canister Fails from drop in CTM Bell	0.000E+00	Canister drops in CTM Bell
51A-NVL-CAN-FAIL-DROPON	Failure of NVL Canister from Dropped Object	1.000E-05	10-Ton object drops on canister
51A-NVL-CAN-FAIL-DRPONWP	Canister fails from Object Dropped on WP	1.000E-05	10-Ton object drops on canister
51A-NVL-CAN-FAIL-IMPACT	Canister failure from Impact	1.000E+00	NVL canister in TC; fails if TC fails
51A-NVL-CAN-FAIL-IN-TC	Failure of NVL Canister in TC	1.000E+00	NVL canister in TC; fails if TC fails
51A-NVL-CAN-FAIL-SIMP	Canister Fails from Side impact by Slide Gate	1.000E-08	Shear event
51A-NVL-CAN-FAIL-TILT	Canister Fails During WPTT Pre-Tiltdown	1.000E-05	Canister tipover in unsealed WP
51A-NVL-CANTC-FAIL-COLL	Failure of NVL Canister in TC from Collision	1.000E-05	Lid unbolted on TC; 2.5 mph collision
51A-NVL-CANTC-FAIL-IMP	Failure of NVL Canister in TC from impact	1.000E-05	Lid unbolted on TC; 2.5 mph impact
51A-NVL-CANWP-FAIL-COLL	Canister in WP Fails from Collision	1.000E+00	Canister fails if WP Fails
51A-NVL-CANWP-FAIL-DERAIL	Canister in WP Fails from Derailment	1.000E+00	Canister fails if WP Fails
51A-NVL-CANWP-FAIL-TILT	Canister in WP Fails from Tiltdown	1.000E+00	Canister fails if WP Fails

Table 6.3-8. Passive Equipment Failure Basic Events used in IHF Event Sequence Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Condition
51A-NVL-CONT-FAIL-IMP	NVL Containment Fails from Impact into Shield Door	1.000E-08	2.5 mph side impact
51A-NVL-SHIELD-FAIL-COLL	WPTT Shield Fails in Low Speed Collision	0.000E+00	2.5 mph collision—shield failure
51A-NVL-SHIELD-FAIL-DERL	WPTT Shield Fails During Derailment	0.000E+00	WPTT shielding failure--derailment
51A-NVL-SHIELD-FAIL-TILT	WPTT Shield Fails During pre-Tilt-down	0.000E+00	WPTT shielding failure--pretiltdown
51A-NVL-SHLDWP-FAIL-TILT	WP Shield Fails from Tilt-down	0.000E+00	WP shielding failure--tiltdown
51A-NVL-TC-FAIL-2-BLOCK	NVL Cask Fails from 2-Block Drop	1.000E-05	30-foot vertical drop
51A-NVL-TC-FAIL-COLLIDE	NVL Cask Fails in Prime Mover Collision	1.000E-08	9 mph end-to-end collision
51A-NVL-TC-FAIL-DERAIL	Failure of NVL Cask from Derailment	1.000E-08	9 mph side impact
51A-NVL-TC-FAIL-DROP	Failure of NVL Cask from Dropping	1.000E-05	15-foot vertical drop
51A-NVL-TC-FAIL-DROPON	Failure of NVL Cask from Object Dropped on Cask	1.000E-05	10-ton drop on TC
51A-NVL-TC-FAIL-OFFPMCOL	NVL Cask Fails from Collision off of Prime Mover	1.000E-08	2.5 localized side impact
51A-NVL-TC-FAIL-SIMP	Failure of NVL Cask from Side Impact	1.000E-08	2.5 mph flat side impact
51A-NVL-TC-FAIL-TIP	Failure of NVL Cask from Tipover	1.000E-05	TC vertical tipover
51A-NVL-WP-FAIL-COLLIDE	WP Fails from Collision	1.000E-05	2.5 mph end-to-end collision
51A-NVL-WP-FAIL-DERAIL	WP Fails from Derailment	1.000E-05	2.5 mph end-to-end collision
51A-NVL-WP-FAIL-DROPON	WP Fails from Object dropped on WP	1.000E-05	10-ton object dropped on WP
51A-NVL-WP-FAIL-TILT	WP Fails from Tilt-down	0.000E+00	WP in WPTT tilt-down
51A-NVL-WPSHLD-FAIL-COLL	WP Shield from Collision	0.000E+00	WP in WPTT shielding failure
51A-NVL-WPSHLD-FAIL-DERL	WP Shield Fails from Derailment	0.000E+00	WP in WPTT shielding failure
51A-NVL-WPTT-COLLIDE-TEV	WP failure due to Collision	1.000E-05	WPTT Collision with TEV
51A-WPSHIELD-FAIL-EXPORT	WP Shield Fails During Export	0.000E+00	WP shielding failure
CTM-SHIELDING	Shielding associated with CTM	0.000E+00	Canister shielding failure in CTM
Thermal PEFA			
51A-HLW-CAN-CONT-PR-FIR	Can Failure in WP in Positioning Room	3.000E-04	Thin wall canister
51A-HLW-CAN-CONT-CUR-FIR	Fire Fails Can in TC	2.000E-06	Thin wall canister
51A-HLW-CAN-CONT-CTM-FIR	Can Failure in CTM	1.000E-004	Thin wall canister
51A-HLW-CAN-CONT-LR-FIR	Can Failure in WP in Loading Room	3.000E-04	Thin wall canister
51A-HLWCAN-WP-FAIL-FIRE	HLW Canister in WP fails in Fire	3.000E-04	Thin wall canister
51A-HLWCAN-WPTT-FAIL-FIR	HLW Canister in WPTT fails in Fire	3.000E-04	Thin wall canister
51A-NVL-CAN-CONT-CTM-FIR	Canister Fails in Fire Involving CTM	9.000E-05	Thick wall canister

Table 6.3-8. Passive Equipment Failure Basic Events used in IHF Event Sequence Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Condition
51A-NVL-CAN-CONT-CTM-FIR	NVL Canister in CTM During Facility Fire	9.000E-05	Thick wall canister
51A-NVL-CAN-CONT-CUR-FIR	Canister Failure Cask Unloading Room	1.000E-06	Thick wall canister
51A-NVL-CAN-CONT-CUR-FIR	NVL Canister in Cask Unloading Room During Fire	1.000E-06	Thick wall canister
51A-NVL-CAN-CONT-LR-FIRE	Canister Fails WP Loading Room	1.000E-04	Thick wall canister
51A-NVL-CAN-CONT-PR-FIRE	Canister Fails WP Positioning Room	1.000E-04	Thick wall canister
51A-NVLCAN-FAILWP-LOR	Canister Fails WP Loadout Room	1.000E-04	Thick wall canister
51A-NVLCAN-FAILWPTT-LOR	Localized Fire Threatens WP in WPTT in Loadout Room	1.000E-04	Thick wall canister
51A-NVL-CAN-FAIL-IN-WP	Failure of NVL Canister in Waste Package	1.000E-04	Thick wall canister
51A-NVL-CAN-FAILS-CTM	NVL Canister Failure in CTM	9.000E-05	Thick wall canister

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; DSTD = DOE standardized canister; ft = feet; HLW = high level radioactive waste; MCO = multicanister overpack; min = minutes; mph = miles per hour; NVL = naval; sec = seconds; ST = site transporter; TAD = transportation, aging, and disposal; TC = transportation cask; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

Table 6.3-9. Fire Analysis for Wastes Types in Specific Configuration

Location	Index	HLW	Naval	Container Type or Location
		1	2	
Positioning/Closure Room (WPTT)	A	3.8E-05	3.8E-05	WP
WPTT in Loadout Room	B	4.9E-07	4.9E-07	WP
WP in TEV in Loadout Room	C	8.8E-08	8.8E-08	WP
On CTT in Unloading Room	D	2.2E-08	1.2E-08	TC
WPTT in Loading Room	E	1.2E-05	3.5E-07	WP
Vestibule/Preparation Area w/SPM (Diesel Present)	F	1.5E-07	2.3E-07	TC
Preparation Area w/o SPM (No Diesel Present)	G	9.3E-07	2.0E-06	TC
On CTT in Preparation Area	H	5.3E-07	1.3E-06	TC
In CTM in Transfer Room	I	6.9E-08	8.1E-08	CTM
Large Fire Threatens TC/NSNF w/SPM Present (Diesel)	J		3.7E-07	TC
Large Fire Threatens TC/NSNF w/o SPM Present (No Diesel)	K		9.7E-06	TC
Large Fire Threatens NSNF in CTM	L		2.0E-07	CTM
Large Fire Threatens NSNF in WP	M		5.9E-05	WP
Large Fire Threatens TC/HLW w/SPM Present (Diesel)	N	2.5E-07		TC
Large Fire Threatens TC/HLW w/o SPM Present (No Diesel)	O	5.1E-06		TC
Large Fire Threatens HLW in CTM	P	1.6E-06		CTM
Large Fire Threatens HLW in WP	Q	1.0E-04		WP

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high level waste; NSNF = naval spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transportation emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Table 6.5-4

Table 6.3-10. Split Fractions for Waste Types in Various Configurations

Naval-Localized Fires			
Reference Index for Table 6.3-12	Basic Event Identifier	Formula for Split Fraction	Resultant Value
(1)	51A-NVL-SPMRC-DIESEL	$[(F2)/(F2+G2+H2)]$	6.5E-02
(2)	51A-NVL-SPMRC-WODIESEL	$[(G2+H2)/(F2+G2+H2)]$	9.4E-01
(3)	51A-PROB-NVLCAN-WPTT-LOR	$[(B2)/(B2+C2)]$	8.5E-01
(4)	51A-PROB-NVLCAN-WP-LOR	$[(C2)/(B2+C2)]$	1.5E-01
Naval-Large Fire			
(5)	51A-NVL-FREQ-DIESEL	$[(J2)/(J2+K2+L2+M2)]$	5.4E-03
(6)	51A-NVL-FREQ-NODIESEL	$[(K2)/(J2+K2+L2+M2)]$	1.4E-01
(7)	51A-NVL-LARGE-FIRE-CTM	$[(L2)/(J2+K2+L2+M2)]$	2.9E-03
(8)	51A-NVL-FREQ-WP-FAILS	$[(M2)/(J2+K2+L2+M2)]$	8.5E-01
HLW-Localized Fire			
(9)	51A-HLWSPMRC-DIESEL	$[(F1)/(F1+G1+H1)]$	9.6E-02
(10)	51A-HLWSPMRC-NODIESEL	$[(G1+H1)/(F1+G1+H1)]$	9.0E-01
(11)	51A-PROB-HLWCAN-WPTT-LOR	$[(B1)/(B1+C1)]$	8.5E-01
(12)	51A-PROB-HLWCAN-WP-LOR	$[(C1)/(B1+C1)]$	1.5E-01
HLW-Large Fire			
(13)	51A-HLW-FREQ-WITH DIESEL	$[(N1)/(N1+O1+P1+Q1)]$	2.3E-03
(14)	51A-HLW-FREQ-NO-DIESEL	$[(O1)/(N1+O1+P1+Q1)]$	4.7E-02
(15)	51A-HLW-LARGE-FIRE-CTM	$[(P1)/(N1+O1+P1+Q1)]$	1.5E-02
(16)	51A-HLW-FREQ-WP-FAILS	$[(Q1)/(N1+O1+P1+Q1)]$	9.4E-01
(17)	51A-HLW-FREQ-NODIESEL	$[(Q1)/(N1+O1+P1+Q1)]$	9.4E-01

NOTE: HLW = high-level waste

Source: Original

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-#HLW-TC-LIFTS	Number of Crane Lifts of HLW TCs	1.00E+00	During preparation activities associated with a HLW TC, there is one lift of a heavy object such as a lift fixture over the cask. Therefore, a value of 1 is assigned to this basic event.	N/A
51A-%-HLW-ON-SPMRC	Percentage of Time HLW is Received on SPMRC	1.67E-01	600 HLW TCs can be received by rail or by truck. 100 HLW TCs with multiple canisters will arrive by railcar and 500 TCs with single canisters will arrive by truck trailer	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
51A-%-HLW-ON-SPMTT	Percentage of Time HLW is Received on SPMTT	8.33E-01	600 HLW TCs can be received by rail or by truck. 100 HLW TCs with multiple canisters will arrive by railcar and 500 TCs with single canisters will arrive by truck trailer	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
51A-CTMOBJLIFTNUMBER-HLW	Number of Object Lifts	1.00E+00	During canister transfer from a HLW TC to a WP, the CTM lifts a lid over the cask. Therefore, a value of 1 is assigned to this basic event.	N/A
51A-CTMOBJLIFTNUMBER-NVL	Number of Objects Lifted	1.00E+00	During canister transfer from a Naval TC to a WP, the CTM lifts a lid over the cask. Therefore, a value of 1 is assigned to this basic event.	N/A
51A-DOORFAIL-IMPACT	Shield Door Fails from Impact	0.00E+00	Failure of shield door can not occur as a result of any collisions within the IHF.	N/A
51A-FIRE-SUPPRESSION	Inadvertent Fire Suppression Actuation	9.30E-07	Fire suppression system inadvertently activates during normal IHF operations (no fire)	Section 6.2.2.9
51A-LIFTS-PER-HLW-CAN	Number of Lifts per HLW Canister	1.00E+00	HLW is lifted out of a TC by the CTM and placed in a WP.	N/A
51A-HLW-FAIL-CAN-DIESEL	Relative Frequency with Diesel Present	2.00E-06	Based on the fire frequency analysis, this value represents the relative frequency for a HLW Canister in the Cask Prep Area with diesel present.	Section 6.5

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-HLW-FREQ WITH DIESEL	Relative Frequency with Diesel Present	2.30E-03	Based on the fire frequency analysis, this value represents relative frequency an HLW canister is possibly subjected to a large facility fire with diesel present.	Table 6.3-10 (13)
51A-HLW-FREQ-NO-DIESEL	Relative Frequency with no Diesel Present	4.67E-02	Based on the fire frequency analysis, this value represents the relative frequency an HLW canister is possibly subjected to a large facility fire without diesel present.	Table 6.3-10 (14)
51A-HLW-FREQ-WODIESEL	Relative Frequency of WP in Large Fire without Diesel	9.37E-01	Based on the fire frequency analysis, this value represents the relative frequency a WP is subject to a possible large facility fire without diesel present.	Table 6.3-10 (17)
51A-HLW-FREQ-WP-FAILS	Relative Frequency of WP in Large Fire	9.37E-01	Based on the fire frequency analysis. This value represents the fraction of time an HLW WP is in the IHF.	Table 6.3-10 (16)
51A-HLW-LARGE-FIRE-CTM	Relative Frequency of Large Fire in CTM	1.45E-02	Based on fire frequency analysis. Large facility fire threatens HLW canister inside the CTM.	Table 6.3-10 (15)
51A-LIFTS-PER-NVL-CAN	Number of Lifts per NVL Canister	1.00E+00	Naval canister is lifted out of a TC by the CTM and placed directly into a WP.	N/A
51A-LOSS-OFFSITE-PWR	Loss of offsite power	2.99E-03	Commercial power reliability requirement	N/A
51A-MODERATOR-ENTERS-CAN	Moderator Enters Canister in a Fire	1.00E+00	Water enters canister during facility fire--conservative value assigned.	Section 6.2.2.7
51A-OBJECTLIFTNUMBER	Number of Object Lifts	1.00E+00	Number of crane lifts that could result in dropping objects on the transpiration cask	N/A
51A-OIL-MODERATOR	Oil Moderator Sources in IHF (Gearbox)	9.00E-05	Crane gearbox leaks oil during normal IHF operations (no fire) that could potentially create a moderator source.	Section 6.2.2.7
51A-OTHER-WATER	Water Moderator Sources Other Than Firer Suppression	1.40E-03	Other water sources provide moderator for canisters such as water pipes or valves in IHF leak.	Section 6.2.2.7
51A-PROB-HLWCAN-WP-LOR	Probability HLW Canister in WP in Loadout Room	1.51E-01	Based on fire frequency analysis. Fire threatens WP with HLW canister in Loadout room.	Table 6.3-10 (12)

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-HLWSPMRC-DIESEL	Fire in Prep Area SPMRC with Diesel	9.61E-02	Based on the fire frequency analysis, this value represents the failure of the HLW canister in a Cask Prep Area fire when diesel is present.	Table 6.3-10 (9)
51A-HLWSPMRC-WODIESEL	Fire in Prep Area SPMRC Without Diesel	9.04E-01	Based on the fire frequency analysis, this value represents the failure of the HLW canister in a Cask Prep Area fire when no diesel is present on the SPMRC.	Table 6.3-10 (10)
51A-PROB-HLWCAN-WPTT-LOR	Probability HLW Canister in WPTT in Loadout Room	8.49E-01	Based on fire frequency analysis. Fire threatens WPTT with HLW canister in Loadout room	Table 6.3-10 (11)
51A-NVL-FREQ-DIESEL	Relative Frequency with Diesel Present	5.35E-03	Based on the fire frequency analysis. Large facility fire when diesel is present threatens naval cask inside the IHF.	Table 6.3-10 (5)
51A-NVL-FREQ-NO-DIESEL	Relative Frequency without Diesel Present	1.39E-01	Based on the fire frequency analysis. Large facility fire when no diesel is present threatens naval cask inside the IHF.	Table 6.3-10 (6)
51A-NVL-FREQ-WP-FAILS	Relative Frequency WP Fails due to Fire	8.53E-01	Based on fire frequency analysis. Large facility fire threatens naval canister inside the IHF.	Table 6.3-10 (8)
51A-NVL-LARGE-FIRE-CTM	Relative Frequency of Large Fire in CTM	2.91E-03	Based on fire frequency analysis. Large facility fire threatens naval canister inside the CTM.	Table 6.3-10 (7)
51A-NVL-SPMRC-WODIESEL	Fire in Preparation Area without Diesel	9.35E-01	Based on Fire frequency analysis. Fire threatens naval transportation cask after SPM has left cask preparation room.	Table 6.3-10 (2)
51A-NVL-SPMRC-DIESEL	Fire in Preparation Area SPMRC with Diesel	6.53E-02	Based on Fire frequency analysis. Fire threatens naval transportation cask while SPM is present in cask preparation room.	Table 6.3-10 (1)
51A-PROB-HLW-WP	Probability of HLW WP Cask in Process	6.00E-01	Probability a HLW canister in WP—based on 600 of 1000 canisters processed through IHF over entire preclosure period	N/A

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-PROB-LEAD	Probability of Lead Casks	1.00E+00	The number of leaded TC received by the IHF is unknown. This value is set to a value of 1.0 to ensure a conservative analysis.	N/A
51A-PROB-NON-LEAD	Probability of Non-Lead Casks	0.00E+00	Since all TCs received by the IHF are considered as leaded casks, then the probability of receiving a non-leaded cask is 0.0	N/A
51A-PROB-NVLCAN-WP-LOR	Probability NVL Canister in WP in Loadout Room	1.51E-01	Based on fire frequency analysis. Fire threatens WP with Naval canister in Loadout room.	Table 6.3-10 (4)
51A-PROB-NVLCAN-WPTT-LOR	Probability NVL Canister in WPTT in Loadout Room	8.49E-01	Based on fire frequency analysis. Fire threatens WPTT with Naval canister in Loadout room	Table 6.3-10 (3)
51A-PROB-NVL-WP	Probability of NVL WP Cask in Process	4.00E-01	Probability a Naval canister in WP	N/A
51A-PWR-LOSS	Loss of Power	4.10E-06	Commercial power reliability requirement	N/A
51A-PWR-LOSS-2	Loss of Power	4.10E-06	Commercial power reliability requirement	N/A
51A-RHSLIFTNUMBER-000001	Number of RHS Lifts	2.00E+00	This value represents the number of lifts performed by the remote handling system during the process of sealing the WP.	N/A
51A-SLIDEGATECLOSES-CAN	Slide Gate Impact Damages Canister	0.00E+00	The port slide gate and the C TM bell slide gate are designed to operate with a low-torque motor that prevent crushing a canister, should the canister be in transit through the gate.	Section 6.0
51A-SPMRC-MILES-IN-IHF	Miles SPMRC travels in IHF	4.00E-02	This value represents the number of miles that the SPMRC will travel in the IHF during normal operations	N/A
51A-TRANSNSCTTLIFTNUMBER	Number of Crane Lifts	1.00E+00	Number of lifts by the 300-ton crane that could potentially drop an object on the TC while the cask is on the CTT	N/A
51A-WPTT-MILES-IN-IHF	Miles WPTT travels during transfer	4.00E-02	This value represents the number of miles that the WPTT will travel in the IHF during normal operations	N/A

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-WELD-DAMAGE	Weld Generates Sufficient Heat to Damage Canister	0.00E+00	Welder malfunction during the inner lid or outer lid welding. Since the welder can not generate sufficient heat to damage the WP, a value of 0.00 is assigned to the event.	N/A
NUM_NVL	Number of Naval Casks	4.00E+02	Number of naval TC processed by the IHF over the preclosure period.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
NUMBER-NAVAL-CANISTERS	Number of Naval Canisters	4.00E+02	400 naval TC containing a single canister will be processed by the IHF over the preclosure period.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
NUM-HLW-CAN	Number of HLW canisters received at IHF over the preclosure period	1.00E+03	There will be 500 single canisters and 100 multi-pack HLW TCs containing up to 5 canisters at the IHF for a total of 1000 canisters.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
NUM-HLW-CSK	Number of HLW casks received during preclosure period	6.00E+02	The total number of HLW TCs processed by the IHF over the preclosure period.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
NUM-HLW-WP	Number of HLW WPs processed over the preclosure period.	2.00E+02	200 HLW WP will be processed by the IHF over the preclosure period.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
NUM-NVL	Number of Naval casks received at IHF over the preclosure period.	4.00E+02	400 naval TCs will be processed over the preclosure period.	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
SHIELD-BELL-DROPS-SUBSUM	Shield bell drops addressed in general CTM drop Events	0.00E+00	Added to the fault trees for completeness.	N/A
NVL-SHIELDING-FAILS5	Naval Trans Cask Shielding Fails--Drops	1.00E-05	PEFA for naval TC shielding failure for drops	Table 6.3-7
NVL-SHIELDING-FAILS8	Naval Trans Cask Shielding Fails--Collisions	1.00E-08	PEFA for naval TC shielding failure for Collisions	Table 6.3-7
HLW-SHIELDING-FAILS5	HLW Trans Cask Shielding Fails--Drops	1.00E-05	PEFA for HLW TC shielding failure for drops	Table 6.3-7
HLW-SHIELDING-FAILS8	HLW Trans Cask Shielding Fails--Collisions	1.00E-08	PEFA for HLW TC shielding failure for collisions	Table 6.3-7
51A-MOD-FIRE-HLW-NOIMP	Moderator Has No Impact on Criticality for HLW	0.00E+00	A moderator source has no impact on HLW—can not critically. Probability set to 0.00	N/A

Table 6.3-11. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
MOD-NOFIRE-HLW-NOIMP	Moderator Has No Criticality Impact on HLW	0.00E+00	A moderator source has no impact on HLW—no criticality. Probability set to 0.00	N/A
51A-MODERATOR-ENTERS-CAN	Moderator Enters Canister in a Fire	1.000E+00	A moderator source enters naval canister during a facility fire.	N/A
51A-PERCENT-RC-RECEIPT	Percentage of time Naval Canister is Received on SPMRC	1.000E+00	All naval waste packages will arrive at the IHF on the SPMRC	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)
51A-PERCENT-TT-RECEIPT	Percentage of time Naval Canister is Received on TT	0.000E+00	No Naval waste packages will arrive at the IHF on the SPMITT	000-PSA-MGR0-01800-000-00A (Ref. 2.2.26)

NOTE: IHF =Initial Handling Facility; CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high-level radioactive waste; SPMRC = site prime mover railcar; SPMITT = site prime mover truck trailer; RHS = remote handling system; SD = shield doors; TC = transportation cask; WP =waste package; WPTT = waste package transfer trolley.

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 detailed description of the HRA is presented in Attachment E.

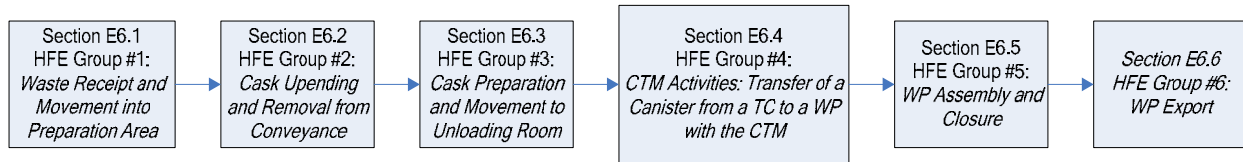
6.4.1 HRA Scope

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 IHF 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 IHF operations were broken into six separate operational steps, as depicted in Figure 6.4-1.



NOTE: CTM = canister transfer machine; HFE =human failure event; TC = transportation cask; WP = waste package.

Source: Original.

Figure 6.4-1. Initial Handling Facility 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 HFES¹:
 - 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 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

¹ Terminology common to nuclear power plants refer to post-initiator non-recovery events as Type C events and recovery events as Type CR events.

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 with 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 phases.

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 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. 2.2.48)*
- *Control of Heavy Loads at Nuclear Power Plants, NUREG-0612 (Ref. 2.2.58)*
- Naval Facilities Engineering Command (NAVFAC) Internet Web Site, Navy Crane Center. The database includes the following information:
 - Naval Crane Center Quarterly Reports (“Crane Corner”) 2001 through 2007
 - Naval Crane Center Fiscal Year 2006 Crane Safety Reports (covers fiscal year 2001 through 2006)
 - Naval Crane Center Fiscal Year 2006 Audit Report
- DOE Occurrence Reporting and Processing System (ORPS) Internet Web Site, Operational Experience Summaries (2002 through 2007)

- Institute of Nuclear Power Operations (INPO) database. 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 independent spent fuel storage installation events (1994 through 2007) 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.

Post-Initiator, Non-Recovery HFEs

Post-initiator, non-recovery 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 an operator's failure to perform the proper action to mitigate the initiating event and/or the unavailability of automatic mitigation function 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. No post-initiator HFEs were identified in this analysis.

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, an aggregated event 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 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 important to safety 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 (Ref. 2.2.47)
- HEART/NARA (Ref. 2.2.81)/(Ref. 2.2.35) THERP with some modifications (Ref. 2.2.77)
- ATHEANA's expert elicitation approach (Ref. 2.2.62).

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. 2.2.77), 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*. NUREG/CR-1278 (Ref. 2.2.77), 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. 2.2.77) 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. 2.2.35). 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 IHF 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
51A-Liddisplace1-HFI-NOD	Operator inadvertently displaces cask lid during preparation activities	12	3	N/A ^b	N/A	Omitted from analysis
51A-OpCaskDrop01-HFI-NOD	Operator drops cask during cask preparation activities	N/A	3	N/A ^b	N/A	Omitted from analysis
51A-OpCICTMGate1-HFI-NOD	Operator inappropriately closes slide or port gate during vertical canister movement and continues lifting	7	4	1.00E-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
51A-OpCollide001-HFI-NOD	Operator causes low-speed collision of auxiliary vehicle with RC, TT, or CTT	1, 2, 3, 4	2, 3	3.00E-03	5	Preliminary
51A-OpCranelntfr-HFI-NOD	Operator causes WP handling crane to interfere with TEV or WPTT	11	6	1.00E-04	10	Preliminary
51A-OpCTCollide2-HFI-NOD	Operator causes low-speed collision of CTT during transfer from preparation station to Cask Unloading Room	5	3	1.00E-03	5	Preliminary
51A-OpCTMDrInt01-HFI-COD	Operator lifts object or canister too high with CTM (two-block)	7	4	1.0	N/A	Preliminary
51A-OpCTMdrop001-HFI-COD	Operator drops object onto canister during CTM operations	7	4	4.00E-07	10	Detailed
51A-OpCTMdrop002-HFI-COD	Operator drops canister during CTM operations	7	4	2.00E-04	10	Detailed
51A-OpCTMImpact1-HFI-COD	Operator moves the CTM while canister or object is below or between levels	7	4	1.00E-03	5	Preliminary
51A-OpCTMImpact2-HFI-COD	Operator causes canister impact with lid during CTM operations (HLW)	7	4	N/A ^b	N/A	Omitted from analysis
51A-OpCTMImpact5-HFI-COD	Operator causes canister impact with SSC during CTM operations (all)	7	4	1.0	N/A	Preliminary
51A-OpCTTImpact1-HFI-NOD	Operator causes an impact between cask and SSC due to crane operations	1, 2, 3, 4	2, 3	3.00E-03	5	Preliminary
51A-OpDirExpose1-HFI-NOD	Operator causes direct exposure during CTM activities (all waste forms)	12	4	1.0	N/A	Preliminary
51A-OpDirExpose2-HFI-NOD	Operator causes direct exposure during CTM activities (transfer into a WP)	12	4	1.00E-04	10	Preliminary
51A-OpDirExpose3-HFI-NOD	Operator causes direct exposure during TEV loading	12	6	3.00E-05	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
51A-OpFailRstInt-HFI-NOM	Operator fails to restore interlock after maintenance	12	4, 6	1.00E-02	3	Preliminary
51A-OpFailSG-HFI-NOD	Operator fails to close the CTM slide gate before lifting shield skirt (while the canister is inside the bell; direct exposure)	12	4	1.00E-3	5	Preliminary
51A-OpFLCollide1-HFI-NOD	Operator causes high-speed collision of auxiliary vehicle with RC, TT, or CTT	1, 2, 3, 4	2, 3	1.0	N/A	Preliminary
51A-OpImpact0000-HFI-NOD	Operator causes impact of cask during transfer from preparation station to Cask Unloading Room	5	3	N/A ^b	N/A	Omitted from analysis
51A-OpNoDiscoAir-HFI-NOD	Operator fails to disconnect air supply from CTT in the Cask Unloading Room	7	4	1.00E-03	5	Preliminary
51A-OpNoUnBolt00-HFI-NOD	Operator fails to fully unbolt the cask lid before moving CTT into the Cask Unloading Room (HLW)	7	4	1.00E-03	5	Preliminary
51A-OpNoUnBoltDP-HFI-NOD	Operator fails to fully unbolt the cask lid before moving CTT into the Cask Unloading Room (naval cask)	7	4	N/A ^b	N/A	Omitted from analysis
51A-OpNVYShield1-HFI-COW	Operator inappropriately removes naval shield ring (direct exposure)	12	3	3.00E-04	5	Preliminary
51A-OpRCCollide1-HFI-NOD	Operator causes low-speed collision between RC and facility SSCs	1	1	3.00E-03	5	Preliminary
51A-OpRCIntCol01-HFI-NOD	Operator causes high-speed collision between RC and facility SSCs	1	1	1.0	N/A	Preliminary
51A-OpRCIntCol2-HFI-NOD	Operator causes MAP to collide into RC	1	1	1.0	N/A	Preliminary
51A-OpSDClose001-HFI-NOD	Operator closes shield door on waste form in conveyance	6	OA (1, 3, 6)	1.0	N/A	Preliminary
51A-OpShieldRing-HFI-NOD	Operator fails to install WP shield ring in WPTT (direct exposure)	12	6	1.00E-04	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
51A-OpSpurMove01-HFI-NOD	Operator causes spurious movement of CTT in the Cask Preparation Area	1, 2, 3, 4	2, 3	1.00E-04	10	Preliminary
51A-OpTEVDrClod-HFI-NOD	Operator begins WP extraction before TEV doors open	11	6	1.00E-03	5	Preliminary
51A-OpTiltDown01-HFI-NOD	Operator prematurely tilts down the WPTT	7, 8, 10	4, 5, 6	1.0	N/A	Preliminary
51A-OpTipover001-HFI-NOD	Operator causes cask to tip over during cask upending and removal	1, 2	2	1.00E-04	10	Preliminary
51A-OpTipover002-HFI-NOD	Operator causes cask to tip over during cask preparation activities	3, 4	3	1.00E-04	10	Preliminary
51A-OpTTCollide1-HFI-NOD	Operator causes low-speed collision between TT and facility SSCs	1	1	3.00E-03	5	Preliminary
51A-OpTTIntCol01-HFI-NOD	Operator causes high-speed collision between TT and facility SSCs	1	1	1.0	N/A	Preliminary
51A-OpTTIntCol2-HFI-NOD	Operator causes MAP to collide into TT	1	1	1.0	N/A	Preliminary
51A-OpTTRollover-HFI-NOD	Operator causes rollover of TT	1	1	N/A ^b	N/A	Omitted from analysis
51A-OpWPCollide1-HFI-NOD	Operator causes low-speed collision of WPTT into SSC	8, 10	5, 6	3.00E-03	5	Preliminary
51A-OpWPInnerLid-HFI-NOD	Operator causes direct exposure during WP loading	12	5	1.00E-04	10	Preliminary
51A-OpWPTiltUp01-HFI-NOD	Operator prematurely tilts up the WPTT	11	6	1.0	N/A	Preliminary
51A-OpWPTTSpur01-HFI-NOD	Operator causes spurious movement of WPTT during canister loading	7	4	1.00E-03	5	Preliminary
Crane drops	Operator drops cask or drops object onto cask during crane operations	1, 2, 3, 4, 9, 11	2, 3, 5, 6	N/A ^{a, b}	n/a	Historic data

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
Improper WP closure	Operator damages canister or fails to properly weld the WP	9	5	N/A ^b	N/A	Omitted from analysis
Load too heavy	Operator causes drop of cask by attempting to lift a load that is too heavy for the crane	N/A	OA	N/A ^b	N/A	Omitted from analysis
Moderator introduced into moderator-controlled area	Operator introduces moderator into a moderator-controlled area of the IHF	N/A	OA	N/A ^b	N/A	Omitted from analysis
RC derailment	Operator causes the RC to derail	1	1	N/A ^{a, b}	N/A	Historic data
Spurious movement of CTT during CTM activities	Operator causes spurious movement of the CTT during CTM activities	7	4	N/A ^b	N/A	Omitted from analysis
TEV Collision	Operator causes TEV to collide with WP or WPTT	11	6	N/A ^b	N/A	Omitted from analysis
WPTT derailment	Operator causes WPTT to derail	8, 10	5, 6	N/A ^{a, b}	N/A	Historic data
WPTT uncontrolled tilt-down	Operator causes an uncontrolled tilt down of the WPTT	10	6	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 is rather addressed in Attachment C, Section C1.3.

^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.

CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HFE = human failure event; HLW = high-level radioactive waste; IHF = Initial Handling Facility; MAP = mobile access platform; N/A = not applicable; OA = over arching (applies to multiple HFE groups); RC = railcar; SSC = structure, system, or component; SSCs = structures, systems, and components; TEV = transport and emplacement vehicle; TT = truck trailer; WP = waste package; WPTT = waste package transfer trolley.

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 is evaluated as to fire vulnerability, and fragility analyses are conducted as needed (Section 6.3.2 and Attachment D).

Fire initiating event frequencies have been calculated for each initiating event identified for the IHF. 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 room areas of the IHF are 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 1.35 is obtained for the IHF (Attachment F, Table F5.2-1). The results of this portion of the analysis are summarized in Table 6.5-1.

As discussed in Sections F4.3.2.1, F5.3, and F5.4 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 (m ²)	Room	Area (m ²)
1001	158	1019	16
1002	502	1020	8
1003	41	1021	10
1200 through 1225	694	1022/24/2024	31
1005	467	1023	184
1006	134	1026	40
1007	172	1027	111
1008	86	2001/2010	218
1009	172	2002	58
1012/1011	1301	2003	307
1013	7	2004	149
1014	18	2005	304
1015/31/30/2009/15	69	2006	220
1016/2016	33	2007	23
1017/2017	61	2008	7
1018/2018	56		
Total Area (sq-m)			5.66E+03
Ignition Frequency (per sq-m/yr)			4.79E-06
Ignition Frequency (per yr)			2.71E-02
Ignition Frequency (over 50-year operating life)			1.35E+00

NOTE: m = meter; sq = square; 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
1001		6					1
1002	95	4					2
1003	2						
1200 through 1225		2				9	
1005	1	2	12.04	5			2
1006			4.88				1
1007			0.08				1
1008			1.03				1
1009				5			2
1012/1011	1	4	23.97	15	100		4
1013	1						
1015/31/30/200 9/15			1				
1016/2016							
1017/2017							
1018/2018							
1019			1				
1020			1				
1021			1				
1022/24/2024			1				
1023	15		4	400			
1026							
1027							
2001	6	2				1	
2002	13						1
2003		3					1
2004			6	117			2

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
2005	1		7				1
2006	1						1
2007	1						
2008							
TOTAL	137	23	64	542	100	10	20

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 event 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 operating life of the surface facilities, and are summarized in Table 6.5-3.

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 preclosure 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 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, Sections F5.6 and F5.8). This software requires input of two parameters (e.g., in the lognormal case, 50% and 97.5% values), and the figures that the simulation will produce results for (initiating event frequencies). 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. This is set within the software to be done 10,000 times to ensure accurate results. 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 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 6.5-3. Residence Fractions

Initiating Event	Residence Fraction
Waste Form in WPTT in Loadout Room	
WP/Naval SNF in WPTT in Loadout Room	5.8E-06
WP/HLW in WPTT in Loadout Room	5.8E-06
Waste Form in WP in TEV in Loadout Room	
WP/Naval SNF in WPTT in TEV in Loadout Room	1.0E-06
WP/HLW in WPTT in TEV in Loadout Room	1.0E-06
Waste Form in Unloading Room	
TC/Naval SNF in Unloading Room	3.2E-06
Threatens TC/HLW in Unloading Room	6.0E-06
Waste Form in Positioning and Closure Rooms	
WP/Naval SNF in Positioning and Closure Rooms	2.7E-04
WP/HLW in Positioning and Closure Rooms	2.7E-04
Waste Form in Loading Room	
WP/Naval SNF in Loading Room	6.2E-06
Threatens WP/HLW in Loading Room	2.0E-04
Waste Form in CTT in Cask Preparation Area	
TC/Naval SNF in CTT in Cask Preparation Area	2.3E-05
TC/HLW in CTT in Cask Preparation Area	9.6E-06
Waste Form on Railcar in the Cask Preparation Area w/ SPM (Diesel Present)	
TC/Naval SNF on Railcar in the Cask Preparation Area w/ SPM (Diesel Present)	1.8E-06
TC/HLW on Railcar in the Cask Preparation Area w/ SPM (Diesel Present)	1.2E-06
Waste Form on Railcar in the Cask Preparation Area w/o SPM (No Diesel Present)	
TC/Naval SNF on Railcar in the Cask Preparation Area w/o SPM (No Diesel Present)	2.0E-5
TC/HLW on Railcar in the Cask Preparation Area w/o SPM (No Diesel Present)	9.4E-06

Table 6.5-3. Residence Fractions (Continued)

Initiating Event	Residence Fraction
Waste Form in CTM in Transfer Room	
Naval SNF in CTM in Transfer Room	1.3E-06
HLW in CTM in Transfer Room	1.1E-06
Large Fire Residence Categories	
TC/Naval SNF w/ SPM (Diesel Present)	1.8E-06
TC/Naval SNF w/o SPM (No Diesel Present)	4.6E-05
Naval SNF in CTM	9.5E-07
Naval SNF in WP	2.8E-04
TC/HLW w/ SPM (Diesel Present)	1.2E-06
TC/HLW w/o SPM (No Diesel Present)	2.4E-05
HLW in CTM	7.4E-06
HLW in WP	4.8E-04

NOTE: CTT = cask transfer trolley; CTM = canister transfer machine; HLW = high-level radioactive waste; SNF = spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transportation emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Tables F5.7-1 and F5.7-2 of Attachment F.

Table 6.5-4. Results from Monte Carlo Simulation of Fire Initiating Event Frequency Distributions

Initiating Event	Equipment	Mean	Median	97.5% Value	EF	Type
Localized Fire Threatens Waste Form in WPTT in Loadout Room	WPTT					
Localized Fire Threatens WP/NSNF in WPTT in Loadout Room		4.9E-07	4.5E-07	1.1E-06	2.1E+00	Lognormal
Localized Fire Threatens WP/HLW in WPTT in Loadout Room		4.9E-07	4.5E-07	1.1E-06	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in WP in TEV Loadout Room	TEV					
Localized Fire Threatens WP/NSNF in TEV in Loadout Room		8.8E-08	7.9E-08	1.9E-07	2.1E+00	Lognormal
Localized Fire Threatens WP/HLW in TEV in Loadout Room		8.8E-08	7.9E-08	1.9E-07	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in Unloading Room	CTT					
Localized Fire Threatens TC/NSNF in Unloading Room		1.2E-08	1.1E-08	2.7E-08	2.2E+00	Lognormal

Table 6.5-4. Results from Monte Carlo Simulation of Fire Initiating Event Frequency Distributions
(Continued)

Initiating Event	Equipment	Mean	Median	97.5% Value	EF	Type
Localized Fire Threatens TC/HLW in Unloading Room		2.2E-08	2.0E-08	5.1E-08	2.2E+00	Lognormal
Localized Fire Threatens Waste Form in Positioning Room	WPTT					
Localized Fire Threatens WP/NSNF in Positioning Room		3.8E-05	3.4E-05	8.3E-05	2.1E+00	Lognormal
Localized Fire Threatens WP/HLW in Positioning Room		3.8E-05	3.4E-05	8.4E-05	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in Loading Room	WPTT					
Localized Fire Threatens WP/NSNF in Loading Room		3.5E-07	3.1E-07	8.5E-07	2.3E+00	Lognormal
Localized Fire Threatens WP/HLW in Loading Room		1.2E-05	1.0E-05	2.8E-05	2.3E+00	Lognormal
Localized Fire Threatens Waste Form in CTT in Cask Preparation Area	CTT					
Localized Fire Threatens TC/NSNF in CTT in Cask Preparation Area		1.3E-06	1.1E-06	3.1E-06	2.3E+00	Lognormal
Localized Fire Threatens TC/HLW in CTT in Cask Preparation Area		5.3E-07	4.6E-07	1.3E-06	2.3E+00	Lognormal
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/SPM (Diesel Present)	RC					
Localized Fire Threatens TC/NSNF on railcar in the Cask Preparation Area w/SPM (diesel present)		2.3E-07	2.1E-07	5.1E-07	2.1E+00	Lognormal
Localized Fire Threatens TC/HLW on railcar in the Cask Preparation Area w/SPM (diesel present)		1.5E-07	1.4E-07	3.5E-07	2.1E+00	Lognormal
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/o SPM (No Diesel Present)	RC					
Localized Fire Threatens TC/NSNF on railcar in the Cask Preparation Area w/o SPM (no diesel present)		2.0E-06	1.8E-06	4.5E-06	2.2E+00	Lognormal
Localized fire threatens TC/HLW on railcar in the Cask Preparation Area w/o SPM (no diesel present)		9.3E-07	8.3E-07	2.1E-06	2.2E+00	Lognormal
Localized Fire Threatens Waste Form in CTM in Transfer Room	CTM					

Table 6.5-4. Results from Monte Carlo Simulation of Fire Initiating Event Frequency Distributions
(Continued)

Initiating Event	Equipment	Mean	Median	97.5% Value	EF	Type
Localized Fire Threatens NSNF in CTM in Transfer Room		8.1E-08	7.1E-08	1.9E-07	2.3E+00	Lognormal
Localized Fire Threatens HLW in CTM in Transfer Room		6.9E-08	6.1E-08	1.7E-07	2.2E+00	Lognormal
Large Fire Threatens TC/NSNF (Diesel)	-	3.7E-07	3.3E-07	8.7E-07	2.2E+00	Lognormal
Large Fire Threatens TC/NSNF (No Diesel)	-	9.7E-06	8.6E-06	2.3E-05	2.2E+00	Lognormal
Large Fire Threatens NSNF in CTM	-	2.0E-07	1.8E-07	4.7E-07	2.2E+00	Lognormal
Large Fire Threatens NSNF in WP	-	5.9E-05	5.3E-05	1.4E-04	2.2E+00	Lognormal
Large Fire Threatens TC/HLW (Diesel)	-	2.5E-07	2.2E-07	5.8E-07	2.2E+00	Lognormal
Large Fire Threatens TC/HLW (No Diesel)	-	5.1E-06	4.5E-06	1.2E-05	2.2E+00	Lognormal
Large Fire Threatens HLW in CTM	-	1.6E-06	1.4E-06	3.7E-06	2.2E+00	Lognormal
Large Fire Threatens HLW in WP	-	1.0E-04	9.1E-05	2.4E-04	2.2E+00	Lognormal

NOTE: CTT = cask transfer trolley; CTM = canister transfer machine; HLW = high-level radioactive waste; NSNF = naval spent nuclear fuel; RC = railcar; SPM = site prime mover; TC = transportation cask; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Table F5.7-6 of Attachment F.

Table 6.5-5 provides the fire analysis data for the basic events in this model.

Table 6.5-5. Basic Events Data Associated with Fire Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-HLW-FREQ WITH DIESEL	Relative Frequency with Diesel Present	2.30E-03	Based on the fire frequency analysis, this value represents relative frequency an HLW canister is possibly subjected to a large facility fire with diesel present.	Table 6.3-10 (13)
51A-HLW-FREQ-NO-DIESEL	Relative Frequency with no Diesel Present	4.67E-02	Based on the fire frequency analysis, this value represents the relative frequency an HLW canister is possibly subjected to a large facility fire without diesel present.	Table 6.3-10 (14)
51A-HLW-FREQ-WODIESEL	Relative Frequency of WP in Large Fire without Diesel	9.37E-01	Based on the fire frequency analysis, this value represents the relative frequency a WP is subject to a possible large facility fire without diesel present.	Table 6.3-10 (17)
51A-HLW-FREQ-WP-FAILS	Relative Frequency of WP in Large Fire	9.37E-01	Based on the fire frequency analysis. This value represents the fraction of time an HLW WP is in the IHF.	Table 6.3-10 (16)
51A-HLW-LARGE-FIRE-CTM	Relative Frequency of Large Fire in CTM	1.45E-02	Based on fire frequency analysis. Large facility fire threatens HLW canister inside the CTM.	Table 6.3-10 (15)
51A-PROB-HLWCAN-WP-LOR	Probability HLW Canister in WP in Loadout Room	1.51E-01	Based on fire frequency analysis. Fire threatens WP with HLW canister in Loadout room.	Table 6.3-10 (12)
51A-HLWSPMRC-DIESEL	Fire in Prep Area SPMRC with Diesel	9.61E-02	Based on the fire frequency analysis, this value represents the failure of the HLW canister in a Cask Prep Area fire when diesel is present.	Table 6.3-10 (9)
51A-HLWSPMRC-WODIESEL	Fire in Prep Area SPMRC Without Diesel	9.04E-01	Based on the fire frequency analysis, this value represents the failure of the HLW canister in a Cask Prep Area fire when no diesel is present on the SPMRC.	Table 6.3-10 (10)
51A-PROB-HLWCAN-WPTT-LOR	Probability HLW Canister in WPTT in Loadout Room	8.49E-01	Based on fire frequency analysis. Fire threatens WPTT with HLW canister in Loadout room	Table 6.3-10 (11)
51A-NVL-FREQ-DIESEL	Relative Frequency with Diesel Present	5.35E-03	Based on the fire frequency analysis. Large facility fire when diesel is present threatens naval cask inside the IHF.	Table 6.3-10 (5)

Table 6.5-5. Basic Events Data Associated with Fire Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
51A-NVL-FREQ-NO-DIESEL	Relative Frequency without Diesel Present	1.39E-01	Based on the fire frequency analysis. Large facility fire when no diesel is present threatens naval cask inside the IHF.	Table 6.3-10 (6)
51A-NVL-FREQ-WP-FAILS	Relative Frequency WP Fails due to Fire	8.53E-01	Based on fire frequency analysis. Large facility fire threatens naval canister inside the IHF.	Table 6.3-10 (8)
51A-NVL-LARGE-FIRE-CTM	Relative Frequency of Large Fire in CTM	2.91E-03	Based on fire frequency analysis. Large facility fire threatens naval canister inside the CTM.	Table 6.3-10 (7)
51A-NVL-SPMRC-WODIESEL	Fire in Preparation Area without Diesel	9.35E-01	Based on Fire frequency analysis. Fire threatens naval transportation cask after SPM has left cask preparation room.	Table 6.3-10 (2)
51A-NVL-SPMRC-DIESEL	Fire in Preparation Area SPMRC with Diesel	6.53E-02	Based on Fire frequency analysis. Fire threatens naval transportation cask while SPM is present in cask preparation room.	Table 6.3-10 (1)
51A-PROB-NVLCAN-WP-LOR	Probability NVL Canister in WP in Loadout Room	1.51E-01	Based on fire frequency analysis. Fire threatens WP with Naval canister in Loadout room.	Table 6.3-10 (4)
51A-PROB-NVLCAN-WPTT-LOR	Probability NVL Canister in WPTT in Loadout Room	8.49E-01	Based on fire frequency analysis. Fire threatens WPTT with Naval canister in Loadout room.	Table 6.3-10 (3)

NOTE: IHF = Initial Handling Facility; CTM = canister transfer machine; HLW = high-level radioactive waste; SPMRC = site prime m over railcar;
TC= transportation cask; WP =waste package; WPTT = waste package transfer trolley.

Source: Original

6.6 NOT USED

6.7 EVENT SEQUENCE FREQUENCY RESULTS

This section discusses the results of the event sequence quantification as produced from the SAPHIRE (Ref. 2.2.70) 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 four tables 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) (Ref. 2.2.70). In SAPHIRE, the quantification of an event sequence is always labeled as a “frequency” in the output formats. The quantification also includes the results of the uncertainty analysis of the number of occurrences.

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 naval SNF canister by a CTM in the IHF 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 naval SNF canister during its transfer by the CTM in the IHF, or the probability of occurrence of a fire that could affect the 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 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 human failure events 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 (Ref. 2.2.70) 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 it occurs, will cause the event sequence to occur. The event sequence frequency is calculated as the sum of frequencies of the cut sets. For computational efficiency, minimal cut sets that have a frequency less than a cutoff value of 10^{-12} are not calculated by SAPHIRE. Such minimal cut sets are insignificant contributors to the number of occurrences of the event sequence over the preclosure period. This value is considered sufficient to ensure that all significant contributors are identified because it would require the sum of 1×10^8 cut sets with a probability of occurrence of 1×10^{-12} over the preclosure period to reach the Category 2 threshold frequency of 1×10^{-4} over the preclosure period.

As an illustration of the above process, the quantification of the event sequence initiated by a drop of a HLW canister during a transfer in the IHF, 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. For IHF, the HVAC system is not required as an ITS system, and is modeled with a failure probability of 1.0.

The event sequence, which leads to an unfiltered radionuclide release that is not important to criticality, starts with an initiator event tree that depicts the number of HLW canisters that are transferred by the CTM in the IHF over the preclosure period. Based on *Waste Form Throughputs for Preclosure Safety Analysis* (Ref. 2.2.26, Table 4), there are 1,000 such transfers. Next, the branch on the initiator event tree that deals with the drop of a canister is selected. In practice, this is done by SAPHIRE through the use of rules, which are assigned to the pivotal event called "INIT-EVENT," the fault tree whose top event models the probability of a HLW canister drop. Multiplying the number of HLW canister transfers by the probability of a drop yields the number of occurrences, over the preclosure period, of the initiating event for the event sequence considered.

SAPHIRE (Ref. 2.2.70) continues the construction of event sequence logic via a transfer to the system-response event tree which provides the basis for quantifying the rest of the event sequence through the use of the pivotal events described in Section 6.1 and Attachment B. First, the breach of the canister, given its drop, is evaluated under the pivotal event called “CANISTER”. SAPHIRE rules are used to ensure that the probability assigned to this pivotal event pertains to the waste form considered in this event sequence—a HLW canister. The next event that appears in the system-response event tree is called “SHIELDING”. This pivotal event has a probability of one, indicating that a loss of shielding is considered to occur if the canister breaches. This modeling conforms to the approach taken in the PCSA, where event sequences that lead to a radionuclide release also embed direct exposure of personnel to radiation that could result from a loss of shielding. The next pivotal event is called “CONFINEMENT.” This event models the failure of HVAC to maintain confinement and perform filtering of the radionuclide release. This pivotal event is quantified with a fault tree. The mission time for the system is 720 hrs (i.e., 30 days). Finally, the last pivotal event is called “MODERATOR.” This event models moderator intrusion into the breached canister. In the event sequence analyzed, no moderator entry occurs, that is, the success branch is followed.

The SAPHIRE event sequence quantification report includes the number of occurrences of each cut set that contributes to an event sequence and the summation over the cut set to yield a number of occurrences of the event sequence over the preclosure period. The internal processes of SAPHIRE provide quantification of cut sets that represent combinations of basic events from respective initiating event trees and pivotal event trees. The summation over such cut sets represents the cumulative frequency of an initiating event (e.g., drop), containment (e.g., canister) breach, confinement unavailability, and moderator availability.

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 (Ref. 2.2.70). 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) standard deviation (i.e., 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 (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 (Ref. 2.3.2), which is performed in *Preclosure Consequence Analyses* (Ref. 2.2.31). Event sequences with a frequency of occurrence less than one chance in 10,000 of occurring before permanent closure of the repository are designated 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 that may occur anywhere within the GROA (Ref. 2.2.31, Table 2 and Section 7). Therefore, dose consequences are determined for a bounding set of postulated Category 2 event sequences, as shown in Table 6.8-1. Because all waste form types and configurations that are applicable to the repository are included in Table 6.8-1, some of the bounding event sequences do not apply to the present analysis. 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 ensuring 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	Breach of uncanistered commercial SNF assembly in pool (one drops onto another)	2 PWR or 2 BWR commercial SNF
2-12*	Uncanistered commercial SNF	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 and noncombustible 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: 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; TAD = transportation, aging and disposal canister. Items marked with an asterisk (*) are not applicable to the IHF.

Source: *Preclosure Consequence Analyses* (Ref. 2.2.31, 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 IHF. 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 for the IHF are as follows.

- Waste package
- Naval SNF canister, by itself or in a transportation cask
- HLW canister, by itself or in a transportation cask.

In SAPHIRE (Ref. 2.2.70), 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 non-minimal 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 in the IHF are partitioned among seven different initiating events such as canister drop, collision, drop of a heavy load on the canister, etc. 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 HLW 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 HLW 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 recalculate 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 calculated 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 frequency or 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 HLW canister drops in the IHF over the preclosure period is essentially controlled, among other things, by the number of HLW 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 to represent the frequency or expected number of occurrences of a given event sequence over the preclosure period, 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 (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 (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, $P = 1 - \exp(-m)$ (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 the Monte Carlo technique 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 the event sequence is based upon the expected number of occurrences over the preclosure period given 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 IHF (Attachment G, Table G-2). Following the final categorization, the event sequences for the respective Category 2 (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) event sequences for the IHF. 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. 2.2.31, 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	Standard Dev	Event Sequence Category	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 Category	Basis for Categorization	Consequence Analysis ¹
ESD12B-NVL-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during preparation activities of a transportation cask containing a naval SNF canister, or during assembly and closure of a waste package containing a naval SNF canister. In this sequence there are no pivotal events	1 naval SNF canister	2.E-01	1.E-01	1.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
ESD07-HLW-SEQ5-RRU	Radionuclide release, unfiltered	This event sequence represents a structural challenge to an HLW canister, during canister transfer by the CTM, resulting in an unfiltered radionuclide release. In this sequence the canister fails, the confinement boundary is not relied upon, and a moderator is excluded from entering the canister.	2 HLW canisters	6.E-02	4.E-02	7.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	2-04
ESD12B-HLW-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during assembly and closure of a waste package containing HLW canisters. In this sequence there are no pivotal events.	5 HLW canisters	4.E-02	4.E-02	2.E-08	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 Category	Basis for Categorization	Consequence Analysis ¹
ESD13-NVL-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a naval SNF canister inside a transportation cask, 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 naval SNF canister	3.E-02	3.E-02	1.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A ²
ESD12C-NVL-SEQ3-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during export of a waste package containing a naval SNF canister. In this sequence there are no pivotal events.	1 naval SNF canister	1.E-02	4.E-03	2.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A ²
ESD12C-HLW-SEQ3-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure during export of a waste package containing HLW canisters. In this sequence there are no pivotal events.	5 HLW canisters	6.E-03	2.E-03	1.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A ²
ESD12A-HLW-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a temporary loss of shielding during CTM operations, while an HLW canister is being transferred. In this sequence there are no pivotal events.	5 HLW canisters	2.E-03	2.E-03	1.E-03	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 Category	Basis for Categorization	Consequence Analysis ¹
ESD12A-NVL-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a temporary loss of shielding during CTM operations, while a naval SNF canister is being transferred. In this sequence there are no pivotal events.	1 naval SNF canister	7.E-04	6.E-04	4.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	N/A ²
ESD13-HLW-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to an HLW canister inside a transportation cask, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence the canister remains intact, and the shielding fails.	5 HLW canisters	7.E-04	6.E-04	3.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	N/A ²

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. 2.2.31, 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. 2.2.18)).

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; DSTD = DOE standardized canister; HLW = high-level radioactive waste; MCO = multicanister overpack; RHS = remote handling system; ST = site transporter; TC = transportation cask; WP = waste package; WPTT = waste package transport trolley.

Source: Original

6.9 IMPORTANT TO 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 unacceptable performance
- 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. 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.

6.9.1 Important to Safety Structures, Systems, and Components

Table 6.9-1 contains the nuclear safety design bases for the IHF ITS SSCs. The event sequence column identifies a representative event sequence that is affiliated with each ITS SSC.

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. The event sequence column identifies a representative event sequence that relies upon the PSC.

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source		
			Safety Function	Controlling Parameters and Values				
DOE And Commercial Waste Package System	DOE and commercial waste package	Entire	Provide containment	1. The mean conditional probability of breach of a sealed waste package resulting from a side impact shall be less than or equal to 1E-08 per impact.	IHF-ESD-11-HLW (Seq. 4-6)	51A-HLW-IMPACT-WP		
				2. The mean conditional probability of breach of a sealed waste package resulting from a drop of a load onto the waste package shall be less than or equal to 1E-05 per drop.			IHF-ESD-11-HLW (Seq. 3-6)	51A-HLW-WP-FAILS-DROPON
				3. The mean conditional probability of breach of a sealed waste package resulting from an end-on impact or collision shall be less than or equal to 1E-05 per impact.				
	HLW	HLW canister	Provide containment	4. The mean conditional probability of breach of an HLW canister resulting from a drop of the canister shall be less than or equal to 3E-02 per drop.	IHF-ESD-07-HLW (Seq. 4-5)	51A-HLW-CAN-FAIL-DROP		
				5. The mean conditional probability of breach of an HLW canister resulting from a side impact or collision shall be less than or equal to 1E-08 per impact.			IHF-ESD-07-HLW (Seq. 7-5)	51A-HLW-CAN-FAIL-COLL
				6. The mean conditional probability of breach of an HLW canister contained within a waste package resulting from the spectrum of fires ^d shall be less than or equal to 3E-04 per fire event.				

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source				
			Safety Function	Controlling Parameters and Values						
Initial Handling Facility		Shield doors (including anchorages)	Protect against ^a direct exposure of personnel	7. The mean conditional probability of breach of an HLW canister contained within a cask resulting from the spectrum of fires shall be less than or equal to 2E-06 per fire event.	IHF-ESD-13-HLW-WP (Seq. 5-5)	51A-PMRC-FAIL-CAN-DIESEL				
				8. The mean conditional probability of breach of an HLW canister located within the CTM shield bell resulting from the spectrum of fires shall be less than or equal to 1E-04 per fire event.	IHF-ESD-13-HLW-WP (Seq. 5-5)	51A-HLW-CAN-CONT-CTM-FIR				
				9. The mean conditional probability of breach of an HLW canister, given the drop of another HLW canister onto the first canister, shall be less than or equal to 3E-02 per drop.	IHF-ESD-07-HLW (Seq. 2-5)	51A-HLW-CAN-FAIL-DROP				
				10. Equipment and personnel shield doors shall have a mean probability of inadvertent opening of less than or equal to 1E-06 per transfer.	IHF-ESD-12A-HLW (Seq. 2)	51A-SHLD-DR-DIRCT-EXP				
				11. An equipment shield door falling onto a waste container as a result of an impact from a conveyance shall be precluded.	Initiating event does not require further analysis. ^c	Table 6.0-2				
				12. The mean probability of a canister drop resulting from a spurious closure of the slide gate shall be less than or equal to 2E-06 per transfer.	IHF-ESD-07-HLW (Seq. 4-5)	GATE-36-109 of 51A-CTM-DROP				
				Cask Port Slide Gate (51A-HTC0-HTCH-00001)		Protect against dropping a canister due to spurious closure of the slide gate	Protect against dropping a canister due to spurious closure of the slide gate			

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source			
			Safety Function	Controlling Parameters and Values					
Mechanical handling system	Cask handling	Waste Package Port Slide Gate (51A-HTC0-HTCH-00002)	Protect against direct exposure to personnel	13. The mean probability of inadvertent opening of a slide gate shall be less than or equal to 1E-09 ^b per transfer.	IHF-ESD-12A-HLW (Seq. 2)	51A-SLIDE-GATE-DIR-EX			
			Preclude canister breach	14. Closure of the slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis. ^c	Table 6.0-2			
			Protect against dropping a canister due to a spurious closure of the slide gate	15. The mean probability of a canister drop resulting from a spurious closure of the slide gate shall be less than or equal to 4E-09 per transfer.	IHF-ESD-12A-HLW (Seq. 2)	51A-SLIDE-GATE-DIR-EX			
			Protect against direct exposure to personnel	16. The mean probability of inadvertent opening of a slide gate shall be less than or equal to 2E-06 per transfer.	IHF-ESD-12A-HLW (Seq. 2)	ESD12A-HLW-SHLD			
			Preclude canister breach	17. Closure of the slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis. ^c	Table 6.0-2			
			Preclude canister drop onto the floor	18. The waste package port slide gate shall be incapable of opening without a waste package transfer trolley with waste package in position to receive a canister.	Initiating event does not require further analysis. ^c	Table 6.0-2			
			Provide containment	19. The mean conditional probability of breach of a canister contained within a sealed cask resulting from a cask drop shall be less than or equal to 1E-05 per drop.	IHF-ESD-01-NVL (Seq. 3-6)	51A-NVL-TC-FAIL-DROP			
			Transportation cask (analyzed as a representative transportation cask)						

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				20. 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 1E-05 per drop.	IHF-ESD-01-NVL (Seq. 2-6)	51A-NVL-TC-FAIL-DROPON
				21. The mean conditional probability of breach of a canister contained within a sealed cask resulting from a side impact or collision shall be less than or equal to 1E-08 per impact.	IHF-ESD-04-NVL (Seq. 7-5)	51A-NVL-CAN-FAIL-SIMP
			Preclude lid contact with canisters	22. The geometry of the casks that carry HLW canisters shall preclude lid contact with canisters following a drop of a cask lid.	IHF-ESD-07-HLW (Seq. 2)	51A-HLW-CAN-FAIL-LID
			Protect against direct exposure to personnel	23. The mean conditional probability of loss of cask gamma shielding resulting from a drop of a cask shall be less than or equal to 1E-05 per drop.	IHF-ESD-02-HLW (Seq. 2-3)	HLW-SHIELDING-FAILS5
				24. 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 1E-08 per impact.	IHF-ESD-02-HLW (Seq. 5-3)	HLW-SHIELDING-FAILS8
				25. The mean conditional probability of loss of cask gamma shielding resulting from drop of a load onto a cask shall be less than or equal to 1E-05 per impact	IHF-ESD-02-HLW (Seq. 6-3)	HLW-SHIELDING-FAILS5

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Nuclear Safety Design Bases			Representative Event Sequence (Sequence Number)	Source
		Component	Safety Function	Controlling Parameters and Values		
		Site Prime Mover	Limit speed	26. The speed of the site prime mover shall be limited to 9 mi/hr.	IHF-ESD-01-HLW (Seq. 4-6)	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	27. The fuel tank of a site prime mover that enters the facility shall preclude fuel tank explosions.	Initiating event does not require further analysis. ^c	Table 6.0-2
		Cask Handling Yoke (51A-HM00-BEAM-00001)	Protect against drop	28. 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
		Cask Handling Crane; 300-ton (51A-HM00-CRN-00001)	Protect against drop	29. The mean probability of dropping a loaded transportation cask from less than two-block height resulting from the failure of a piece of equipment in the load-bearing path shall be less than or equal to 3E-05 per transfer.	IHF-ESD-02-HLW (Seq. 2-6)	51A-CRN3-DROPHLW-CRN-DRP
			Protect against drop	30. The mean probability of dropping a loaded cask from the two-block height resulting from the failure of a piece of equipment in the load-bearing path shall be less than or equal to 4E-07 per transfer.	IHF-ESD-02-HLW (Seq. 3-6)	51A-CRN3-2-BLOCK-CRN-TBK
			Limit drop height	31. The two-block drop height shall not exceed 40 ft from the bottom of the shortest cask to the floor.	IHF-ESD-02-HLW (Seq. 3-6)	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 IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Protect against drop of a load onto a cask	32. The mean probability of dropping a load onto a loaded cask or its contents shall be less than or equal to 3E-05 per cask handled.	IHF-ESD-02-HLW (Seq. 6-6)	51A-CRN3-DROPON-CRN-DRP
			Limit speed	33. The speed of the Cask Handling Crane trolley and bridge shall be limited to 20 ft/min.	IHF-ESD-02-HLW (Seq. 5-6)	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.)
		Cask transfer trolley (and pedestals) Trolley (51A-HM00-TRLY-00001) Cask Pedestals (51A-HM00-PED-00001-2)	Limit speed	34. The speed of the CTT shall be limited to 2.5 mi/hr.	IHF-ESD-05-HLW (Seq. 3-5)	This parameter limits the conditional probability of canister breach given a collision to the appropriate value from Table 6.3-7.
		Naval Cask Pedestal (51A-HM00-PED-00003)	Protect against spurious movement	35. 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 1E-09 ^b per transfer.	IHF-ESD-07-NVL (Seq. 3-5)	51A-7-CTT-SPURMOVE
		Cask preparation crane; 30-ton (51A-HM00-CRN-00002)	Protect against drop	36. The mean probability of a drop of a load onto a loaded cask shall be less than or equal to 3E-05 per transfer	IHF-ESD-04-NVL (Seq. 4-5)	51A-CRN3-DROPON-CRN-DRP

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
	Cask Handling/ Cask Receipt	Naval cask lift bail (51A-HMC0-BEAM-00001)	Protect against drop	37. The naval cask lift bail is an integral part of the load-bearing path. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements
		Naval cask lift plate (51A-HMC0-HEQ-00005)	Protect against drop	38. The naval cask lift plate 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 / Cask Preparation	Rail Cask Lid Adapters (51A-HMH0-HEQ-00002)	Protect against drop	39. The rail cask lid adapter is integral to the load-bearing path for the HLW rail cask lid. See Cask Handling Crane requirements.	See Cask Handling Crane requirements	See Cask Handling Crane requirements
	Waste Transfer/ Canister Transfer	Canister Transfer Machine (51A-HTC0-FHM-00001)	Protect against drop	40. The mean probability of drop of a canister from below the two-block height due to the failure of a piece of equipment in the load-bearing path shall be less than or equal to 2E-04 per transfer.	IHF-ESD-07-HLW (Seq. 4-5)	51A-CTM-DROP
			Protect against drop	41. The mean probability of drop of a canister from the two-block height due to the failure of a piece of equipment in the load-bearing path shall be less than or equal to 3E-08 per transfer.	IHF-ESD-07-HLW (Seq. 5-5)	CTM-2-BLOCK
			Limit drop height	42. The two-block drop height shall not exceed 40 ft from the bottom of a canister to the cavity floor of the transportation cask or waste package.	IHF-ESD-07-HLW (Seq. 5-5)	This parameter limits the conditional probability of canister breach given a two-block drop to the appropriate value from Table 6.3-7.

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Protect against drop of a load onto a canister	43. The mean probability of drop of a load onto a canister shall be less than or equal to 1E-03 per transfer by the CTM.	IHF-ESD-07-HLW (Seq. 2-5)	51A-CTM-HLW-DROPON
			Protect against spurious movement	44. The mean probability of spurious movement of the CTM while a canister is being lifted or lowered shall be less than or equal to 7E-09 ^b per transfer.	IHF-ESD-07-HLW (Seq. 3-5)	CTM-SHEAR
			Preclude canister breach	45. Closure of the CTM slide gate shall be incapable of breaching a canister.	Initiating event does not require further analysis. ^c	Table 6.0-2
			Preclude non-flat-bottom drop of a naval SNF canister	46. The CTM shall preclude non-flat-bottom drops of naval canisters.	Initiating event does not require further analysis. ^c	Table 6.0-2

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Protect against direct exposure of personnel	47. The mean probability of inadvertent radiation streaming due to 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 1E-04 per transfer.	IHF-ESD-12B-HLW (Seq. 2)	ESD12B-HLW-SHLD-RING
			Limit speed	48. The speed of the CTM trolley and bridge shall be limited to 20 ft/min.	IHF-ESD-07-HLW (Seq. 7-5)	This parameter limits the conditional probability of canister 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.)
			Protect against drop	49. The mean frequency of drop by the CTM of the naval SNF canister resulting in breach of the canister shall be less than or equal to 2E-05 over the preclosure period.	IHF-ESD-07-NVL (Seq. 4-5)	IHF-ESD-07-NVL (Seq. 4-5)
		CTM Grapple (51A-HTC0-HEQ-00001) Canister grapples (51A-HTC0-HEQ-00003, 51A-HTC0-HEQ-00004)	Protect against drop	50. The grapples are an integral part of the load-bearing path. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
			Protect against drop of a load onto a canister	51. The grapples are an integral part of the load-bearing path. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.
		Naval Canister Lifting Adapter (51A-HTC0-HEQ-00005)	Protect against drop of a canister	52. The naval canister lifting adapter is an integral part of the load-bearing path of the CTM. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.
		DOE Waste Package Inner Lid Grapple (51A-HTC0-HEQ-00007)	Protect against the drop of a load onto a canister	53. The lid grapple is an integral part of the load-bearing path of the CTM. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
		Naval Waste Package Inner Lid Grapple (51A-HTC0-HEQ-00008)	Protect against the drop of a load onto a canister	54. The lid grapple is an integral part of the load-bearing path of the CTM. See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.	See Canister Transfer Machine requirements.
	Waste Package Loadout	Waste Package Transfer Trolley (including Pedestals, Seismic Rail Restraints, and Rails) (Trolley: 51A-HL00-TRLY-00001) (Pedestals: 51A-HL00-PED-00001-4)	Preclude rapid tilt-down	55. The WPTT shall be incapable of uncontrolled tilt-down.	Initiating event does not require further analysis. ^c	Table 6.0-2
			Limit speed	56. The speed of the WPTT shall be limited to 2.5 mi/hr.	IHF-ESD-08-NVL (Seq. 2-5)	This parameter limits the conditional probability of canister breach given a collision to the appropriate value from Table 6.3-7.

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Naval SNF Waste Package System	Naval SNF Waste Package	Entire	Protect against spurious movement	57. The mean probability of spurious movement of the WPTT while a canister is being lowered by the CTM shall be less than or equal to 1E-09 ^b per transfer.	IHF-ESD-07-NVL (Seq. 3-5)	51A-7-WPTT-SPURMOVE
				58. The mean conditional probability of breach of a sealed waste package resulting from a side impact shall be less than or equal to 1E-08 per impact.	IHF-ESD-11-NVL (Seq. 4-6)	51A-WP-FAIL-EXPORT
				59. The mean conditional probability of breach of a sealed waste package resulting from a drop of a load onto the waste package shall be less than or equal to 1E-05 ^e per drop.	IHF-ESD-11-NVL (Seq. 3-6)	51A-WP-FAIL-EXPORT ^e
	Naval SNF Canister	Naval SNF canister (analyzed as a representative canister)	Provide containment	60. The mean conditional probability of breach of a sealed waste package resulting from an end-on impact or collision shall be less than or equal to 1E-05 per impact.	IHF-ESD-11-NVL (Seq. 5-6)	51A-NVL-WPTT-COLLIDE-TEV
				61. The mean frequency of drop by the CTM of the naval SNF canister resulting in breach of the canister shall be less than or equal to 2E-05 over the preclosure period.	IHF-ESD-07-NVL (Seq. 4-5)	IHF-ESD-07-NVL (Seq. 4-5)
				62. 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 1E-05 per drop.	IHF-ESD-07-NVL (Seq. 2-5)	51A-NVL-CAN-FAIL-DROPON
				63. The mean conditional probability of breach of a canister resulting from a side impact or collision shall be less than or equal to 1E-08 per impact.	IHF-ESD-07-NVL (Seq. 6-5)	51A-NVL-CAN-FAIL-COLL

Table 6.9-1 Preclosure Nuclear Safety Design Bases for the IHF ITS SSCs (Continued)

System or Facility (System Code)	Subsystem (As Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				64. 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 1E-06 per fire event.	IHF-ESD-13-NVL (Seq. 8-6)	51A-NVL-FAIL-CAN-DIESEL
				65. 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 1E-04 per fire event.	IHF-ESD-13-NVL (Seq. 8-6)	51A-NVL-CAN-CONT-CTM-FIR
				66. The mean conditional probability of breach of a canister contained within a waste package resulting from the spectrum of fires shall be less than or equal to 1E-04 per fire event.	IHF-ESD-13-NVL (Seq. 8-6)	51A-NVL-CAN-CONT-LR-FIRE

NOTES: ^aProtect against' in this table means either 'reduce the probability of' or 'reduce the frequency of'. Extremely low probabilities are reported in this table as 1E-09. Increasing the source probability to 1E-09 does not impact the categorization of event sequences.

^bDesign requirement is applied to reduce the frequency of any event sequence that could result in damage to a waste container to Beyond Category 2.

^cThe term "spectrum of fires" refers to the variations in the intensity and duration of the fire that are considered along with conditions that control the rate of heat transfer to the container (Attachment D, Section D2.1).

^dIn this instance, a value of 1E-08 was used for the calculation. This probability bounds the estimated probability, as discussed in Attachment D, Section D1.4.4. The probability given in the nuclear safety design basis is higher, 1E-05. The stated nuclear safety design basis is supported by the analysis because the frequencies of the affected event sequences are below the Category 2 threshold by more than three orders of magnitude (the difference between the value used and the value stated in the nuclear safety design basis).

^eCTM = canister transfer machine; CTT = cask transfer trolley; DOE = U.S. Department of Energy; HLW = high-level radioactive waste; SNF = spent nuclear fuel; WPTT = waste package transfer trolley.

Source: Original

Table 6.9-2. Summary of Procedural Safety Controls for the IHF Facility

Item	SSC	Procedural Safety Control	Basis for Selection	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.	IHF-ESD-04-NVL (Seq. 3-5)
2	Site Prime Mover	The site prime mover is disconnected or secured to prevent motion before waste handling operations begin.	This control limits the probability of spurious movement of the site prime mover and resulting collision or tipover.	IHF-ESD-01-HLW (Seq. 4-6)
3	WPTT	Personnel are verified to be outside of the WP Positioning Room and the WP Loadout Room prior to movement of a loaded WP into the WP Positioning Room or the WP Loadout Room.	This control limits the probability of operators receiving a direct exposure during the loading of a WP into the TEV.	IHF-ESD-12C-NVL (Seq. 2)
4	CTM Naval SNF canister	Verify that the naval canister lifting adapter is fully detached from the naval SNF canister before using the CTM to remove the naval canister lifting adapter and shield ring.	HRA quantification is based on this PSC being in place. This control protects the canister from a drop by the CTM during the removal of the naval canister lifting adapter and shield ring.	IHF-ESD-07-NVL (Seq. 2-5)
5	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 exposure/residence times and reliability data to calculate the probability of an initiating event, or the probability of seismic induced failures that lead to an event sequence. 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.
6	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.	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.	IHF-ESD-07-HLW (Seq. 9-5)
7	CTM	At completion of a canister transfer operation, the port slide gates are	While the CTM is being used to perform transfer operations, the	IHF-ESD-12A-NVL (Seq. 2)

Table 6.9-2. Summary of Procedural Safety Controls for the IHF Facility (Continued)

Item	SSC	Procedural Safety Control	Basis for Selection	Representative Event Sequence
	Port Slide Gates	verified to be closed	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 present and the slide gate open.	
9	CTM	Prior to lifting or lowering a naval canister, the CTM guide sleeve is to be verified to have been lowered.	This control limits the probability that a naval canister is not in a vertical orientation during transfer such that any potential drops would be flat bottom drops.	IHF-ESD-07-NVL (Seq. 4-5)
10	HLW	The individual radionuclide inventories per HLW canister are limited to the values presented in consequence analysis.	This control is to ensure that the dose consequences from Category 2 event sequences involving HLW are within the values presented in the consequence analysis.	Applies to all event sequence end states that result in release of radioactivity from HLW.

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; HRA = human reliability analysis; ITS = important-to-safety ; PCSA = Preclosure Safety Analysis; SSC = systems, structures, and components; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

7. RESULTS AND CONCLUSIONS

This analysis report on the IHF and its predecessor companion report, the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28), 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 at 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* (Ref. 2.2.64). The identification and development of the event sequences is limited to those that might lead to the 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-1
Quantification of event sequences	Calculation of probability distributions for the numbers of occurrences of internal event sequence groups over the preclosure period	Table G-2
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 structures, systems, and components as important to safety	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	List 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	List 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 9 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	Waste Forms	
		HLW	Naval
DE-SHIELD-DEGRADE	Direct exposure due to degradation of shielding	None	None
DE-SHIELD-LOSS	Direct exposure due to loss of shielding	4	4
RR-UNFILTERED	Radionuclide release, unfiltered	1	None
RR-FILTERED	Radionuclide release, filtered	None	None
RR-UNFILTERED-ITC	Radionuclide release, unfiltered, also important to criticality	None	None
RR-FILTERED-ITC	Radionuclide release, filtered, also important to criticality	None	None
ITC	Important to criticality	None	None

Source: Original

Summary of Conservatism

It should be noted that the event sequence identification and categorization were conducted with conservatisms that increase confidence in the results. These conservatisms include those listed below.

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 orders 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 will be leaded casks. Because non-leaded 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 40 feet for casks and 45 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; i.e., the canister is not relied upon to reduce the probability of containment failure.
11. Transportation casks are analyzed without impact limiters even for those event sequences in 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 or 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 HVAC system that provides confinement of radioactive material releases following a waste form drop is not relied upon and is modeled with a failure probability of 1.0. This conservative consideration leads to unfiltered event sequence frequencies higher than are realistically expected.

14. The human reliability analysis screening values used for human failure events are typically one or more orders of magnitude higher than values that would be 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 relying 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, it considers that a certain number of HLW canisters are handled in IHF without subtracting that number from the number considered to be handled in the CRCF, which is the total number received at the repository. As a result, the allocated numbers, especially for the IHF, are higher than is realistically expected. This conservatism applies especially to the IHF because, although the IHF is designed to handle HLW canisters, it is preferable to handle virtually all of them in the CRCF where they can be loaded into codisposal waste packages along with DOE SNF. Including this conservatism in the analysis yields calculated event sequence frequencies that are higher than is realistically expected.

ATTACHMENT A
EVENT TREES

CONTENTS

	Page
A1 INTRODUCTION	A-9
A2 READER'S GUIDE TO THE EVENT TREE DESCRIPTIONS	A-9
A3 SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES	A-10
A4 EVENT TREE DESCRIPTIONS	A-11
A4.1 EVENT TREES FOR IHF-ESD-01	A-11
A4.2 EVENT TREES FOR IHF-ESD-02	A-16
A4.3 EVENT TREES FOR IHF-ESD-03	A-20
A4.4 EVENT TREES FOR IHF-ESD-04	A-23
A4.5 EVENT TREES FOR IHF-ESD-05	A-26
A4.6 EVENT TREES FOR IHF-ESD-06	A-29
A4.7 EVENT TREES FOR IHF-ESD-07	A-31
A4.8 EVENT TREES FOR IHF-ESD-08	A-36
A4.9 EVENT TREES FOR IHF-ESD-09	A-39
A4.10 EVENT TREES FOR IHF-ESD-10	A-41
A4.11 EVENT TREES FOR IHF-ESD-11	A-44
A4.12 EVENT TREES FOR IHF-ESD-12	A-48
A4.13 EVENT TREES FOR IHF-ESD-13	A-49
A5 EVENT TREES	A-56

FIGURES

	Page
A5-1. Example Initiator Event Tree Showing Navigation Aids	A-56
A5-2. Event Tree IHF-ESD-01-HLW – Receipt of HLW TC in the Cask Preparation Area	A-59
A5-3. Event Tree IHF-RESP-TC1 – Response for Incoming Transportation Cask	A-60
A5-4. Event Tree IHF-ESD-01-NVL – Receipt of Naval TC in the Cask Preparation Area and Transfer to CTT	A-61
A5-5. Event Tree IHF-ESD-02-HLW – HLW TC Upending and Removal from Conveyance.....	A-62
A5-6. Event Tree IHF-ESD-02-NVL – Remove Impact Limiters from NVL TC.....	A-63
A5-7. Event Tree IHF-ESD-03-HLW – HLW TC Preparation Activities.....	A-64
A5-8. Event Tree IHF-ESD-04-NVL – Naval TC Preparation Activities	A-65
A5-9. Event Tree IHF-RESP-CAN1 – Response for Canister	A-66
A5-10. Event Tree IHF-ESD-05-HLW – Transfer HLW TC on CTT from Cask Preparation Area to Cask Unloading Room.....	A-67
A5-11. Event Tree IHF-RESP-CAN2-HLW – Response for HLW Canister Mishap with CTM.....	A-68
A5-12. Event Tree IHF-ESD-05-NVL – Transfer Naval TC on CTT from Cask Preparation Area to Cask Unloading Room.....	A-69
A5-13. Event Tree IHF-RESP-CAN2-NVL – Response for NVL Canister Mishap with CTM.....	A-70
A5-14. Event Tree IHF-ESD-06-HLW – CTT with HLW TC Collides with Shield Door to Cask Unloading Room.....	A-71
A5-15. Event Tree IHF-ESD-06-NVL – CTT with Naval TC Collides with Shield Door to Cask Unloading Room.....	A-72
A5-16. Event Tree IHF-ESD-07-HLW – Transfer a HLW Canister with the CTM	A-73
A5-17. Event Tree IHF-ESD-07-NVL – Transferring a NVL Canister with the CTM.....	A-74
A5-18. Event Tree IHF-ESD-08-HLW – Transfer HLW WP on WPTT from WP Loading Room to WP Positioning Room	A-75
A5-19. Event Tree IHF-RESP-WP1 – Response for Moving Unsealed WP.....	A-76
A5-20. Event Tree IHF-ESD-08-NVL – Transfer Naval WP on WPTT from WP Loading Room to WP Positioning Room	A-77
A5-21. Event Tree IHF-ESD-09-HLW – Assembly and Closure of the HLW WP	A-78
A5-22. Event Tree IHF-RESP-WP2 – Response for WP during Closure	A-79

FIGURES (Continued)

	Page
A5-23. Event Tree IHF-ESD-09-NVL – Assembly and Closure of the Naval WP	A-80
A5-24. Event Tree IHF-ESD-10-HLW – Transfer HLW WP on WPTT from WP Positioning Room to WP Loadout Room	A-81
A5-25. Event Tree IHF-RESP-WP3 – Response for Sealed WP	A-82
A5-26. Event Tree IHF-ESD-10-NVL – Transfer Naval WP on WPTT from WP Positioning Room to WP Loadout Room	A-83
A5-27. Event Tree IHF-ESD-11-HLW – Export HLW WP from IHF	A-84
A5-28. Event Tree IHF-ESD-11-NVL – Export Naval WP from IHF	A-85
A5-29. Event Tree IHF-ESD-12A-HLW – Direct Exposure during Canister Transfer	A-86
A5-30. Event Tree IHF-ESD-12A-NVL – Direct Exposure during Canister Transfer	A-87
A5-31. Event Tree IHF-ESD-12B-HLW – Direct Exposure due to Improper Installation of Shield Ring	A-88
A5-32. Event Tree IHF-ESD-12B-NVL – Direct Exposure due to Improper Installation of Shield Ring	A-89
A5-33. Event Tree IHF-ESD-12C-HLW – Direct Exposure during Export of Loaded WP	A-90
A5-34. Event Tree IHF-ESD-12C-NVL – Direct Exposure during Export of Loaded WP	A-91
A5-35. Event Tree IHF-ESD-13-HLW-CAN – Fire Affects the Facility	A-92
A5-36. Event Tree IHF-RESP-FIRE – Response for Fires	A-93
A5-37. Event Tree IHF-ESD-13-HLW-CSK – Fire Affects the Facility	A-94
A5-38. Event Tree IHF-ESD-13-HLW-WP – Fire Affects the Facility	A-95
A5-39. Event Tree IHF-ESD-13-NVL – Fire Affects the Facility	A-96

TABLES

	Page
A4.1-1. Summary of Event Trees for IHF-ESD-01	A-11
A4.1-2. Initiating Event Assignments for IHF-ESD-01.....	A-12
A4.1-3. Basic Event Associated with the TRANSCASK Pivotal Events of IHF-ESD- IHF-ESD-01	A-14
A4.1-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-01	A-14
A4.1-5. Basic Event Associated with the SHIELDING Pivotal Events of IHF-ESD-01	A-15
A4.1-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF- ESD-01.....	A-15
A4.1-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF- ESD-01.....	A-16
A4.2-1. Summary of Event Trees for IHF-ESD-02	A-16
A4.2-2. Initiating Event Assignments for IHF-ESD-02.....	A-17
A4.2-3. Basic Event Associated with the TRANSCASK Pivotal Events of IHF- ESD-02.....	A-18
A4.2-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-02	A-19
A4.2-5. Basic Event Associated with the SHIELDING Pivotal Events of IHF-ESD-02	A-19
A4.2-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF- ESD-02.....	A-20
A4.2-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF- ESD-02.....	A-20
A4.3-1. Summary of Event Trees for IHF-ESD-03	A-21
A4.3-2. Initiating Event Assignments for IHF-ESD-03.....	A-21
A4.3-3. Basic Event Associated with the TRANSCASK Pivotal Events of IHF- ESD-03.....	A-22
A4.3-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-03	A-22
A4.3-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-03...	A-22
A4.3-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF- ESD-03.....	A-23
A4.3-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-03	A-23
A4.4-1. Summary of Event Trees for IHF-ESD-04	A-23
A4.4-2. Initiating Event Assignments for IHF-ESD-04.....	A-24
A4.4-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-04	A-25

TABLES (Continued)

	Page
A4.4-4. Basic Event Associated with the SHIELDING Pivotal Events of IHF-ESD-04	A-25
A4.4-5. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-04.....	A-25
A4.4-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-04.....	A-26
A4.5-1. Summary of Event Trees for IHF-ESD-05	A-26
A4.5-2. Initiating Event Assignments for IHF-ESD-05.....	A-27
A4.5-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-05	A-27
A4.5-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-05...	A-28
A4.5-5. Basic Events Associated with the CONFINEMENT Pivotal Events of IHF-ESD-05.....	A-28
A4.5-6. Basic Events Associated with the MODERATOR Pivotal Events of IHF-ESD-05	A-28
A4.6-1. Summary of Event Trees for IHF-ESD-06	A-29
A4.6-2. Initiating Event Assignments for IHF-ESD-06.....	A-30
A4.6-3. Fault Trees Associated with the CELL-DOOR Pivotal Events of IHF-ESD-06....	A-30
A4.6-4. Fault Trees Associated with the CONTAINMENT Pivotal Events of IHF-ESD-06.....	A-30
A4.6-5. Fault Trees Associated with the SHIELDING Pivotal Events of IHF-ESD-06	A-31
A4.6-6. Fault Trees Associated with the CONFINEMENT Pivotal Events of IHF-ESD-06.....	A-31
A4.6-7. Fault Trees Associated with the MODERATOR Pivotal Events of IHF-ESD-06.....	A-31
A4.7-1. Summary of Event Trees for IHF-ESD-07	A-32
A4.7-2. Initiating Event Assignments for IHF-ESD-07.....	A-33
A4.7-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-07	A-34
A4.7-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-07...	A-34
A4.7-5. Basic Events Associated with the CONFINEMENT Pivotal Events of IHF-ESD-07.....	A-35
A4.7-6. Basic Events Associated with the MODERATOR Pivotal Events of IHF-ESD-07	A-35
A4.8-1. Summary of Event Trees for IHF-ESD-08	A-36
A4.8-2. Initiating Event Assignments for IHF-ESD-08.....	A-37

TABLES (Continued)

	Page
A4.8-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-08	A-37
A4.8-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-08...	A-38
A4.8-5. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-08.....	A-38
A4.8-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-08.....	A-38
A4.9-1. Summary of Event Trees for IHF-ESD-09	A-39
A4.9-2. Initiating Event Assignments for IHF-ESD-09.....	A-39
A4.9-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-09	A-40
A4.9-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-09...	A-40
A4.9-5. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-09.....	A-40
A4.9-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-09	A-41
A4.10-1. Summary of Event Trees for IHF-ESD-10	A-41
A4.10-2. Initiating Event Assignments for IHF-ESD-10.....	A-42
A4.10-3. Basic Event Associated with the Waste Package Pivotal Events of IHF-ESD-10.....	A-42
A4.10-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-10	A-43
A4.10-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-10...	A-43
A4.10-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-10.....	A-44
A4.10-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-10.....	A-44
A4.11-1. Summary of Event Trees for IHF-ESD-11	A-45
A4.11-2. Initiating Event Assignments for IHF-ESD-11.....	A-45
A4.11-3. Basic Event Associated with the Waste Package Pivotal Events of IHF-ESD-11	A-46
A4.11-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-11	A-46
A4.11-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-11...	A-47
A4.11-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-11.....	A-47

TABLES (Continued)

	Page
A4.11-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-11	A-48
A4.12-1. Summary of Event Trees for IHF-ESD-12	A-48
A4.12-2. Initiating Event Assignments for IHF-ESD-12.....	A-49
A4.13-1. Summary of Event Trees for IHF-ESD-13	A-50
A4.13-2. Initiating Event Assignments for IHF-ESD-13.....	A-51
A4.13-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-13	A-52
A4.13-4. Fault Tree Associated with the SHIELDING Pivotal Events of IHF-ESD-13	A-54
A4.13-5. Fault Tree Associated with the CONFINEMENT Pivotal Events of IHF-ESD-13	A-54
A4.13-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-13	A-55
A5-1. Relation of Event Sequence Diagrams to Event Trees	A-57

ATTACHMENT A EVENT TREES

A1 INTRODUCTION

This attachment presents event trees that are derived from the ESDs in Attachment F of the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28). 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 A5-39 according to the “hierarchy ordering” rules in SAPHIRE. The first rule is that event trees are presented in alphabetical order (which is also ESD order). For example, the event trees associated with IHF-ESD-01 appear first, and those associated with IHF-ESD-02 appear after that, and so on. The second rule is that the first initiator event tree associated with the ESD appears first and the corresponding system response event tree is 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 (IHF-ESD-01-HLW) associated with the first ESD (IHF-ESD-01) is the first event tree figure. Then the system response event tree (IHF-RESP-TC1) appears, followed by the remaining initiator event trees for the ESD (IHF-ESD-01-NVL). 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). 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.

WP. This pivotal event represents the success or failure of the waste package to contain radioactive material after the impact caused by the initiating event. The failure of this pivotal event leads to loss of the waste package's containment function. The failure probability for this pivotal event depends on the selection of initiating event and is determined by PEFA, and is given in Table 6.3-4 in Section 6.3.2.2.

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 the loss of the cask's containment function. The failure probability for this pivotal event is determined by PEFA, and is given in Table 6.3-4 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, and the cask transfer machine shield bell, which 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 this instance refers to an unspecified degree of shielding degradation due to the impact.

CONFINEMENT. This pivotal event represents the success or failure of the HVAC system in continuing to provide 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 the physical properties of the waste form. HLW is not subject to the possibility of criticality; therefore, all moderator trees pertaining to criticality sequences for HLW are set to “0.00E+00.”

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 that represents equipment failure modes and human failure events that can initiate the specific event. The fault tree models are, in turn, linked to basic events that provide the failure frequencies. Some of the pivotal events represent failure of equipment whose failure probabilities are linked to a separately developed basic event and not to a fault tree.

A4 EVENT TREE DESCRIPTIONS

A4.1 EVENT TREES FOR IHF-ESD-01

IHF-ESD-01 covers event sequences associated with receipt of a truck trailer or railcar carrying a transportation cask (Ref. 2.2.28, Figure F-1). This ESD covers two types of transportation casks: naval and HLW. Corresponding to each type of cask is an initiator event tree (Table A4.1-1). Although the initiator event trees transfer to the same system-response event tree, it 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 IHF-ESD-01

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing HLW canisters	Initiator: IHF-ESD-01-HLW Response: IHF-RESP-TC1	600
Transportation cask containing a naval canister	Initiator: IHF-ESD-01-NVL Response: IHF-RESP-TC1	400

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

A4.1.1 Initiating Events for IHF-ESD-01

The following initiating events are associated with IHF-ESD-01. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.1-2. In this ESD, some of the initiating events apply to both naval SNF and HLW. Others apply only to HLW or to naval SNF. The differences are due to the fact that naval casks do not arrive by truck and naval casks are lifted from the railcar with impact limiters attached whereas HLW casks are lifted after removal of the impact limiters.

Table A4.1-2. Initiating Event Assignments for IHF-ESD-01

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Railcar derailment	IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAIL	51A-%-HLW-ON-SPMRC AND 51A-SPMRC-DERAIL-DER-FOM AND 51A-SPMRC-MILES-IN-IHF
	IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAIL	51A-SPMRC-DERAIL-DER-FOM AND 51A-SPMRC-MILES-IN-IHF
Truck trailer rollover	IHF-ESD-01-HLW	ESD01-HLW-SPMTTROLL	Screened out (Section 6.0.3)
Railcar or truck trailer collision	IHF-ESD-01-HLW	ESD01-HLW-COLLIDE	[(51A-%-HLW-ON-SPMRC) AND (51A-SPMRC-COLLISION)] OR [(51A-%-HLW ON SPMTT) AND (51A-SPMTT-COLLISION)]
	IHF-ESD-01-NVL	ESD01-NVL-COLLIDE	[(51A-% NVL ON SPMRC) AND (51A-SPMRC-COLLISION)] OR [(51A-% NVL ON SPMTT) AND (51A-SPMTT-COLLISION)]
Crane drops object on cask	IHF-ESD-01-NVL	ESD01-NVL-DROPON	ESD01-NVL-DROPON
Crane drops cask (ordinary)		ESD01-NVL-DRP-CSK	(51A-CRN3-DROPNVL-CRN-DRP) AND (51A-TRANSNSCTTLIFTNUMBER)
Crane drops cask (two-block)		ESD01-NVL-2BLK-CSK	51A-CRN3-2-BLOCK-CRN-TBK AND 51A-TRANSNSCTTLIFTNUMBER
Collision of suspended cask		ESD01-NVL-COL-CSK	51A-TC-IMPACT-SPM
Tipover of cask		ESD01-NVL-TIPOVER	51A-OPTIPOVER001-HFI-NOD

NOTE: ^a This column may contain fault trees and basic events logically connected as noted. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

The following initiating events apply to both waste forms.

Railcar Derailment. This initiating event accounts for the potential impact to the transportation cask on the railcar due to a derailment.

Conveyance Collision. This initiating event covers the potential impact to the transportation cask on the conveyance due to a collision with another vehicle.

The following initiating event applies only to HLW.

Truck Trailer Rollover. This initiating event accounts for the potential impact to the transportation cask on the truck trailer due to a rollover. The fault tree accounts for the fraction of casks received that are truck casks as opposed to rail casks. This fraction is set to 0 for naval casks because naval casks will only arrive by rail. In addition, rollover is not considered possible under the conditions inside the IHF. Therefore, the probability of truck rollover per truck cask received is modeled as a single-event fault tree with guaranteed success (Section 6.0.3).

For this ESD, the following initiating events apply only to naval SNF.

Crane drops object on cask. 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. The initiating event is specified as a probability of object drop per cask.

Crane drops cask from operational height or below. 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 initiating event is specified as a probability of a drop per cask.

Crane drops cask 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 during transfer by the cask handling crane. The initiating event is specified as a probability of a drop per cask.

Cask suspended from crane collides with facility structures or equipment. This initiating event covers the potential impact to the transportation cask due to a collision of the cask due to various causes. The initiating event is specified as a probability of impact per cask.

Cask tips over after having been removed from the railcar. This initiating event covers the potential impact to the transportation cask due to a tipover. The initiating event is specified as a probability of tipover per cask.

A4.1.2 System Response Event Tree IHF-RESP-TC1

The pivotal events that appear in IHF-RESP-TC1 are indicated below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

TRANSCASK. 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 TRANSCASK Pivotal Events of IHF-ESD-IHF-ESD-01

Initiator Event Tree	Initiating Event Name	Name Assigned to TRANSCASK	Associated Fault Tree or Basic Event ^a
IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAILED	ESD01-HLW-SPMRCDERAIL-TC	51A-HLW-TCASK-FAIL-DEDERAIL
	ESD01-HLW-TTROLL	ESD01-HLW-SPMTTROLL-TC	51A-HLW-TCASK-FAIL-ROLL
	ESD01-HLW-COLLIDE	ESD01-HLW-COLLIDE-TC	51A-HLW-TCASK-FAIL-COLL
IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAILED	ESD01-NVL-SPMRCDERAIL-TC	51A-NVL-TC-FAIL-DEDERAIL
	ESD01-NVL-COLLIDE	ESD01-NVL-COLLIDE-TC	51A-NVL-TC-FAIL-COLLIDE
	ESD01-NVL-DROPON	ESD01-NVL-DROPON-TC	51A-NVL-TC-FAIL-DROPON
	ESD01-NVL-DRP-CSK	ESD01-NVL-DRP-CSK-TC	51A-NVL-TC-FAIL-DROP
	ESD01-NVL-2BLK-CSK	ESD01-NVL-2BLK-CSK-TC	51A-NVL-TC-FAIL-2-BLOCK
	ESD01-NVL-COL-CSK	ESD01-NVL-COL-CSK-TC	51A-NVL-TC-FAIL-OFFPFCOLL
	ESD01-NVL-TIPOVER	ESD01-NVL-TIPOVER-TC	51A-NVL-TC-FAIL-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

CANISTER. Table A4.1-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-01

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAILED	HLW-CAN-INCASK	51A-CAN-FAIL-IN-TC
	ESD01-HLW-SPMTTROLL		
	ESD01-HLW-COLLIDE		
IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAILED	NVL-CAN-INCASK	51A-NVL-CAN-FAIL-IN-TC
	ESD01-NVL-COLLIDE		
	ESD01-NVL-DROPON		
	ESD01-NVL-DRP-CSK		
	ESD01-NVL-2BLK-CSK		
	ESD01-NVL-COL-CSK		
	ESD01-NVL-TIPOVER		

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 A4.1-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-5. Basic Event Associated with the SHIELDING Pivotal Events of IHF-ESD-01

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAIL	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD01-HLW-SPMTTROLL		
	ESD01-HLW-COLLIDE		
IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAIL	NVL-TC-SHIELD8	NVL-SHIELDING-FAILS8
	ESD01-NVL-COLLIDE	NVL-TC-SHIELD8	NVL -SHIELDING-FAILS8
	ESD01-NVL-DROPON	NVL-TC-SHIELD5	NVL -SHIELDING-FAILS5
	ESD01-NVL-DRP-CSK	NVL-TC-SHIELD5	NVL -SHIELDING-FAILS5
	ESD01-NVL-2BLK-CSK	NVL-TC-SHIELD5	NVL -SHIELDING-FAILS5
	ESD01-NVL-COL-CSK	NVL-TC-SHIELD8	NVL -SHIELDING-FAILS8
	ESD01-NVL-TIPOVER	NVL-TC-SHIELD8	NVL -SHIELDING-FAILS8

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 A4.1-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.1-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-01

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAIL	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD01-HLW-SPMTTROLL		
	ESD01-HLW-COLLIDE		
IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAIL	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD01-NVL-COLLIDE		
	ESD01-NVL-DROPON		
	ESD01-NVL-DRP-CSK		
	ESD01-NVL-2BLK-CSK		
	ESD01-NVL-COL-CSK		
	ESD01-NVL-TIPOVER		

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 A4.1-7 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.1-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-01

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-01-HLW	ESD01-HLW-SPMRC DERAIL	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD01-HLW-SPMTTROLL		
	ESD01-HLW-COLLIDE		
IHF-ESD-01-NVL	ESD01-NVL-SPMRC DERAIL	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD01-NVL-COLLIDE		
	ESD01-NVL-DROPON		
	ESD01-NVL-DRP-CSK		
	ESD01-NVL-2BLK-CSK		
	ESD01-NVL-COL-CSK		
	ESD01-NVL-TIPOVER		

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 IHF-ESD-02

IHF-ESD-02 delineates the event sequences that arise after a mechanical challenge to the transportation cask that occurs in the Cask Preparation Area during removal of impact limiters, upending and transfer of the HLW cask to the CTT, and removal of impact limiters from the naval transportation cask (Ref. 2.2.28, Figure F-2). This ESD covers two types of transportation casks: naval and HLW. Corresponding to each type of cask is an initiator event tree (Table A4.2-1). Although the initiator event trees transfer to the same system-response event tree, it 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 IHF-ESD-02

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing HLW canisters	Initiator: IHF-ESD-02-HLW Response: IHF-RESP-TC1	600
Transportation cask containing a naval canister	Initiator: IHF-ESD-02-NVL Response: IHF-RESP-TC1	400

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

A4.2.1 Initiating Events for IHF-ESD-02

The following initiating events are associated with IHF-ESD-02. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.2-2.

Drop of HLW transportation cask from operational height or below. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from below or at normal operational height during transfer by the cask handling crane. The initiating event is specified as a probability of a drop per cask.

Drop of HLW transportation cask from above operational height. This initiating event accounts for the potential impact to the transportation cask due to having been dropped from above normal operational height during transfer by the cask handling crane. The initiating event is specified as a probability of a drop per cask.

Unplanned conveyance movement causes HLW transportation cask impact due to collision with equipment or structure. This initiating event covers the potential impact to the transportation cask on the conveyance due to a collision with another vehicle.

Collision with equipment or structure involving side impact to HLW or naval transportation cask (during transfer by crane). This initiating event covers the potential impact to the transportation cask due to a collision of the cask due to various causes. The initiating event is specified as a probability of impact per cask.

Drop of heavy object (such as handling equipment) onto the naval or HLW transportation cask. 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. The initiating event is specified as a probability of object drop per cask.

HLW transportation cask tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The initiating event is specified as a probability of tipover per cask.

Table A4.2-2. Initiating Event Assignments for IHF-ESD-02

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Drop of HLW transportation cask from operational height or below	IHF-ESD-02-HLW	ESD02-HLW-DROP	(51A-#HLW-TC-LIFTS) AND (51A-CRN3-DROPHLW-CRN-DRP)
Drop of HLW transportation cask from above operational height	IHF-ESD-02-HLW	ESD02-HLW-2BLK	(51A-#HLW-TC-LIFTS) AND (51A-CRN3-2-BLOCK-CRN-TBK)
Unplanned conveyance movement	IHF-ESD-02-HLW	ESD02-HLW-SPURMOVE	ESD02-HLW-SPURMOVE

Table A4.2-2. Initiating Event Assignments for IHF-ESD-02 (Continued)

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Collision with equipment or structure during transfer by crane	IHF-ESD-02-HLW	ESD02-HLW-SIDEIMP	ESD02-HLW-SIDEIMP
	IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP	ESD02-NVL-SIDEIMP
Drop of heavy object (such as handling equipment) onto the naval or HLW transportation cask	IHF-ESD-02-HLW	ESD02-HLW-DROPON	ESD02-HLW-DROPON
	IHF-ESD-02-NVL	ESD02-NVL-DROPON	ESD02-NVL-DROPON
HLW transportation cask tipover	IHF-ESD-02-HLW	ESD02-HLW-TIP-CSK	51A-OPTIPOVER001-HFI-NOD

NOTE: ^a This column may contain fault trees and basic events logically connected as noted. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.2.2 System Response Event Tree IHF-RESP-TC1

The pivotal events that appear in IHF-RESP-TC1 are indicated below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

TRANSCASK. 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 TRANSCASK Pivotal Events of IHF-ESD-02

Initiator Event Tree	Initiating Event Name	Name Assigned to TRANSCASK	Associated Fault Tree or Basic Event ^a
IHF-ESD-02-HLW	ESD02-HLW-DROP	ESD02-HLW-DROP-TC	51A-HLW-TC-FAIL-DROP
	ESD02-HLW-2BLK	ESD02-HLW-2BLK-TC	51A-HLW-TC-FAIL-2BLK
	ESD02-HLW-SPURMOVE	ESD02-HLW-SPUR-TC	51A-HLW-TC-FAIL-SPURMOVE
	ESD02-HLW-SIDEIMP	ESD02-HLW-SIDEIMP-TC	51A-HLW-TC-FAIL-SIMP
	ESD02-HLW-DROPON	ESD02-HLW-DROPON-TC	51A-HLW-TC-FAIL-DROPON
	ESD02-HLW-TIP-CSK	ESD02-HLW-TIP-CSK-TC	51A-HLW-TC-FAIL-TIPOVER
IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP	ESD02-NVL-SIDEIMP-TC	51A-NVL-TC-FAIL-SIMP
	ESD02-NVL-DROPON	ESD02-NVL-DROPON-TC	51A-NVL-TC-FAIL-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

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 IHF-ESD-02

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-02-HLW	ESD02-HLW-DROP	HLW-CAN-INCASK	51A-CAN-FAIL-IN-TC
	ESD02-HLW-2BLK		
	ESD02-HLW-SPURMOVE		
	ESD02-HLW-SIDEIMP		
	ESD02-HLW-DROPON		
	ESD02-HLW-TIP-CSK		
IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP	NVL-CAN-INCASK	51A-CAN-FAIL-IN-TC
	ESD02-NVL-DROPON		

NOTE: ^aThis 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 IHF-ESD-02

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-02-HLW	ESD02-HLW-DROP	HLW-TC-SHIELD5	HLW-SHIELDING-FAILS5
	ESD02-HLW-2BLK	HLW-TC-SHIELD5	HLW-SHIELDING-FAILS5
	ESD02-HLW-SPURMOVE	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD02-HLW-SIDEIMP	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD02-HLW-DROPON	HLW-TC-SHIELD5	HLW-SHIELDING-FAILS5
	ESD02-HLW-TIP-CSK	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP	NVL-TC-SHIELD8	NAVAL-SHIELDING-FAILS8
	ESD02-NVL-DROPON	NVL-TC-SHIELD5	NAVAL-SHIELDING-FAILS5

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-02

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-02-HLW	ESD02-HLW-DROP	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD02-HLW-2BLK		
	ESD02-HLW-SPURMOVE		
	ESD02-HLW-SIDEIMP		
	ESD02-HLW-DROPON		
	ESD02-HLW-TIP-CSK		
IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP		
	ESD02-NVL-DROPON		

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-02

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-02-HLW	ESD02-HLW-DROP	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD02-HLW-2BLK		
	ESD02-HLW-SPURMOVE		
	ESD02-HLW-SIDEIMP		
	ESD02-HLW-DROPON		
	ESD02-HLW-TIP-CSK		
IHF-ESD-02-NVL	ESD02-NVL-SIDEIMP	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD02-NVL-DROPON		

NOTE: ^aThis 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 IHF-ESD-03

This ESD delineates the event sequences that arise after a mechanical challenge to the HLW transportation cask that occurs in the Cask Preparation Area during cask preparation activities involving the cask preparation crane (Ref. 2.2.28, Figure F-3). This ESD applies to the HLW transportation casks (Table A4.3-1). 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 A4.3-1. Summary of Event Trees for IHF-ESD-03

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing HLW canisters	Initiator: IHF-ESD-03-HLW Response: IHF-RESP-TC1	600

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

A4.3.1 Initiating Events for IHF-ESD-03

The following initiating events are associated with IHF-ESD-03. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.3-2.

Cask Tipover. This initiating event covers the potential impact to the transportation cask due to a tipover. The initiating event is specified as a probability of tipover per cask.

Collision Involving Side Impact to Cask. This initiating event covers the potential impact to the transportation cask due to a collision of the cask due to various causes. The initiating event is specified as a probability of impact per cask.

Object Dropped on Cask. 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. The initiating event is specified as a probability of object drop per cask.

Table A4.3-2. Initiating Event Assignments for IHF-ESD-03

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Cask tipover	IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	ESD03-HLW-CASKTIP
Side impact		ESD03-HLW-SIMPACT	ESD03-HLW-SIMPACT
Object dropped on cask		ESD03-HLW-DROPON	ESD03-HLW-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

A4.3.2 System Response Event Tree IHF-RESP-TC1

The pivotal events that appear in IHF-RESP-TC1 are indicated below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

TRANSCASK. Table A4.3-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-3. Basic Event Associated with the TRANSCASK Pivotal Events of IHF-ESD-03

Initiator Event Tree	Initiating Event	Name Assigned to TRANSCASK	Associated Fault Tree or Basic Event ^a
IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	ESD03-HLW-CASKTIP-TC	51A-HLW-TC-TIPOVER
	ESD03-HLW-SIMPACT	ESD03-HLW-SIMPACT-TC	51A-HLW-TC-FAIL-SIMP
	ESD03-HLW-DROPON	ESD03-HLW-DROPON-TC	51A-HLW-TC-FAIL-DROPON

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.3-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-03

Initiator Event Tree	Initiating Event	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	HLW-CAN-INCASK	51A-CAN-FAIL-IN-TC
	ESD03-HLW-SIMPACT		
	ESD03-HLW-DROPON		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.3-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.3-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-03

Initiator Event Tree	Initiating Event	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD03-HLW-SIMPACT	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD03-HLW-DROPON	HLW-TC-SHIELD5	HLW-SHIELDING-FAILS5

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.3-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.3-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-03

Initiator Event Tree	Initiating Event	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD03-HLW-SIMPACT		
	ESD03-HLW-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 A4.3-7 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.3-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-03

Initiator Event Tree	Initiating Event	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-03-HLW	ESD03-HLW-CASKTIP	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD03-HLW-SIMPACT		
	ESD03-HLW-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

A4.4 EVENT TREES FOR IHF-ESD-04

IHF-ESD-04 covers event sequences that arise after a mechanical challenge to the naval canister inside the transportation cask associated with removal of the cask lid (Ref. 2.2.28, Figure F-4). This includes event sequences that arise during removal of the lid and other actions to prepare the canister for removal from the cask (Figure F-4 and Section 6.1.2.7, Node 7). This ESD applies to the naval transportation cask containing a single naval SNF canister. 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 (Table A4.4-1). 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 IHF-ESD-04

Waste Form Units	Associated Event Trees	Number of Waste Form Units
Unsealed transportation cask containing a naval canister	Initiator: IHF-ESD-04-NVL Response: IHF-RESP-CAN1	400

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

A4.4.1 Initiating Events for IHF-ESD-04

The following initiating events are associated with IHF-ESD-04. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.4-2.

Side Impact to Cask. This initiating event covers an impact to the side of the cask due to improper movement by the cask preparation crane. The probability of this initiating event per cask received is modeled as a fault tree and is discussed in Attachment B. The initiating event is specified as a probability of a tipover per cask handled.

Drop of Heavy Load onto Cask. This initiating event covers the drop of a heavy object onto the cask by the cask preparation crane. The probability of this initiating event per cask received is modeled as a fault tree and is discussed in Attachment B. The initiating event is specified as a probability of a drop per cask.

Cask Tipover. This initiating event covers a tipover of the unsealed transportation cask due to an improper interaction of the cask or cask transfer trolley with the cask handling crane or cask preparation crane (Table A4.4-2). The probability of this initiating event per cask received is modeled as a fault tree and is discussed in Attachment B. The initiating event is specified as a probability of a tipover per cask.

Table A4.4-2. Initiating Event Assignments for IHF-ESD-04

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Side impact	IHF-ESD-04-NVL	ESD04-NVL-SIMPACT	ESD04-NVL-SIMPACT
Drop of heavy load onto cask		ESD04-NVL-DROPON	ESD04-NVL-DROPON
Cask tipover		ESD04-NVL-CASKTIP	ESD04-NVL-CASKTIP

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 IHF-RESP-CAN1

The pivotal events that appear in IHF-RESP-CAN1 are listed below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.4-3 indicates the basic events that are associated with this pivotal event for each initiating event.

Table A4.4-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-04

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-04-NVL	ESD04-NVL-SIMPACT	ESD04-NVL-SIMPACT-TC	51A-NVL-TC-FAIL-SIMP
	ESD04-NVL-DROPON	ESD04-NVL-DROPON-CAN	51A-NVL-CAN-FAIL-DROPON
	ESD04-NVL-CASKTIP	ESD04-NVL-CASKTIP-TC	51A-NVL-TC-FAIL-TIP

NOTE: ^aThis 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 IHF-ESD-04

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-04-NVL	ESD04-NVL-SIMPACT	NVL-TC-SHIELD8	NAVAL-SHIELDING-FAILS8
	ESD04-NVL-DROPON	NVL-TC-SHIELD5	NAVAL-SHIELDING-FAILS5
	ESD04-NVL-CASKTIP	NVL-TC-SHIELD8	NAVAL-SHIELDING-FAILS8

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.4-5 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.4-5. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-04

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-04-NVL	ESD04-NVL-SIMPACT	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD04-NVL-DROPON		
	ESD04-NVL-CASKTIP		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.4-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.4-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-04

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-04-NVL	ESD04-NVL-SIMPACT	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD04-NVL-DROPON		
	ESD04-NVL-CASKTIP		

NOTE: ^aThis 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 IHF-ESD-05

IHF-ESD-05 covers event sequences that arise after a mechanical challenge to a loaded CTT that occurs during movement of the CTT from the Cask Preparation Area to the Cask Unloading Room (Ref. 2.2.28, Figure F-5). This ESD applies to the following waste forms:

- Naval SNF canister in a transportation cask
- HLW canister in a transportation cask.

Table A4.5-1 summarizes the event trees for IHF-ESD-05. 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 IHF-ESD-05

Waste Form Units	Associated Event Trees	Number of Waste Form Units
Transportation cask containing HLW canisters	Initiator: IHF-ESD-05-HLW Response: IHF-RESP-CAN2-HLW	600
Transportation cask containing a naval canister	Initiator: IHF-ESD-05-NVL Response: IHF-RESP-CAN2-NVL	400

NOTE: HLW = high-level radioactive waste.

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

A4.5.1 Initiating Events for IHF-ESD-05

The following initiating events are associated with IHF-ESD-05. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.5-2.

CTT or cask catches crane hook or rigging resulting in impact to cask. This initiating event addresses an impact to the cask caused by the crane operator during the movement of HLW. This is an HFE event described in Attachment E. The initiating event is specified as a probability of a side impact per cask handled.

CTT impact collision with another vehicle, facility structures, or equipment (except shield door). This initiating event addresses a collision either as a result of moving the CTT from the Cask Preparation Room to the Cask Unloading Room or with another vehicle operating in the IHF. The initiating event is specified as a probability of a collision with vehicle, facility structures or equipment per cask handled.

Table A4.5-2. Initiating Event Assignments for IHF-ESD-05

Initiating Event Description	Initiating Event Name	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
CTT or cask catches crane hook or rigging, resulting in impact to cask	IHF-ESD-05-HLW	ESD05-HLW-CTT-IMPACT	51A-OPIMPACT0000-HFI-NOD
CTT impact collision with another vehicle, facility structures, or equipment (except shield door)		ESD05-HLW-CTT-COLLIDE	51A-OPCTCOLLIDE2-HFI-NOD OR 51A CTT-FAIL-STOP

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events; CTT = cask transfer trolley.

Source: Original

A4.5.2 System Response Event Tree IHF-RESP-CAN2-HLW and IHF-RESP-CAN2-NVL

The pivotal events that appear in IHE-RESP-CAN2-HLW and IHF-RESP-NVL are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names. The pivotal events are summarized in Section A3.

CANISTER. Table A4.5-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.5-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-05

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-05-HLW	ESD05-HLW-CTT-IMPACT	ESD05-HLW-IMPACT-TC	51A-HLW-CANTC-FAIL-IMP
	ESD05-HLW-CTT-COLLIDE	ESD05-HLW-COLLIDE-TC	51A-HLW-CANTC-FAIL-COLL
IHF-ESD-05-NVL	ESD05-NVL-CTT-IMPACT	ESD05-NVL-IMPACT-TC	51A-NVL-CANTC-FAIL-IMP
	ESD05-NVL-CTT-COLLIDE	ESD05-NVL-COLLIDE-TC	51A-NVL-CANTC-FAIL-COLL

NOTE: ^aThis 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 Events Associated with the SHIELDING Pivotal Events of IHF-ESD-05

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-05-HLW	ESD05-HLW-CTT-IMPACT	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
	ESD05-HLW-CTT-COLLIDE		
IHF-ESD-05-NVL	ESD05-NVL-CTT-IMPACT	NVL-TC-SHIELD8	NAVAL-SHIELDING-FAILS8
	ESD05-NVL-CTT-COLLIDE		

NOTE: ^aThis 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 Events Associated with the CONFINEMENT Pivotal Events of IHF-ESD-05

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-05-HLW	ESD05-HLW-CTT-IMPACT	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD05-HLW-CTT-COLLIDE		
IHF-ESD-05-NVL	ESD05-NVL-CTT-IMPACT		
	ESD05-NVL-CTT-COLLIDE		

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.5-6. Basic Events Associated with the MODERATOR Pivotal Events of IHF-ESD-05

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-05-HLW	ESD05-HLW-CTT-IMPACT	MOD-NOFIRE	MOD-NOFIRE-HLW-NOIMP
	ESD05-HLW-CTT-COLLIDE		
IHF-ESD-05-NVL	ESD05-NVL-CTT-IMPACT	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-OTHER-WATER) OR (51A-FIRE-SUPPRESSION)
	ESD05-NVL-CTT-COLLIDE		

NOTE: ^aThis 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 IHF-ESD-06

IHF-ESD-06 covers event sequence for a mechanical challenge from a CTT moving either a HLW or NVL transportation cask and colliding with the Cask Unloading Room shield door (Ref. 2.2.28, Figure F-6). For the CTT, the shield door involved is the door from the Cask Preparation Area to the Cask Unloading Room. Corresponding to each type of cask is an initiator event tree (Table A4.6-1).

The conveyance could collide into a stationary shield door or a moving shield door could collide into the conveyance. Since the shield doors are designed in accordance with the applicable provisions of *American National Standard Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities* (Ref. 2.2.9) to withstand the load and acceleration produced by a DBGM-2 seismic event, it is reasonable to conclude that the shield doors would remain attached to their moorings in the event of a slow speed (maximum of 2.5 mph) collision of a conveyance with the shield door. Therefore the analysis only evaluates the impact of a moving shield door with the conveyance.

Although the initiator event tree transfers 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 A4.6-1. Summary of Event Trees for IHF-ESD-06

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing multiple HLW canisters	Initiator: IHF-ESD-06-HLW Response: IHF-ESD-06-HLW	100
Transportation cask containing a single HLW canister	Initiator: IHF-ESD-06-HLW Response: IHF-ESD-06-HLW	500
Transportation cask containing a Naval canister	Initiator: IHF-ESD-06-NVL Response: IHF-ESD-06-NVL	400

NOTE: HLW = high-level radioactive waste.

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

A4.6.1 Initiating Events for IHF-ESD-06

The following initiating events are associated with IHF-ESD-06. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.6-2.

Mechanical Challenge to a Transportation Cask. This initiating event represents a potential impact to the transportation cask from a CTT collision with the Cask Unloading Room shield door. The probability of impact per transfer is described in Attachment B. The initiating event is specified as a probability of a drop per cask.

Table A4.6-2. Initiating Event Assignments for IHF-ESD-06

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Mechanical challenge from CTT collision with shield door	IHF-ESD-06-HLW	ESD06-HLW-IMPACT	51A-CTT-COLLIDE-SDR
	IHF-ESD-06-NVL	ESD06-NVL-IMPACT	

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events; CTT = cask transfer trolley.

Source: Original

A4.6.2 System Response Event Tree IHF-ESD-06

The pivotal events that appear in IHF-ESD-06 are listed and summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CELL-DOOR. The conditional probability that the CTT collides with shield door for all waste forms and initiating events as shown in Table A4.6-3.

Table A4.6-3. Fault Trees Associated with the CELL-DOOR Pivotal Events of IHF-ESD-06

Initiator Event Tree	Initiating Event Name	Name Assigned to CELL-DOOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-06-HLW	ESD06-HLW-IMPACT	ESD06-HLW-IMPACT-DOORFAI	51A-DOORFAIL-IMPACT
IHF-ESD-06-NVL	ESD06-NVL-IMPACT	ESD06-NVL-IMPACT-DOORFAI	51A-NVL-DOOR-FAILS

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONTAINMENT. Table A4.6-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.6-4. Fault Trees Associated with the CONTAINMENT Pivotal Events of IHF-ESD-06

Initiator Event Tree	Initiating Event Name	Name Assigned to CONTAINMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-06-HLW	ESD6-HLW-IMPACT	ESD6-HWL-IMPACT-CONT	51A-HLW-CONT-FAIL-IMP
IHF-ESD-06-NVL	ESD6-NVL-IMPACT	ESD6-NVL-IMPACT-CONT	51A-NVL-CONT-FAIL-IMP

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.6-5 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.6-5. Fault Trees Associated with the SHIELDING Pivotal Events of IHF-ESD-06

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-06-HLW	ESD06-HLW-IMPACT	HLW-TC-SHIELD8	HLW-SHIELDING-FAILS8
IHF-ESD-06-NVL	ESD06-NVL-IMPACT	NVL-TC-SHIELD8	NVL-SHIELDING-FAILS8

NOTE: ^aThis 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. Fault Trees Associated with the CONFINEMENT Pivotal Events of IHF-ESD-06

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-06-HLW	ESD06-HLW-IMPACT	HVAC-CONF	HVAC-CONFINEMENT-FAILS
IHF-ESD-06-NVL	ESD06-NVL-IMPACT		

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.6-7. Fault Trees Associated with the MODERATOR Pivotal Events of IHF-ESD-06

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-06-HLW	ESD06-HLW-IMPACT	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
IHF-ESD-06-NVL	ESD06-NVL-IMPACT	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-OTHER-WATER) OR (51A-FIRE-SUPPRESSION)

NOTE: ^aThis 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 IHF-ESD-07

IHF-ESD-07 covers event sequences associated with the transfer of a canister from a TC to WP with the CTM (Ref. 2.2.28, Figure F-7). This ESD covers all canister types. Corresponding to each canister type is an initiator event tree (Table A4.7-1). 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 A4.7-1. Summary of Event Trees for IHF-ESD-07

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Transportation cask containing multiple HLW canisters	Initiator: IHF-ESD-07-HLW Response: IHF-RESP-CAN1	100
Transportation cask containing a single HLW canister	Initiator: IHF-ESD-07-HLW Response: IHF-RESP-CAN1	500
Transportation cask containing a naval canister	Initiator: IHF-ESD-07-NVL Response: IHF-RESP-CAN1	400

NOTE: HLW = high-level radioactive waste.

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

A4.7.1 Initiating Events for IHF-ESD-07

The following initiating events are associated with IHF-ESD-07. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.7-2. The initiating events are specified as frequency of occurrence per canister.

Impact Associated with Lid Removal. This initiating event covers the potential impact during HLW cask lid removal due to a human failure to remove all of the lid bolts.

Canister Drop from Operational Height. This initiating event accounts for the potential impact to the canister due to having been dropped from the normal operational height during transfer by the CTM.

Impact to Canister due to Conveyance Movement. This initiating event covers the potential impact to the canister due to untimely movement of the CTT, site transporter, or WPTT during loading or unloading of the canister.

Side Impact to Canister. This initiating event covers the potential impact to the canister due to a CTM collision.

Object Dropped on Canister. This initiating event covers the potential impact to the canister due to the drop of a heavy object (e.g., cask lid) by the CTM.

Canister Drop inside Bell. This initiating event accounts for the potential impact to the canister due to having been dropped on the second floor during horizontal transfer by the CTM.

Canister Drop above Operational Height. This initiating event accounts for the potential impact to the canister due to having been dropped from above the normal operational height during transfer by the CTM.

Canister Collision or Impact. This initiating event accounts for a potential canister collision or impact.

Table A4.7-2. Initiating Event Assignments for IHF-ESD-07

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Transfer of a Canister from a TC to a WP with CTM	IHF-ESD-07-HLW	ESD07-HLW-DROPON	51A-CTMOBJLIFTNUMBER-HLW AND 51A-CTM-HLW-DROPON
		ESD07-HLW-IMPACT	51A-7-CTT-SPURMOVE OR 51A-7-WPTT-SPURMOVE OR CTM-SHEAR
		ESD07-HLW-DROP	51A-LIFTS-PER-HLW-CAN AND 51A-CTM-DROP
		ESD07-HLW-2BLK	51A-LIFTS-PER-HLW-CAN AND CTM-2-BLOCK
		ESD07-HLW-SIDEIMP	51A-LIFTS-PER-HLW-CAN AND 51A-SLIDEGATECLOSES-CAN
		ESD07-HLW-COLLISION	CTM-COLLISION
		ESD07-HLW-DROPIN	ESD07-HLW-DROPIN
		ESD07-HLWW-LIDIMP	ESD07-HLW-LIDIMP
	IHF-ESD-07-NVL	ESD07-NVL-DROPON	ESD07-NVL-DROPON
		ESD07-NVL-IMPACT	51A-7-CTT-SPURMOVE OR 51A-7-WPTT-SPURMOVE OR CTM-SHEAR
		ESD07-NVL-DROP	51A-LIFTS-PER-NVL-CAN AND 51A-CTM-DROP
		ESD07-NVL-2BLK	51A-LIFTS-PER-NVL-CAN AND CTM-2-BLOCK
		ESD07-NVL-SIDEIMP	51A-LIFTS-PER-NVLCAN AND 51A-SLIDEGATECLOSES-CAN
		ESD07-NVL-COLLISION	CTM-COLLISION
		ESD07-NVL-DROPIN	ESD07-NVL-DROPIN

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events; CTM = canister transfer machine; TC = transportation cask; WP = waste package.

Source: Original

A4.7.2 Pivotal Events

The pivotal events that appear in the event tree are listed below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.7-3 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.7-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-07

Initiator Event Tree	Initiator Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-07-HLW	ESD07-HLW-DROPON	ESD07-HLW-DROPON-CAN	51A-HLW-CAN-FAIL-DROPON
	ESD07-HLW-IMPACT	ESD07-HLW-IMPACT-CAN	51A-HLW-CAN-FAIL-IMPACT
	ESD07-HLW-DROP	ESD07-HLW-DROP-CAN	51A-HLW-CAN-FAIL-DROP
	ESD07-HLW-2BLK	ESD07-HLW-2BK-CAN	51A-HLW-CAN-FAIL-2BLK
	ESD07-HLW-SIDEIMP	ESD07-HLW-SIDEIMP-CAN	51A-HLW-CAN-FAIL-SIMP
	ESD07-HLW-COLLISION	ESD07-HLW-COLLISION-CAN	51A-HLW-CAN-FAIL-COLL
	ESD07-HLW-DROPIN	ESD07-HLW-DROPIN-CAN	51A-HLW-CAN-FAIL-DROPIN
	ESD07-HLWW-LIDIMP	ESD07-HLW-LIDIMP-CAN	51A-HLW-CAN-FAIL-LID
IHF-ESD-07-NVL	ESD07-NVL-DROPON	ESD07-NVL-DROPON-CAN	51A-NVL-CAN-FAIL-DROPON
	ESD07-NVL-IMPACT	ESD07-NVL-IMPACT-CAN	51A-NVL-CAN-FAIL-IMPACT
	ESD07-NVL-DROP	ESD07-NVL-DROP-CAN	51A-NVL-CAN-FAIL-DROP
	ESD07-NVL-2BLK	ESD07-NVL-2BLK-CAN	51A-NVL-CAN-FAIL-2BLK
	ESD07-NVL-SIDEIMP	ESD07-NVL-SIDEIMP-CAN	51A-NVL-CAN-FAIL-SIMP
	ESD07-NVL-COLLISION	ESD07-NVL-COLLISION-CAN	51A-NVL-CAN-FAIL-COLL
	ESD07-NVL-DROPIN	ESD07-NVL-DROPIN-CAN	51A-NVL-CAN-FAIL-DROPIN

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.7-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-07

Initiator Event Tree	Initiator Event Name	Name Assigned to CONTAINMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-07-HLW	ESD07-HLW-DROPON	CTM-SHIELDING	51A-CTM-SHIELD-DEGRADE
	ESD07-HLW-IMPACT		
	ESD07-HLW-DROP		
	ESD07-HLW-2BLK		
	ESD07-HLW-SIDEIMP		
	ESD07-HLW-COLLISION		
	ESD07-HLW-DROPIN		
	IHF-ESD-07-NVL		
ESD07-NVL-IMPACT			
ESD07-NVL-DROP			
ESD07-NVL-2BLK			
ESD07-NVL-SIDEIMP			
ESD07-NVL-COLLISION			

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.7-5 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.7-5. Basic Events Associated with the CONFINEMENT Pivotal Events of IHF-ESD-07

Initiator Event Tree	Initiator Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-07-HLW	ESD07-HLW-DROPON	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD07-HLW-IMPACT		
	ESD07-HLW-DROP		
	ESD07-HLW-2BLK		
	ESD07-HLW-SIDEIMP		
	ESD07-HLW-COLLISION		
	ESD07-HLW-DROPIN		
IHF-ESD-07-NVL	ESD07-NVL-DROPON		
	ESD07-NVL-IMPACT		
	ESD07-NVL-DROP		
	ESD07-NVL-2BLK		
	ESD07-NVL-SIDEIMP		
	ESD07-NVL-COLLISION		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.7-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.7-6. Basic Events Associated with the MODERATOR Pivotal Events of IHF-ESD-07

Initiator Event Tree	Initiator Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-07-HLW	ESD07-HLW-DROPON	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD07-HLW-IMPACT		
	ESD07-HLW-DROP		
	ESD07-HLW-2BLK		
	ESD07-HLW-SIDEIMP		
	ESD07-HLW-COLLISION		
	ESD07-HLW-DROPIN		

Table A4.7-6. Basic Events Associated with the MODERATOR Pivotal Events of IHF-ESD-07
(Continued)

Initiator Event Tree	Initiator Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ES07-NVL	ESD07-NVL-DROPON	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-OTHER-WATER) OR (51A-FIRE-SUPPRESSION)
	ESD07-NVL-IMPACT		
	ESD07-NVL-DROP		
	ESD07-NVL-2BLK		
	ESD07-NVL-SIDEIMP		
	ESD07-NVL-COLLISION		

NOTE: ^aThis 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 IHF-ESD-08

IHF-ESD-08 covers event sequences associated with movement of the WPTT within the Waste Package Positioning Room from the waste package loading position to the waste package closure position (Ref. 2.2.28, Figure F-8). This ESD covers all canister types that are loaded into waste packages in the IHF. Corresponding to each waste form unit is an initiator event tree (Table A4.8-1). 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 A4.8-1. Summary of Event Trees for IHF-ESD-08

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package containing 5 HLW canisters	Initiator: IHF-ESD-08-HLW Response: IHF-RESP-WP1	200
Waste package containing 1 naval waste canister	Initiator: IHF-ESD-08-NVL Response: IHF-RESP-WP1	400

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

A4.8.1 Initiating Events for IHF-ESD-08

The following initiating events are associated with IHF-ESD-08. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.8-2.

WPTT Derailment. This initiating event accounts for the potential derailment of the WPTT.

WPTT Collision with Facility Structures or Facility Equipment. This initiating event accounts for the potential impact to the waste package due to a WPTT collision with facility structures or facility equipment.

Premature Tilt-down of the WPTT. This initiating event accounts for the potential impact to the waste package due to a premature tilt-down of the WPTT.

Table A4.8-2. Initiating Event Assignments for IHF-ESD-08

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
WPTT derailment	IHF-ESD-08-HLW	ESD08-HLW-DERAIL	51A-WPTT-DERAIL-DER-FOM AND 51A-WPTT-MILES-IN-IHF
	IHF-ESD-08-NVL	ESD08-NVL-DERAIL	
WPTT collision	IHF-ESD-08-HLW	ESD08-HLW-COLLIDE	51A-OPWPCOLLIDE1-HFI-NOD OR WPTT-FAIL-TO-STOP
	IHF-ESD-08-NVL	ESD08-NVL-COLLIDE	
Premature tilt-down	IHF-ESD-08-HLW	ESD08-HLW-TILT	ESD08-HLW-TILT
	IHF-ESD-08-NVL	ESD08-NVL-TILT	ESD08-NVL-TILT

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

A4.8.2 System Response Event Tree IHF-RESP-WP1

The pivotal events that appear in IHF-RESP-WP1 are listed below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.8-3 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.8-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-08

Initiator Event Tree	Initiating Event	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-08-HLW	ESD08-HLW-DERAIL	ESD08-HLW-DERAIL-CAN	51A-HLW-CAN-FAIL-DERAIL
	ESD08-HLW-COLLIDE	ESD08-HLW-COLLIDE-CAN	51A-HLW-CAN-FAIL-COLL
	ESD08-HLW-TILT	ESD08-HLW-TILT-CAN	51A-HLW-CAN-FAIL-TILT
IHF-ESD-08-NVL	ESD08-NVL-DERAIL	ESD08-NVL-DERAIL-CAN	51A-NVL-CAN-FAIL-DERAIL
	ESD08-NVL-COLLIDE	ESD08-NVL-COLLIDE-CAN	51A-NVL-CAN-FAIL-COLL
	ESD08-NVL-TILT	ESD08-NVL-TILT-CAN	51A-NVL-CAN-FAIL-TILT

NOTE: ^aThis 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 shielding (waste package lid, shield ring, and WPTT shielding) to provide its shielding function after the impact caused by the initiating event. Failure of shielding in this instance refers to an unspecified degree of shielding degradation due to the impact. Table A4.8-4 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.8-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-08

Initiator Event Tree	Initiating Event	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-08-HLW	ESD08-HLW-DETRAIL	ESD08-HLW-DETRAIL-SHIELD	51A-HLW-WPSHLD-FAIL-DETRL
	ESD08-HLW-COLLIDE	ESD08-HLW-COLLIDE-SHIELD	51A-HLW-SHIELD-FAIL-COLL
	ESD08-HLW-TILT	ESD08-HLW-TILT-SHIELD	51A-HLW-SHIELD-FAIL-TILT
IHF-ESD-08-NVL	ESD08-NVL-DETRAIL	ESD08-NVL-DETRAIL-SHIELD	51A-NVL-SHIELD-FAIL-DETRL
	ESD08-NVL-COLLIDE	ESD08-NVL-COLLIDE-SHIELD	51A-NVL-SHIELD-FAIL-COLL
	ESD08-NVL-TILT	ESD08-NVL-TILT-SHIELD	51A-NVL-SHIELD-FAIL-TILT

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-08

Initiator Event Tree	Initiating Event	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event
IHF-ESD-08-HLW	ESD08-HLW-DETRAIL	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD08-HLW-COLLIDE		
	ESD08-HLW-TILT		
IHF-ESD-08-NVL	ESD08-NVL-DETRAIL		
	ESD08-NVL-COLLIDE		
	ESD08-NVL-TILT		

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-08

Initiator Event Tree	Initiating Event	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-08-HLW	ESD08-HLW-DETRAIL	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD08-HLW-COLLIDE		
	ESD08-HLW-TILT		
IHF-ESD-08-NVL	ESD08-NVL-DETRAIL	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD08-NVL-COLLIDE		
	ESD08-NVL-TILT		

NOTE: ^aThis 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 IHF-ESD-09

IHF-ESD-09 covers event sequences associated with the assembly and closure of the waste package (Ref. 2.2.28, Figure F-9). This ESD covers waste packages. Corresponding to each waste form unit is an initiator event tree (Table A4.9-1). 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 A4.9-1. Summary of Event Trees for IHF-ESD-09

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package containing 5 HLW canisters	Initiator: IHF-ESD-09-HLW Response: IHF-RESP-WP2	200
Waste package containing 1 naval waste canister	Initiator: IHF-ESD-09-NVL Response: IHF-RESP-WP2	400

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

A4.9.1 Initiating Events for IHF-ESD-09

The following initiating events are associated with IHF-ESD-09. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.9-2.

Welding Damages Canister. This initiating event accounts for the potential impact to the waste package due to a thermal challenge from the welding equipment.

Remote Handling System Drops Object. This initiating event accounts for the potential impact to the waste package due to the drop of an object by the RHS.

Table A4.9-2. Initiating Event Assignments for IHF-ESD-09

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Welding damages canister	IHF-ESD-09-HLW	ESD09-HLW-WELD	51A-WELD-DAMAGE
	IHF-ESD-09-NVL	ESD09-NVL-WELD	
RHS drops object	IHF-ESD-09-HLW	ESD09-HLW-DROPON	ESD09-HLW-DROPON
	IHF-ESD-09-NVL	ESD09-NVL-DROPON	ESD09-NVL-DROPON

NOTE: ^aThis 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-WP2

The pivotal events that appear in RESPONSE-WP2 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 specifies the fault tree or 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 IHF-ESD-09

Initiator Event Tree	Initiating Event	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-09-HLW	ESD09-HLW-WELD	ESD09-HLW-WELD-CAN	51A-HLW-WPCAN-FAIL-WELD
	ESD09-HLW-DROPON	ESD09-HLW-DROPON-CAN	51A-HLW-CAN-FAIL-DRPONWP
IHF-ESD-09-NVL	ESD09-NVL-WELD	ESD09-NVL-WELD-CAN	51A-NVL-CAN-FAIL-WELD
	ESD09-NVL-DROPON	ESD09-NVL-DROPON-CAN	51A-NVL-CAN-FAIL-DRPONWP

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.9-4. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-09

Initiator Event Tree	Initiating Event	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-09-HLW	ESD09-HLW-WELD	ESD09-HLW-WELD-WP	51A-HLW-WP-FAIL-WELD
	ESD09-HLW-DROPON	ESD09-HLW-DROPON-WP	51A-HLW-WP-FAILS-DROPON
IHF-ESD-09-NVL	ESD09-NVL-WELD	ESD09-NVL-WELD-WP	51A-NVL-WP-FAILS-WELD
	ESD09-NVL-DROPON	ESD09-NVL-DROPON-WP	51A-NVL-WP-FAIL-DROPON

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-09

Initiator Event Tree	Initiating Event	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-09-HLW	ESD09-HLW-WELD	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD09-HLW-DROPON		
IHF-ESD-09-NVL	ESD09-NVL-WELD		
	ESD09-NVL-DROPON		

NOTE: ^aThis 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 specifies the fault tree or 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 IHF-ESD-09

Initiator Event Tree	Initiating Event	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-09-HLW	ESD09-HLW-WELD	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD09-HLW-DROPON		
IHF-ESD-09-NVL	ESD09-NVL-WELD	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD09-NVL-DROPON		

NOTE: ^aThis 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 IHF-ESD-10

IHF-ESD-10 covers event sequences associated with the transfer of a waste package from the Waste Package Positioning Room to the WPTT docking station (Ref. 2.2.28, Figure F-10). This ESD covers all waste forms that are loaded into waste packages in the IHF. Corresponding to each waste form unit is an initiator event tree (Table A4.10-1). 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 A4.10-1. Summary of Event Trees for IHF-ESD-10

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package containing 5 HLW canisters	Initiator: IHF-ESD-10-HLW Response: IHF-RESP-WP3	200
Waste package containing 1 naval waste canister	Initiator: IHF-ESD-10-NVL Response: IHF-RESP-WP3	400

NOTE: HLW = high-level radioactive waste.

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

A4.10.1 Initiating Events for IHF-ESD-10

The following initiating events are associated with IHF-ESD-10. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.10-2.

WPTT Derailment. This initiating event accounts for the potential derailment of the WPTT during movement.

WPTT Collision. This initiating event accounts for the potential impact to the transportation cask due to a WPTT collision.

WPTT Premature Tilt-down. This initiating event accounts for the potential tilt-down of the WPTT during movement.

Table A4.10-2. Initiating Event Assignments for IHF-ESD-10

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
WPTT derailment	IHF-ESD-10-HLW	ESD10-HLW-DERAIL	51A-WPTT-DERAIL-DER-FOM AND 51A-WPTT-MILES-IN-IHF
	IHF-ESD-10-NVL	ESD10-NVL-DERAIL	
WPTT collision	IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	51A-OPWPCOLLIDE1-HFI-NOD OR WPTT-T2-FAIL-TO-STOP
	IHF-ESD-10-NVL	ESD10-NVL-COLLIDE	
Premature tilt-down	IHF-ESD-10-HLW	ESD10-HLW-TILT	ESD10-HLW-TILT
	IHF-ESD-10-NVL	ESD10-NVL-TILT	ESD10-NVL-TILT

NOTE: ^aThis 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 IHF-RESP-WP3

The pivotal events that appear in IHF-RESP-WP3 are listed below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

WP. Table A4.10-3 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.10-3. Basic Event Associated with the Waste Package Pivotal Events of IHF-ESD-10

Initiator Event Tree	Initiating Event	Name Assigned to WP	Associated Fault Tree or Basic Event ^a
IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	ESD10-HLW-COLLIDE-WP	51A-HLW-WP-FAIL-COLLIDE
	ESD10-HLW-DERAIL	ESD10-HLW-DERAIL-WP	51A-HLW-WP-FAIL-DERAIL
	ESD10-HLW-TILT	ESD10-HLW-TILT-WP	51A-HLW-WP-FAIL-TILT
IHF-ESD-10-NVL	ESD10-NVL-COLLIDE	ESD10-NVL-COLLIDE-WP	51A-NVL-WP-FAIL-COLLIDE
	ESD10-NVL-DERAIL	ESD10-NVL-DERAIL-WP	51A-NVL-WP-FAIL-DERAIL
	ESD10-NVL-TILT	ESD10-NVL-TILT-WP	51A-NVL-WP-FAIL-TILT

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.10-4 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.10-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-10

Initiator Event Tree	Initiating Event	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	ESD10-HLW-COLLIDE-CAN	51A-HLW-CANWP-FAIL-COLL
	ESD10-HLW-DERAIL	ESD10-HLW-DERAIL-CAN	51A-HLW-CANWP-FAIL-DERAIL
	ESD10-HLW-TILT	ESD10-HLW-TILT-CAN	51A-HLW-CANWP-FAIL-TILT
IHF-ESD-10-NVL	ESD10-NVL-COLLIDE	ESD10-NVL-COLLIDE-CAN	51A-NVL-CANWP-FAIL-COLL
	ESD10-NVL-DERAIL	ESD10-NVL-DERAIL-CAN	51A-NVL-CANWP-FAIL-DERAIL
	ESD10-NVL-TILT	ESD10-NVL-TILT-CAN	51A-NVL-CANWP-FAIL-TILT

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

SHIELDING. Table A4.10-5 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.10-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-10

Initiator Event Tree	Initiating Event	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	ESD10-HLW-COLLIDE-SHIELD	51A-HLW-SHLDWP-FAIL-COLL
	ESD10-HLW-DERAIL	ESD10-HLW-DERAIL-SHIELD	51A-HLW-WPSHLD-FAIL-DERAIL
	ESD10-HLW-TILT	ESD10-HLW-TILT-SHIELD	51A-HLW-SHLDWP-FAIL-TILT
IHF-ESD-10-NVL	ESD10-NVL-COLLIDE	ESD10-NVL-COLLIDE-SHIELD	51A-NVL-WPSHLD-FAIL-COLL
	ESD10-NVL-DERAIL	ESD10-NVL-DERAIL-SHIELD	51A-NVL-WPSHLD-FAIL-DERAIL
	ESD10-NVL-TILT	ESD10-NVL-TILT-SHIELD	51A-NVL-SHLDWP-FAIL-TILT

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.10-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.10-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-10

Initiator Event Tree	Initiating Event	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD10-HLW-DERAIL		
	ESD10-HLW-TILT		
IHF-ESD-10-NVL	ESD10-NVL-COLLIDE		
	ESD10-NVL-DERAIL		
	ESD10-NVL-TILT		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.10-7 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.10-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-10

Initiator Event Tree	Initiating Event	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-10-HLW	ESD10-HLW-COLLIDE	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD10-HLW-DERAIL		
	ESD10-HLW-TILT		
IHF-ESD-10-NVL	ESD10-NVL-COLLIDE	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD10-NVL-DERAIL		
	ESD10-NVL-TILT		

NOTE: ^aThis 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 IHF-ESD-11

This ESD delineates the event sequences that arise after a mechanical challenge to the waste package that occurs during the export of a waste package from the IHF (Ref. 2.2.28, Figure F-11). This includes event sequences associated with the waste package handling crane, the waste package transfer carriage, and the TEV. This ESD applies to the following waste forms:

- Naval SNF in a waste package
- HLW in a waste package.

Corresponding to each waste form unit is an initiator event tree (Table A4.11-1). 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 A4.11-1. Summary of Event Trees for IHF-ESD-11

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package containing HLW canisters	Initiator: IHF-ESD-11-HLW Response: IHF-RESP-WP3	200
Waste package containing a naval canister	Initiator: IHF-ESD-11-NVL Response: IHF-RESP-WP3	400

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

A4.11.1 Initiating Events for IHF-ESD-11

The following initiating events are associated with IHF-ESD-11. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.11-2.

TEV collision. This initiating event refers to a TEV in motion in the Waste Package Loadout Room.

Impact due to object dropped on waste package. The waste package handling crane could drop the waste package shield ring on a loaded waste package in the WPTT.

Crane interference with TEV or WPTT. Improper operation of a crane could cause an impact to a waste package.

Impact due to malfunction of the WPTT or the waste package transfer carriage. This initiating event refers to an impact that could be caused by an improper tilting or lateral motion of the WPTT or improper operation of the transfer carriage.

Table A4.11-2. Initiating Event Assignments for IHF-ESD-11

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
TEV collision	IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	51A-TEV-COLLISION
	IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL	
Impact due to object dropped on waste package	IHF-ESD-11-HLW	ESD11-HLW-DROPON	ESD11-HLW-DROPON
	IHF-ESD-11-NVL	ESD11-NVL-DROPON	ESD11-NVL-DROPON
Crane interference with TEV or WPTT	IHF-ESD-11-HLW	ESD11-HLW-CRANE	51A-OPCRANEINTFR-HFI-NOD
	IHF-ESD-11-NVL	ESD11-NVL-CRANE	
Impact due to malfunction of the WPTT or the waste package transfer carriage	IHF-ESD-11-HLW	ESD11-HLW-COLLISION	51A-OPTEVDRCLDSD-HFI-NOD OR 51A-WP-SHEAR OR 51A-WPTT-PRE-DEPARTURE
	IHF-ESD-11-NVL	ESD11-NVL-COLLISION	

NOTE: ^aThis 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 System Response Event Tree IHF-RESP-WP3

The pivotal events that appear in IHF-RESP-WP3 are summarized below. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

WP-CONTAIN. Table A4.11-3 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.11-3. Basic Event Associated with the Waste Package Pivotal Events of IHF-ESD-11

Initiator Event Tree	Initiating Event	Name Assigned to WP-CONTAIN	Associated Fault Tree or Basic Eventa
IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	ESD11-HLW-WP	51A-FAIL-EXPORT
	ESD11-HLW-DROPON		
	ESD11-HLW-CRANE		
	ESD11-HLW-COLLISION		
IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL	ESD11-NVL-WP	
	ESD11-NVL-DROPON		
	ESD11-NVL-CRANE		
	ESD11-NVL-COLLISION		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CANISTER. Table A4.11-4 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.11-4. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-11

Initiator Event Tree	Initiating Event	Name Assigned to CANISTER	Associated Fault Tree or Basic Eventa
IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	ESD11-HLW-CAN	51A-CAN-FAIL-EXPORT
	ESD11-HLW-DROPON		
	ESD11-HLW-CRANE		
	ESD11-HLW-COLLISION		
IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL	ESD11-NVL-CAN	
	ESD11-NVL-DROPON		
	ESD11-NVL-CRANE		
	ESD11-NVL-COLLISION		

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.11-5. Basic Events Associated with the SHIELDING Pivotal Events of IHF-ESD-11

Initiator Event Tree	Initiating Event	Name Assigned to WP-SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	ESD11-HLW-SHIELD	51A-WPSHIELD-FAIL-EXPORT
	ESD11-HLW-DROPON		
	ESD11-HLW-CRANE		
	ESD11-HLW-COLLISION		
IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL	ESD11-NVL-SHIELD	
	ESD11-NVL-DROPON		
	ESD11-NVL-CRANE		
	ESD11-NVL-COLLISION		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

CONFINEMENT. Table A4.11-6 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.11-6. Basic Event Associated with the CONFINEMENT Pivotal Events of IHF-ESD-11

Initiator Event Tree	Initiating Event	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	HVAC-CONF	HVAC-CONFINEMENT-FAILS
	ESD11-HLW-DROPON		
	ESD11-HLW-CRANE		
	ESD11-HLW-COLLISION		
IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL		
	ESD11-NVL-DROPON		
	ESD11-NVL-CRANE		
	ESD11-NVL-COLLISION		

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events.

Source: Original

MODERATOR. Table A4.11-7 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.11-7. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-11

Initiator Event Tree	Initiating Event	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-11-HLW	ESD11-HLW-TEV-COLL	MOD-NOFIRE-HLW	MOD-NOFIRE-HLW-NOIMP
	ESD11-HLW-DROPON		
	ESD11-HLW-CRANE		
	ESD11-HLW-COLLISION		
IHF-ESD-11-NVL	ESD11-NVL-TEV-COLL	MOD-NOFIRE	(51A-OIL-MODERATOR) OR (51A-FIRE-SUPPRESSION) OR (51A-OTHER-WATER)
	ESD11-NVL-DROPON		
	ESD11-NVL-CRANE		
	ESD11-NVL-COLLISION		

NOTE: ^aThis 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 IHF-ESD-12

IHF-ESD-12 covers event sequences associated with direct exposure during various operations (Ref. 2.2.28, Figure F-12). This ESD covers all waste forms. Basic rules instruct SAPHIRE where to look for the fault tree that models each initiating event (Table A4.12-1). The assignments made in the rules files are indicated in this section.

Table A4.12-1. Summary of Event Trees for IHF-ESD-12

Waste Form Unit	Associated Self-Contained Initiating Event Trees	Number of Waste Form Units
HLW canister	IHF-ESD-12A-HLW	1000
Naval canister	IHF-ESD-12A-NVL	400
HLW waste package	IHF-ESD-12B-HLW	200
Naval cask or waste package	IHF-ESD-12B-NVL	400
HLW waste package	IHF-ESD-12C-HLW	200
Naval waste package	IHF-ESD-12C-NVL	400

NOTE: HLW = high-level radioactive waste.

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

A4.12.1 Initiating Events for IHF-ESD-12

The following initiating events are associated with IHF-ESD-12. There are no pivotal events associated with IHF-ESD-12. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.12-2.

Temporary loss of shielding of the CTM shield bell while the canister is being lifted from a transportation cask. A loss of shielding could occur if the shield skirt is inadvertently lifted during canister transfer or if canister transfer proceeds before the shield skirt is lowered. A loss of shielding could also occur if the canister is lifted so high that it protrudes from the top of the shield bell. Because the elevation of the shield bell is fixed due to its rigid attachment to the shield bell trolley, it is not possible to cause a loss of shielding by inadvertently lifting the shield bell.

Inadvertent displacement of the naval cask shield ring from cask or waste package or improper installation of waste package shield ring on waste package. These event sequences could occur in the Cask Preparation Area or the Waste Package Loadout Room.

Direct exposure during waste package closure. This could occur due to the inadvertent opening of a personnel or equipment shield door.

Direct exposure during exporting a loaded waste package. This could occur due to the inadvertent opening of a personnel or equipment shield door.

Table A4.12-2. Initiating Event Assignments for IHF-ESD-12

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Temporary loss of shielding of the CTM shield bell while the canister is being lifted from a transportation cask	IHF-ESD-12A-HLW	ESD12A-HLW-SHLD	ESD12A-HLW-SHLD
	IHF-ESD-12A-NVL	ESD12A-NVL-SHLD	ESD12A-NVL-SHLD
Loss of shielding during preparation activities or during WP closure	IHF-ESD-12B-HLW	ESD12B-HLW-SHLD	ESD12B-HLW-SHLD-DE OR ESD12B-HLW-SHLD-RING
	IHF-ESD-12B-NVL	ESD12B-NVL-SHLD	ESD12B-NVL-SHLD-DE OR ESD12B-HLW-SHLD-RING
Direct exposure during exporting a loaded waste package	IHF-ESD-12C-HLW	ESD12C-HLW-SHLD-FACDR	51A-OPDIREXPOSE3-HFI-NOD
	IHF-ESD-12C-NVL	ESD12C-NVL-SHLD-FACDR	

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events; CTM = canister transfer machine.

Source: Original

A4.13 EVENT TREES FOR IHF-ESD-13

IHF-ESD-13 covers event sequences associated with fires in the IHF (Ref. 2.2.28, Figure F-13). This ESD covers all applicable waste forms (Table A4.13-1). 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 A4.13-1. Summary of Event Trees for IHF-ESD-13

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
HLW canisters except when in a sealed or unsealed transportation cask or a sealed or unsealed waste package	Initiator: IHF-ESD-13-HLW-CAN Response: IHF-RESP-FIRE	1,000
HLW canister in a sealed or unsealed transportation cask	Initiator: IHF-ESD-13-HLW-CSK Response: IHF-RESP-FIRE	600
HLW canister in a sealed or unsealed waste package	Initiator: IHF-ESD-13-HLW-WP Response: IHF-RESP-FIRE	200
Naval canister anywhere in the facility	Initiator: IHF-ESD-13-NVL Response: IHF-RESP-FIRE	400

NOTE: HLW = high-level radioactive waste.

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

A4.13.1 Initiating Events for IHF-ESD-13

The following initiating events are associated with IHF-ESD-13. The assignments made within SAPHIRE for quantification of these initiating events are indicated in Table A4.13-2.

Localized fire affecting a canister in the CTM. This initiating event accounts for the potential impact from a fire that threatens a canister being transferred by the CTM.

Localized fire in Cask Unloading Room. This initiating event accounts for the potential impact from a fire in the Cask Unloading Room.

Localized fire in Cask Preparation Area. This initiating event accounts for the potential impact from a fire in the Cask Preparation Area.

Localized fire in Waste Package Loadout Room. This initiating event accounts for the potential impact from a fire in the Waste Package Loadout Room.

Localized fire in Waste Package Loading Room. This initiating event accounts for the potential impact from a fire in the Waste Package Loading Room.

Localized fire in Waste Package Positioning Room. This initiating event accounts for the potential impact from a fire in the Waste Package Positioning Room.

Large fire in IHF. This initiating event accounts for the potential impact from a large fire in the IHF.

Table A4.13-2. Initiating Event Assignments for IHF-ESD-13

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment by Basic Rules	SAPHIRE Assignment at Fault Tree Level ^a
Localized fire affecting a canister in the CTM	IHF-ESD-13-HLW-CAN	ESD13-HLW-CAN-CTM-FIRE	51A-HLW-CAN-CTM-FIRE
	IHF-ESD-13-HLW-CSK	N/A	N/A
	IHF-ESD-13-HLW-WP	N/A	N/A
	IHF-ESD-13-NVL	ESD13-NVL-CAN-CTM-FIRE	51A-HLW-CAN-CTM-FIRE
Localized fire in Cask Unloading Room	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CUR-FIRE	51A-HLW-CSK-CUR-FIRE
	IHF-ESD-13-HLW-WP	N/A	N/A
	IHF-ESD-13-NVL	ESD13-NVL-CSK-CUR-FIRE	51A-NVL-CSK-CUR-FIRE
Localized fire in Cask Preparation Area	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CPA-FIRE	51A-HLW-CSK-CPA-FIRE
	IHF-ESD-13-HLW-WP	N/A	N/A
	IHF-ESD-13-NVL	ESD13-NVL-CSK-CPA-FIRE	51A-NVL-CSK-CPA-FIRE
Localized fire in Waste Package Loadout Room	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	N/A	N/A
	IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LOR-FIRE	51A-HLW-WP-LOR-FIRE
	IHF-ESD-13-NVL	ESD13-NVL-WP-LOR-FIRE	51A-NVL-WP-LOR-FIRE
Localized fire in Waste Package Loading Room	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	N/A	N/A
	IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LR-FIRE	51A-HLW-WP-LR-FIRE
	IHF-ESD-13-NVL	ESD13-NVL-WP-LR-FIRE	51A-NVL-WP-LR-FIRE
Localized fire in Waste Package Positioning Room	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	N/A	N/A
	IHF-ESD-13-HLW-WP	ESD13-HLW-WP-PR-FIRE	51A-HLW-WP-PR-FIRE
	IHF-ESD-13-NVL	ESD13-NVL-WP-PR-FIRE	51A-NVL-WP-PR-FIRE
Large fire in IHF	IHF-ESD-13-HLW-CAN	N/A	N/A
	IHF-ESD-13-HLW-CSK	N/A	N/A
	IHF-ESD-13-HLW-WP	ESD13-HLW-LG-FIRE	51A-HLW-LG-FIRE
	IHF-ESD-13-NVL	ESD13-NVL-LG-FIRE	51A-NVL-LARGE-FIRE

NOTE: ^aThis column may contain fault trees and basic events. See Attachment B for fault trees and Attachment C for basic events; CTM = canister transfer machine; IHF – Initial Handling Facility.

Source: Original

A4.13.2 System Response Event Tree IHF-RESP-FIRE

The pivotal events that appear in IHF-RESP-FIRE are listed below and summarized in Section A3. The accompanying tables show the association of pivotal event names with basic event or fault tree names.

CANISTER. Table A4.13-3 specifies the fault tree or 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 IHF-ESD-13

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event^a
IHF-ESD-13-HLW-CAN	ESD13-HLW-CAN-CTM-FIRE	ESD13-HLW-CANF-CTM-FIRE	51A-HLW-CAN-CONT-CTM-FIR
IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CUR-FIRE	ESD13-HLW-CANF-CUR-FIRE	51A-HLW-CAN-CONT-CUR-FIR
	ESD13-HLW-CSK-CPA-FIRE	ESD13-HLW-CANF-CPA-FIRE	[(51A-HLW-SPMRC-DIESEL) AND (51A-HLW-CAN-DIESEL)] OR [(51A-HLW-SPMRC-WODIESEL) AND (51A-HLW-FAILCAN-WODIESEL)]
IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LOR-FIRE	ESD13-HLW-CANF-LOR-FIRE	[(51A-PROB-HLWCAN-WPTT-LOR) AND (51A-HLWCAN-WPTT-FAIL-FIR)] OR [(51A-PROB-HLWCAN-WP-LOR) AND (51A-HLWCAN-WP-FAIL-FIRE)]
	ESD13-HLW-WP-LR-FIRE	ESD13-HLW-CANF-LR-FIRE	51A-HLW-CAN-CONT-LR-FIR
	ESD13-NVL-WP-PR-FIRE	ESD13-NVL-CANF-PR-FIRE	51A-HLW-CAN-CONT-PR-FIR
	ESD13-HLW-LG-FIRE	ESD13-HLW-CANF-LG-FIRE	[(51A-HLW-FREQ-DIESEL) AND (51A-HLW-CAN-WDIESEL)] OR [(51A-HLW-LARGE-FIRE-CTM) AND (51A-HLW-CAN-FAILS-CTM)] OR [(51A-HLW-FREQ-NO-DIESEL) AND (51A-HLW-CAN-FAIL-NOD)] OR [(51A-HLW-FREQ-WP-FAILS) AND (51A-HLW-CAN-FAIL-IN-WP)]

Table A4.13-3. Basic Events Associated with the CANISTER Pivotal Events of IHF-ESD-13 (Continued)

Initiator Event Tree	Initiating Event Name	Name Assigned to CANISTER	Associated Fault Tree or Basic Event ^a
IHF-ESD-13-NVL	ESD13-NVL-CAN-CTM-FIRE	ESD13-NVL-CANF-CTM-FIRE	51A-NVL-CAN-CONT-CTM-FIRE
	ESD13-NVL-CSK-CUR-FIRE	ESD13-NVL-CANF-CUR-FIRE	51A-NVL-CAN-CONT-CUR-FIRE
	ESD13-NVL-CSK-CPA-FIRE	ESD13-NVL-CANF-CPA-FIRE	[(51A-NVL-SPMRC-DIESEL) AND (51A-NVL-FAIL-CAN-DIESEL)] OR [(51A-NVL-SPMRC-WODIESEL) AND (51A-NVL-FAILCAN-WODIESEL)]
	ESD13-NVL-WP-LOR-FIRE	ESD13-NVL-CANF-LOR-FIRE	[(51A-PROB-NVLCAN-WPTT-LOR) AND (51A-NVLCAN-FAILWPTT-LOR)] OR [(51A-PROB-NVLCAN-WP-LOR) AND (51A-NVLCAN-WP-FAIL-LOR)]
	ESD13-NVL-WP-LR-FIRE	ESD13-NVL-CANF-LR-FIRE	51A-NVL-CAN-CONT-LR-FIRE
	ESD13-NVL-WP-PR-FIRE	ESD13-NVL-CANF-PR-FIRE	51A-NVL-CAN-CONT-PR-FIRE
	ESD13-NVL-LG-FIRE	ESD13-NVL-CANF-LG-FIRE	[(51A-NVL-CAN-FAIL-NOD) AND (51A-NVL-FREQ-NO-DIESEL)] OR [(51A-NVL-CAN-FAIL-IN-WP) AND (51A-NVL-FREQ-WP-FAILS)] OR [(51A-NVL-CAN-FAILS-CTM) AND (51A-NVL-LARGE-FIRE-CTM)] OR [(51A-FREQ-DIESEL-PRESENT) AND (51A-NVL-CAN-WDIESEL)]

NOTE: ^aThis 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 shielding provided by the transportation cask, CTM shield bell, WPTT shield compartment, TEV shield compartment, or shield doors as a result of the initiating event. Table A4.13-4 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.13-4. Fault Tree Associated with the SHIELDING Pivotal Events of IHF-ESD-13

Initiator Event Tree	Initiating Event Name	Name Assigned to SHIELDING	Associated Fault Tree or Basic Event ^a
IHF-ESD-13-HLW-CAN	ESD13-HLW-CAN-CTM-FIRE	ESD13-HLW-SHLD-FIRE	51A-HLW-CAN-SHIELD-CTM
IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CUR-FIRE	ESD13-HLW-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS
	ESD13-HLW-CSK-CPA-FIRE	ESD13-HLW-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS
IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LOR-FIRE	ESD13-HLW-SHLD-FIRE	51A-HLW-CAN-SHIELD-CTM
	ESD13-HLW-WP-LR-FIRE	ESD13-HLW-SHLD-FIRE	51A-HLW-CAN-SHIELD-CTM
	ESD13-NVL-WP-PR-FIRE	ESD13-HLW-SHLD-FIRE	51A-HLW-CAN-SHIELD-CTM
	ESD13-HLW-LG-FIRE	ESD13-HLW-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS
IHF-ESD-13-NVL	ESD13-NVL-CAN-CTM-FIRE	ESD13-NVL-SHLD-FIRE	51A-NVL-SHLD-FIRE-FAILS
	ESD13-NVL-CSK-CUR-FIRE	ESD13-NVL-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS
	ESD13-NVL-CSK-CPA-FIRE	ESD13-NVL-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS
	ESD13-NVL-WP-LOR-FIRE	ESD13-NVL-SHLD-FIRE	51A-NVL-SHLD-FIRE-FAILS
	ESD13-NVL-WP-LR-FIRE	ESD13-NVL-SHLD-FIRE	51A-NVL-SHLD-FIRE-FAILS
	ESD13-NVL-WP-PR-FIRE	ESD13-NVL-SHLD-FIRE	51A-NVL-SHLD-FIRE-FAILS
	ESD13-NVL-LG-FIRE	ESD13-NVL-TC-SHLD-FIRE	51A-TC-SHLD-FIRE-FAILS

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event.

Table A4.13-5. Fault Tree Associated with the CONFINEMENT Pivotal Events of IHF-ESD-13

Initiator Event Tree	Initiating Event Name	Name Assigned to CONFINEMENT	Associated Fault Tree or Basic Event ^a
IHF-ESD-13-HLW-CAN	ESD13-HLW-CAN-CTM-FIRE	HVAC-CONF	HVAC-CONFINEMENT-FAILS
IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CUR-FIRE		
	ESD13-HLW-CSK-CPA-FIRE		
IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LOR-FIRE		
	ESD13-HLW-WP-LR-FIRE		
	ESD13-NVL-WP-PR-FIRE		
	ESD13-HLW-LG-FIRE		
IHF-ESD-13-NVL	ESD13-NVL-CAN-CTM-FIRE		
	ESD13-NVL-CSK-CUR-FIRE		
	ESD13-NVL-CSK-CPA-FIRE		
	ESD13-NVL-WP-LOR-FIRE		
	ESD13-NVL-WP-LR-FIRE		
	ESD13-NVL-WP-PR-FIRE		
	ESD13-NVL-LG-FIRE		

NOTE: ^aThis 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 specifies the fault tree or basic event that is associated with this pivotal event for each initiating event (introduction of liquid moderator).

Table A4.13-6. Basic Event Associated with the MODERATOR Pivotal Events of IHF-ESD-13

Initiator Event Tree	Initiating Event Name	Name Assigned to MODERATOR	Associated Fault Tree or Basic Event ^a
IHF-ESD-13-HLW-CAN	ESD13-HLW-CAN-CTM-FIRE	MOD-FIRE-HLW	51A-MOD-FIRE-HLW-NOIMP
IHF-ESD-13-HLW-CSK	ESD13-HLW-CSK-CUR-FIRE		
	ESD13-HLW-CSK-CPA-FIRE		
IHF-ESD-13-HLW-WP	ESD13-HLW-WP-LOR-FIRE		
	ESD13-HLW-WP-LR-FIRE		
	ESD13-NVL-WP-PR-FIRE		
	ESD13-HLW-LG-FIRE		
IHF-ESD-13-NVL	ESD13-NVL-CAN-CTM-FIRE	MOD-FIRE	51A-MODERATOR-ENTERS-CAN
	ESD13-NVL-CSK-CUR-FIRE		
	ESD13-NVL-CSK-CPA-FIRE		
	ESD13-NVL-WP-LOR-FIRE		
	ESD13-NVL-WP-LR-FIRE		
	ESD13-NVL-WP-PR-FIRE		
	ESD13-NVL-LG-FIRE		

NOTE: ^aThis 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 IET 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.

Number of waste forms processed over facility	Identify initiating events			
NUMBER-WAS	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		
		2	T => 2	RESPONSE-SAMPLE
		3	T => 2	RESPONSE-SAMPLE
		4	T => 2	RESPONSE-SAMPLE

Indicates transfer to the system response event tree on Sheet 2

Indicates the name of the system response event tree

Sheet number appears here on each sheet

INIT-EVENT - Sample Initiating Event Tree

2007/10/24 Sheet 1

Source: Original

Figure A5-1. Example Initiator Event Tree Showing Navigation Aids

Table A5-1. Relation of Event Sequence Diagrams to Event Trees

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
IHF-ESD-01	Event Sequences for Activities Associated with Receipt of Naval or HLW TC on RC or TT in Cask Preparation Area and Upending and Transfer of Naval TC to CTT	ESD-01-HLW ESD-01-NVL	Figure A5-2 Figure A5-4	IHF-RESP-TC1 IHF-RESP-TC1	Figure A5-3
IHF-ESD-02	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending and Transfer of HLW Cask to CTT and Removal of Impact Limiters from Naval TC	ESD-02-HLW ESD-02-NVL	Figure A5-5 Figure A5-6	IHF-RESP-TC1 IHF-RESP-TC1	Figure A5-3 Figure A5-3
IHF-ESD-03	Event Sequences for Activities Associated with Cask Preparation Activities Associated with Unbolting and Lid Adapter Installation for the HLW Cask	ESD-03-HLW	Figure A5-7	IHF-RESP-TC1	Figure A5-3
IHF-ESD-04	Event Sequences for Activities Associated with Removal of the Naval Cask Lid and Installing the Naval Canister Lifting Adapter	ESD-04-NVL	Figure A5-8	IHF-RESP-CAN1	Figure A5-9
IHF-ESD-05	Event Sequences for Activities Associated with Transfer of a Cask on CTT from Cask Preparation Area to Cask Unloading Room	ESD-05-HLW ESD-05-NVL	Figure A5-10 Figure A5-12	IHF-RESP-CAN2-HLW IHF-RESP-CAN2-NVL	Figure A5-11 Figure A5-13
IHF-ESD-06	Event Sequences for Activities Associated with Collision of CTT with Cask Unloading Room Shield Door	ESD-06-HLW ESD-06-NVL	Figure A5-14 Figure A5-15	N/A N/A	N/A N/A
IHF-ESD-07	Event Sequences for Activities Associated with the Transfer of a Canister to or from a TC to a WP with CTM	ESD-07-HLW ESD-07-NVL	Figure A5-16 Figure A5-17	IHF-RESP-CAN1 IHF-RESP-CAN1	Figure A5-9 Figure A5-9
IHF-ESD-08	Event Sequences for Activities Associated with WP Transfer from WP Loading Room to Closing Position in WP Positioning Room below WP Closure Room	ESD-08-HLW ESD-08-NVL	Figure A5-18 Figure A5-20	IHF-RESP-WP1 IHF-RESP-WP1	Figure A5-19 Figure A5-19

Table A5-1. Relation of Event Sequence Diagrams to Event Trees (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
IHF-ESD-09	Event Sequences for Activities Associated with Assembly and Closure of the WP	ESD-09-HLW ESD-09-NVL	Figure A5-21 Figure A5-23	IHF-RESP-WP2 IHF-RESP-WP2	Figure A5-22 Figure A5-22
IHF-ESD-10	Event Sequences for Activities Associated with the Transfer of the WP from the WP Positioning Room to the WPTT Docking Station	ESD-10-HLW ESD-10-NVL	Figure A5-24 Figure A5-26	IHF-RESP-WP3 IHF-RESP-WP3	Figure A5-25 Figure A5-25
IHF-ESD-11	Event Sequences for Activities Associated with Exporting a WP	ESD-11-HLW ESD-11-NVL	Figure A5-27 Figure A5-28	IHF-RESP-WP3 IHF-RESP-WP3	Figure A5-25 Figure A5-25
IHF-ESD-12	Event Sequences for Activities Associated with Direct Exposure During Various Activities	ESD-12A-HLW ESD-12A-NVL ESD-12B-HLW ESD-12B-NVL ESD-12C-HLW ESD-12C-NVL	Figure A5-29 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34	N/A	N/A
IHF-ESD-13	Event Sequences Associated with Fires Occurring in the IHF	ESD-13-HLW-CAN ESD-13-HLW-CSK ESD-13-HLW-WP ESD-13-NVL	Figure A5-35 Figure A5-37 Figure A5-38 Figure A5-39	IHF-RESP-FIRE IHF-RESP-FIRE IHF-RESP-FIRE IHF-RESP-FIRE	Figure A5-36 Figure A5-36 Figure A5-36 Figure A5-36

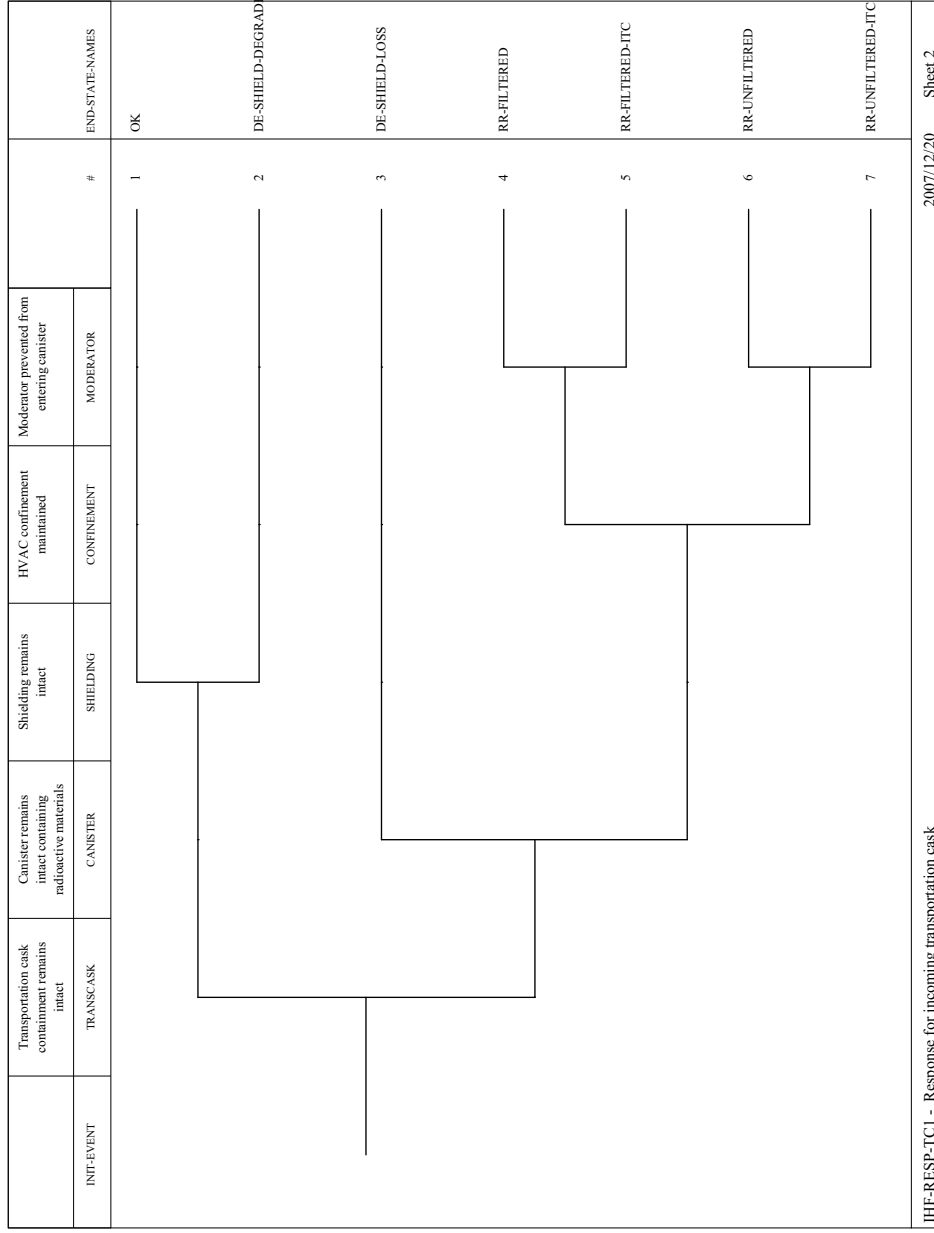
NOTE: CAN = canister; CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HLW = high-level radioactive waste; IHF = Initial Handling Facility; NVL = naval; RC = railcar; RESP = response; TC = transportation cask; TT = truck trailer; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

Number of HLW casks received by IHF during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-CSK	INIT-EVENT		
			1	OK
		Railcar derailment	2 T => 2	IHF-RESP-TC1
		HLW TT rollover	3 T => 2	IHF-RESP-TC1
		RC/TT collision	4 T => 2	IHF-RESP-TC1
IHF-ESD-01-HLW - Receipt of HLW TC in the Cask Preparation Area				2007/12/04 Sheet 1

Source: Original

Figure A5-2. Event Tree IHF-ESD-01-HLW –
Receipt of HLW TC in the Cask
Preparation Area



Source: Original

Figure A5-3. Event Tree IHF-RESP-TC1 – Response for Incoming Transportation Cask

Number of naval casks received by IHF over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		Crane drops object	2 T => 2	IHF-RESP-TCI
		Crane drops TC from operational height	3 T => 2	IHF-RESP-TCI
		Crane drops TC from above operational height	4 T => 2	IHF-RESP-TCI
		Railcar derailment	5 T => 2	IHF-RESP-TCI
		RC collision	6 T => 2	IHF-RESP-TCI
		Cask collision off railcar	7 T => 2	IHF-RESP-TCI
		Naval TC tipover	8 T => 2	IHF-RESP-TCI
IHF-ESD-01-NVL - Receipt of naval TC in the Cask Preparation Area and transfer to CTT				
				2008/01/04
				Sheet 3

Source: Original

Figure A5-4. Event Tree IHF-ESD-01-NVL -
Receipt of Naval TC in the Cask
Preparation Area and Transfer to
CTT

Number of HLW casks received by IHF over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-CSK	INIT-EVENT		
			1	OK
		Cask drop from operational height	2 T => 2	IHF-RESP-TC1
		Cask drop from above operational height	3 T => 2	IHF-RESP-TC1
		Unplanned conveyance movement	4 T => 2	IHF-RESP-TC1
		Collision with side impact	5 T => 2	IHF-RESP-TC1
		Dropped object	6 T => 2	IHF-RESP-TC1
		HLW TC tip over	7 T => 2	IHF-RESP-TC1
IHF-ESD-02-HLW - HLW TC upending and removal from conveyance				
				2007/10/26 Sheet 4

Source: Original

Figure A5-5. Event Tree IHF-ESD-02-HLW – HLW TC Upending and Removal from Conveyance

Number of Naval Casks		#	XFER-TO-RESP-TREES
NUM_NVL	INIT-EVENT		
		1	OK
	Side Impact	2 T => 2	IHF-RESP-TC1
	Drop of Heavy Object	3 T => 2	IHF-RESP-TC1
IHF-ESD-02-NVL - Remove Impact Limiters from NVL TC			2007/12/05 Sheet 5

Source: Original

Figure A5-6. Event Tree IHF-ESD-02-NVL -
Remove Impact Limiters from NVL
TC

Number of HLW casks received by the IHF over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-CSK	INIT-EVENT		
			1	OK
		Cask tips over	2 T => 2	IHF-RESP-TC1
		Side impact	3 T => 2	IHF-RESP-TC1
		Dropped object	4 T => 2	IHF-RESP-TC1
IHF-ESD-03-HLW - HLW TC preparation activities				
				2007/10/26 Sheet 6

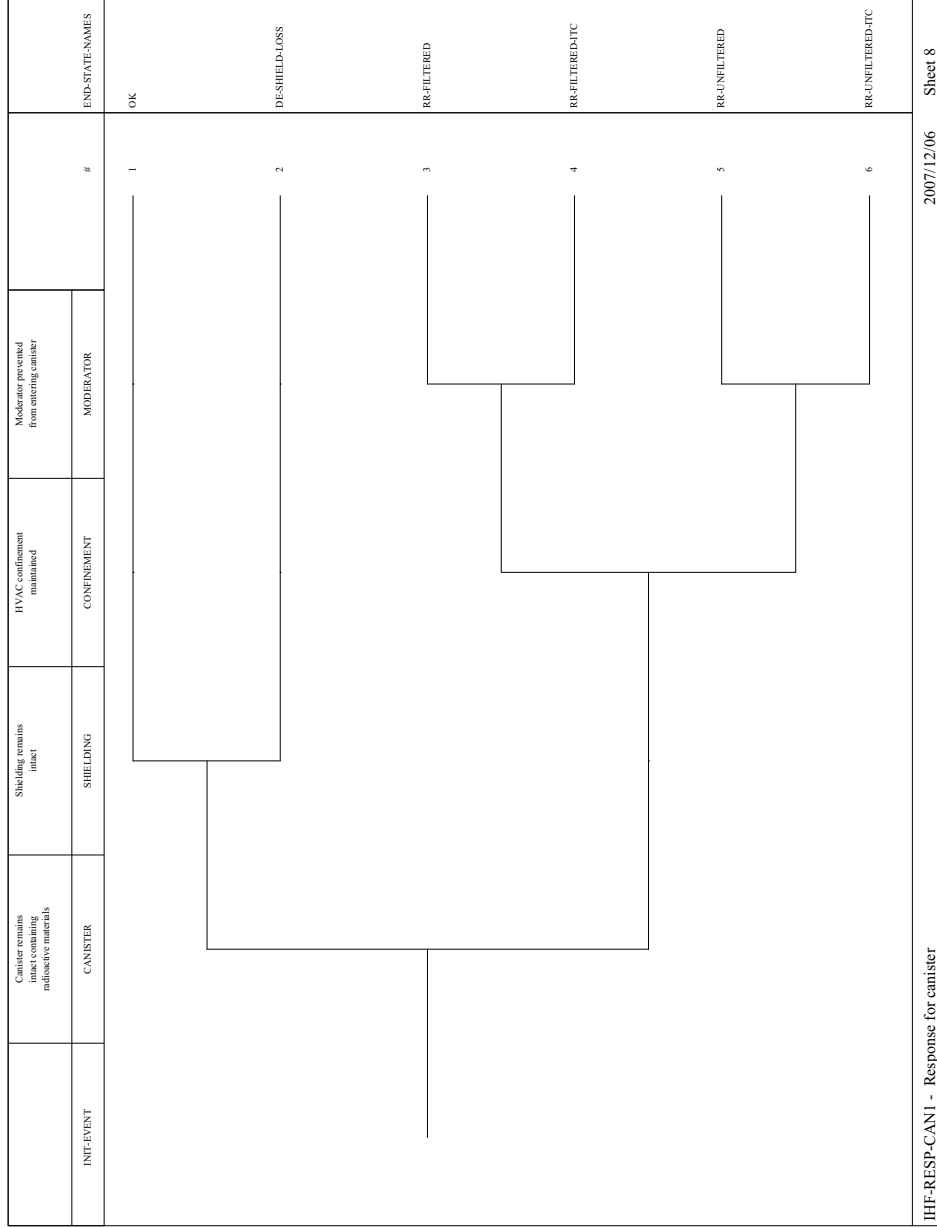
Source: Original

Figure A5-7. Event Tree IHF-ESD-03-HLW –
HLW TC Preparation Activities

Number of naval casks received by IHF over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		Cask tips over	2	IHF-RESP-CANI
		Side impact	3	IHF-RESP-CANI
		Dropped object	4	IHF-RESP-CANI
IHF-ESD-04-NVL - Naval TC preparation activities				2007/12/04 Sheet 7

Source: Original

Figure A5-8. Event Tree IHF-ESD-04-NVL –
Naval TC Preparation Activities



IHF-RESP-CAN1 - Response for canister

2007/12/06

Sheet 8

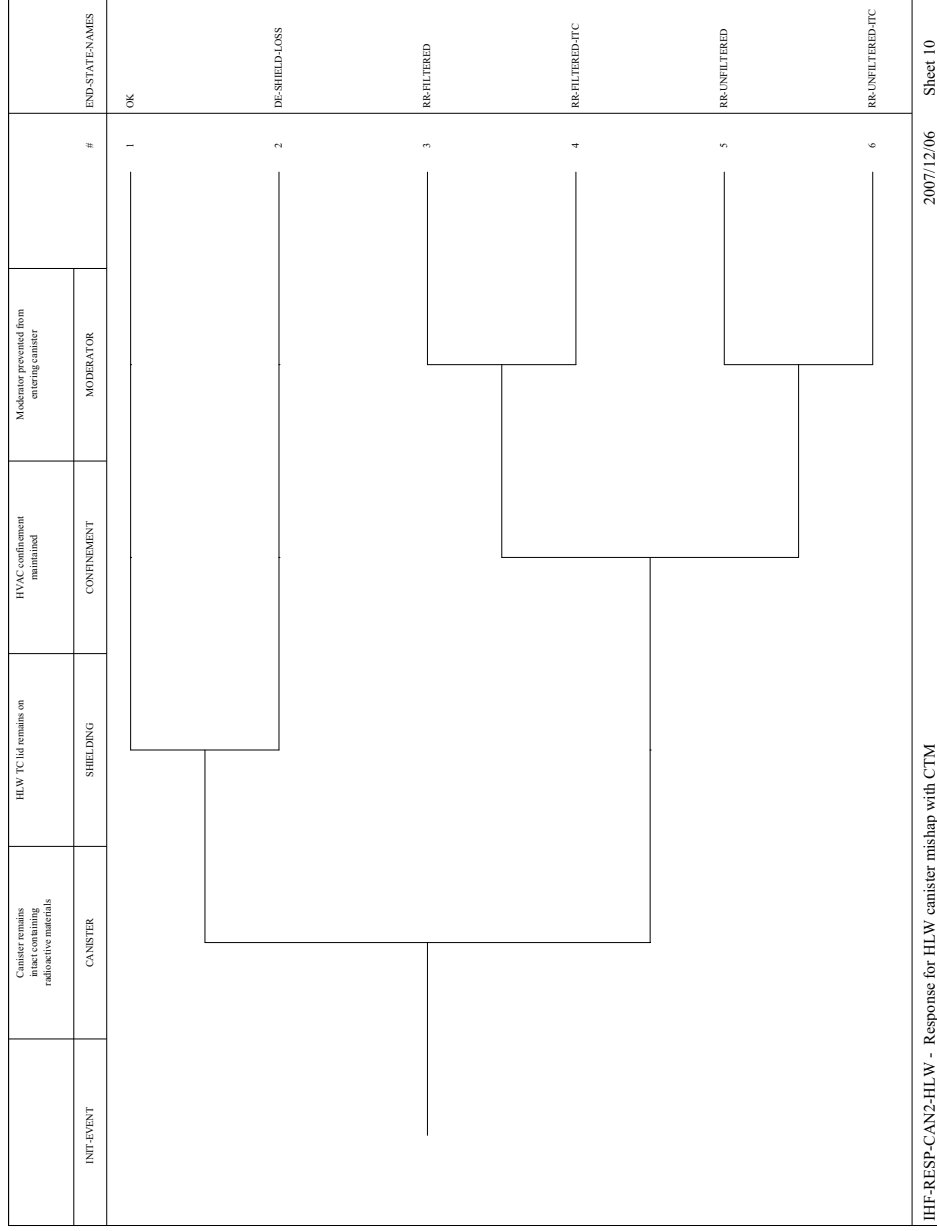
Source: Original

Figure A5-9. Event Tree IHF-RESP-CAN1 -
Response for Canister

Number of HLW casks received during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-CSK	INIT-EVENT		
			1	OK
		Crane-induced impact to TC	2	IHF-RESP-CAN2-HLW
		CTT Collision	3	IHF-RESP-CAN2-HLW
IHF-ESD-05-HLW - Transfer HLW TC on CTT from Cask Preparation Area to Cask Unloading Room				2007/1220 Sheet 9

Source: Original

Figure A5-10. Event Tree IHF-ESD-05-HLW –
Transfer HLW TC on CTT from
Cask Preparation Area to Cask
Unloading Room



IHF-RESP-CAN2-HLW - Response for HLW canister mishap with CTM

2007/12/06

Sheet 10

Source: Original

Figure A5-11. Event Tree IHF-RESP-CAN2-HLW - Response for HLW Canister Mishap with CTM

Number of naval casks received during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		Crane-induced impact to TC	2	IHF-RESP-CAN2-NVL
		CTT Collision	3	IHF-RESP-CAN2-NVL
IHF-ESD-05-NVL - Transfer Naval TC on CTT from Cask Preparation Area to Cask Unloading Room				2007/10/26 Sheet 11

Source: Original

Figure A5-12. Event Tree IHF-ESD-05-NVL –
Transfer Naval TC on CTT from
Cask Preparation Area to Cask
Unloading Room

INT-EVENT	Canister remains intact containing radioactive materials CANISTER	Naval cask shield ring remains in place SHIELD-RING	HVAC confinement maintained CONFINEMENT	Moderator prevented from entering canister		#	END-STATE-NAMES
					MODERATOR		
		1	OK				
		2	DE-SHIELD-LOSS				
		3	RR-FILTERED				
		4	RR-FILTERED-ITC				
		5	RR-UNFILTERED				
		6	RR-UNFILTERED-ITC				
IHF-RESP-CAN2-NVL - Response for NVL canister mishap with CTM							
							2007/12/06 Sheet 12

Source: Original

Figure A5-13. Event Tree IHF-RESP-CAN2-NVL - Response for NVL Canister Mishap with CTM

Number of HLW casks received during preclosure period	CTT avoids collision with shield door	Door remains on tracks and does not fall onto CTT	Casker containment boundary remains intact	Shielding remains intact	HVAC Confinement boundary intact	Moderator prevented from entering casker	#	END-STATE-NAMES	
									INT-EVENT
							1	OK	
							2	OK	
							3	DE-SHIELD-LOSS	
							4	RR-FILTERED	
							5	RR-FILTERED-ITC	
							6	RR-UNFILTERED	
							7	RR-UNFILTERED-ITC	
							8	OK	
							9	DE-SHIELD-LOSS	
							10	RR-FILTERED	
							11	RR-FILTERED-ITC	
							12	RR-UNFILTERED	
							13	RR-UNFILTERED-ITC	
IHf-ESD-06-HLW - CTT with HLW TC collides with shield door to Cask Unloading Room								2007/10/26	Sheet 13

Source: Original

Figure A5-14. Event Tree IHf-ESD-06-HLW –
CTT with HLW TC Collides with
Shield Door to Cask Unloading
Room

Number of fuel casks received at IHF over the preclusion period	CTT avoids collision with shield door	Door remains on tracks and does not fall onto CTT	Caskster containment boundary remains intact	Shielding remains intact	HVAC Confinement boundary intact	Moderator prevented from entering caskster	#	ENDSTATE-NAMES
NUM-NVL	INF-EVENT	CELL-DOOR	CONTAINMENT	SHIELDING	CONFINEMENT	MODERATOR	1	OK
							2	OK
							3	DESIELDALOSS
							4	RR-FILTERED
							5	RR-FILTERED>ITC
							6	RR-UNFILTERED
							7	RR-UNFILTERED>ITC
							8	OK
							9	DESIELDALOSS
							10	RR-FILTERED
							11	RR-FILTERED>ITC
							12	RR-UNFILTERED
							13	RR-UNFILTERED>ITC

IHF-ESD-06-NVL - CTT with naval TC collides with shield door to Cask Unloading Room

2007/10/26

Sheet 14

Source: Original

Figure A5-15. Event Tree IHF-ESD-06-NVL – CTT with Naval TC Collides with Shield Door to Cask Unloading Room

Number of HLW Canisters received during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-CAN	INIT-EVENT		
			1	OK
		Object dropped onto canister		
		Canister impact due to movement of CTM, CTT, WPTT	2 T => 8	IHF-RESP-CANI
			3 T => 8	IHF-RESP-CANI
		Canister drop from operational height	4 T => 8	IHF-RESP-CANI
		Canister drop from above operational height	5 T => 8	IHF-RESP-CANI
		Side impact to canister	6 T => 8	IHF-RESP-CANI
		Canister collision or impact	7 T => 8	IHF-RESP-CANI
		Canister dropped inside CTM	8 T => 8	IHF-RESP-CANI
		HLW TC impact - lid removal	9 T => 8	IHF-RESP-CANI
IHF-ESD-07-HLW - Transferring a HLW canister with the CTM				2007/12/04 Sheet 15

Source: Original

Figure A5-16. Event Tree IHF-ESD-07-HLW –
Transfer a HLW Canister with
the CTM

Number of naval canisters received during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		Object dropped onto canister	2	IHF-RESP-CANI
		CTM, CTT, WPTT movement	3	IHF-RESP-CANI
		Canister drop from operational height	4	IHF-RESP-CANI
		Canister drop from above op. height	5	IHF-RESP-CANI
		Side impact to canister	6	IHF-RESP-CANI
		Canister collision or impact	7	IHF-RESP-CANI
		Canister dropped inside CTM	8	IHF-RESP-CANI
IHF-ESD-07-NVL - Transferring a NVL canister with the CTM				
				2007/12/04 Sheet 16

Source: Original

Figure A5-17. Event Tree IHF-ESD-07-NVL –
Transferring a NVL Canister with
the CTM

Number of HLW WPs loaded during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-WP	INIT-EVENT		
			1	OK
		WPTT collision	2	IHF-RESP-WP1
		Premature WPTT tilt-down	3	IHF-RESP-WP1
		WPTT derailment	4	IHF-RESP-WP1

IHF-ESD-08-HLW - Transfer HLW WP on WPTT from WP Loading Room to WP Positioning Room

2007/11/05 Sheet 17

Source: Original

Figure A5-18. Event Tree IHF-ESD-08-HLW – Transfer HLW WP on WPTT from WP Loading Room to WP Positioning Room

INIT-EVENT	Canister remains intact containing radioactive materials CANISTER	WP remains within WPTT shields SHIELDING	HVAC Confinement boundary intact CONFINEMENT	Moderator prevented from entering container		#	END-STATE-NAMES	
					MODERATOR			
						1	OK	
						2	DE-SHIELD-LOSS	
						3	RR-FILTERED	
						4	RR-FILTERED-ITC	
						5	RR-UNFILTERED	
						6	RR-UNFILTERED-ITC	
IHF-RESP-WP1 - Response for moving unsealed WP							2007/12/12	Sheet 18

Source: Original

Figure A5-19. Event Tree IHF-RESP-WP1 –
Response for Moving Unsealed
WP

Number of naval WPs loaded over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		WPTT collision	2	IHF-RESP-WP1
		Premature WPTT tilt-down	3	IHF-RESP-WP1
		WPTT derailment	4	IHF-RESP-WP1
IHF-ESD-08-NVL - Transfer Naval WP on WPTT from WP Loading Room to WP Positioning Room				2007/11/05 Sheet 19

Source: Original

Figure A5-20. Event Tree IHF-ESD-08-NVL – Transfer Naval WP on WPTT from WP Loading Room to WP Positioning Room

Number of WPs with HLW canisters loaded during the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-WP	INIT-EVENT		
			1	OK
		Welding damages canister	2	IHF-RESP-WP2
		RHS drops object onto WP lid	3	IHF-RESP-WP2
IHF-ESD-09-HLW - Assembly and closure of the HLW WP				2007/12/20 Sheet 20

Source: Original

Figure A5-21. Event Tree IHF-ESD-09-HLW – Assembly and Closure of the HLW WP

INIT-EVENT	Canister remains intact containing radioactive materials CANISTER	Shielding associated with WP and WPTT remains in place WP	HVAC Confinement boundary intact CONFINEMENT	Moderator prevented from entering canister MODERATOR	#	END-STATE-NAMES
					1	OK
					2	DE-SHIELD-LOSS
					3	RR-FILTERED
					4	RR-FILTERED-ITC
					5	RR-UNFILTERED
					6	RR-UNFILTERED-ITC
IHf-RESP-WP2 - Response for WP during closure						2007/10/26 Sheet 21

Source: Original

Figure A5-22. Event Tree IHf-RESP-WP2 – Response for WP during Closure

Number of naval WPs loaded during preclosure period	Identify initiating events	#	XFER-TO-RESP-TREE
NUM-NVL	INIT-EVENT		
		1	OK
	Welding damages canister	2 T => 21	IHF-RESP-WP2
	RHS drops object onto WP lid	3 T => 21	IHF-RESP-WP2
IHF-ESD-09-NVL - Assembly and closure of the naval WP			2007/10/26 Sheet 22

Source: Original

Figure A5-23. Event Tree IHF-ESD-09-NVL –
Assembly and Closure of the
Naval WP

Number of WPs with HLW canisters loaded during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-WP	INIT-EVENT		
			1	OK
		WPTT derailment	2	IHF-RESP-WP3
		Improper tilt-down or departure of WPTT	3	IHF-RESP-WP3
		WPTT collision	4	IHF-RESP-WP3
IHF-ESD-10-HLW - Transfer HLW WP on WPTT from WP Positioning Room to WP Loadout Room				2007/10/26 Sheet 23

Source: Original

Figure A5-24. Event Tree IHF-ESD-10-HLW –
Transfer HLW WP on WPTT
from WP Positioning Room to
WP Loadout Room

INT-EVENT	WP-CONTAIN	WP containment remains intact	Canister remains intact containing radioactive materials	Canister	WP remains within WPTT shields	SHIELDING	HVAC Confinement boundary intact	CONFINEMENT	Moderator prevented from entering canister	MODERATOR	#	END-STATE-NAMES	
											1	OK	
											2	DE-SHIELD-LOSS	
											3	DE-SHIELD-LOSS	
											4	RR-FILTERED	
											5	RR-FILTERED-ITC	
											6	RR-UNFILTERED	
											7	RR-UNFILTERED-ITC	
IHF-RESP-WP3 - Response for sealed WP												2007/12/04	Sheet 24

Source: Original

Figure A5-25. Event Tree IHF-RESP-WP3 –
Response for Sealed WP

Number of WPs with naval canisters loaded over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		WPTT derailment	2 T => 24	IHF-RESP-WP3
		Improper tilt-down or departure of WPTT	3 T => 24	IHF-RESP-WP3
		WPTT collision	4 T => 24	IHF-RESP-WP3
IHF-ESD-10-NVL - Transfer naval WP on WPTT from WP Positioning Room to WP Loadout Room				
				2007/10/26
				Sheet 25

Source: Original

Figure A5-26. Event Tree IHF-ESD-10-NVL –
Transfer Naval WP on WPTT
from WP Positioning Room to
WP Loadout Room

Number of WPs with HLW canisters loaded during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-HLW-WP	INIT-EVENT		
			1	OK
		TEV collision	2	IHF-RESP-WP3
		Object drop onto WP	3	IHF-RESP-WP3
		Crane interference	4	IHF-RESP-WP3
		WPTT or WPTC malfunction	5	IHF-RESP-WP3
IHF-ESD-11-HLW - Export HLW WP from IHF				2007/10/26 Sheet 26

Source: Original

Figure A5-27. Event Tree IHF-ESD-11-HLW –
Export HLW WP from IHF

Number of WPs with naval canisters loaded during preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		TEV collision	2 T => 24	IHF-RESP-WP3
		Object drop onto WP	3 T => 24	IHF-RESP-WP3
		Crane interference	4 T => 24	IHF-RESP-WP3
		WPTT or WPTC malfunction	5 T => 24	IHF-RESP-WP3
IHF-ESD-11-NVL - Export naval WP from IHF				2007/11/03 Sheet 27

Source: Original

Figure A5-28. Event Tree IHF-ESD-11-NVL –
Export Naval WP from IHF

Number of HLW canisters received at IHF over the preclosure period	Shielding remains effective during canister transfer	#	END-STATE-NAMES
NUM-HLW-CAN	INIT-EVENT		
		1	OK
	Loss of Shielding Associated with Canister Transfer	2	DE-SHIELD-LOSS

IHF-ESD-12A-HLW - Direct exposure during canister transfer

2007/12/04 Sheet 28

Source: Original

Figure A5-29. Event Tree IHF-ESD-12A-HLW –
Direct Exposure during Canister
Transfer

Number of naval casks received during preclosure period	Shielding remains effective during canister transfer	#	END-STATE-NAMES
NUM-NVL	INIT-EVENT		
	<p style="text-align: center;">Loss of Shielding Associated with Canister Transfer</p>	<p style="text-align: center;">1</p>	<p style="text-align: center;">OK</p>
		<p style="text-align: center;">2</p>	<p style="text-align: center;">DE-SHIELD-LOSS</p>

IHF-ESD-12A-NVL - Direct exposure during canister transfer

2007/11/20

Sheet 29

Source: Original

Figure A5-30. Event Tree IHF-ESD-12A-NVL –
Direct Exposure during Canister
Transfer

Number of HLW WPs loaded over the preclosure period	Correct installation of WP shield ring	#	END-STATE-NAMES
NUM-HLW-WP	INIT-EVENT		
	<p data-bbox="544 1228 1089 1192">Loss of Shielding During Prep Activities or WP Closure</p>	<p data-bbox="532 821 553 842">1</p> <p data-bbox="532 722 553 764">OK</p>	
IHF-ESD-12B-HLW - Direct exposure due to improper installation of WP shield ring		<p data-bbox="1078 821 1099 842">2</p> <p data-bbox="1078 560 1099 764">DE-SHIELD-LOSS</p>	2008/02/27 Sheet 23

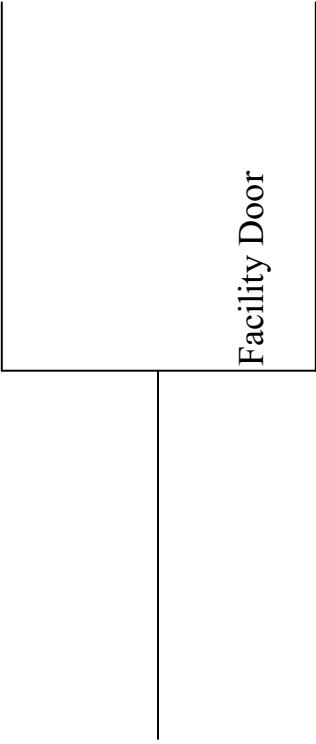
Source: Original

Figure A5-31. Event Tree IHF-ESD-12B-HLW - Direct Exposure due to Improper Installation of Shield Ring

Number of naval WPs loaded over the preclosure period	Correct installation of WP shield ring	#	END-STATE-NAMES
NUM-NVL	INIT-EVENT		
	<p data-bbox="540 1199 1092 1199">_____</p> <p data-bbox="540 1199 1092 1199">Loss of Shielding During Prep Activities or WP Closure</p> <p data-bbox="540 1199 1092 1199">_____</p>	<p data-bbox="532 825 540 846">1</p> <p data-bbox="532 720 540 762">OK</p>	<p data-bbox="1076 562 1092 762">DE-SHIELD-LOSS</p>
<p data-bbox="1182 1098 1201 1654">IHF-ESD-12B-NVL - Direct exposure due to improper installation of WP shield ring</p> <p data-bbox="1182 478 1201 646">2008/02/27 Sheet 24</p>			

Source: Original

Figure A5-32. Event Tree IHF-ESD-12B-NVL –
Direct Exposure due to Improper
Installation of Shield Ring

Number of HLW casks received during preclosure period	Direct exposure avoided during export of loaded WP		#	END-STATE-NAMES
NUM-HLW-WP	INIT-EVENT			
			1	OK
IHF-ESD-12C-HLW - Direct exposure during export of loaded WP			2	DE-SHIELD-LOSS

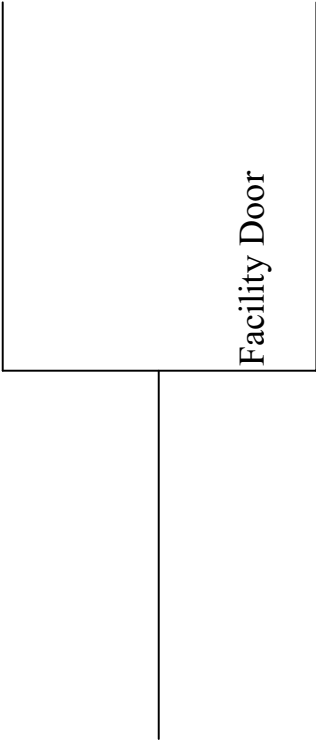

2008/02/26 Sheet 25

Source: Original

Figure A5-33. Event Tree IHF-ESD-12C-HLW
– Direct Exposure during Export
of Loaded WP

A-90

March 2008

Number of NVL canisters received over the preclosure period	Direct exposure during export of loaded WP	#	END-STATE-NAMES
NUM-NVL	INIT-EVENT		
		1	OK
		2	DE-SHIELD-LOSS
IHF-ESD-12C-NVL - Direct exposure during export of loaded WP			2008/02/26 Sheet 26

Source: Original

Figure A5-34. Event Tree IHF-ESD-12C-NVL –
Direct Exposure during Export of
Loaded WP

Number of HLW canisters processed over the preclosure period	Identify initiating events		XFER-TO-RESP-TREE
NUM-HLW-CAN	INIT-EVENT	#	
		<p>1</p> <p>Localized fire: canister in transfer room</p> <p>2 T => 35</p>	<p>OK</p> <p>IHF-RESP-FIRE</p>
IHF-ESD-13-HLW-CAN - Fire affects the facility			
			2007/10/26 Sheet 34

Source: Original

Figure A5-35. Event Tree IHF-ESD-13-HLW-CAN – Fire Affects the Facility

INIT-EVENT	Canister remains intact containing radioactive materials CANISTER	Shielding survives fire intact SHIELDING	HVAC confinement maintained CONFINEMENT	Moderator prevented from entering canister		#	END-STATE-NAMES
				MODERATOR			
						1	OK
						2	DE-SHIELD-LOSS
						3	RR-FILTERED
						4	RR-FILTERED-ITC
						5	RR-UNFILTERED
						6	RR-UNFILTERED-ITC
IHf-RESP-FIRE - Response for fires							2007/11/09 Sheet 35

Source: Original

Figure A5-36. Event Tree IHf-RESP-FIRE –
Response for Fires

Number of HLW TCs received over the preclosure period	Identify initiating events			XFER-TO-RESP-TREE
NUM-HLW-CSK	INIT-EVENT	#		
		1	OK	
	Localized fire: TC in unloading room	2 T => 35	IHF-RESP-FIRE	
IHF-ESD-13-HLW-CSK - Fire affects the facility	Localized fire: TC in cask prep area	3 T => 35	IHF-RESP-FIRE	
			2007/12/20	Sheet 36

Source: Original

Figure A5-37. Event Tree IHF-ESD-13-HLW-CSK -Fire Affects the Facility

Number of HLW WPs received over the preclosure period	Identify initiating events		#	XFER-TO-RESP-FREE
	NUM-HLW-WP	INIT-EVENT		
			1	OK
		Localized fire: WP in loadout room	2 T => 35	IHF-RESP-FIRE
		Localized fire: WP in loading room	3 T => 35	IHF-RESP-FIRE
		Localized fire: WP in positioning room	4 T => 35	IHF-RESP-FIRE
		Large fire affects entire facility	5 T => 35	IHF-RESP-FIRE
IHF-ESD-13-HLW-WP - Fire affects the facility				2007/11/21 Sheet 37

Source: Original

Figure A5-38. Event Tree IHF-ESD-13-HLW-WP - Fire Affects the Facility

Number of naval canisters received over the preclosure period	Identify initiating events		#	XFER-TO-RESP-TREE
	NUM-NVL	INIT-EVENT		
			1	OK
		Localized fire: WP in loadout room	2 T => 35	IHF-RESP-FIRE
		Localized fire: WP in loading room	3 T => 35	IHF-RESP-FIRE
		Localized fire: WP in unloading room	4 T => 35	IHF-RESP-FIRE
		Localized fire: WP in positioning room	5 T => 35	IHF-RESP-FIRE
		Localized fire: TC in cask prep area	6 T => 35	IHF-RESP-FIRE
		Localized fire: canister in transfer room	7 T => 35	IHF-RESP-FIRE
		Large fire affects entire facility	8 T => 35	IHF-RESP-FIRE
IHF-ESD-13-NVL - Fire affects the facility				2007/11/21 Sheet 38

Source: Original

Figure A5-39. Event Tree IHF-ESD-13-NVL –
Fire Affects the Facility

ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

CONTENTS

	Page
ACRONYMS AND ABBREVIATIONS	B1-12
ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES.....	B1-14
B1 SITE PRIME MOVER ANALYSIS – FAULT TREES.....	B1-14
B1.1 REFERENCES	B1-14
B1.2 SITE PRIME MOVER DESCRIPTION	B1-14
B1.3 DEPENDENCIES AND INTERACTIONS ANALYSIS	B1-17
B1.4 SITE PRIME MOVER RELATED FAILURE SCENARIOS	B1-18
B2 CASK TRANSFER TROLLEY ANALYSIS – FAULT TREES	B2-1
B2.1 REFERENCES	B2-1
B2.2 CASK TRANSFER TROLLEY DESCRIPTION	B2-1
B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS	B2-8
B2.4 CTT-RELATED FAILURE SCENARIOS	B2-9
B3 LOADING/UNLOADING ROOM SHIELD DOOR AND SLIDE GATE FAULT TREE ANALYSIS.....	B3-1
B3.1 REFERENCES	B3-1
B3.2 SLIDE GATE AND SHIELD DOOR SYSTEM DESCRIPTION.....	B3-1
B3.3 DEPENDENCIES AND INTERACTIONS	B3-2
B3.4 SLIDE GATE AND SHIELD DOOR FAILURE SCENARIOS	B3-3
B4 IHF CANISTER TRANSFER MACHINE FAULT TREE ANALYSIS.....	B4-1
B4.1 REFERENCES	B4-1
B4.2 CANISTER TRANSFER MACHINE DESCRIPTION.....	B4-2
B4.3 DEPENDENCIES AND INTERACTIONS	B4-12
B4.4 CTM-RELATED FAILURE SCENARIOS	B4-12
B5 WASTE PACKAGE TRANSFER TROLLEY ANALYSIS – FAULT TREES	B5-1
B5.1 REFERENCES	B5-1
B5.2 SYSTEM DESCRIPTION.....	B5-2
B5.3 DEPENDENCIES AND INTERACTIONS ANALYSIS	B5-8
B5.4 RELATED FAILURE SCENARIOS	B5-9
B6 PIVOTAL EVENT ANALYSIS.....	B6-1
B6.1 FAULT TREES INVOLVING DROPPING AN OBJECT.....	B6-1
B6.2 IMPACT TO A CASK BY ANOTHER VEHICLE OR OBJECT.....	B6-3
B6.3 IMPACT TO A CASK DUE TO SPURIOUS MOVEMENT.....	B6-5
B6.4 LOSS OF SHIELDING LEADING TO DIRECT EXPOSURE	B6-9
B6.5 MODERATOR SOURCE	B6-16

FIGURES

	Page
B1.2-1. Site Prime Mover Simplified Block Diagram Intra-Site and In-Facility	B1-16
B1.4-1. Uncertainty Results of the SPMRC Collides with IHF Structures Fault Tree.....	B1-22
B1.4-2. Cut set Generation Results for the SPMRC Collides with IHF Structures Fault Tree	B1-23
B1.4-3. SPMRC Collides with IHF Structures	B1-25
B1.4-4. SPMRC Fails to Stop.....	B1-26
B1.4-5. SPMRC Exceeds Safe Speed.....	B1-27
B1.4-6. Uncertainty Results of the SPMTT Collides with IHF Structures Fault Tree	B1-31
B1.4-7. Cut Set Generation Results for the SPMTT Collides with IHF Structures Fault Tree	B1-32
B1.4-8. SPMTT Collision in IHF	B1-34
B1.4-9. Equipment Failure Causes Collision.....	B1-35
B1.4-10. SPMTT Failure to Stop.....	B1-36
B1.4-11. SPMTT Exceeds Safe Speed	B1-37
B1.4-12. Uncertainty Results of the SPMRC Derailment Fault Tree.....	B1-40
B1.4-13. Cut Set Generation Results for SPMRC Derailment”	B1-40
B1.4-14. SPMRC Derailment in IHF.....	B1-41
B1.4-15. SPMTT Rollover in IHF	B1-44
B2.2-1. Cask Transfer Trolley	B2-2
B2.2-2. Schematic of the CTT Control System	B2-6
B2.4-1. Uncertainty Results of Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading.....	B2-12
B2.4-2. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading.....	B2-12
B2.4-3. Fault Tree for Spurious Movement of the CTT in the Cask Preparation Area During Cask Loading.....	B2-15
B2.4-4. Fault Tree for Air Supply Failure	B2-16
B2.4-5. Uncertainty Results of the Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation.....	B2-19
B2.4-6. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation.....	B2-19
B2.4-7. Fault Tree for Spurious Movement of the CTT During Cask Preparation	B2-21

FIGURES (Continued)

	Page
B2.4-8. Uncertainty Results for the Collision of CTT during Cask Transfer Fault Tree	B2-24
B2.4-9. Cut Set Generation Results for the Collision of CTT during Cask Transfer Fault Tree	B2-24
B2.4-10. Fault Tree for Collision of the CTT During Cask Transfer (Page 1).....	B2-26
B2.4-11. Fault Tree for Collision of the CTT During Cask Transfer (Page 2).....	B2-27
B2.4-12. Uncertainty Results for the Spurious Movement of the CTT in the Cask Unloading Room Fault Tree	B2-30
B2.4-13. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Unloading Room Fault Tree	B2-30
B2.4-14. Fault Tree for Spurious Movement of the CTT in the Cask Unloading Room	B2-32
B3.4-1. Uncertainty Results for the Inadvertent Opening of the Shield Door Fault Tree	B3-5
B3.4-2. Cut Set Generation Results for the Inadvertent Opening of the Shield Door Fault Tree	B3-6
B3.4-3. Fault Trees for Inadvertent Opening of the Shield Door	B3-8
B3.4-4. Uncertainty Results for Inadvertent Opening of Slide Gate	B3-11
B3.4-5. Cut Set Generation Results for Inadvertent Opening of Slide Gate	B3-11
B3.4-6. Fault Trees for Inadvertent Opening of the Slide Gate.....	B3-13
B3.4-7. Uncertainty Results for Shield Door Closes on Conveyance Fault Tree.....	B3-16
B3.4-8. Cut Set Generation Results for Shield Door Closes on Conveyance Fault Tree	B3-16
B3.4-9. Fault Trees for Shield Door Closes on Conveyance.....	B3-18
B4.2-1. Canister Transfer Machine Elevation	B4-2
B4.2-2. Canister Transfer Machine Cross Section.....	B4-3
B4.2-3. Canister Hoist Instrumentation	B4-5
B4.2-4. Shield Skirt and Slide Gate Instrumentation.....	B4-6
B4.2-5. Trolley Instrumentation	B4-7
B4.2-6. Bridge Instrumentation	B4-8
B4.4-1. Uncertainty Results of the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree	B4-19
B4.4-2. Cut Set Generation Results for the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree	B4-20

FIGURES (Continued)

	Page
B4.4-3. CTM Drop Fault Tree Sheet 1	B4-22
B4.4-4. CTM Drop Fault Tree Sheet 2	B4-23
B4.4-5. CTM Drop Fault Tree Sheet 3	B4-24
B4.4-6. CTM Drop Fault Tree Sheet 4	B4-25
B4.4-7. CTM Drop Fault Tree Sheet 5	B4-26
B4.4-8. CTM Drop Fault Tree Sheet 6	B4-27
B4.4-9. CTM Drop Fault Tree Sheet 7	B4-28
B4.4-10. CTM Drop Fault Tree Sheet 8	B4-29
B4.4-11. CTM Drop Fault Tree Sheet 9	B4-30
B4.4-12. CTM Drop Fault Tree Sheet 10	B4-31
B4.4-13. CTM Drop Fault Tree Sheet 11	B4-32
B4.4-14. CTM Drop Fault Tree Sheet 12	B4-33
B4.4-15. Uncertainty Results of the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree	B4-38
B4.4-16. Cut Set Generation Results for the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree	B4-39
B4.4-17. CTM High Drops from Two Blocking Event Sheet 1	B4-41
B4.4-18. CTM High Drops from Two Blocking Event Sheet 2	B4-42
B4.4-19. CTM High Drops from Two Blocking Event Sheet 3	B4-43
B4.4-20. Uncertainty Results of the Drop of Object onto Canister Fault Tree	B4-51
B4.4-21. Cut Set Generation Results for the Drop of Object onto Canister Fault Tree	B4-51
B4.4-22. Drop of Object onto Cask Sheet 1	B4-54
B4.4-23. Drop of Object onto Cask Sheet 2	B4-55
B4.4-24. Drop of Object onto Cask Sheet 3	B4-56
B4.4-25. Drop of Object onto Cask Sheet 4	B4-57
B4.4-26. Drop of Object onto Cask Sheet 5	B4-58
B4.4-27. Drop of Object onto Cask Sheet 6	B4-59
B4.4-28. Drop of Object onto Cask Sheet 7	B4-60
B4.4-29. Drop of Object onto Cask Sheet 8	B4-61
B4.4-30. Drop of Object onto Cask Sheet 9	B4-62
B4.4-31. Drop of Object onto Cask Sheet 10	B4-63

FIGURES (Continued)

	Page
B4.4-32. Drop of Object onto Cask Sheet 11	B4-64
B4.4-33. Drop of Object onto Cask Sheet 12	B4-65
B4.4-34. Uncertainty Results of the Canister Impact Fault Tree.....	B4-70
B4.4-35. Cut Set Generation Results for the Canister Impact Fault Tree.....	B4-70
B4.4-36. CTM Collision Sheet 1	B4-73
B4.4-37. CTM Collision Sheet 2	B4-74
B4.4-38. CTM Collision Sheet 3	B4-75
B4.4-39. CTM Collision Sheet 4	B4-76
B4.4-40. CTM Collision Sheet 5	B4-77
B4.4-41. Uncertainty Results of the CTM Movement Subjects Canister to Shearing Forces Fault Tree	B4-81
B4.4-42. Cut Set Generation Results for the CTM Movement Subjects Canister to Shearing Forces Fault Tree	B4-82
B4.4-43. CTM Shear Sheet 1	B4-84
B4.4-44. CTM Shear Sheet 2.....	B4-85
B4.4-45. CTM Shear Sheet 3.....	B4-86
B5.2-1. Waste Package Transfer Trolley.....	B5-2
B5.2-2. Waste Package Transfer Carriage.....	B5-3
B5.2-3. Schematic of the Waste Package Transfer Trolley Control System.....	B5-6
B5.4-1. Uncertainty Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-12
B5.4-2. Cut Set Generation Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-13
B5.4-3. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-15
B5.4-4. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued).....	B5-16
B5.4-5. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued).....	B5-17
B5.4-6. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-18
B5.4-7. Uncertainty Results for Impact of the WPTT with a Structure Fault Tree.....	B5-21

FIGURES (Continued)

	Page
B5.4-8. Cut Set Generation Results for Impact of the WPTT with a Structure Fault Tree	B5-21
B5.4-9. Fault Tree for Impact of the WPTT with a Structure.....	B5-23
B5.4-10. Fault Tree for Impact of the WPTT into a Structure during Waste Package Transfer (Continued).....	B5-24
B5.4-11. Uncertainty Results for the Derailment of the WPTT Fault Tree.....	B5-26
B5.4-12. Cut Set Generation Results for the Derailment of the WPTT Fault Tree.....	B5-26
B5.4-13. Fault Tree for Derailment of the WPTT	B5-27
B5.4-14. Uncertainty Results for the Premature Tilt-down of the WPTT Fault Tree.....	B5-30
B5.4-15. Cut Set Generation Results for the Premature Tilt-down of the WPTT Fault Tree	B5-30
B5.4-16. Fault Tree for Premature Tilt-down of the WPTT	B5-32
B5.4-17. Uncertainty Results for Malfunction of WPTT or Waste Package Transfer Carriage.....	B5-35
B5.4-18. Cut Set Generation Results for Malfunction of WPTT or Waste Package Transfer Carriage	B5-35
B5.4-19. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage	B5-37
B5.4-20. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage (Continued)	B5-38
B5.4-21. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage (Continued)	B5-39
B6.1-1. Typical 300-Ton Crane “Drop-On” Fault Tree	B6-2
B6.1-2. Typical RHS Crane “Drop-On” Fault Tree	B6-3
B6.2-1. Typical Side Impact Fault Tree.....	B6-4
B6.2-2. Typical Side Impact with Spurious Movement of CTT Fault Tree	B6-5
B6.3-1. Spurious Movement of the Crane or CTT Fault Tree.....	B6-6
B6.3-2. Spurious Movement of the Crane Fault Tree.....	B6-7
B6.3-3. Typical Tipover Fault Tree	B6-8
B6.3-4. Fault Tree for Spurious Movement CTM, CTT or WPTT during Lift.....	B6-9
B6.4-1. Typical Direct Exposure Fault Tree due to Shield Door or Slide Gate Opening.....	B6-11
B6.4-2. Direct Exposure from HLW due to Loss of Shielding	B6-12
B6.4-3. Direct Exposure from HLW due to Improper Assembly of Shield Ring	B6-13

FIGURES (Continued)

	Page
B6.4-4. Direct Exposure from HLW during Closure of the WP	B6-14
B6.4-5. Direct Exposure from NVL Canister due to Loss of Shielding	B6-15
B6.4-6. Direct Exposure from NVL Canister due to Improper Assembly of Shield Ring.....	B6-16
B6.5-1. Moderator Source from Fire Suppression and AHUs.....	B6-18
B6.5-2. Moderator Source in a Fire	B6-19

TABLES

	Page
B1.3-1. Dependencies and Interactions Analysis	B1-18
B1.4-1. ESD Cross Reference with SPMRC/SPMTT Fault Trees	B1-18
B1.4-2. Basic Event Probability for SPMRC Collision.....	B1-21
B1.4-3. Cut Sets for SPMRC Collides with IHF Structures	B1-23
B1.4-4. Basic Event Probability for SPMTT Collides with IHF Structures.....	B1-30
B1.4-5. Cut Sets for SPMTT Collides with IHF Structures	B1-32
B1.4-6. Basic Event Probability for SPMRC Derailment.....	B1-39
B1.4-7. Cut sets for SPMRC Derailment.....	B1-41
B2.3-1. Dependencies and Interactions Analysis	B2-8
B2.4-1. Basic Event Probabilities for Spurious Movement of the CTT during Cask Loading B2-10	
B2.4-2. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading.....	B2-13
B2.4-3. Basic Event Probabilities for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation.....	B2-18
B2.4-4. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation.....	B2-20
B2.4-5. Basic Event Probability for Collision of CTT during Cask Transfer	B2-23
B2.4-6. Cut Sets for Collision of the CTT During Cask Transfer	B2-25
B2.4-7. Basic Event Probability for Spurious Movement of the CTT in the Cask Unloading Room.....	B2-29
B2.4-8 Spurious Movement of the CTT in the Cask Unloading Room	B2-31
B3.3-1. Dependencies and Interactions Analysis	B3-3
B3.4-1. Basic Event Probabilities for Inadvertent Opening of the Shield Door.....	B3-4
B3.4-2. Cut Sets for Inadvertent Opening of Shield Door.....	B3-6
B3.4-3. Basic Event Probabilities for Inadvertent Opening of Slide Gate	B3-10
B3.4-4. Cut Sets for Inadvertent Opening of Slide Gate	B3-12
B3.4-5. Basic Event Probabilities for Shield Door Closes on Conveyance.....	B3-15
B3.4-6. Cut Sets for Shield Door Closes on Conveyance.....	B3-17
B4.3-1. Dependencies and Interactions Analysis	B4-12

TABLES (Continued)

	Page
B4.4-1. Basic Event Probability for the Canister Drop from Below Canister Drop Height Limit Fault Tree	B4-17
B4.4-2. Human Failure Events.....	B4-19
B4.4-3. Dominant Cut Sets for Canister Drop from Below the Canister Design-Limit Drop Height	B4-20
B4.4-4. Basic Event Probability for the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree.....	B4-37
B4.4-5. Dominant Cut Sets for the Canister Drop from Above the Canister Design Limit Drop Height.....	B4-40
B4.4-6. Basic Event Probability for the Drop of Object onto Canister Fault Tree.....	B4-47
B4.4-7. Human Failure Events.....	B4-50
B4.4-8. Dominant Cut Sets for the “Drop of Object onto Canister Fault” Tree.....	B4-52
B4.4-9. Basic Event Probability for the Canister Impact Fault Tree	B4-68
B4.4-10. Human Failure Events.....	B4-69
B4.4-11. Dominant Cut Sets for the Canister Impact Fault Tree.....	B4-71
B4.4-12. Basic Event Probability for the CTM Movement Subjects Canister to Shearing Forces Fault Trees.....	B4-80
B4.4-13. Dominant Cut Sets for the CTM Movement Subjects Canister to Shearing Forces Fault Tree	B4-82
B5.3-1. Dependencies and Interactions Analysis	B5-8
B5.4-1. Basic Event Probabilities for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-11
B5.4-2. Cut Sets for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters	B5-13
B5.4-3. Basic Event Probabilities for Impact of the WPTT with a Structure.....	B5-20
B5.4-4. Cut Sets for Impact of the WPTT with a Structure.....	B5-22
B5.4-5. Basic Event Probabilities for Derailment of the WPTT During Waste Package Transfer B5-25	
B5.4-6. Cut Sets for Derailment of the WPTT	B5-27
B5.4-7. Basic Event Probabilities for Premature Tilt-down of the WPTT	B5-29
B5.4-8. Cut Sets for Premature Tilt-down of the WPTT	B5-31
B5.4-9. Basic Event Probabilities for Malfunction of WPTT or Waste Package Transfer Carriage Malfunction during Waste Package Export.....	B5-34

TABLES (Continued)

	Page
B5.4-10. Cut Sets for Malfunction of WPTT or Waste Package Transfer Carriage During Waste Package Export.....	B5-36
B6.1-1. Drop-On Fault Trees.....	B6-1
B6.2-1. Transportation Cask Impact Fault Trees.....	B6-3
B6.3-1. Transportation Cask Impacts or Tipover Fault Trees.....	B6-5
B6.4-1. Direct Exposure Fault Trees.....	B6-10
B6.5-1 Moderator Events during IHF Operations.....	B6-17

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 Sections B1 through B5, on a system basis. The pivotal event fault trees are presented in Section B6. 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 Motor Vehicle Safety. 49 U.S.C. 301.
- B1.1.3 49 CFR 571. 2007. Transportation: Federal Motor Vehicle Safety Standards.

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 both Intra-Site and within the Canister Receipt and Closure Facility (CRCF), Wet Handling Facility (WHF), Initial Handling Facility (IHF), and Receipt Facility (RF).

Movement of the site prime mover railcar (SPMRC) or site prime mover truck trailer (SPMTT) within the IHF is limited to the Cask Preparation Area (Room 1012).

Transportation casks arriving at the IHF on railcar or truck trailer can contain:

- High-level radioactive waste canisters
- Naval canisters.

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.

A diesel engine provides the energy to operate the SPM outside the facilities. Inside the IHF, the SPM is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

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, a 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 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 national rail transportation system. Performance standards are addressed in the Association of American Railroads (AAR) Standard S-2043: *Performance Specification for Trains Used to Haul High Level Radioactive Material* (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

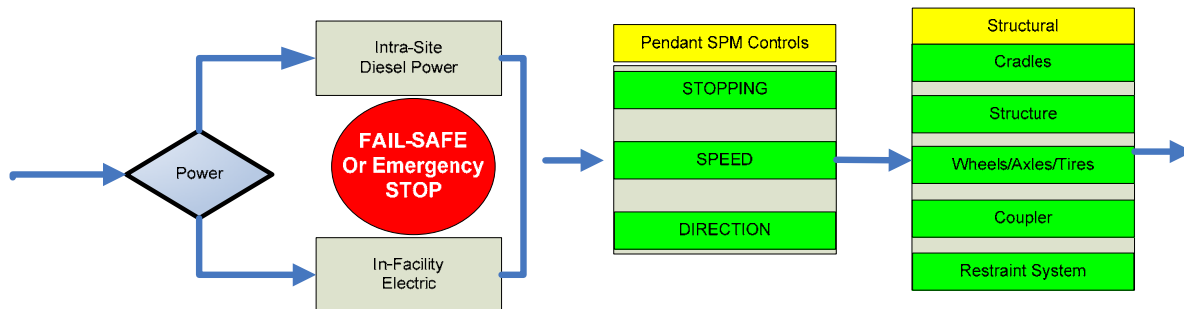
Title 49, U.S.C. Part 301, Section 30111 (Ref. B1.1.2). The requirements are delineated in 49 CFR Part 571 (Ref. B1.1.3).

B1.2.2.4 Subsystems

The SPMRC and SPMTT systems are composed of four subsystems:

1. Power plant—A diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all intrasite operations. For operations conducted inside facilities, the SPM is connected to the facility 480 V, 3-phase, 60-Hz power supply.
2. Vehicle controls—During IHF operations, the operator controls the SPM at the operator’s console inside the SPM. For all operations inside of facilities, the operator controls the SPM with either a remote (wireless) controller or through a pendant connected to the vehicle.
3. 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.
4. Brakes—For the railcar, brakes comply with FRA requirements; for the truck trailer, the braking system complies with 49 CFR Part 571, Transportation (Ref. B1.1.3).

A simplified block diagram of the functional components on the SPMRC/SPMTT is shown in Figure B1.2-1.



Source: Original

Figure B1.2-1. Site Prime Mover Simplified Block Diagram 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 or truck trailer outside the entrance to the facility such that the railcar/truck trailer is pushed into the facility. The SPM diesel engine is shut down and the outer door is opened. Facility power is connected to the SPM for all operations inside the facility.¹

The operator connects the pendant controller or uses a remote (wireless) controller to move the railcar/truck trailer into the facility. Once inside, the outer door is closed. Once in position in the Cask Preparation Area, the SPM is disconnected from the railcar/truck trailer. The outer 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 outer door is 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 remains 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 is deemed to be unserviceable and turned in for maintenance. Unserviceable vehicles are not used.

If an unserviceable state is identified during movement, the SPM is immediately placed 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 systems, 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.

¹ The SPM is never operated inside a facility using the diesel engine.

Table B1.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Structural	Material failure Coupler Wheels/tires/axle	—	—	—	—
Brakes	Material failure	—	—	Failure to engage (set)	—
Power plant	Speed limiter 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 four top events for the SPM operating inside the IHF:

1. SPMRC collides with IHF structures.
2. SPMTT collides with IHF structures.
3. SPMRC derailment.
4. SPMTT rollover.

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 SPMRC/SPMTT Fault Trees

IHF ESD Number	SPMRC Collision	SPMTT Collision	SPMRC Derailment	SPMTT Rollover
ESD-01-NVL	X	—	X	—
ESD-01-HLW	X	X	X	X

NOTE: ESD = event sequence diagram; HLW = high-level radioactive waste; IHF = Initial Handling Facility; NVL = naval; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.

Source: Original

B1.4.1 SPMRC Collides with IHF Structures

B1.4.1.1 Description

The two fault trees for SPMRC collision within the IHF are identical for each type of transportation cask. Collision can occur as a result of human error or mechanical failures. Mechanical failures leading to a collision consist of the SPM failure to stop when 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 maintaining 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 performs a controlled stop. Once stopped, the SPM stops all movement or operations and enters 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 facility 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 miles per hour. The power plant in the SPM has been sized to preclude simultaneous operations.

B1.4.1.3 Design Requirements and Features

Requirements

Since the dominant contributor to a SPM 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 at the preparation area 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 miles per hour.

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 is the equivalent of a “deadman switch.” On the loss of AC power, the SPM performs a controlled stop. Once stopped, the SPM enters the lock mode state. The lock mode state is not reversible without specific operator action.

Design 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 responds by removing power from the propulsion system on the SPM.

Testing and Maintenance

Requirements

No maintenance or testing is permitted on a SPM loaded with a transportation cask.

Design Features

None.

B1.4.1.4 Fault Tree Model

The fault tree model for “SPMRC Collides with IHF Structures” accounts for both human error and/or SPMRC mechanical problems that could result in a collision. Once the SPMRC has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the railcar and the SPM moves out of the facility.

The fault tree for SPMRC and SPMTT are identical and a split fraction is used to account for the number/type of transportation casks that arrive at the IHF on either a railcar or truck trailer. The fault tree for the SPMTT is discussed in the next section.

The top event is a collision of the SPMRC in the IHF 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 SPMRC collision fault trees. The mission time is set at one hour which is conservative because it does not require more than one hour to disconnect the SPM from the railcar and remove it from the facility.

Table B1.4-2. Basic Event Probability for SPMRC Collision

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-OPRCCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000
51A-OPRCINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
51A-OPRCINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
51A-PWR-LOSS	1	4.100E-006	4.100E-006	0.000E+000	0.000E+000
51A-RC---BRP001--BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMRC-BRK000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMRC-BRP000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMRC-BRP001-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMRC-CBP001-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
51A-SPMRC-CBP001-CBP-SHC	3	1.880E-008	0.000E+000	1.880E-008	1.000E+000
51A-SPMRC-CPL00-CPL-FOH	3	1.910E-006	0.000E+000	1.910E-006	1.000E+000
51A-SPMRC-CT000--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
51A-SPMRC-CT001--CT-SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
51A-SPMRC-CT001-CT-FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
51A-SPMRC-CT002--CT--FOH	3	6.880E-005	0.000E+000	6.880E-005	1.000E+000
51A-SPMRC-G6500--G65-FOH	3	1.160E-005	0.000E+000	1.160E-005	1.000E+000
51A-SPMRC-HC001--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-SPMRC-HC001-HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
51A-SPMRC-IEL011-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-SPMRC-MOE000-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
51A-SPMRC-SC021--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
51A-SPMRC-SEL021-SEL-FOH	3	4.160E-006	0.000E+000	4.160E-006	1.000E+000
51A-SPMRC-STU01-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; Prob. = probability.

Source: Original

B1.4.1.5.1 Human Failure Events

Three human errors have been identified for this fault tree. Both HFEs of operator initiates a runaway and operator causes a collision with mobile platform, are assigned a screening failure probability of 1.00E+00. A detailed analysis of operator causes collision is addressed in Section 6.4 and Attachment E.

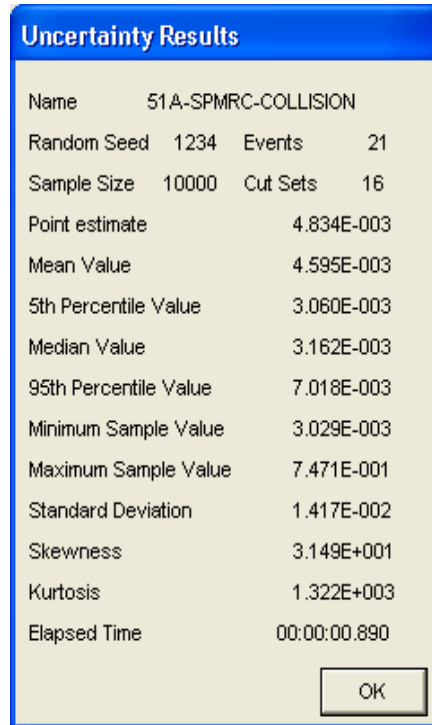
1. Operator causes a collision (51A-OPRCCOLLIDE1-HFI-NOD)
2. Operator initiates runaway (51A-OPRCINTCOL01-HFI-NOD)
3. Operator causes a collision with mobile platform (51A-OPRCINTCOL02-HFI-NOD).

B1.4.1.5.2 Common-Cause Failures

There are no common-cause failures (CCFs) identified for this fault tree.

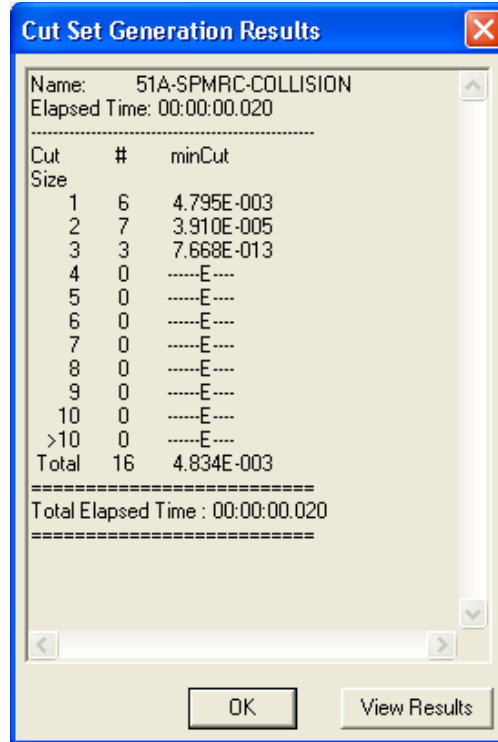
B1.4.1.6 Uncertainty and Cut Set Generation Results

Figure B1.4-1 contains the uncertainty results obtained from running the fault tree for “SPMRC Collides with IHF Structures” using a cutoff probability of 1E-12. Figure B1.4-2 provides the cut set generation results for the “SPMRC Collides with IHF Structures” Fault Tree.



Source: Original

Figure B1.4-1. Uncertainty Results of the SPMRC Collides with IHF Structures Fault Tree



Source: Original

Figure B1.4-2. Cut set Generation Results for the SPMRC Collides with IHF Structures Fault Tree

B1.4.1.7 Cut Sets

Table B1.4-3 contains the cut sets for “SPMRC Collides with IHF Structures”. The probability of failure is 4.83E-03.

Table B1.4-3. Cut Sets for SPMRC Collides with IHF Structures

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMRC-COLLISION	62.07	3.000E-003	51A-OPRCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	51A-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	51A-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	51A-OPRCINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000

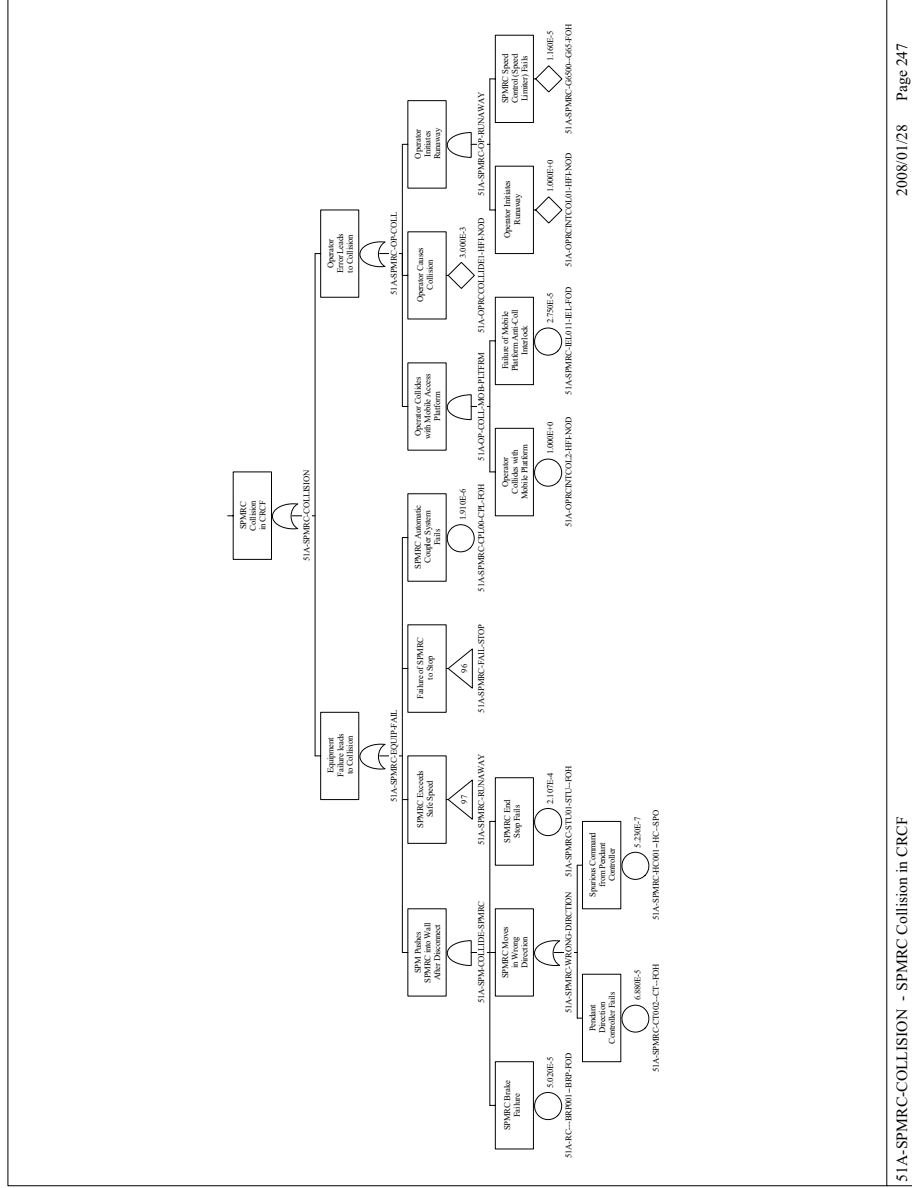
Table B1.4-3. Cut Sets for SPMRC Collides with IHF Structures (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
			51A-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.8E-005
	0.24	1.160E-005	51A-OPRCINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			51A-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	51A-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	51A-SPMRC-CT001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	51A-SPMRC-CPL00-CPL-FOH	Railcar Automatic Coupler System Fails	1.9E-006
		4.834E-003	= Total		
4.83E-03 = Total					

NOTE: Freq. = frequency; Prob. = probability; SPMRC = site prime mover railcar.

Source: Original

B1.4.1.8 Fault Trees



51A-SPMRC-COLLISION - SPMRC Collision in CRCF 2008/01/28 Page 247

Source: Original

Figure B1.4-3. SPMRC Collides with IHF Structures

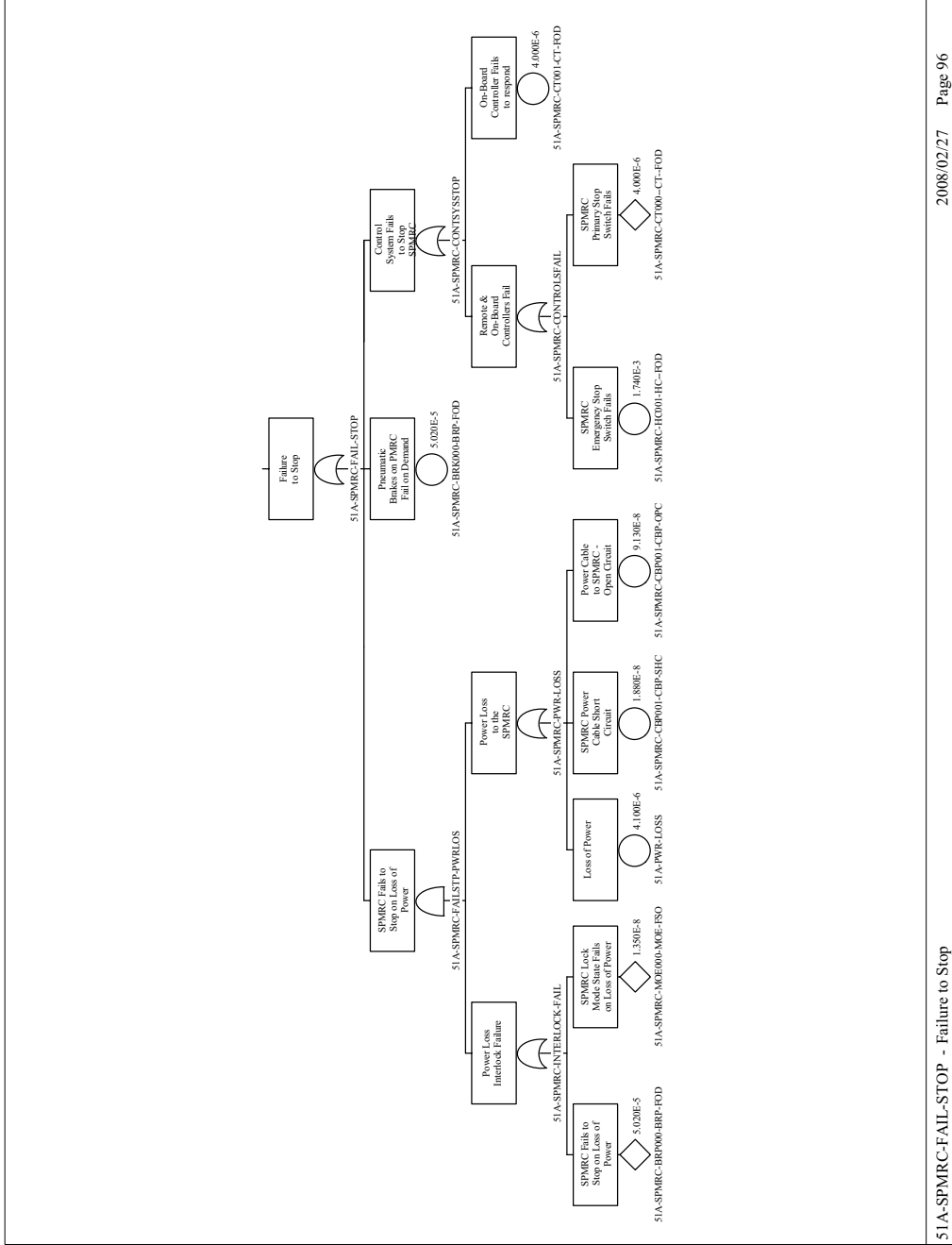
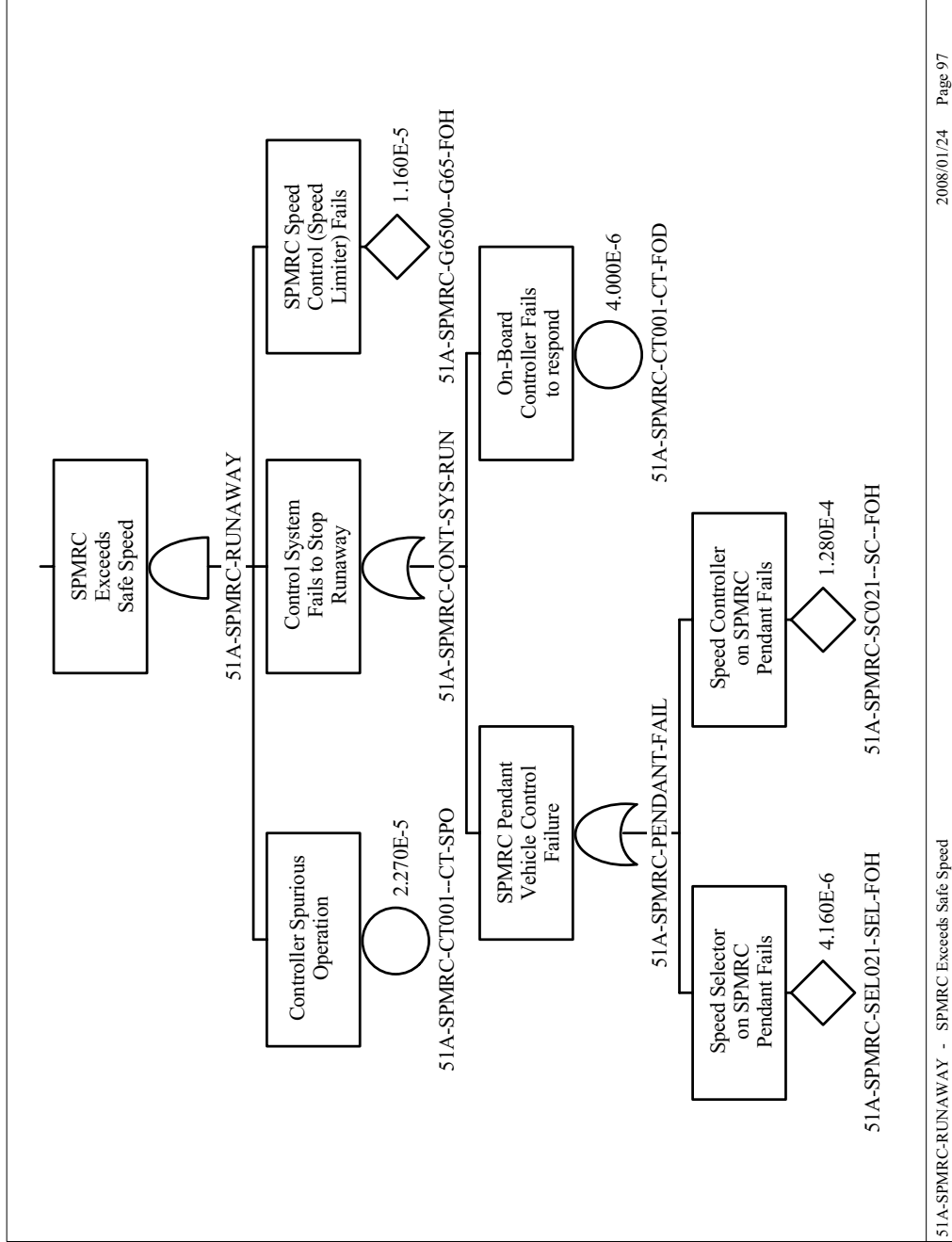


Figure B1.4-4. SPMRC Fails to Stop



Source: Original

Figure B1.4-5. SPMRC Exceeds Safe Speed

B1-27

March 2008

B1.4.2 SPMTT Collides with IHF Structures

B1.4.2.1 Description

The two fault trees for SPMTT collision within the IHF are identical with the exception of the number of transportation casks that are processed at the IHF for each configuration. Collision 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.

B1.4.2.2 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. At anytime there is a loss of power detected, the SPM performs a controlled stop. Once stopped, the SPM stops all movement and enters into “lock mode” safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM. The SPM remains in this fail safe mode until power is returned and restarted by the operator.

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 miles per hour. 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 Requirements and Design Features

Requirements

Since the dominant contributor to 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 truck trailer at the preparation area 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 SPMTT. The drive system contains both a speed limiter and a transmission constraint which limits the maximum speed of the SPM to 9.0 miles per hour.

Common-Cause Failures

There are no CCFs identified for this fault tree.

B1.4.2.4 System Configuration and Operating Conditions

Requirements

Two means of stopping the SPM is 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 state. The lock mode 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 responds by removing power from the propulsion system.

Testing and Maintenance

Requirements

There is no maintenance or testing permitted on a SPMTT loaded with a transportation cask.

Design Feature

None.

B1.4.2.5 Fault Tree Model

The fault tree model for “SPMTT Collides with IHF Structures” accounts for both human error and for SPMTT hardware problems that could result in collision. There is only one movement within the IHF. Once the SPMTT has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the truck trailer and it is moved out of the facility.

The fault trees for SPMRC and SPMTT are identical and a split fraction is used to account for the number/type of transportation casks that arrive at the IHF on either the railcar or truck trailer.

The top event is a collision of the SPMTT in the IHF 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 (Figure B1.4-9) including failure to stop (Figure B1.4-10) or exceeding a safe speed (Figure B1.4-11). 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.

B1.4.2.6 Basic Event Data

Table B1.4-4 contains a list of basic events used in the “SPMTT Collides with IHF Structures” fault trees. The mission time has been set at one hour which is conservative because it does not require more than one hour to disconnect the SPM from the rail car and remove it from the facility.

Table B1.4-4. Basic Event Probability for SPMTT Collides with IHF Structures

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-OPTTCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000
51A-OPTTINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
51A-OPTTINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
51A-PWR-LOSS	1	4.100E-006	4.100E-006	0.000E+000	0.000E+000
51A-SPMTT-BRK000-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMTT-BRP001-BRP-FOD	1	5.020E-005	5.020E-005	0.000E+000	0.000E+000
51A-SPMTT-CBP002-CBP-OPC	3	9.130E-008	0.000E+000	9.130E-008	1.000E+000
51A-SPMTT-CBP003-CBP-SHC	3	1.880E-008	0.000E+000	1.880E-008	1.000E+000
51A-SPMTT-CPL00-CPL-FOH	3	1.910E-006	0.000E+000	1.910E-006	1.000E+000
51A-SPMTT-CT000--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
51A-SPMTT-CT001--CT--FOD	1	4.000E-006	4.000E-006	0.000E+000	0.000E+000
51A-SPMTT-CT002--CT--FOH	3	6.880E-005	0.000E+000	6.880E-005	1.000E+000
51A-SPMTT-G65000-G65-FOH	3	1.160E-005	0.000E+000	1.160E-005	1.000E+000
51A-SPMTT-HC001-HC-FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
51A-SPMTT-HC002--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-SPMTT-IEL102-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-SPMTT-MOE000-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
51A-SPMTT-SC001--CT--SPO	1	2.270E-005	2.270E-005	0.000E+000	0.000E+000
51A-SPMTT-SC021--SC--FOH	3	1.280E-004	0.000E+000	1.280E-004	1.000E+000
51A-SPMTT-SEL021-SEL-FOH	3	4.160E-006	0.000E+000	4.160E-006	1.000E+000
51A-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; Prob. = probability.

Source: Original

B1.4.2.6.1 Human Failure Events

Three human errors have been identified for this fault tree. Both “operator initiates a runaway” and “operator causes a collision with mobile platform” are assigned a screening failure probability of 1.00E+00. A detailed analysis of “operator causes collision” is addressed in Section 6.4 and Attachment E.

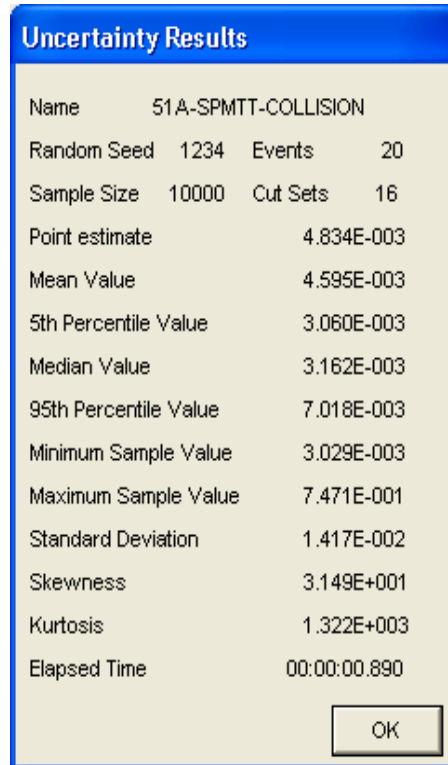
1. Operator causes collision (51A-OPTTCOLLIDE1-HFI-NOD).
2. Operator initiates runaway (51A-OPTTINTCOL01-HFI-NOD).
3. Operator causes a collision with mobile platform (51A-OPTTINTCOL02-HFI-NOD).

B1.4.2.6.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

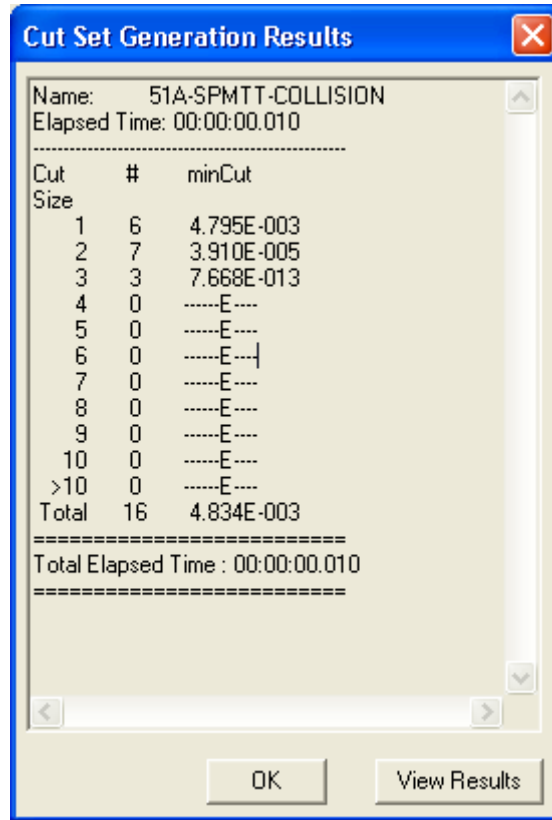
B1.4.2.7 Uncertainty and Cut Set Generation Results

Figure B1.4-6 contains the uncertainty results obtained from running the fault tree for “SPMTT Collides with IHF Structures” using a cutoff probability of 1E-12. Figure B1.4-7 provides the cut set generation results for the “SPMTT Collides with IHF Structures” fault tree.



Source: Original

Figure B1.4-6. Uncertainty Results of the SPMTT Collides with IHF Structures Fault Tree



Source: Original

Figure B1.4-7. Cut Set Generation Results for the SPMTT Collides with IHF Structures Fault Tree

B1.4.2.8 Cut Sets

Table B1.4-5 contains the cut sets for “SPMTT Collides with IHF Structures”. The probability of failure is 4.83E-03

Table B1.4-5. Cut Sets for SPMTT Collides with IHF Structures

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMTT-COLLISION	62.07	3.000E-003	51A-OPRCCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	36.00	1.740E-003	51A-SPMTT-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.7E-003
	1.04	5.020E-005	51A-SPMTT-BRP000-BRP-FOD	Brake (Pneumatic) Failure on Demand Brake (Pneumatic) Failure on Demand PMRC Fails to Stop on Loss of Power	5.0E-005

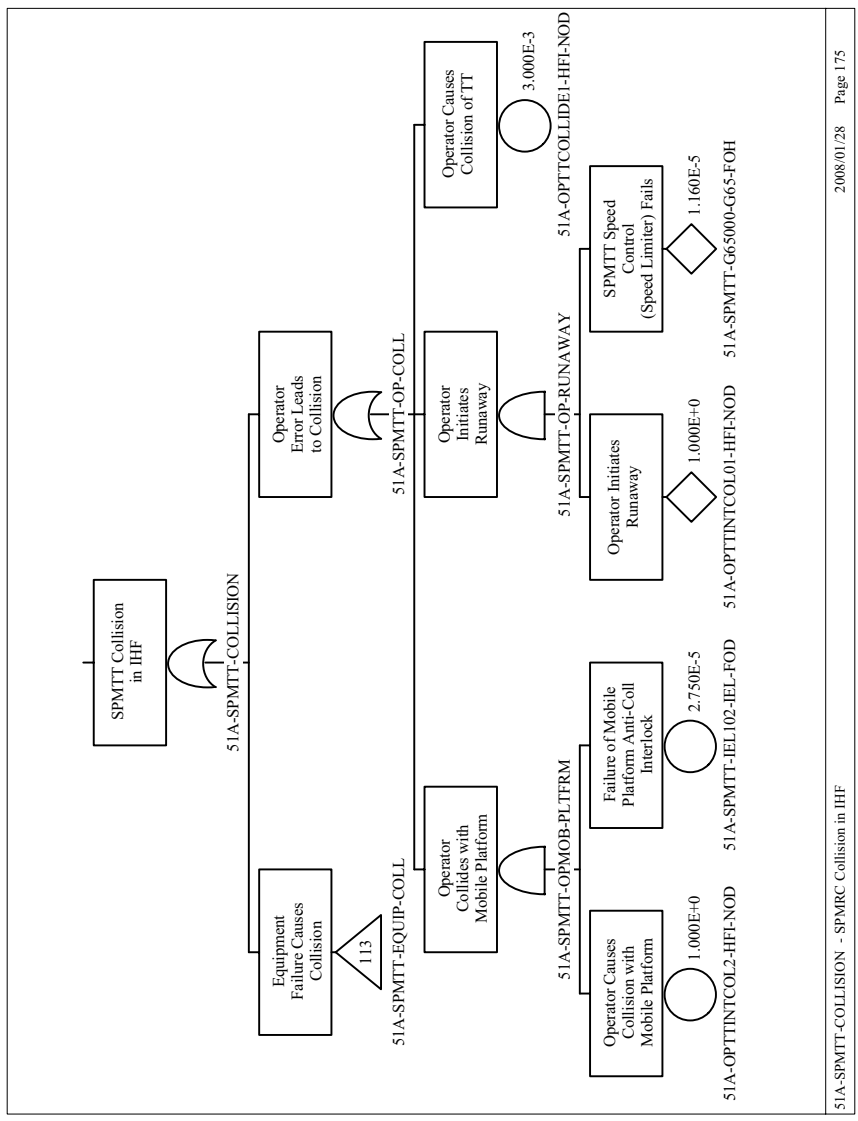
Table B1.4-5. Cut Sets for SPMTT Collides with IHF Structures (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
	0.57	2.750E-005	51A-OPRCINTCOL02-HFI-NOD	Operator Causes Collision with Mobile Platform	1.0E+000
			51A-SPMTT-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	2.8E-005
	0.24	1.160E-005	51A-OPRCINTCOL01-HFI-NOD	Operator Initiates Runaway	1.0E+000
			51A-SPMTT-G65000-G65-FOH	SPMTT Speed Control (Governor) Fails	1.2E-005
	0.08	4.000E-006	51A-SPMTT-CT000--CT--FOD	SPMTT Primary Stop Switch Fails	4.0E-006
	0.08	4.000E-006	51A-SPMTT-CT0001-CT-FOD	On-Board Controller Fails to Respond	4.0E-006
	0.04	1.910E-006	51A-SPMTT-CPL00-CPL-FOH	Automatic Coupler System Fails	1.9E-006
		4.834E-003	= Total		

NOTE: Freq. = frequency; Prob. = probability; SPMTT = site prime mover truck trailer; TT = truck trailer.

Source: Original

B1.4.2.9 Fault Trees



Source: Original

Figure B1.4-8. SPMITT Collision in IHF

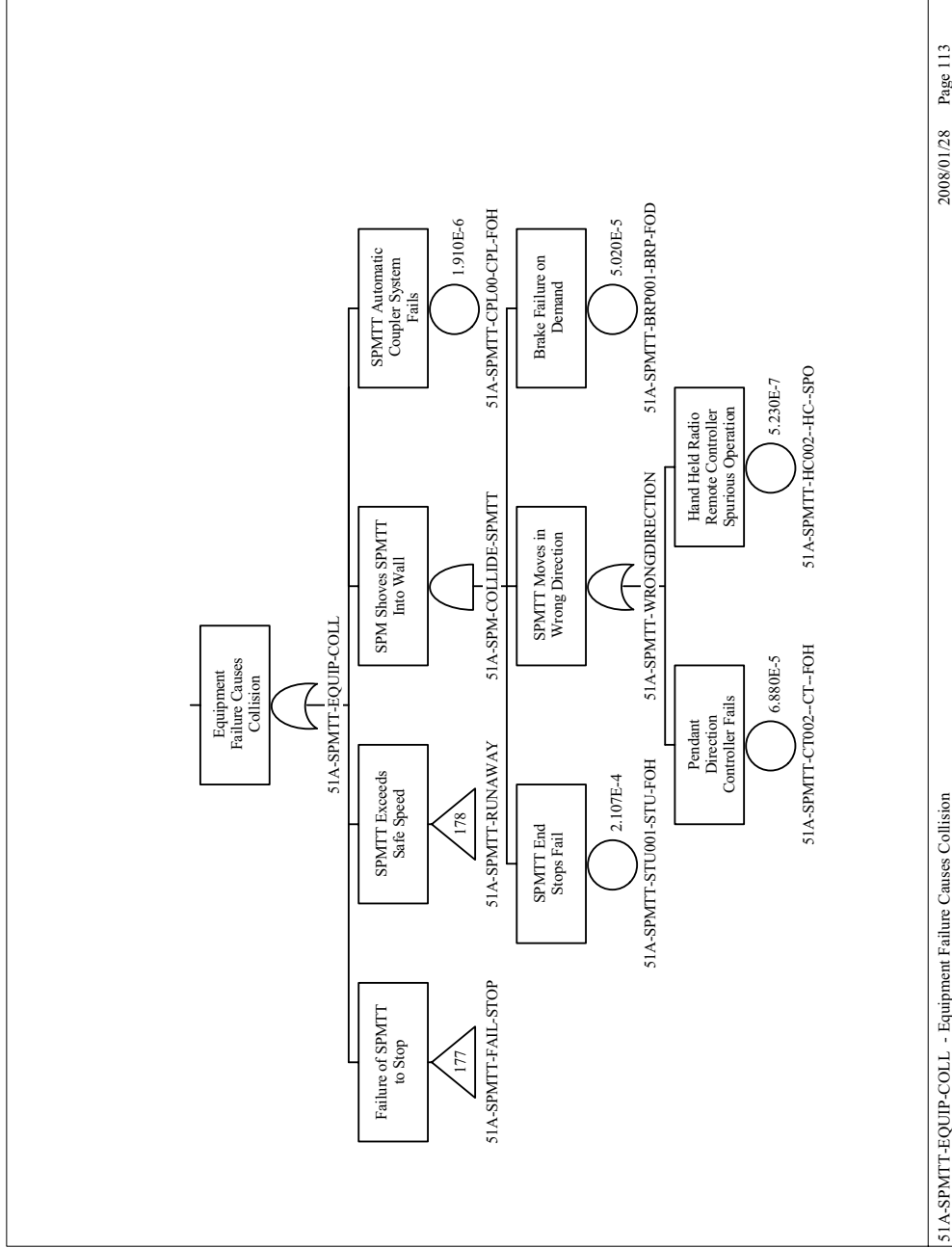
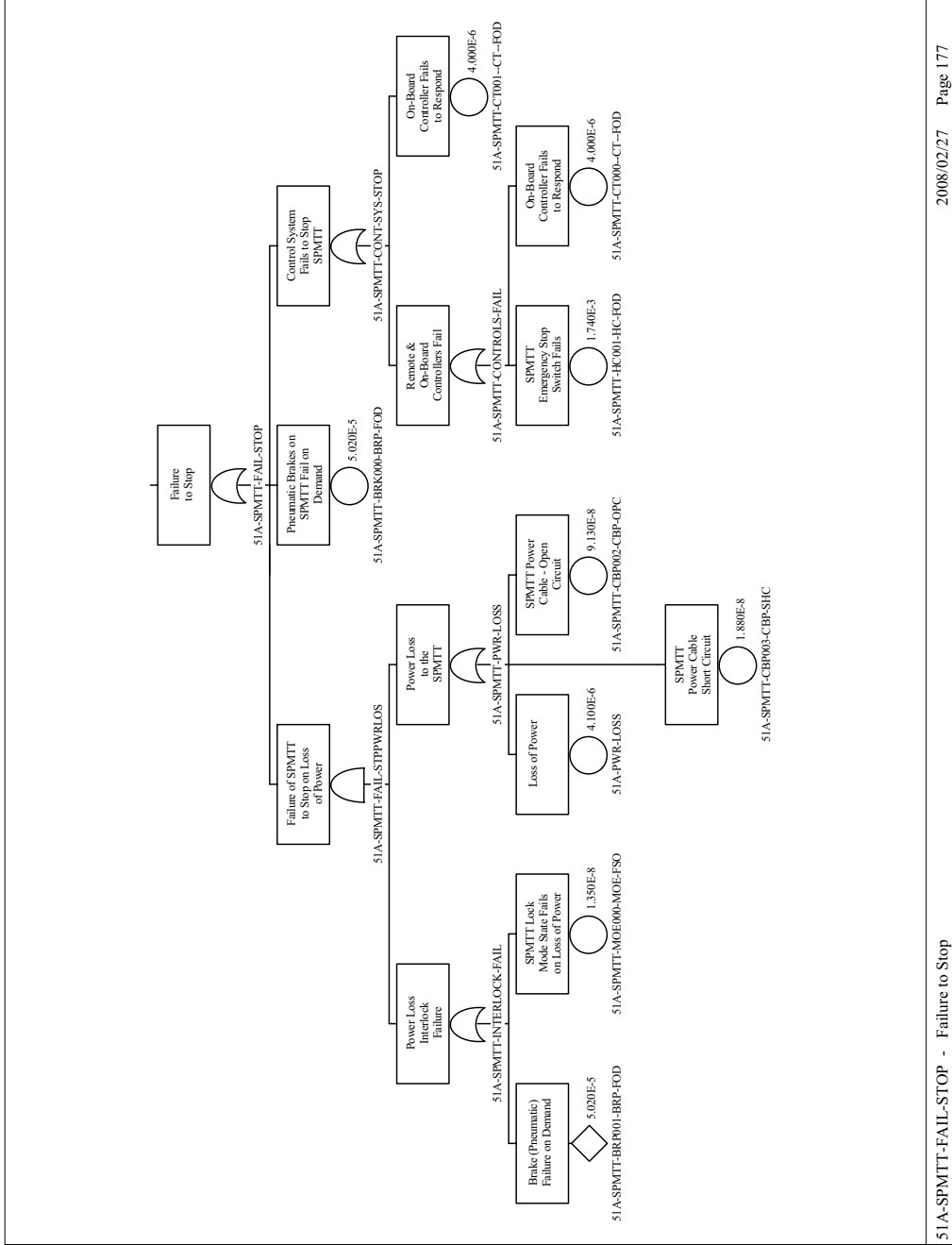


Figure B1.4-9. Equipment Failure Causes Collision



Source: Original

Figure B1.4-10. SPMTT Failure to Stop

B1-36

March 2008

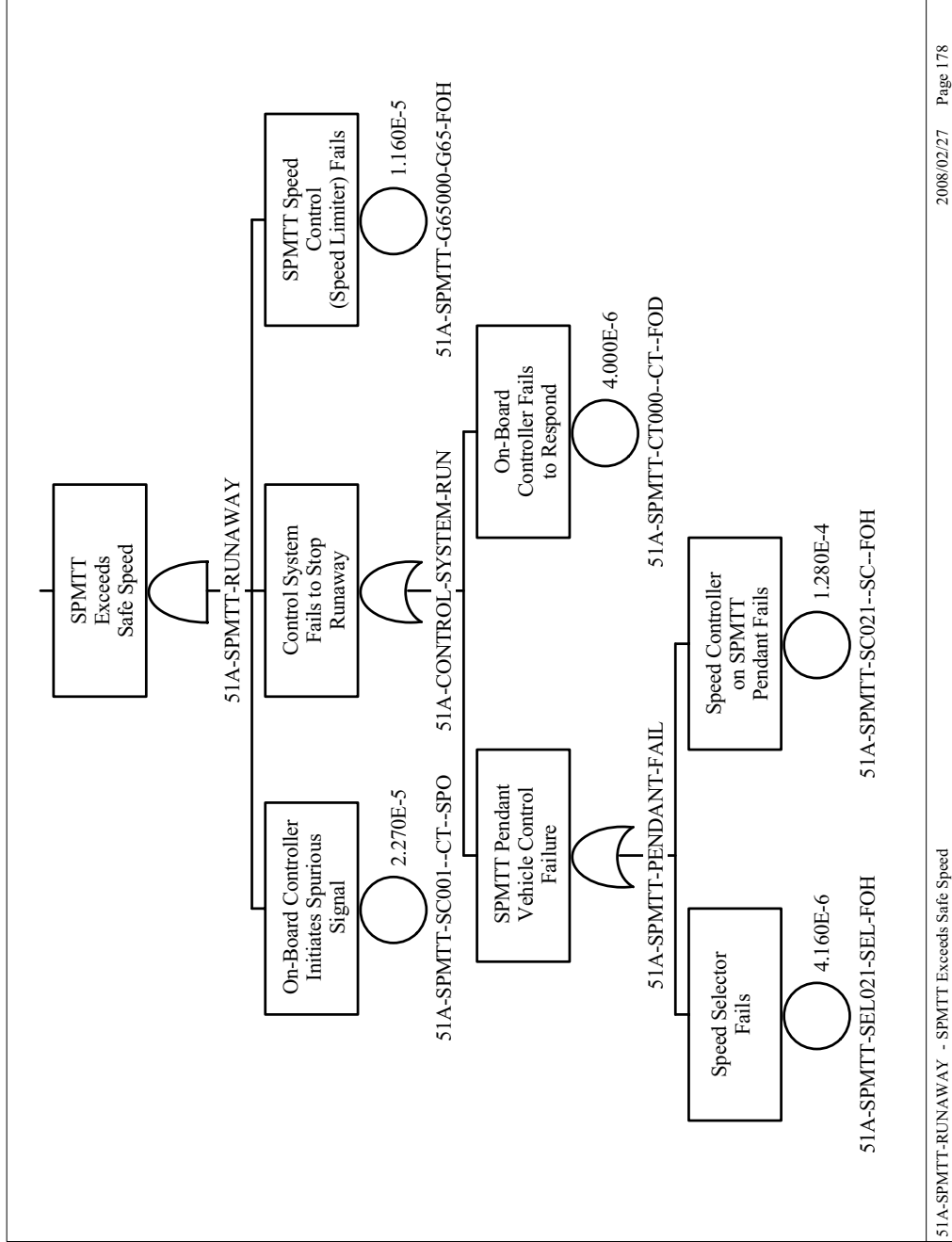


Figure B1.4-11. SPMTT Exceeds Safe Speed

B1.4.3 SPMRC Derailment

B1.4.3.1 Description

The two fault trees for SPMRC derailment within the IHF are identical with the exception of the number of transportation casks that are processed at the IHF for each configuration. Derailment is characterized by a basic event that accounts for the probability of a railcar derailment per mile of travel within the IHF.

This fault tree considers the potential for the SPM to derail during movement of the railcar to the preparation area. The top event is “SPMRC Derails Causing Impact to Transportation Cask.” This fault tree is shown in Figure B1.4-14.

The probability of derailment is based on historical data for train derailment at low speeds and is discussed in the section on data development (Attachment C, Section C4). The probability of derailment per mile is multiplied by the number of miles the SPM travels inside the Cask Preparation Area (approximately 4.00E-02 miles).

B1.4.3.2 Success Criteria

The success criteria for this fault tree are that the SPMRC does not derail during the transport process.

B1.4.3.3 Requirements and Design Features

System Configuration and Operating Conditions

Requirements

The railcar design requirements must comply with AAR Standard S-2043 *Performance Specification for Trains Used to Carry High-Level Radioactive Material* (Ref. B1.1.1).

Design Feature

The design features of the railcar must be in compliance with AAR Standard S-2043 *Performance Specification for Trains Used to Carry High-Level Radioactive Material* (Ref. B1.1.1).

Testing and Maintenance

Requirements

No maintenance or testing is permitted on a railcar loaded with a transportation cask.

Design Feature

None

B1.4.3.4 Fault Tree Model

The fault tree model for “SPMRC Derailment” consists of the probability for a railcar derailment per mile of travel time multiplied by 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 SPMRC Derailment fault trees.

Table B1.4-6. Basic Event Probability for SPMRC Derailment

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-SPMRC-DERAIL-DER-FOM	3	1.180E-005	0.000E+000	1.180E-005	1.000E+000
51A-SPMRC-MILES-IN-IHF	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; Miss. = mission; Prob. = probability; V = value.

Source: Original

The calculated probability of a derailment inside the IHF 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

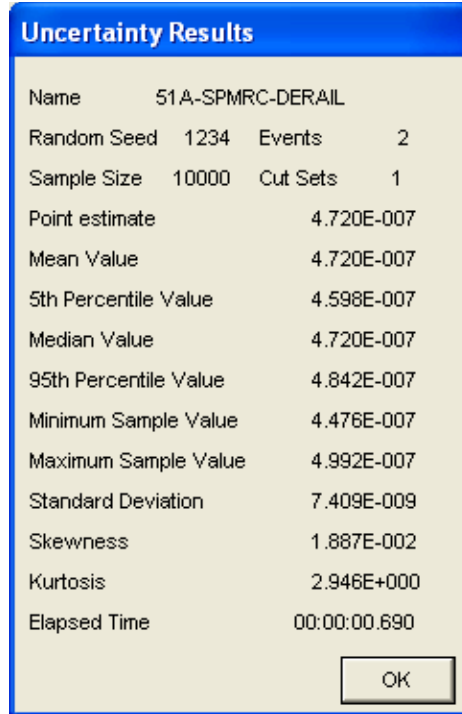
There are no human errors identified for this fault tree.

B1.4.3.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

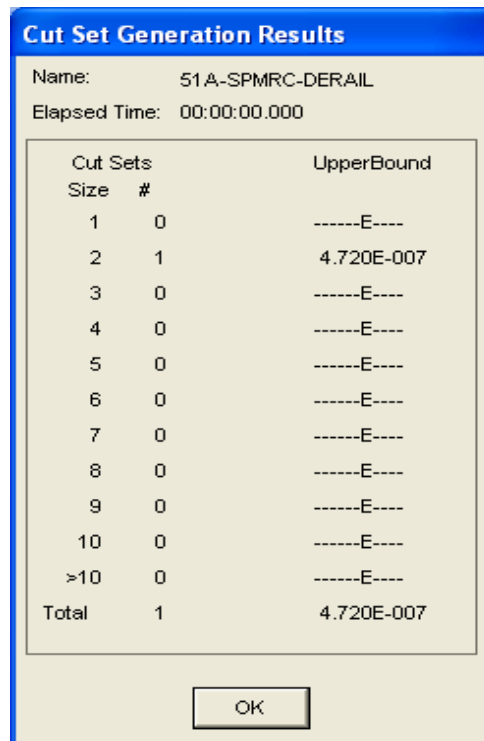
B1.4.3.6 Uncertainty and Cut Set Generation Results

Figure B1.4-12 contains the uncertainty results obtained from running the fault tree for “SPMRC Derailment” using a cutoff probability of 1E-12. Figure B1.4-13 provides the cut set generation results for the “SPMRC Derailment” fault tree.



Source: Original

Figure B1.4-12. Uncertainty Results of the SPMRC Derailment Fault Tree



Source: Original

Figure B1.4-13. Cut Set Generation Results for SPMRC Derailment"

B1.4.3.7 Cut sets

Tables B1.4-7 contains the cut sets for “SPMRC Derailment”. The probability of derailment per cask is 4.72E-07.

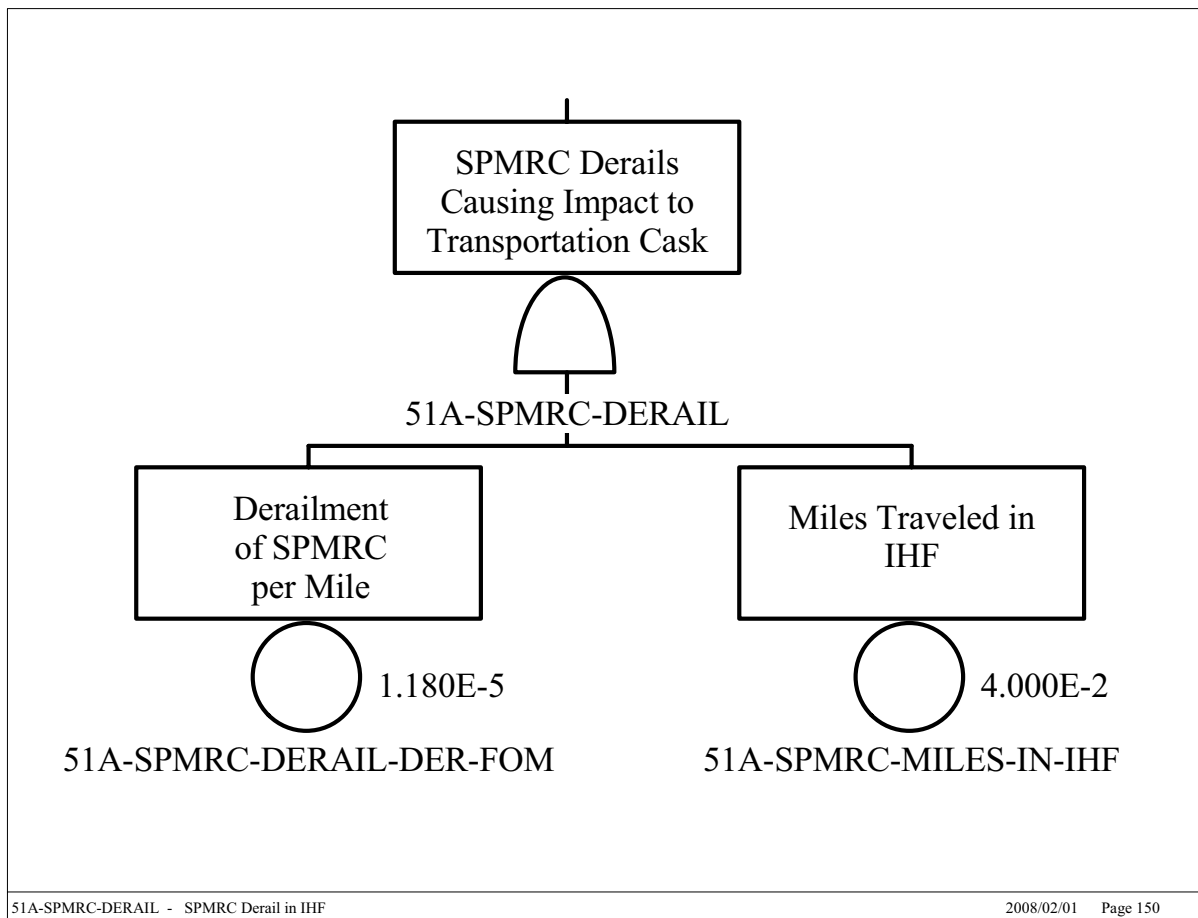
Table B1.4-7. Cut sets for SPMRC Derailment

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-SPMRC- DERAIL	100.00	4.720E-007	51A-SPMRC-DERAIL- DER-FOM	Derailment of a rail car per mile	1.2E-005
			51A-SPMRC-MILES-IN- IHF	Miles traveled in IHF	4.0E-002
4.720E-007 = Total					

NOTE: Freq. = frequency; IHF = Initial Handling Facility Prob. = probability.

Source: Original

B1.4.3.8 Fault Trees



Source: Original

Figure B1.4-14. SPMRC Derailment in IHF

B1.4.4 SPMTT Rollover in the IHF

B1.4.4.1 Description

The fault trees for “SPMTT Rollover in the IHF” 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 IHF Cask Preparation Area.

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.

The success criterion is that no rollover occurs while transferring the trailer into the IHF with the site prime mover.

B1.4.4.3 Requirements and Design Features

System Configuration and Operating Conditions

Requirements

Trailers used for the movement of transportation casks are designed in accordance with the requirements contained in NHTSA requirements as authorized by Title 49 U.S.C. 30111. Transportation: Federal Motor Vehicle Safety Standards (Ref. B1.1.2). The requirements are delineated in 49 CFR Part 571 (Ref. B1.1.3).

While backing the SPMTT through the Cask Preparation Area, at least one walker-spotter is required to ensure no objects are in the path of the SPMTT and to stop the driver from jackknifing the trailer.

Design Feature

None.

Testing and Maintenance

Requirements

No maintenance or testing is permitted on a truck trailer loaded with a transportation cask.

Design Feature

None.

B1.4.4.4 Fault Tree Model

The fault tree model for SPMTT rollover (Figure B1.4-15) consists of a single human error associated with the operator jackknifing the truck trailer when positioning it in the IHF.

B1.4.4.5 Basic Event Data

A rollover within the IHF can only occur if the driver of the SPMTT jackknifes the truck trailer.

There is only one basic event (51A-OPTTROLLOVER-HFI-NOT) consisting of a human error causing a jackknife of the trailer shown in Figure B1.4-15.

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 the limited space within the Cask Preparation Area and the inability of the trailer to jackknife in such a small space (as discussed in Section 6.0, Table 6.0-2).

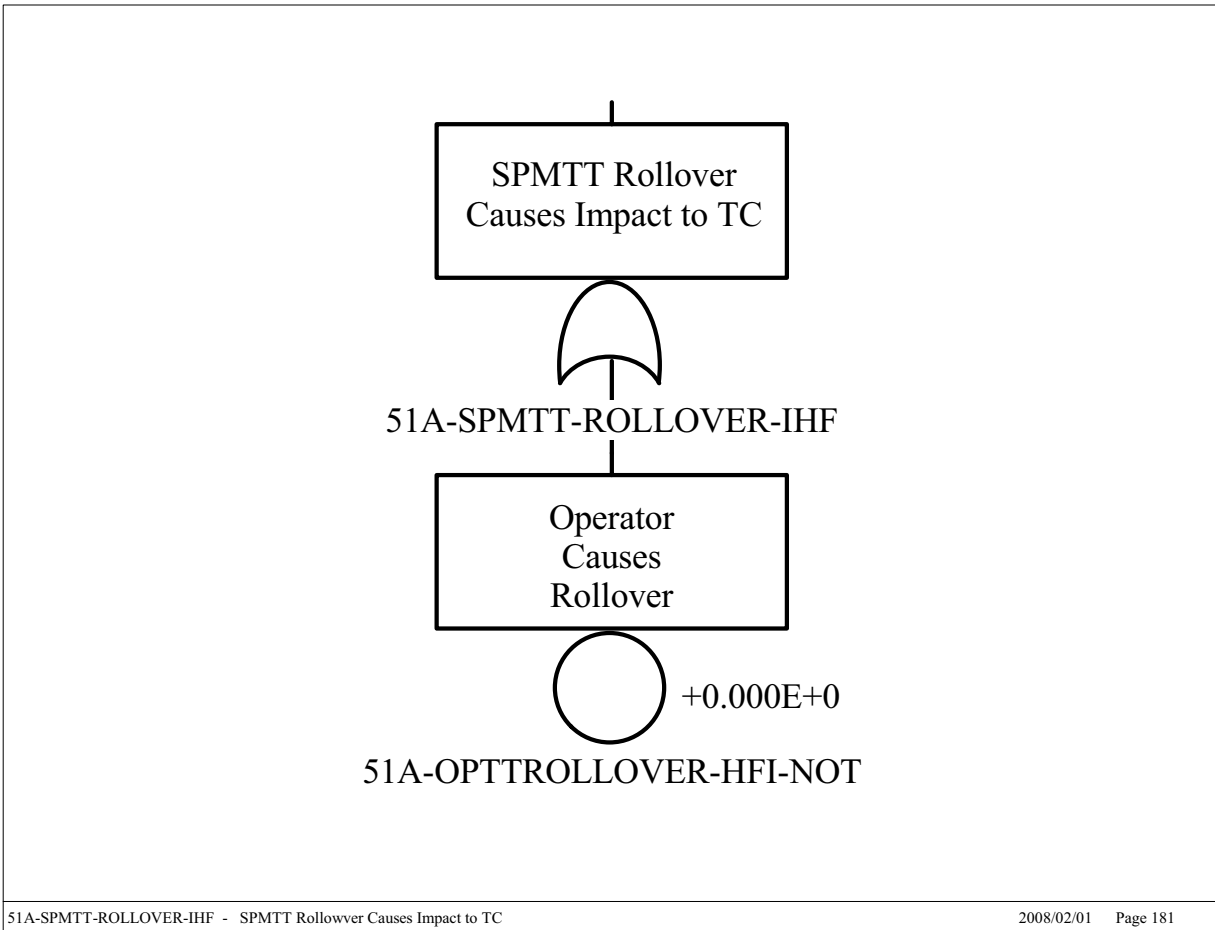
B1.4.4.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

B1.4.4.6 Uncertainty and Cut Set Generation Results

Because there is only a single basic event that is assessed as having zero probability of occurrence, there are no uncertainty values or cut sets to be calculated.

B1.4.4.7 Fault Tree



Source: Original

Figure B1.4-15. SPMTT Rollover in IHF

B2 CASK TRANSFER TROLLEY ANALYSIS – FAULT TREES

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.

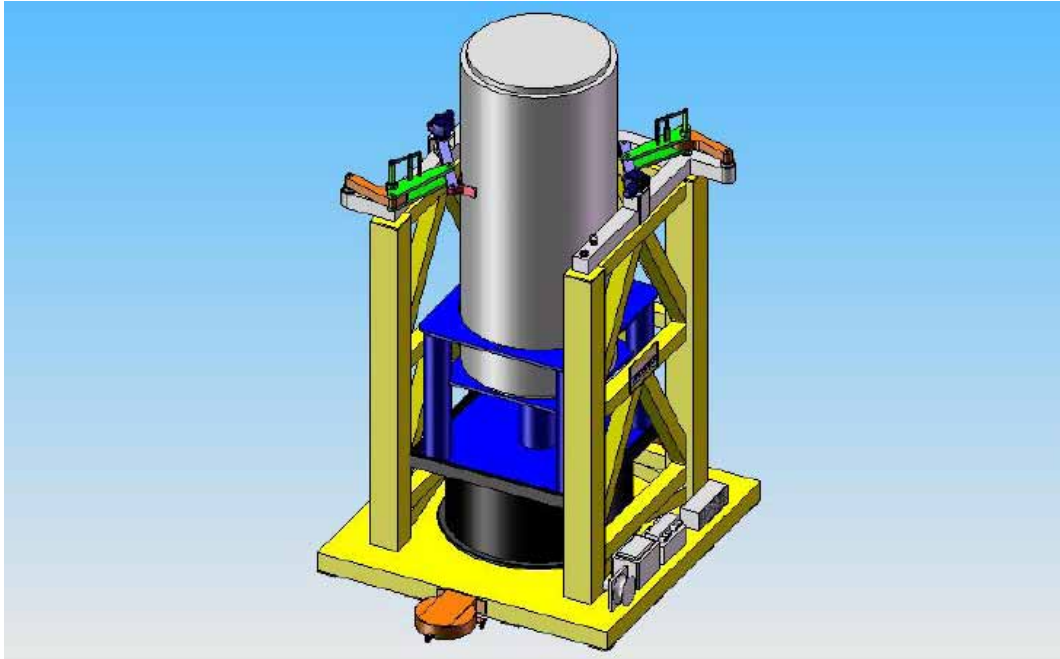
B2.1.2 *BSC (Bechtel SAIC Company) 2007. *Preliminary Throughput Study for the Initial Handling Facility*. 51A-30R-IH00-00100-000-001. Las Vegas, Nevada. Bechtel SAIC Company. ACC: ENG.20071102.0021.

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 is used to transport 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 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, different pedestals are used to position the top of the cask at the appropriate height above 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 in. 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 Canister Transfer Area using bumpers and stops that are bolted to the floor of the Cask Unloading Room with bolts that 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 does not 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 inch to 7/8 inch. 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 1½ inch 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 allow adjustment and verification of pressure/flow for each individual bearing. There are two interlocks for the air; one pressure monitor verifies 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-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. 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 0-10 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 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 presses both handles to allow air to flow to the CTT to levitate and move it 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.

There 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.

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.

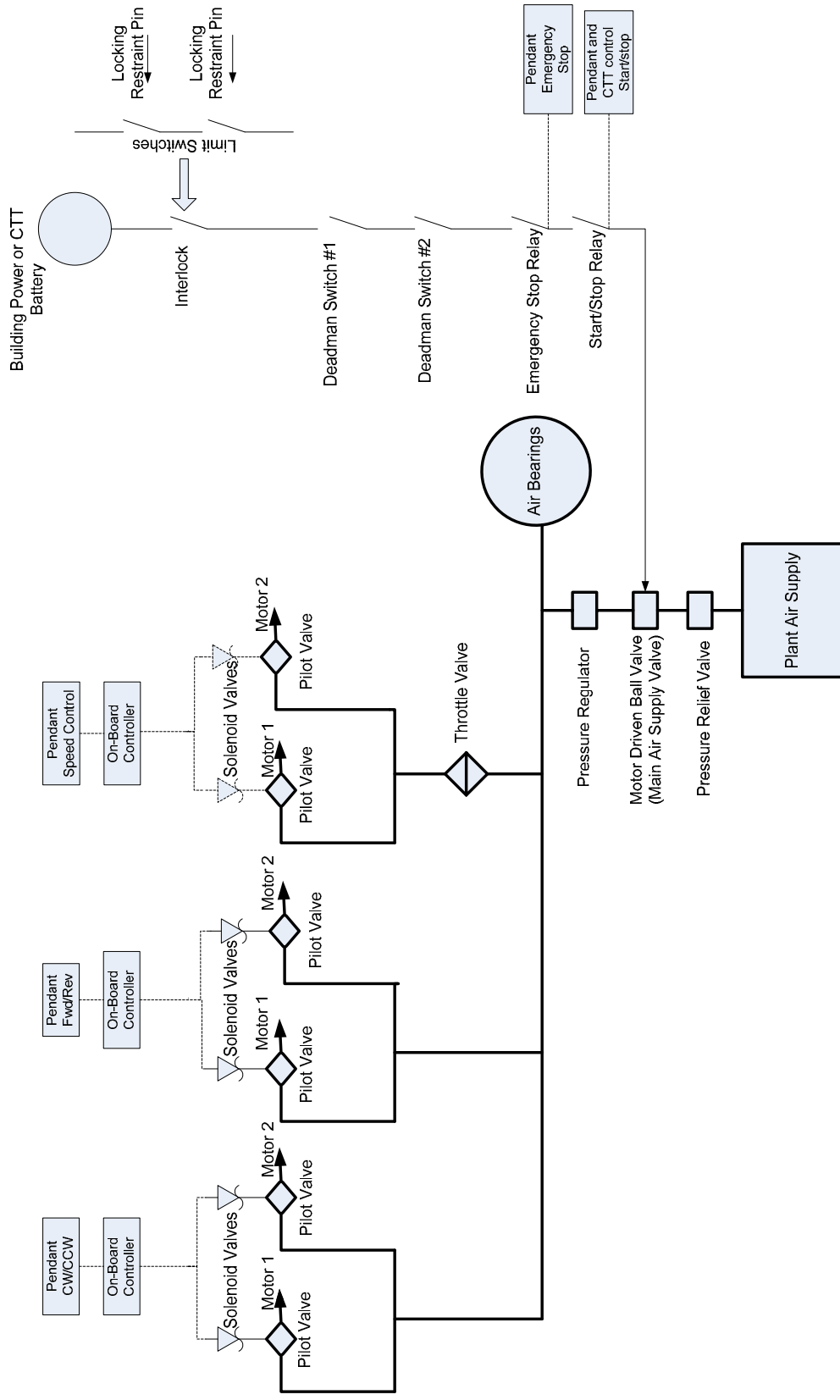
B2.2.3 Operation

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 air bearings and drive motors to operate. Once all preparations of the cask are complete, the trolley can be moved to the Cask Unloading Room using the pendant controls.



Source: Modified from (Ref. B2.1.3)

Figure B2.2-2. Schematic of the CTT Control System

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 Cask Unloading Room require 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 be disconnected 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 unit is external to the transfer 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 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 by the emergency stop buttons on the pendant and on the CTT. The speed controls slow down and stop the CTT by controlling the air flow through 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 occurs. 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 operator controls are needed 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 structures, systems or 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, 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	—

Table B2.3-1. Dependencies and Interactions Analysis (Continued)

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
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 CTT during cask transfer
4. Spurious Movement of the CTT in the Cask Unloading 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 Cask Unloading Room. This fault tree is described in a separate section involving inadvertent shield door closure that satisfies ESD-6, 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-2, initiating event “Unplanned Carrier Movement Causes Transportation Cask Impact.” 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 (Figure B2.4-3). 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 an impact to occur resulting in 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 which prevents power to the main air supply valve until both 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 Inputs

Table B2.4-1 contains a list of basic events used in the fault tree (Figures B2.4-3 and B2.4-4) for “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	Calc. Type^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time^a
51A-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
51A-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-CTT--SV301---SV--FOH	3	8.120E-007	0.000E+000	8.120E-007	1.000E+000
51A-CTT--ZS301---ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000

Table B2.4-1. Basic Event Probabilities for Spurious Movement of the CTT during Cask Loading
(Continued)

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTT--ZS302---ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
51A-OPSPURMOV01-HFI-NOD	1	1.000E-004	1.000E-004	0.000E+000	0.000E+000
51A-PIN-LIMIT-SW-CCF	3	5.076E-005	5.076E-005	0.000E+000	0.000E+000
51A--CTT--SV401--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-FWDREVM1-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-FWDREVM2-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-SVROTM1--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-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

B2.4.1.5.1 Human Failure Events

One operator error involves initiation of spurious movement. The operator error is 51A-OPSPURMOVE01-HFI-NOD.

B2.4.1.5.2 Common-Cause Failures

One common-cause failure (CCF) 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 failure criteria (Table C3-1, CCCG = 2). The common-cause failure is 51A-PIN-LIMIT-SW-CCF.

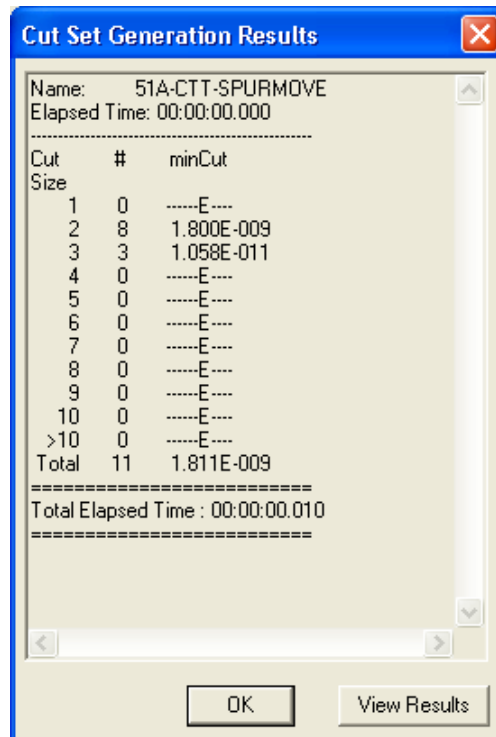
B2.4.1.6 Uncertainty and Cut Set Generation Results

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-12. 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 Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading



Source: Original

Figure B2.4-2. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading

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 1.811E-09.

Table B2.4-2. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-CTT-SPURMOVE	76.22	1.380E-009	51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005
			51A-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement	1.0E-004
	17.30	3.133E-010	51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005
	1.10	1.992E-011	51A-CTT-FWDREVM1-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	1.10	1.992E-011	51A-CTT-FWDREVM2-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SV401-SV-FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.9E-005
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM1-SV-FOH	Failure of SV Providing Rotation to Motor 1	4.9E-005
	1.10	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM2-SV-FOH	Failure of SV Providing Rotation to Motor 2	4.9E-005
	0.47	8.585E-012	51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004

Table B2.4-2 Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area during Cask Loading (Continued)

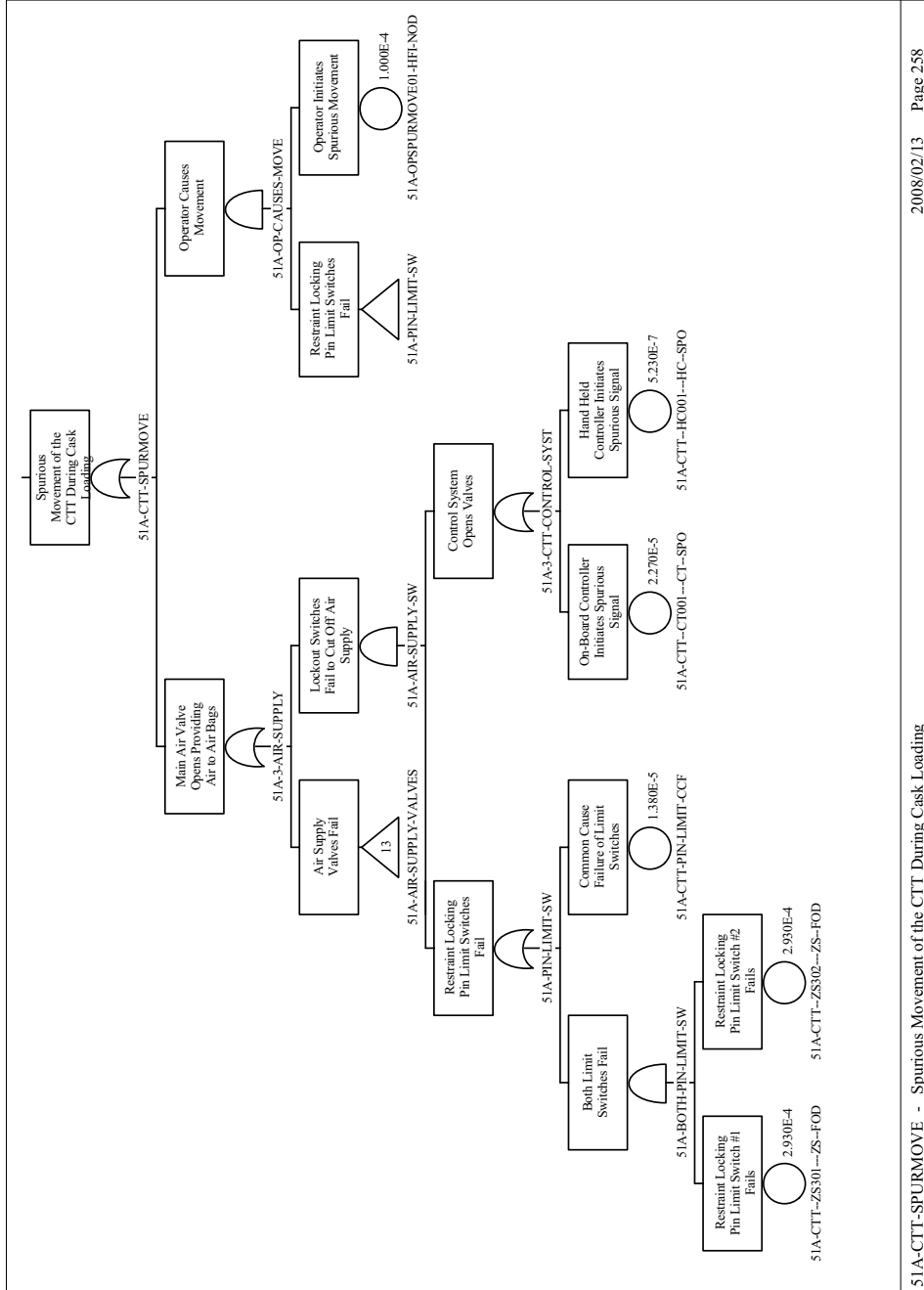
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004
			51A-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement	1.0E-004
	0.40	7.217E-012	51A-CTT--HC001---HC--SPO	Hand Held Controller Initiates Spurious Signal	5.2E-007
			51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	1.4E-005
	0.11	1.949E-012	51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004
	0.00	4.490E-014	51A-CTT--HC001---HC--SPO	Hand Held Controller Initiates Spurious Signal	5.2E-007
			51A-CTT--ZS301---ZS--FOD	Restraint Locking Pin Limit Switch #1 Fails	2.9E-004
			51A-CTT--ZS302---ZS--FOD	Restraint Locking Pin Limit Switch #2 Fails	2.9E-004
1.811E-009 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

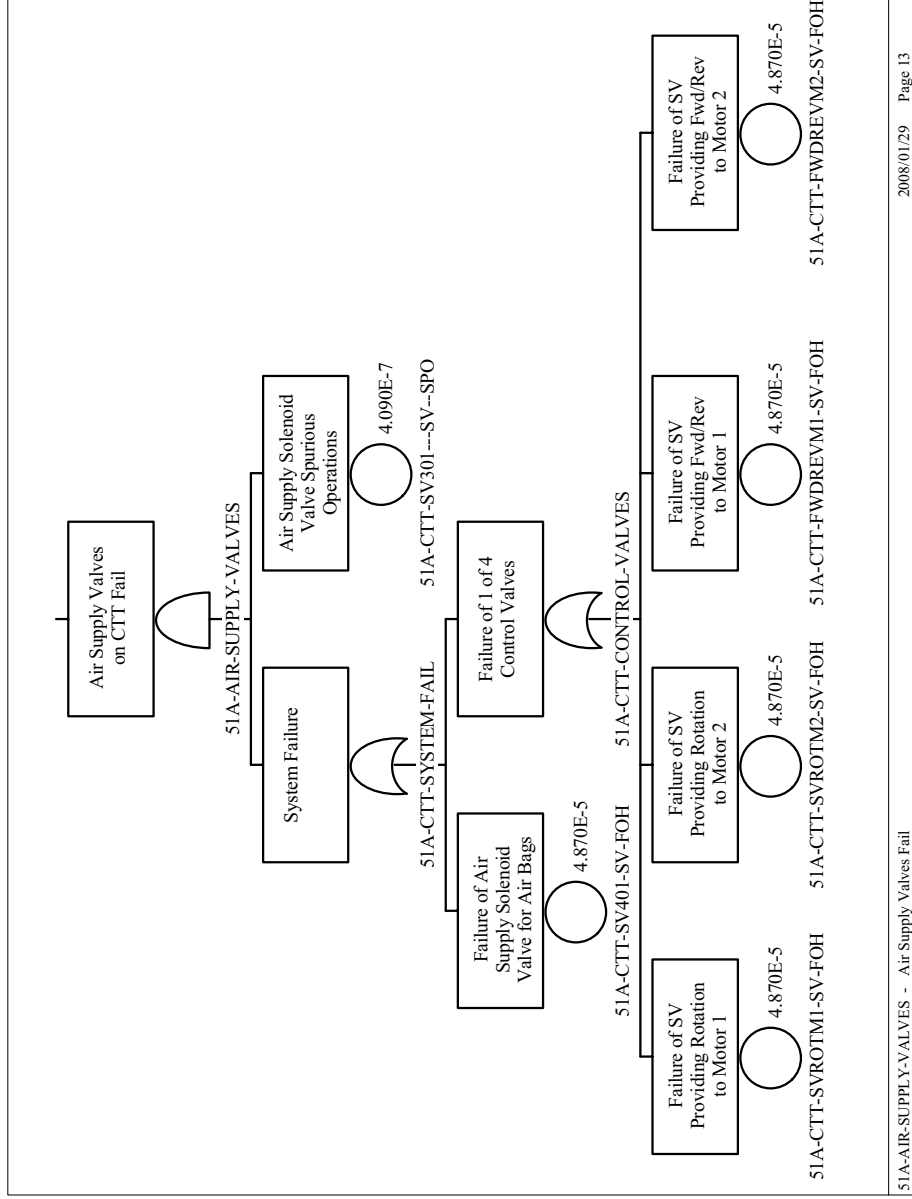
B2.4.1.8 Fault Trees

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.



51A-CTT-SPURMOVE - Spurious Movement of the CTT During Cask Loading

Figure B2.4-3. Fault Tree for Spurious Movement of the CTT in the Cask Preparation Area During Cask Loading



2008/01/29 Page 13

51A-AIR-SUPPLY-VALVES - Air Supply Valves Fail

Source: Original

Figure B2.4-4. Fault Tree for Air Supply 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-3 and ESD-4, initiating event “Side Impact to Cask.” The top event is “Spurious Movement of the CTT during Cask Preparation” 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 in the Cask Preparation Area 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 (Figure B2.4-7) for “Spurious Movement of the CTT in the Cask Preparation Room during Cask Preparation”.

Table B2.4-3. Basic Event Probabilities for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
51A-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-CTT--SV301---SV--SPO	3	8.120E-007	0.000E+000	8.120E-007	1.000E+000
51A-OPSPURMOVE01-HFI-NOD	1	1.000E-004	1.000E-004	0.000E+000	0.000E+000
51A--CTT--SV401--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
51A-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-CTT-FWDREVM1-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-FWDREVM2-SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-SVROTM1--SV--FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-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

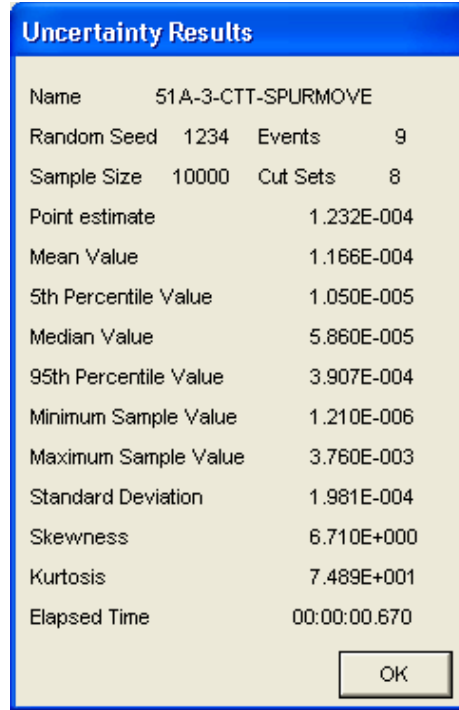
One operator error (51A-OPSPURMOVE01-HFI-NOD) involves initiation of spurious movement.

B2.4.2.5.2 Common-Cause Failures

There is no CCF associated with this fault tree.

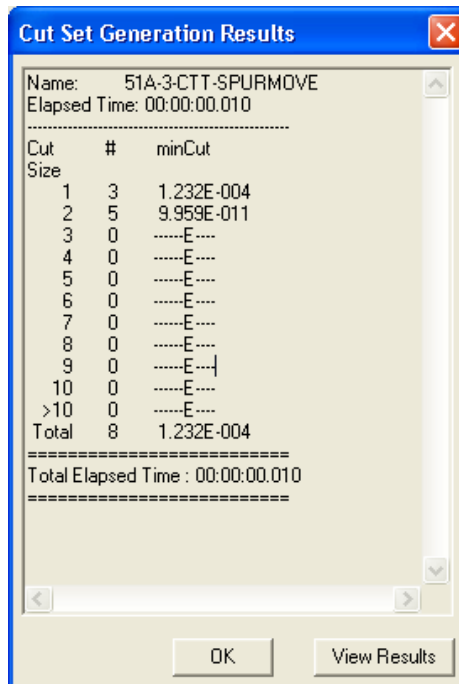
B2.4.2.6 Uncertainty and Cut Set Generation Results

Figure B2.4-5 contains the uncertainty results obtained from running the fault tree for “Spurious Movement of the CTT in the Cask Preparation Room during Cask Preparation” using a cutoff probability of 1E-12. Figure B2.4-6 provides the cut set generation results for “Spurious Movement of the CTT in the Cask Preparation Room during Cask Preparation.”



Source: Original

Figure B2.4-5. Uncertainty Results of the Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation



Source: Original

Figure B2.4-6. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Preparation Area 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 loading is 1.232E-004 with operator initiation of “Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation”.

Table B2.4-4. Cut Sets for Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation

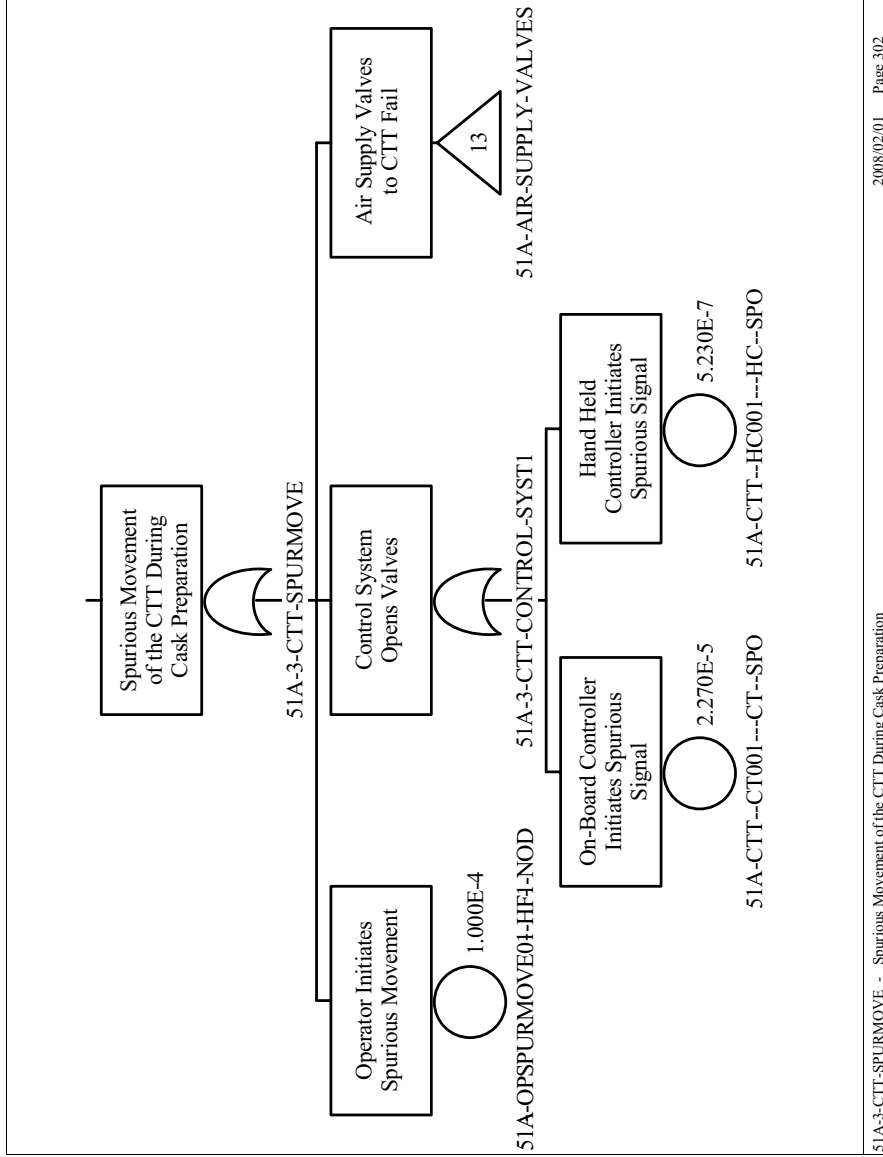
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-3-CTT-SPURMOVE	81.16	1.000E-004	51A-OPSPURMOVE01-HFI-NOD	Operator Initiates Spurious Movement	1.0E-004
	18.42	2.270E-005	51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
	0.42	5.230E-007	51A-CTT--HC001---HC--SPO	Hand Held Controller Initiates Spurious Signal	5.2E-007
	0.00	1.992E-011	51A-CTT-FWDREVM1-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 1	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	0.00	1.992E-011	51A-CTT-FWDREVM2-SV-FOH	Failure of SV Providing Fwd/Rev to Motor 2	4.9E-005
			51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
	0.00	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SV401-SV-FOH	Failure of Air Supply Solenoid Valve for Air Bags	4.9E-005
	0.00	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM1-SV-FOH	Failure of SV Providing Rotation to Motor 1	4.9E-005
	0.00	1.992E-011	51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	4.1E-007
			51A-CTT-SVROTM2-SV-FOH	Failure of SV Providing Rotation to Motor 2	4.9E-005
1.232E-004 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B2.4.2.8 Fault Trees

The fault tree for “Spurious Movement of the CTT in the Cask Preparation Area During Cask Preparation” is shown in Figures B2.4-7. Note that the transfer gate 13 in Figure B2.4-7 refers to the fault tree in Figure B2.4-4.



2008/02/01 Page 302

51A-3-CTT-SPURMOVE - Spurious Movement of the CTT During Cask Preparation

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 with a structure or object while moving a cask from the Cask Preparation Room to the Cask Unloading Room. This satisfies ESD-6, pivotal event “Site Transporter or CTT Impact Collision with Another Vehicle, Facility Structure or Equipment.” The top event is “CTT Collision into Structure.” This fault tree is shown in Figures B2.4-10 and 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 backwards. 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 fpm 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 to 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 a collision with any object, including the shield door, during transfer of a cask from the Cask Preparation Room to the Cask Unloading Room. A collision of the CTT could cause damage to the transportation cask.

B2.4.3.3 Design Features and Requirements

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 for a collision of the CTT into an object or structure during transfer of a cask from the cask preparation room to the canister unloading area. 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 CTT during Cask Transfer”.

Table B2.4-5. Basic Event Probability for Collision of CTT during Cask Transfer

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTT--DSW000--ESC-CCF	1	1.180E-005	1.180E-005	1.180E-005	0.000E+000
51A-CTT--DSW001--ESC-FOD	1	2.500E-004	2.500E-004	0.000E+000	0.000E+000
51A-CTT--DSW002--ESC-FOD	1	2.500E-004	2.500E-004	0.000E+000	0.000E+000
51A-HTC--HC021---HC--FOD	1	1.740E-003	1.740E-003	0.000E+000	0.000E+000
51A-HTC--SV601---SV--FOD	1	6.280E-004	6.490E-004	0.000E+000	0.000E+000
51A-HTC--SV602---SV--FOD	1	6.280E-004	6.490E-004	0.000E+000	0.000E+000
51A-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

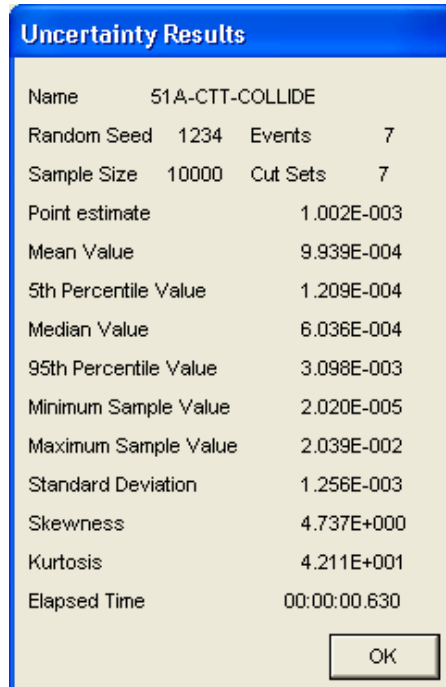
A collision may be caused by an operator error (51A-OPCTTCOLLID2-HFI-NOD) failing to stop the CTT.

B2.4.3.5.2 Common-Cause Failures

One CCF (51A-CTT--DSW000--ESC-CCF) involves failure of both deadman switches, both of which must be pressed for the main air supply valve to open.

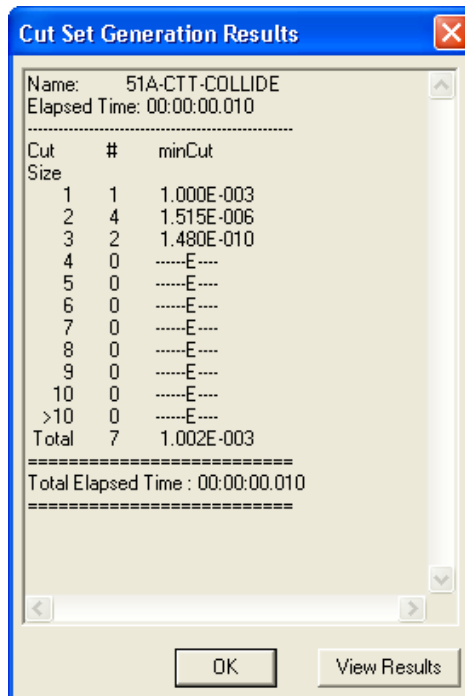
B2.4.3.6 Uncertainty and Cut Set Generation Results

Figure B2.4-8 contains the uncertainty results obtaining from running the fault trees for “Collision of the CTT during Cask Transfer”. Figure B2.4-9 provides the cut set generation results for “Collision of the CTT during Cask Transfer”.



Source: Original

Figure B2.4-8. Uncertainty Results for the Collision of CTT during Cask Transfer Fault Tree



Source: Original

Figure B2.4-9. Cut Set Generation Results for the Collision of CTT during Cask Transfer Fault Tree

B2.4.3.7 Cut Sets

Table B2.4-6 contains the cut sets for the collision of the CTT during cask movement from the Cask Preparation Room to the Cask Unloading Room. The total probability per cask loading is 1.002E-03 with operator error the dominant cause of collision.

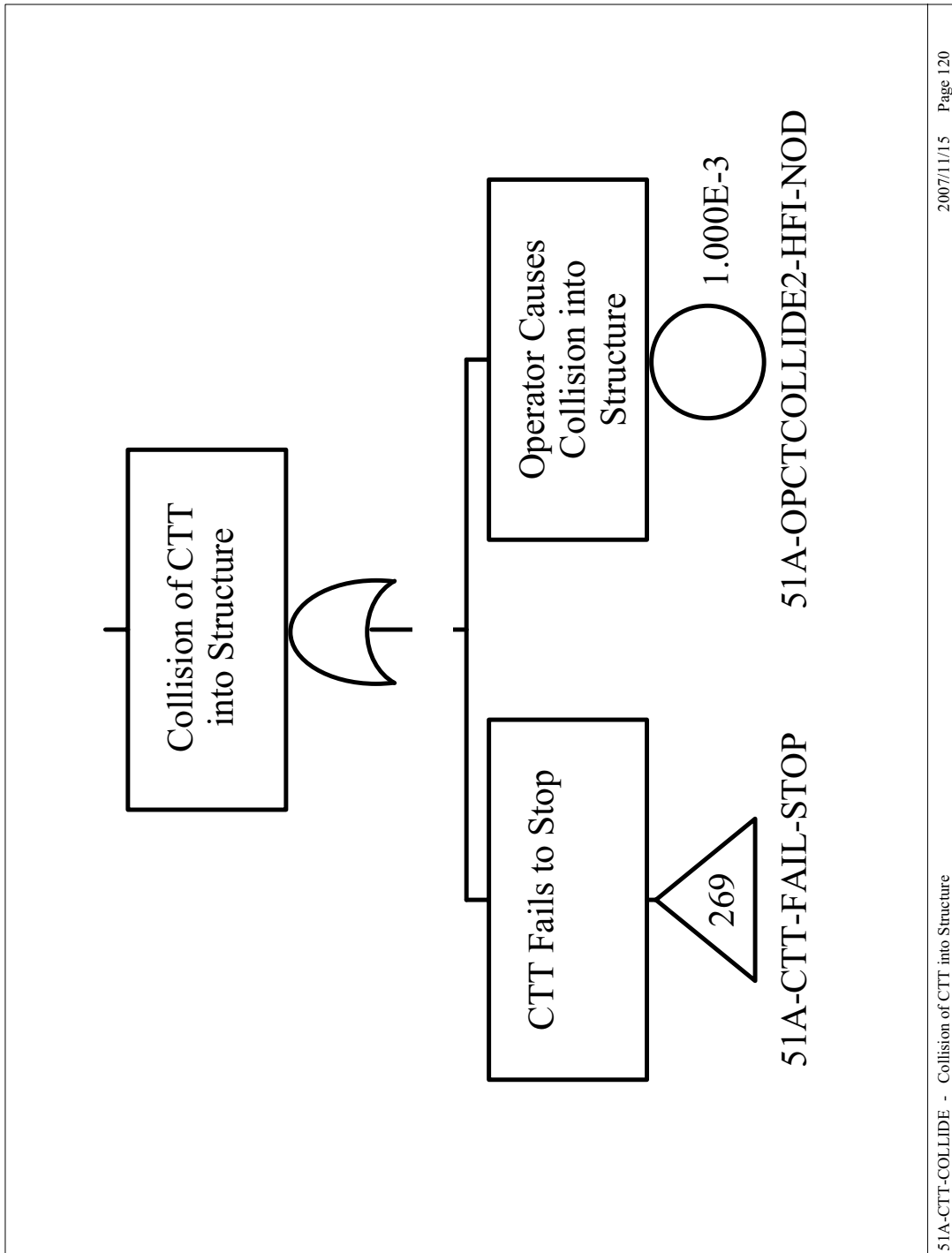
Table B2.4-6. Cut Sets for Collision of the CTT During Cask Transfer

Fault Tree	Cut set %	Prob./Freq.	Basic Event	Description	Probability
51A-CTT-COLLIDE	99.85	1.000E-003	51A-OPCTCOLLIDE2-HFI-NOD	Operator Causes Collision into Structure	1.0E-003
	0.11	1.093E-006	51A-CTT--HC021---HC-FOD	Remote Controller Transmits Wrong Instruction	1.7E-003
			51A-CTT--SV601---SV--FOD	Main Air Supply Valve Fails on Demand	6.3E-004
	0.04	3.944E-007	51A-CTT--SV601---SV--FOD	Main Air Supply Valve Fails on Demand	6.3E-004
			51A-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	6.3E-004
	0.00	2.053E-008	51A-CTT--DSW000--ESC-CCF	Common Cause Failure of Dead man Switches	1.2E-005
			51A-CTT--HC021---HC-FOD	Remote Controller Transmits Wrong Instruction	1.7E-003
	0.00	7.410E-009	51A-CTT--DSW000--ESC-CCF	Common Cause Failure of Dead man Switches	1.2E-005
			51A-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	6.3E-004
	0.00	1.088E-010	51A-CTT--DSW001--ESC-FOD	Dead man Switch #1 Fails Closed	2.5E-004
			51A-CTT--DSW002--ESC-FOD	Dead man Switch #2 Fails Closed	2.5E-004
			51A-CTT--HC021---HC-FOD	Remote Controller Transmits Wrong Instruction	1.7E-003
	0.00	3.925E-011	51A-CTT--DSW001--ESC-FOD	Dead man Switch #1 Fails Closed	2.5E-004
			51A-CTT--DSW002--ESC-FOD	Dead man Switch #2 Fails Closed	2.5E-004
			51A-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	6.3E-004
1.002E-003 = Total					

NOTE: Freq. = frequency; Prob. = probability.

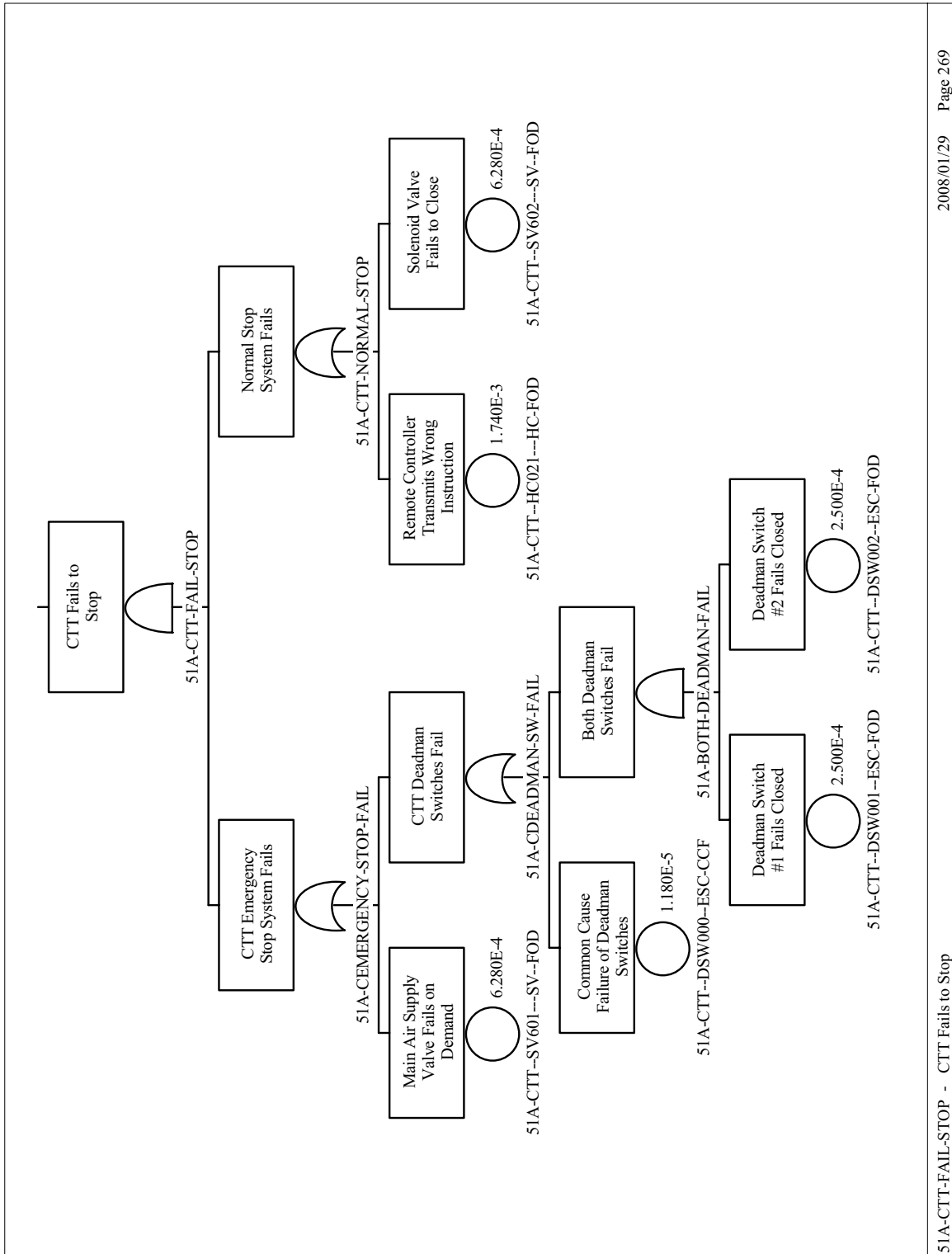
Source: Original

B2.4.3.8 Fault Trees



Source: Original

Figure B2.4-10. Fault Tree for Collision of the CTT During Cask Transfer (Page 1)



2008/01/29 Page 269

51A-CTT-FAIL-STOP - CTT Fails to Stop

Source: Original

Figure B2.4-11. Fault Tree for Collision of the CTT During Cask Transfer (Page 2)

B2.4.4 Spurious Movement of the CTT in the Cask Unloading 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 ESD-7, initiating event “Canister Impact Due to Movement of CTT During Lift.” The top event is “Spurious Movement during Canister Transfer” which is defined as unplanned movement of the CTT while the canister is extracted from the transportation cask. This fault tree is shown in Figures B2.4-14.

Spurious movement is prevented in the Cask Unloading 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 Cask Unloading Room, the operator must disconnect the air supply hose to the CTT for the shield door to be closed, or the shield door cuts 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 Cask Unloading 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 an impact to occur and/or shear resulting in damage to the canister.

B2.4.4.3 Design Features and Requirements

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 Cask Unloading 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 for 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 (Figure B2.4-14) for “Spurious Movement of the CTT in the Cask Unloading Room”.

Table B2.4-7. Basic Event Probability for Spurious Movement of the CTT in the Cask Unloading Room

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CR-IEL00A-IEL-FOD	3	2.750E-005	0.000E+000	2.740E-005	1.000E+000
51A-CR-IEL00B-IEL-FOD	3	2.750E-005	0.000E+000	2.740E-005	1.000E+000
51A-CR-IELCCF-IEL-FOD	1	1.290E-006	1.290E-006	0.000E+000	0.000E+000
51A-CTT--CT001---CT--SPO	3	2.270E-005	0.000E+000	2.270E-005	1.000E+000
51A-CTT--HC001---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-CTT--SV301---SV--SPO	3	4.090E-007	0.000E+000	4.090E-007	1.000E+000
51A-OPNODISCOAIR-HFI-NOD	1	1.000E-003	1.000E-003	0.000E+000	0.000E+000
51A-CTT-SV401-SV-FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-FWDREVM1-SV-FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-FWDREVM2-SV-FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-CTT-SVROTM1-SV-FOH	3	4.870E-005	0.000E+000	4.870E-005	1.000E+000
51A-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

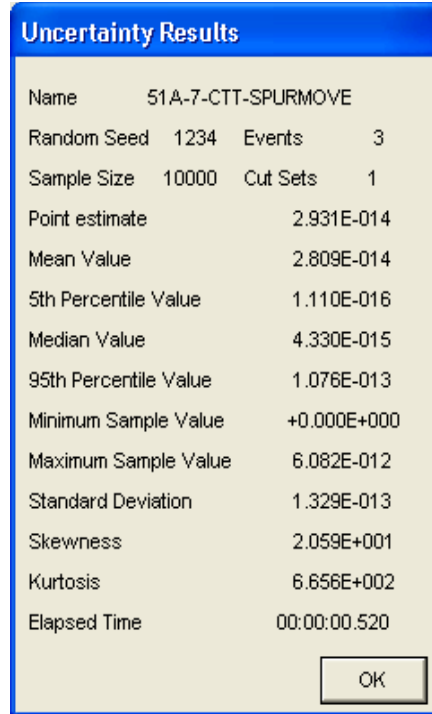
One operator error (51A-OPNODISCOAIR-HFI-NOD) involves failure to disconnect the air supply.

B2.4.4.5.2 Common-Cause Failures

One CCF involves failure of both shield door interlocks allowing the shield door to close and the slide port gate to open.

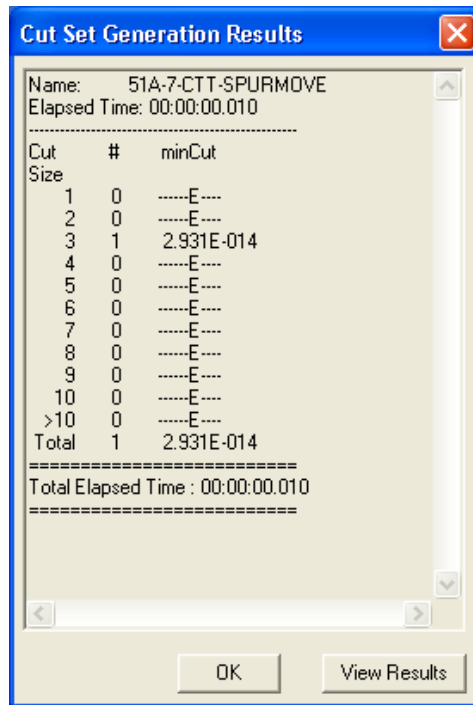
B2.4.4.6 Uncertainty and Cut Set Generation Results

Figure B2.4-12 contains the uncertainty results obtained from running the fault trees for “Spurious Movement of the CTT in the Cask Unloading Room”, using a cutoff probability of 1E-12, while extracting the canister from the transportation cask in the Cask Unloading Room. Figure B2.4-13 provides the cut set generation results for “Spurious Movement of the CTT in the Cask Unloading Room”.



Source: Original

Figure B2.4-12. Uncertainty Results for the Spurious Movement of the CTT in the Cask Unloading Room Fault Tree



Source: Original

Figure B2.4-13. Cut Set Generation Results for Spurious Movement of the CTT in the Cask Unloading Room Fault Tree

B2.4.4.7 Cut Sets

Table B2.4-8 contains the cut sets for spurious movement of the CTT in the Cask Unloading Room. The total probability per cask loading is 2.93E-14.

Table B2.4-8 Spurious Movement of the CTT in the Cask Unloading Room

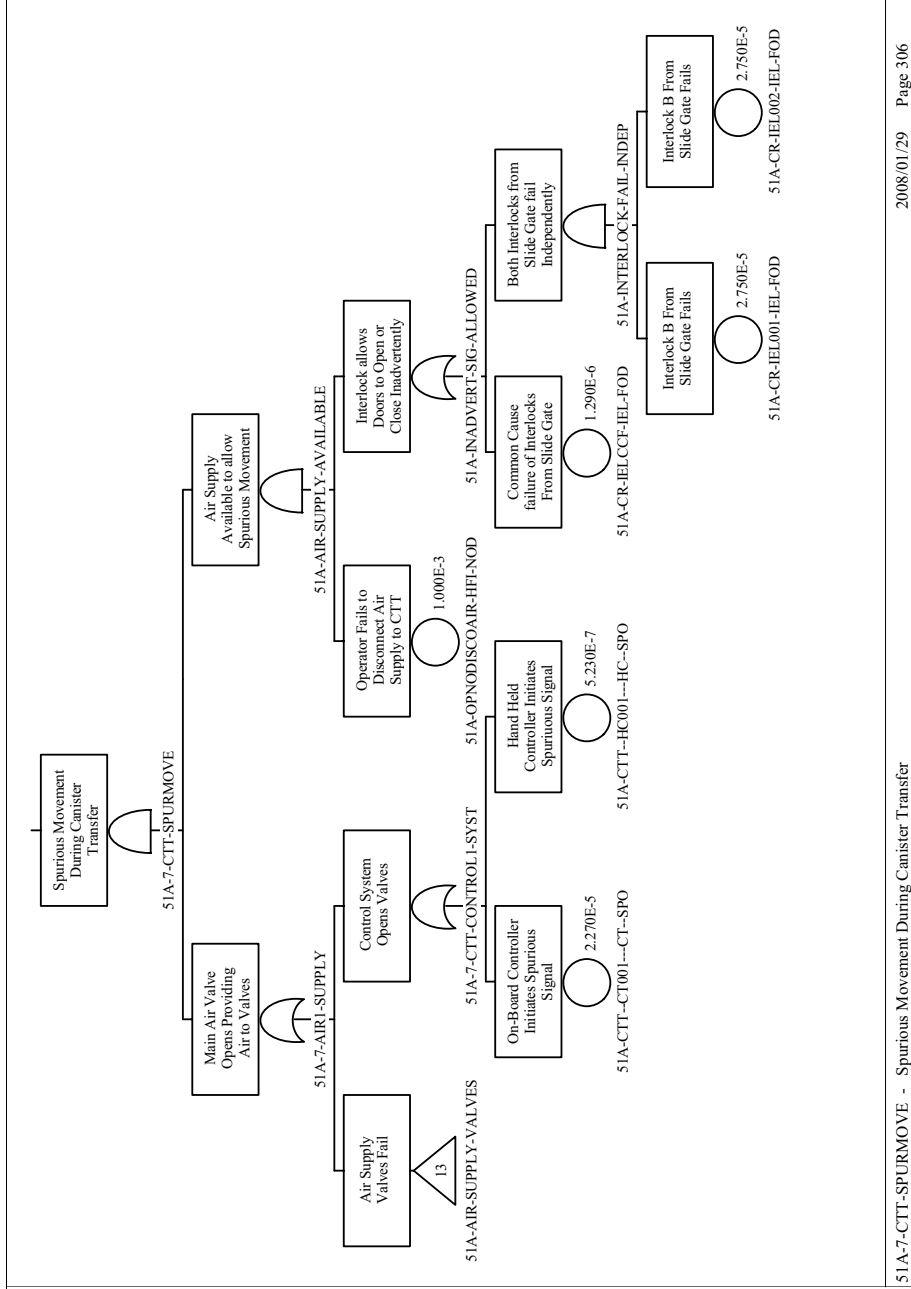
Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-7-CTT-SPURMOVE	99.91	2.928E-014	51A-CR-IELCCF-IEL-CCF	Common Cause failure of Interlocks From Slide Gate	1.3E-006
			51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	2.3E-005
			51A-OPNODISCOAIR-HFI-NOD	Operator Fails to Disconnect Air Supply to CTT	1.0E-003
2.931E-014 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B2.4.4.8 Fault Trees

The fault tree for “Spurious Movement of the CTT in the Cask Unloading Room” is shown in Figures B2.4-14. Note that the transfer gate 13 in Figure B2.4-14 refers to the fault tree in Figure B2.4-4.



51A-7-CTT-SPURMOVE - Spurious Movement During Canister Transfer

Figure B2.4-14. Fault Tree for Spurious Movement of the CTT in the Cask Unloading Room

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 (*), if any, fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B3.1.1 BSC 2007. *Initial Handling Facility General Arrangement Ground Floor Plan*. 51A-P10-IH00-00102-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0017.

B3.1.2 BSC 2007. *Initial Handling Facility General Arrangement Second Floor Plan*. 51A-P10-IH00-00103-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0018.

B3.1.3 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.

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

Each of the IHF Cask Preparation Area (room number 1012) and Waste Package Loading Room (room number 1007) have a slide gate providing access to the Canister Transfer Area (room number 2005) and a shield door providing access to either the Cask Preparation Area (room number 1012) or the Waste Package Loadout Room (room number 1005) (Ref. B3.1.1) and (Ref. B3.1.2). 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 Waste Package Loadout Room and Cask Unloading Room.

B3.2.2 Operations Description

The Cask Unloading Room shield doors are opened to allow cask-carrying equipment, such as the site prime mover (SPM), to enter the room. Once equipment is positioned properly in the Cask 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 CTM to perform cask unloading operations. Waste package loading operations in the Waste Package Loading Room are analogous to cask unloading operations. The slide gate is opened to allow waste package loading access if the shield doors are closed. Once loading is complete and the slide gate is closed, the shield doors are opened by operator action to allow waste package 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 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 with an 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 Waste Package Loading Room/Cask Unloading Room and the Canister Transfer Area. 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. 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. B3.1.4 and Ref. B3.1.3).

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 dependencies.
3. Spatial dependence.

4. Human dependence.
5. Failures based on external events.

Table B3.3-1. Dependencies and Interactions Analysis

Structures, Systems, 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 sensor	—	—	—	—
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.
2. Inadvertent opening of the slide gate.
3. Shield door closes on conveyance.

In all cases a conservative mission time of one hour per canister transfer was used for each fault tree. The time required to transfer a canister from the CTT to a waste package, or traverse a shield door opening is significantly less than one hour.

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 a waste package 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 loading or unloading. 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 criterion for this failure scenario requires 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 Features and Requirements

Redundant hardware 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 the 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 Cask 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 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 the Shield Door

Basic Event	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CR---IELCCF--IEL-CCF	Common-cause failure of interlocks from slide gate	3	1.30E-06	0.00E+00	1.30E-06	1.00E+00
51A-CR---IEL00A—IEL-FOD	Interlock A from slide gate fails	3	2.75E-05	0.00E+00	2.75E-05	1.00E+00
51A-CR---IEL00B—IEL-FOD	Interlock B from slide gate fails	3	2.75E-05	0.00E+00	2.75E-05	1.00E+00
51A-CR---PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3	3.65E-07	0.00E+00	3.65E-07	1.00E+00
51A-CR-CASK-UNLOADING	Canister is exposed during mid-unloading	1	1.00E+00	1.00E+00	0.00E+00	1.00E+00
51A-OPDIREXPOSE1-HFI-NOD	Operator Mistakenly Opens Door	1	1.00E+00	1.00E+00	0.00E+00	1.00E+00

NOTE: ^a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B3.4.1.5.1 Human Failure Events

One 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 and the interlock must fail. The screening value used for this HFE has a probability of 1.0E+00 (Table E7-1).

B3.4.1.5.2 Common-Cause Failures

One common-cause failure 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 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.

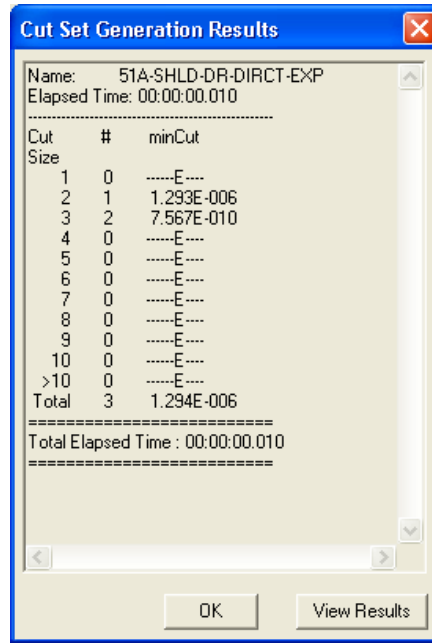
B3.4.1.6 Uncertainty and Cut Set Generation Results

Figure B3.4-1 contains the uncertainty results obtained from running the fault trees for “Inadvertent Opening of the Shield Door” while unloading cask, using a cutoff probability of 1E-15. Figure B3.4-2 provides the cut set generation results for the “Inadvertent Opening of the Shield Door” fault tree.

Uncertainty Results	
Name	51A-SHLD-DR-DIRECT-EXP
Random Seed	1234 Events 6
Sample Size	10000 Cut Sets 3
Point estimate	1.294E-006
Mean Value	1.295E-006
5th Percentile Value	1.269E-006
Median Value	1.294E-006
95th Percentile Value	1.322E-006
Minimum Sample Value	1.225E-006
Maximum Sample Value	2.069E-006
Standard Deviation	1.969E-008
Skewness	8.159E+000
Kurtosis	2.676E+002
Elapsed Time	00:00:00.550
OK	

Source: Original

Figure B3.4-1. Uncertainty Results for the Inadvertent Opening of the Shield Door Fault Tree



Source: Original

Figure B3.4-2. Cut Set Generation Results for the Inadvertent Opening of the Shield Door Fault Tree

B3.4.1.7 Cut Sets

Given the small size of this fault tree, all cut sets 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
51A-SHLD-DR-DIRECT-EXP	99.94	1.293E-006	51A-CR---IELCCF--IEL-CCF	Common-cause failure of interlocks from slide gate	1.3E-006
			51A-OPDIREXPOSE1-HFI-NOD	Operator mistakenly opens door	1.0E+000
	0.06	7.563E-010	51A-CR---IEL00A--IEL-FOD	Interlock A from slide gate fails	2.8E-005
			51A-CR---IEL00B--IEL-FOD	Interlock B from slide gate fails	2.8E-005
			51A-OPDIREXPOSE1-HFI-NOD	Operator mistakenly opens door	1.0E+000

Table B3.4-2. Cut sets for Inadvertent Opening of Shield Door (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
	0.00	4.719E-013	51A--CR-CASK-UNLOADING	Canister is exposed during mid-unloading	1.0E+000
			51A-CR---IELCCF--IEL-CCF	Common-cause failure of interlocks from slide gate	1.3E-006
			51A-CR-PLC001-PLC-SPO	Inadvertent signal sent due to PLC failure	3.6E-007
1.294E-006 = Total					

NOTE: Freq. = frequency; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.1.8 Fault Trees

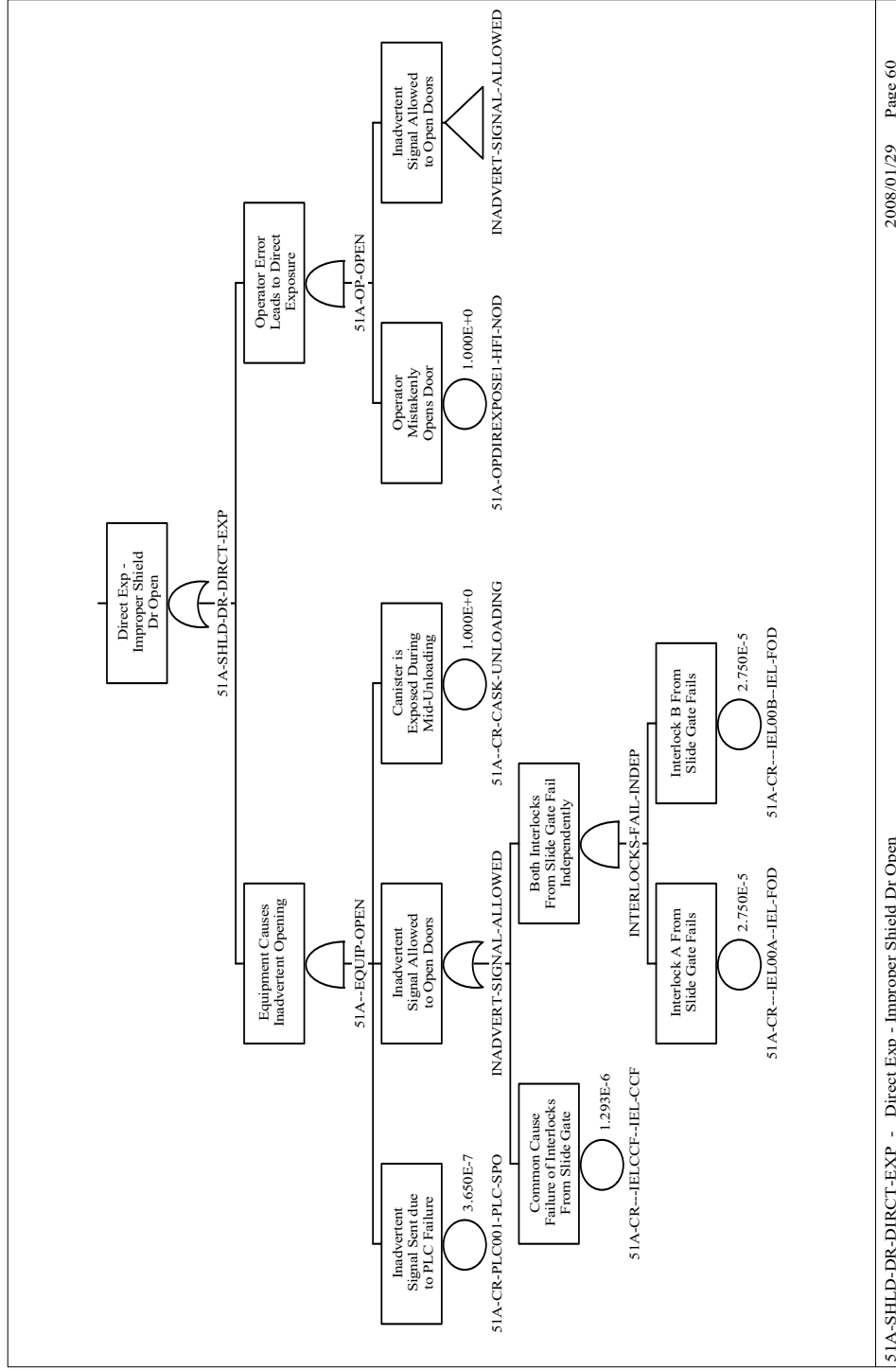


Figure B3.4-3. Fault Trees for Inadvertent Opening of the Shield Door

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 Area 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 the 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 Features and Requirement

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 “Slide Gate Inadvertently Opens 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.

The screening value of 1.0 is used for this event.

Table B3.4-3. Basic Event Probabilities for Inadvertent Opening of Slide Gate

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CR---IEL001--IEL-FOD	Skirt interlock failed	1	2.74E-05	2.74E-05	0.00E+00	1.00E+00
51A0-CR---PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3	3.65E-07	0.00E+00	3.65E-07	1.00E+00
51A-OPFAILRSTINT-HFI-NOM	Operator fails to reset interlock after maintenance	1	1.00E-02	1.00E-02	0.00E+00	1.00E+00

NOTE: ^a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.2.5.1 Human Failure Events

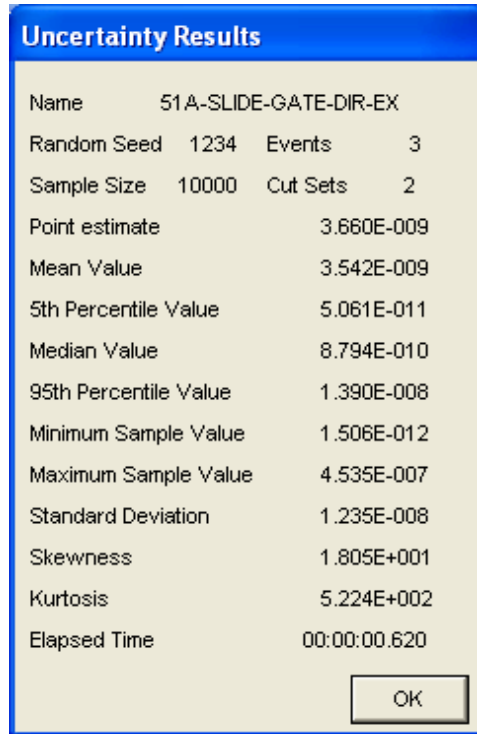
One HFE is modeled in the fault tree. This HFE is a combination of operator actions and interlock failures that can result in the slide gate being opened when the shield skirt is raised. The development of this event is presented in detail as part of the Human Reliability Analysis in Section 6.4 (Table 6.4-1) and Attachment E.

B3.4.2.5.2 Common-Cause Failures

No common-cause failures identified.

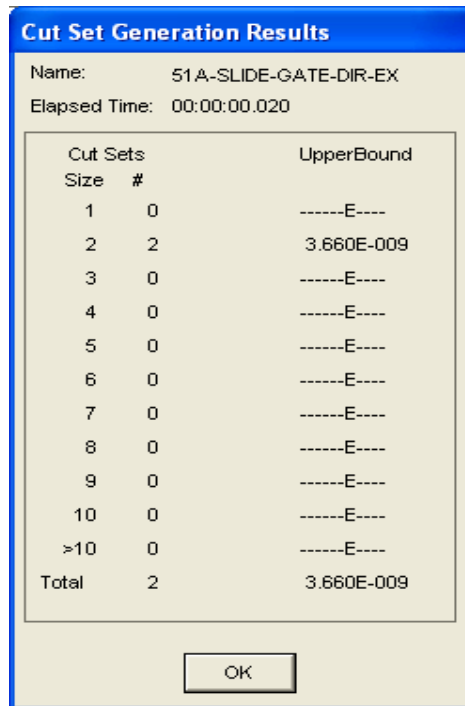
B3.4.2.6 Uncertainty and Cut Set Generation

Figure B3.4-4 contains the uncertainty results obtaining from running the fault tree for “Inadvertent Opening of Slide Gate” using a cutoff probability of 1E-15. Figure B3.4-5 provides the cut set generation results for “Inadvertent Opening of Slide Gate” fault tree.



Source: Original

Figure B3.4-4. Uncertainty Results for Inadvertent Opening of Slide Gate



Source: Original

Figure B3.4-5. Cut Set Generation Results for Inadvertent Opening of Slide Gate

B3.4.2.7 Cut Sets

Table B3.4-4 contains the cut sets for “Inadvertent Opening of Slide Gate”.

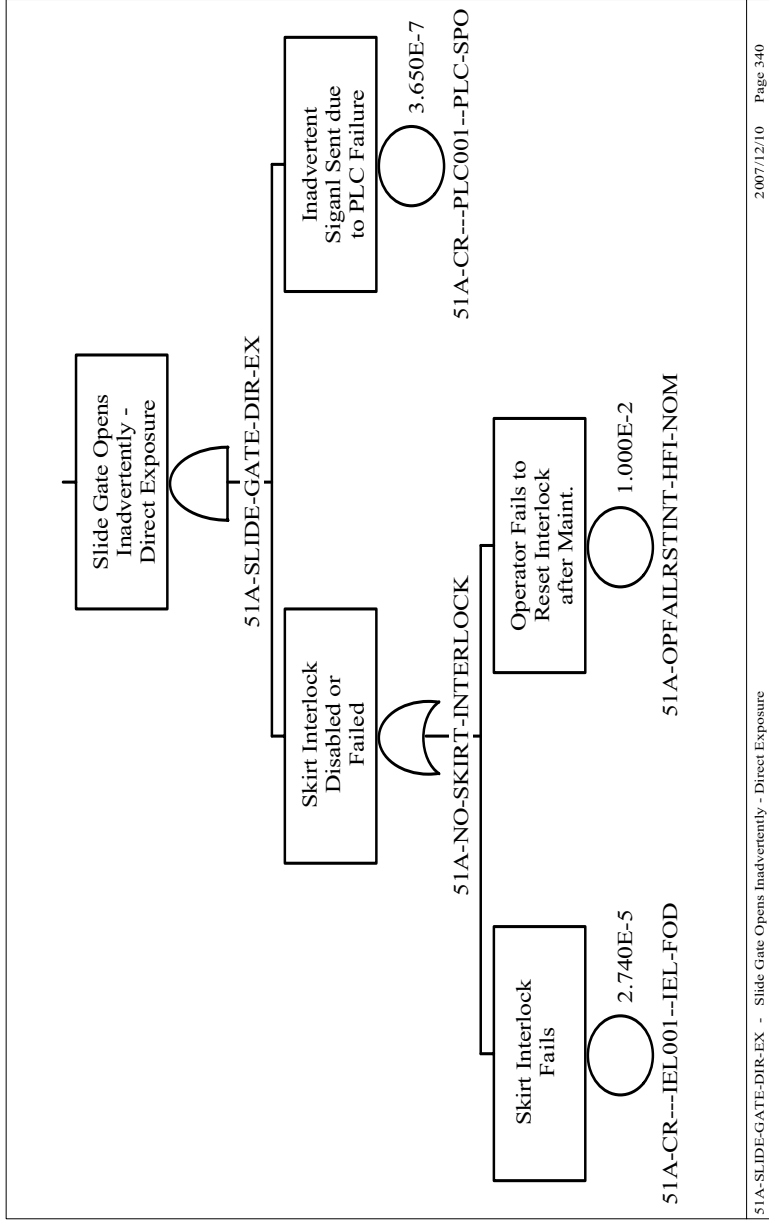
Table B3.4-4. Cut Sets for Inadvertent Opening of Slide Gate

Fault Tree	% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
51A-SLIDE-GATE-DIR-EXP	99.73	99.73	3.65E-09	51A-CR---PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3.65E-07
				51A-OPFAILRSTINT-HFI-NOM	Operator fails to reset interlock after maintenance	1.00E-02
	100.00	0.27	1.00E-11	51A-CR---IEL001--IEL-FOD	Skirt interlock failed	2.74E-05
				51A-CR---PLC001--PLC-SPO	Inadvertent signal sent due to PLC failure	3.65E-07

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 Waste Package Loadout Room/Cask Unloading Room are closed as casks or waste packages are transferred to/from the Cask Unloading Room/Waste Package Loadout Room, 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 the shield doors from causing damage to casks or waste packages 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 or 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.

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.

The screening value of 1.0 is used for this event.

Table B3.4-5. Basic Event Probabilities for Shield Door Closes on Conveyance

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	tau	Miss. Time ^a
51A-OPSDCLOSE001-HFI-NOD	Operator initiates shield door closure on CTT	1	1.00E+00	1.00E+00	0.00E+00		1.00E+00
51A-SD---PLC001--PLC-SPO	Spurious signal from PLC closes door	3	3.65E-07	0.00E+00	3.65E-07		1.00E+00
51A-SD---SRU001--SRU-FOH	Ultrasonic obstruction sensor fails	7	2.078E-002	0.00E+00	9.62E-05	4.38E+02	
51A-SD---TL000---TL--CCF	Common-cause failure of over torque sensors	3	6.801E-04	1.00E+00	3.78E-06		3.60E+02
51A-SD---TL001---TL--FOH	Motor #1 over torque sensor fails	3	1.435E-02	0.00E+00	8.05E-05		3.60E+02
51A-SD---TL002---TL--FOH	Motor #1 over torque sensor fails	3	1.435E-02	0.00E+00	8.05E-05		3.60E+02

NOTE: ^a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; CTT = cask transfer trolley; Fail. = failure; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.3.5.1 Human Failure Events

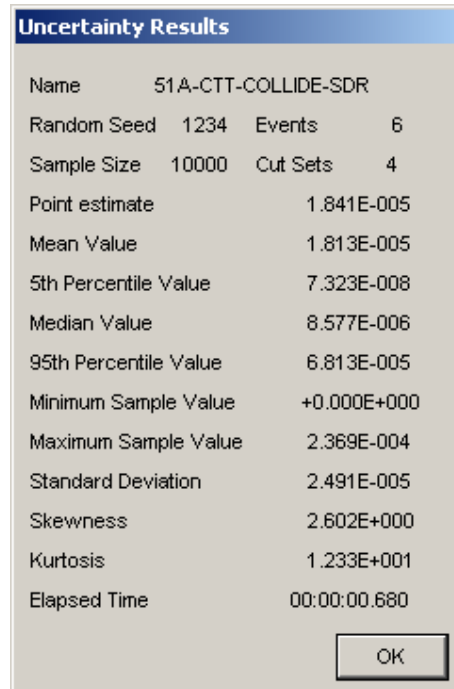
One human failure event (51A-OPSDCLOSE001-HFI-NOD) is modeled in the fault tree as an operator attempting to close the shield doors while a conveyance is between the doors. The screening value used for this HFE has a probability of 1.0E+00. The development of this event is presented in detail as part of the Human Reliability Analysis in Attachment E.

B3.4.3.5.2 Common-Cause Failures

One common-cause failure, failure of the shield door over torque sensors, is considered. This common-cause failure allows the shield doors to continue to attempt to close on an obstruction is encountered, in this case the conveyance.

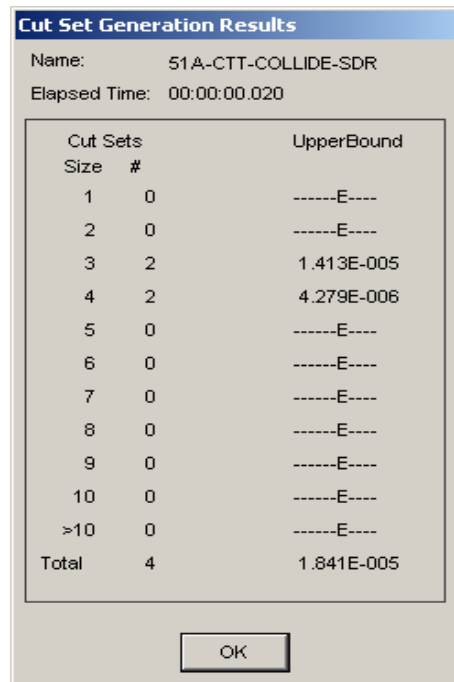
B3.4.3.6 Uncertainty and Cut Set Generation

Figure B3.4-7 contains the uncertainty results obtained from running the fault tree “Shield Door Closes on Conveyance” using a 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 Shield Door Closes on Conveyance Fault Tree



Source: Original

Figure B3.4-8. Cut Set Generation Results for 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”.

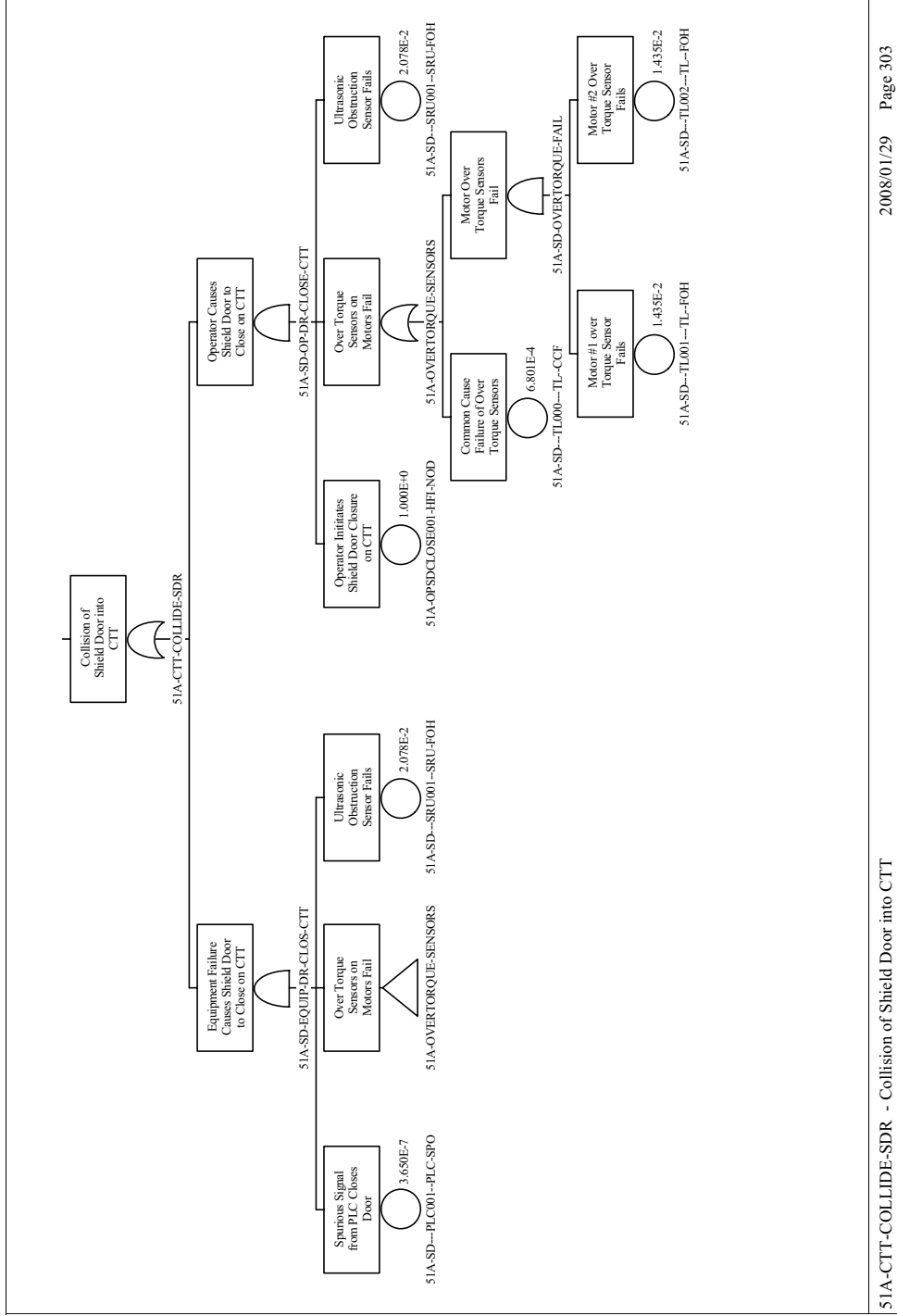
Table B3.4-6. Cut Sets for Shield Door Closes on Conveyance

Fault Tree	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
51A-CTT-COLLIDE SDR	76.76	1.41E-05	51A-OPSDCLOSE001-HFI-NOD	Operator Initiates Shield Door Closure on CTT	1.00E+00
			51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.10E-02
			51A-SD---TL000---TL--CCF	Common-Cause Failure of Over Torque Sensors	6.80E-04
	23.24	4.28E-06	51A-OPSDCLOSE001-HFI-NOD	Operator Initiates Shield Door Closure on CTT	1.00E+00
			51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.10E-02
			51A-SD---TL001---TL--FOH	Motor #1 over Torque Sensor Fails	1.40E-02
	0	5.16E-12	51A-SD---TL002---TL--FOH	Motor #2 Over Torque Sensor Fails	1.40E-02
			51A-SD---PLC001--PLC-SPO	Spurious Signal from PLC Closes Door	3.60E-07
			51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.10E-02
	0	1.56E-12	51A-SD---TL000---TL--CCF	Common-Cause Failure of Over Torque Sensors	6.80E-04
			51A-SD---PLC001--PLC-SPO	Spurious Signal from PLC Closes Door	3.60E-07
			51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	2.10E-02
			51A-SD---TL001---TL--FOH	Motor #1 over Torque Sensor Fails	1.40E-02
			51A-SD---TL002---TL--FOH	Motor #2 Over Torque Sensor Fails	1.40E-02
		1.84E-05 = Total			

NOTE: CTT = cask transfer trolley; Fail. = failure; PLC = programmable logic controller; Prob. = probability.

Source: Original

B3.4.3.8 Fault Trees



2008/01/29 Page 303

51A-CTT-COLLIDE-SDR - Collision of Shield Door into CTT

Source: Original

Figure B3.4-9. Fault Trees for Shield Door Closes on Conveyance

B4 IHF CANISTER TRANSFER MACHINE FAULT TREE ANALYSIS

B4.1 REFERENCES

Design Inputs

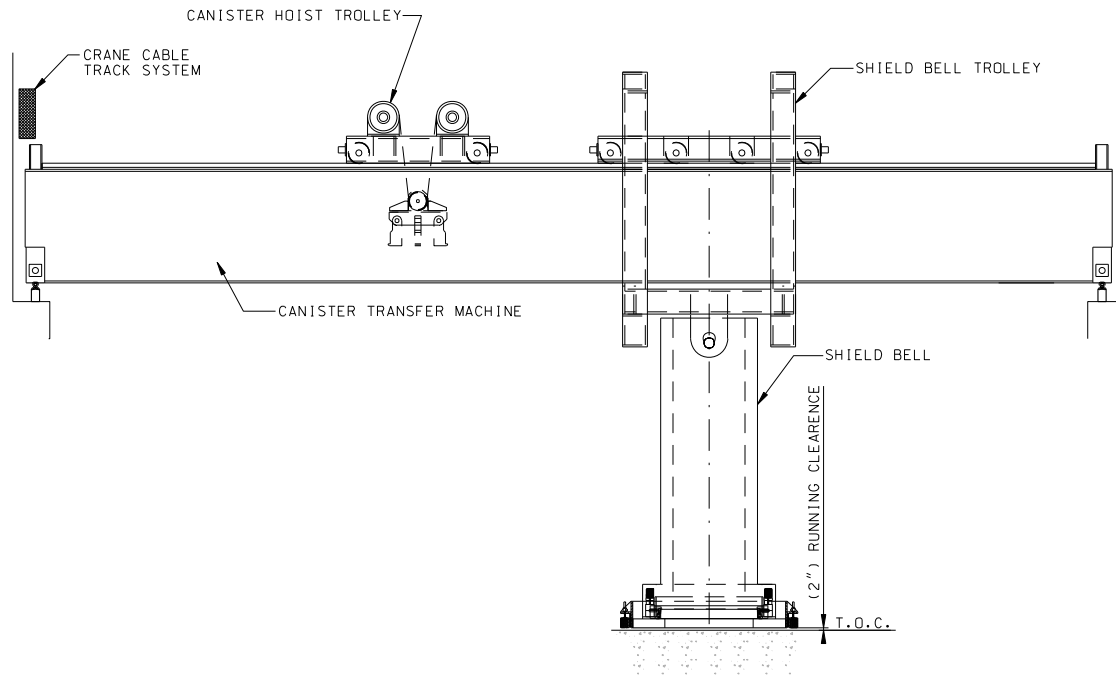
The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *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.

- B4.1.1 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. ISBN: 0-7918-2923-1. TIC: 257672.
- 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 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. *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.
- B4.1.8 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.

B4.2 CANISTER TRANSFER MACHINE DESCRIPTION

The canister transfer machine (CTM) operates in the Canister Transfer Area of the IHF. Its function is to transfer waste canisters from a cask on a canister transfer trolley (CTT) or from an aging overpack on a site transporter to another cask or overpack, or to a waste package supported by a waste package transfer trolley (WPTT). The ports in the floor of the Canister Transfer Area provide access to the Cask Unloading Room and Waste Package Loadout 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 6 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.



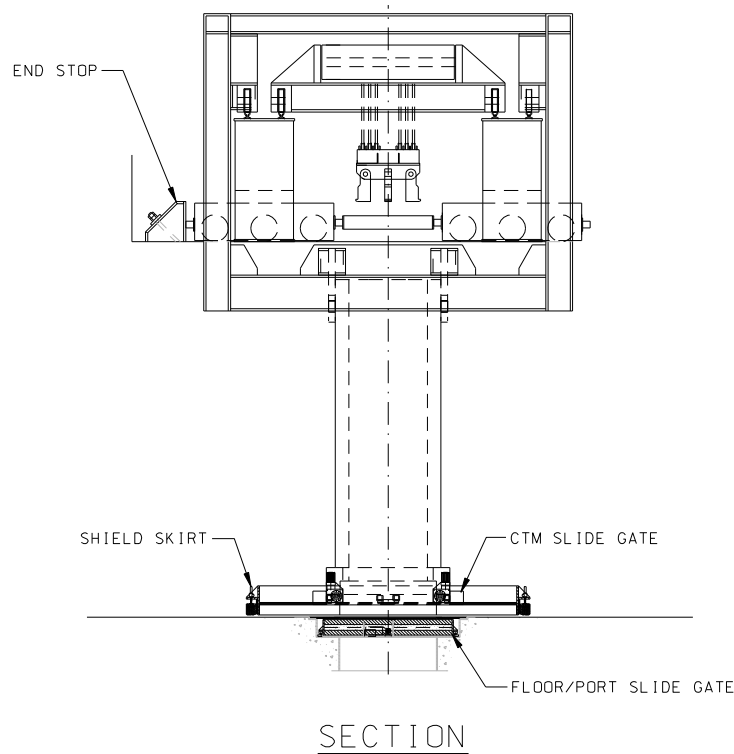
Source: Modified from (Ref B4.1.8)

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.



NOTE: CTM = canister transfer machine.

Source: Ref B4.1.8

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. B4.1.7. 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 programmable logic controllers (PLCs), the operation of these non-important to safety (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 disengaged
- 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.

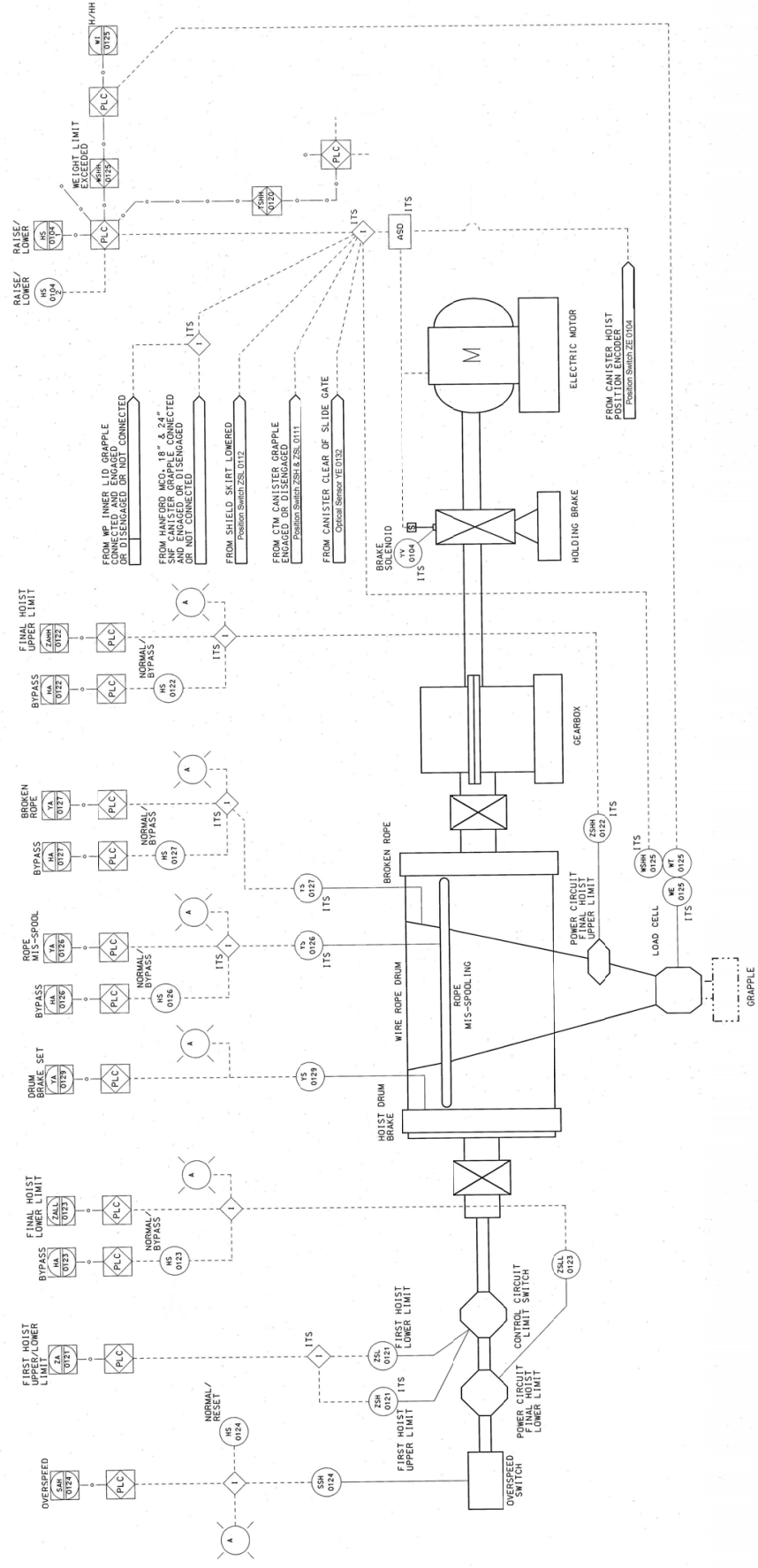
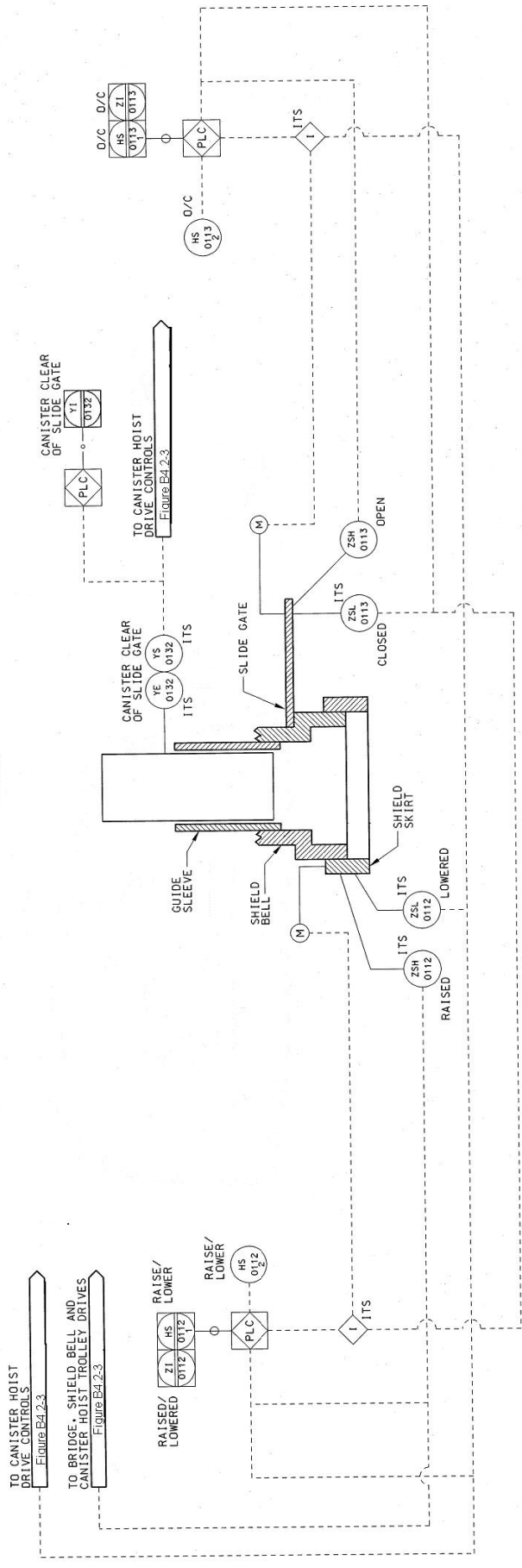


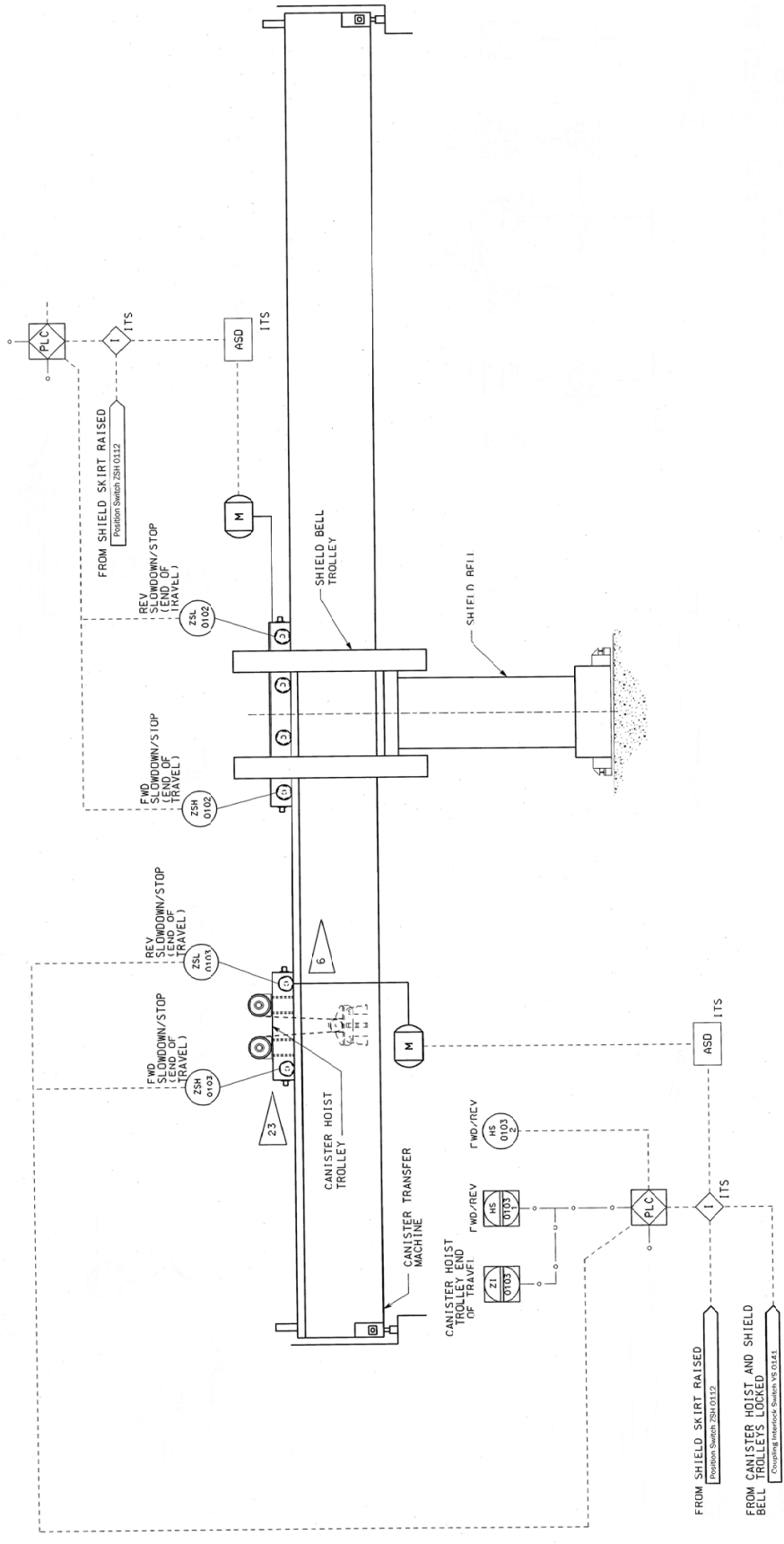
Figure B4.2-3. Canister Hoist Instrumentation

Source: Modified from Ref. B4.1.6



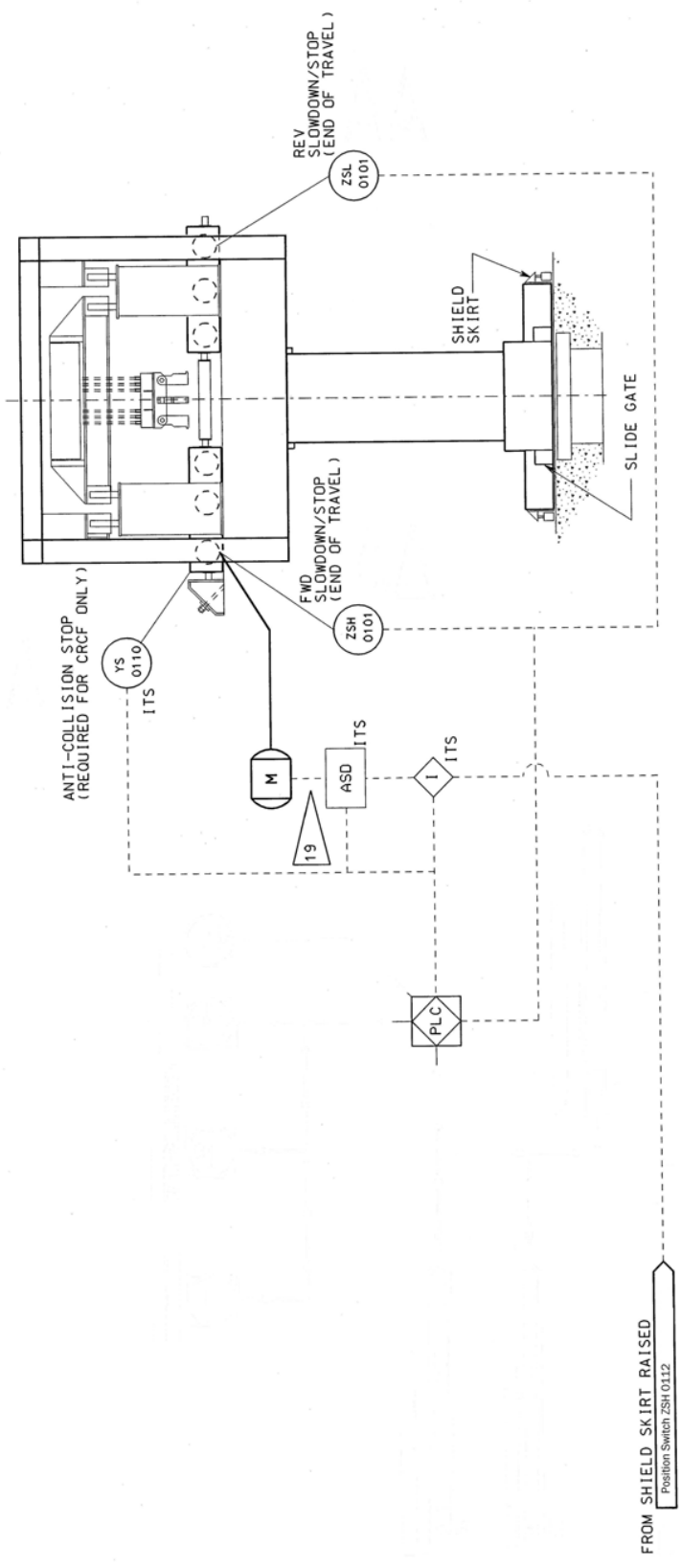
Source: Modified from Ref B4.1.6

Figure B4.2.4. Shield Skirt and Slide Gate Instrumentation



Source: Modified from Ref. B4.1.3.

Figure B4.2-5. Trolley Instrumentation



Source: Modified from Ref. B4.1.3.

Figure B4.2-6. Bridge Instrumentation

B4.2.1 CTM Bridge

The bridge design meets the requirements of ASME NOG-1-2004 (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 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.

B4.2.2 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.

B4.2.3 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 does not allow the grapple to disengage when a load is suspended from the canister grapple.

Additional grapples are required for handling high-level radioactive waste (HLW) canisters. The additional canister grapples are manually attached to the CTM canister grapple and limit switches ensure that a proper and complete connection is made.

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).

B4.2.4 ITS CTM Normal Operations

A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to a waste package. For this operation a loaded transportation cask, secured in the cask transfer trolley, is positioned below the transfer port in the Cask Unloading Room. The cask lid is in place but unbolted. Similarly, an empty waste package secured by the waste package

transfer trolley is positioned under the adjacent transfer port in the Waste Package Loading Room.

The CTM is moved to a position over 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. For HLW casks, 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 Canister Transfer Area. 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 waste package 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 waste package and the grapple is disengaged from the canister.

For HLW waste packages, a waste package inner lid (shield plug) is also placed using the CTM after the waste package is loaded.

The CTM canister grapple is used for handling naval canisters. Other grapples are needed to access the smaller diameter HLW canisters. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Area floor. The CTM hoist is lowered through the shield bell until the CTM grapple is accessible in the room below for canister grapple attachment.

A transportation cask containing one or more HLW canisters is positioned in the Cask Unloading Room. A waste package shield plug (inner lid) with a spreader ring is placed in a lid staging area. An empty waste package is positioned in the loading station of the Waste Package Positioning Room prior to starting the canister transfer operation.

The CTM machine with the correct grapple is used to transfer a HLW canister from the transportation cask to the waste package. After placement of all canisters in the waste package the last step is to place a shield plug in the waste package. This completes a typical loading operation for a HLW type waste package.

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

B4.2.5 ITS CTM Off-Normal 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.

B4.2.6 ITS CTM Testing and Maintenance

The CTM is operated, if not on a continual basis, regularly (e.g., once a shift). Most component functionality is verified during CTM operation. For those components that are not exercised during routine operations (e.g., bridge and trolley end-of-travel end stops, hoist upper limit position switches) routine verification of functionality is required.

B4.2.7 Testing and Maintenance

B4.2.7.1 Requirements

Testing of components not exercised during routine operation of the CTM is tested annually at a minimum.

B4.2.7.2 Design Feature

Normal maintenance is performed in accordance with manufacturer's recommendations; maintenance is performed only when the CTM is not in use.

B4.2.8 Fault Trees

B4.2.8.1 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 one hour. Most lifts/transfers require less than one hour. When a transfer consists of several separate activities (e.g., auxiliary equipment movements, lifts, and transfers) each of these activities require less than an hour, but all have been assigned a one-hour mission time.

B4.2.8.2 Design Features

Common-cause failures have been included for three events. Two 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) 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 the 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 dependencies
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	—	—	—	—
Shield 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. Canister drop from below the canister design-limit drop height. 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 Area ports to the loading/unloading areas that can occur before the bell slide gate is closed).

2. Canister drop from above the canister design-limit drop height
3. Drop of object onto 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 Drop 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

The success criterion for the CTM is the prevention of a canister drop from any cause, during the lift, lateral movement, and lower 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, stops 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 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 canister transfer machine, 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 Area, 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 canister transfer machine. The CTM has several trolleys that govern lateral movements, one controls the movement of the CTM bridge, 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 locked together during transfer operations). Spurious actuation of a trolley motor after the grapple is attached to a canister and before the load is lifted above the Canister Transfer Room 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 canister transfer machine, 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 human failure event is a screening value of 0.001, i.e., it is a conservative estimate based upon predetermined characteristics of the human failure event (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 “Canister Drop from Below the Canister Design-Limit Drop Height” fault trees. Included are the HFEs and the common-cause failure events identified in those two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is 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 canister transfer machine. 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 B4.4-1. Basic Event Probability for the Canister Drop from Below Canister Drop Height Limit Fault Tree

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-#ZSH0112-ZS-FOH	Shield Skirt Position Switch Fails	3	5.784E-05	0.000E+00	7.230E-06	8.000E+00
51A-CTM--CBL0001-WNE-BRK	Wire rope breaks	1	2.000E-06	2.000E-06	0.000E+00	0.000E+00
51A-CTM--CBL0002-WNE-BRK	Wire rope breaks	1	2.000E-06	2.000E-06	0.000E+00	0.000E+00
51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	1	9.400E-08	9.400E-08	9.400E-08	0.000E+00
51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	1	4.000E-08	4.000E-08	0.000E+00	0.000E+00
51A-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
51A-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure to Hold	3	2.011E-04	0.000E+00	8.380E-06	2.400E+01
51A-CTM--EQL-SHV-BLK-FOD	Equalizer sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--HOLDBRK-BRK-FOD	Brake Failure on Demand	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3	3.520E-05	0.000E+00	4.400E-06	8.000E+00
51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--MISSPOOL-DM-MSP	CTM Mis-spool event	3	6.860E-07	0.000E+00	6.860E-07	1.000E+00
51A-CTM--OVERSP--ZS-FOD	Hoist Motor Speed Limit Switch Fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--PORTGT1-MOE-SPO	Spurious port gate 1 motor operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM--PORTGT1-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM--PORTGT2-MOE-SPO	Spurious port gate 2 motor operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM--TROLLY-MOE-SPO	Trolley Motor Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM--UPPERBL-BLK-FOD	Upper sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--WTO125--SRP-FOD	Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	0.000E+00	0.000E+00
51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
51A-CTM-DRTRN-CT-FOD	CTM Drive Train Protection and Fail Det. Ctl Failure	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
51A-CTM-DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Fails on Demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00

Table B4.4-1. Basic Event Probability for the Canister Drop from Below Canister Drop Height Limit Fault Tree (Continued)

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM-HOISTMT-MOE-FTR	CTM hoist Motor (Electric) Fails to Run	3	6.500E-06	0.000E+00	6.500E-06	1.000E+00
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Ctl Interlock Fails on Demand	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
51A-CTM-PLC0101-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-PLC01021-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operations	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-PLC0103-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-SLIDEGT1-IEL-FOD	CTM Slide Gate Interlock Fails	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
51A-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	0.000E+00	0.000E+00
51A-CTM-WT0125-SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	0.000E+00	0.000E+00
51A-CTM-WTSW125-ZS-FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM-YS01129-ZS-FOD	CTM Drum Brake Ctl Circuit Limit Switch 1129 Fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
51A-LOSS-OFFSITE-PWR	Loss of off site power	1	2.990E-03	2.990E-03	0.000E+00	0.000E+00
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	1	2.000E-04	2.000E-04	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; CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

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 the operator actions and an 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
51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close

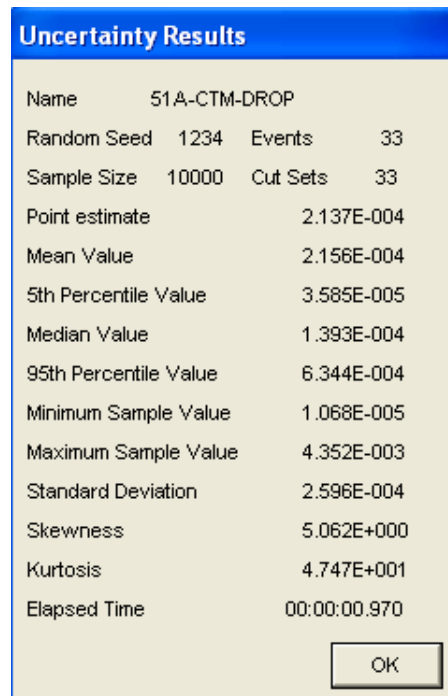
Source: Original

B4.4.1.5.2 Common-Cause Failures

One common-cause event was considered in the evaluation of this top event. The common-cause failure considered is the common-cause failure of the hoist cables.

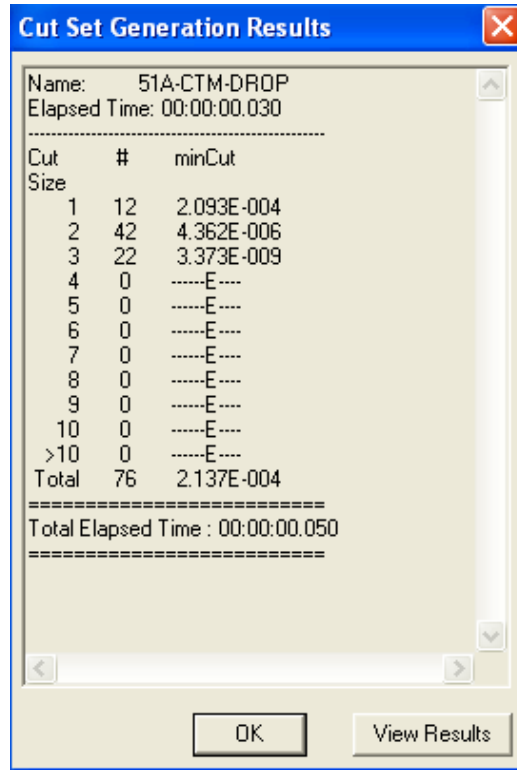
B4.4.1.6 Uncertainty and Cut Set Generation

Figure B4.4-1 contains the uncertainty results obtaining from running the fault trees for the “Canister Drop from Below the Canister Design-Limit Drop Height” using a cutoff of 1E-15. Figure B4.4-2 provides the cut set generation results for “Canister Drop from Below the Canister Design-Limit Drop Height”.



Source: Original

Figure B4.4-1. Uncertainty Results of the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the Canister Drop from Below the Canister Design-Limit Drop Height Fault Tree

B4.4.1.7 Cut Sets

Table B4.4-3 contains the top 20 cut sets for the “Canister Drop from Below the Canister Design-Limit Drop Height”.

Table B4.4-3. Dominant Cut Sets for Canister Drop from Below the Canister Design-Limit Drop Height

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
93.60	93.60	2.000E-04	51A-OPCTMDROP002-HFI-COD	Operator causes drop of less than design height limit	2.000E-04
95.47	1.87	3.990E-06	51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
96.07	0.60	1.280E-06	51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	1.280E-06
96.67	0.60	1.280E-06	51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	1.280E-06
97.21	0.54	1.150E-06	51A-CTM--EQL-SHV-BLK-FOD	equalizer sheaves structural failure	1.150E-06
97.75	0.54	1.150E-06	51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1.150E-06

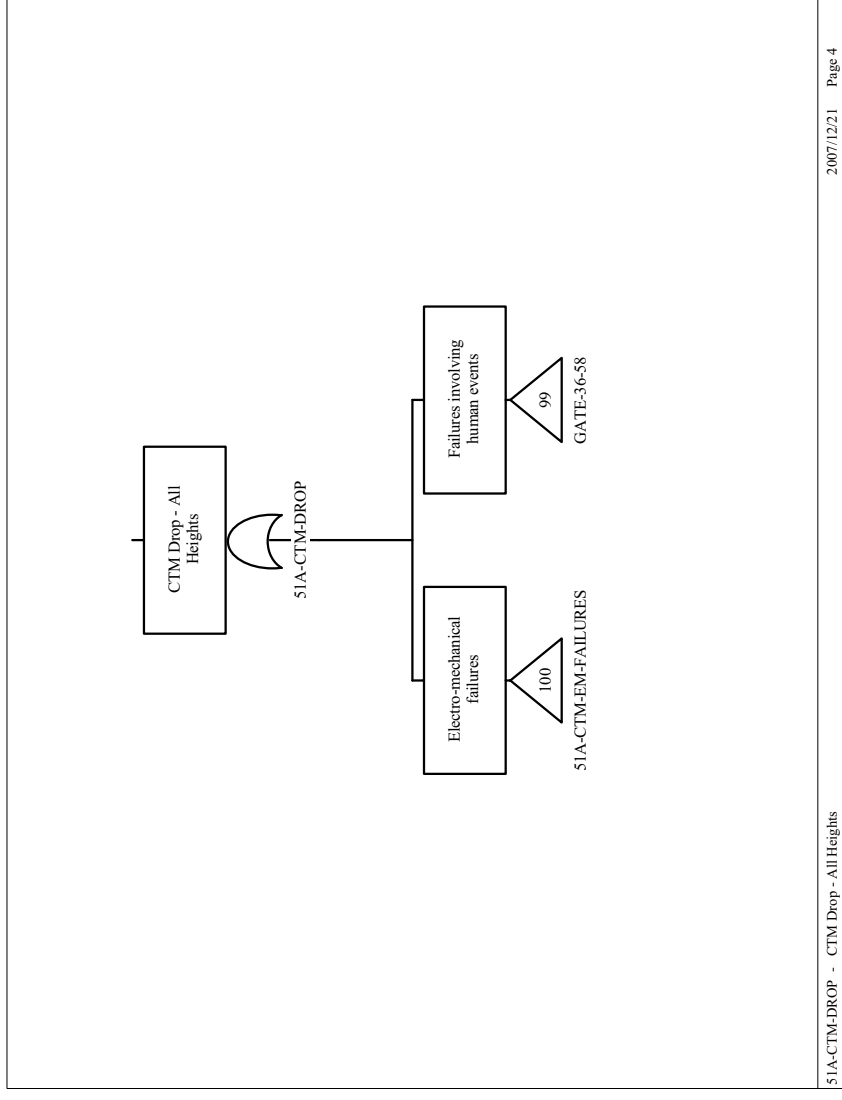
Table B4.4-3 Dominant Cut Sets for the CTM Canister Drop (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.29	0.54	1.150E-06	51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1.150E-06
98.83	0.54	1.150E-06	51A-CTM--UPPERBL-BLK-FOD	upper sheaves structural failure	1.150E-06
99.15	0.32	6.740E-07	51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	6.740E-07
99.47	0.32	6.740E-07	51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	6.740E-07
99.79	0.32	6.740E-07	51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	6.740E-07
99.93	0.14	2.930E-07	51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	2.930E-04
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.97	0.04	9.400E-08	51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.400E-08
99.99	0.02	4.000E-08	51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	4.000E-08
100.00	0.02	3.520E-08	51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3.520E-05
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
100.00	0.01	2.750E-08	51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Ctl Interlock Fails on Demand	2.750E-05
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
100.00	0.00	2.689E-09	51A-CTM--PORTGT2-MOE-SPO	spurious port gate 2 motor operation	6.740E-07
			51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
100.00	0.00	2.689E-09	51A-CTM--TROLLY-MOE-SPO	Trolley Motor Spurious Operation	6.740E-07
			51A-CTM-WT0125-SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	3.990E-03
100.00	0.00	2.689E-09	51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
			51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) spurious Operation	6.740E-07
100.00	0.00	2.689E-09	51A-CTM--PORTGT1-MOE-SPO	spurious port gate1 motor operation	6.740E-07
			51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03

NOTE: CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller; Prob. = probability.

Source: Original

B4.4.1.8 Fault Trees

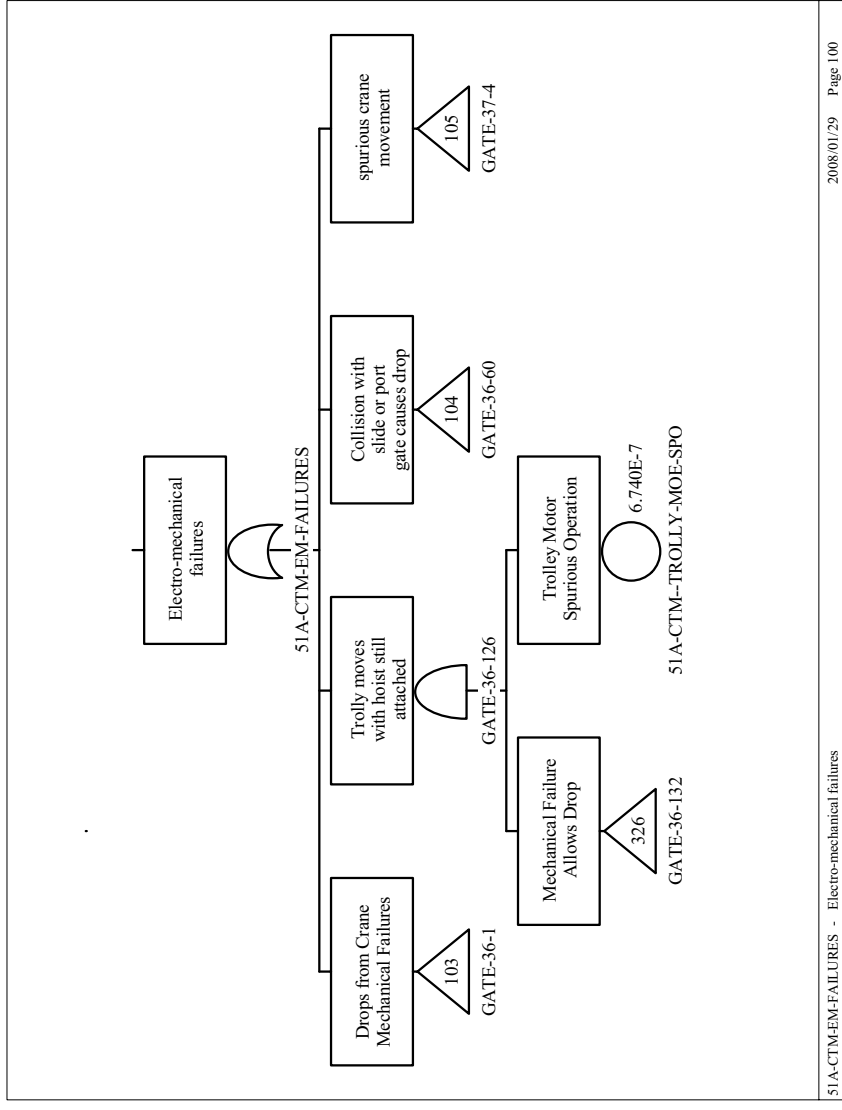


Source: Original

Figure B4.4-3. CTM Drop Fault Tree Sheet 1

B4-22

March 2008



2008/01/29 Page 100

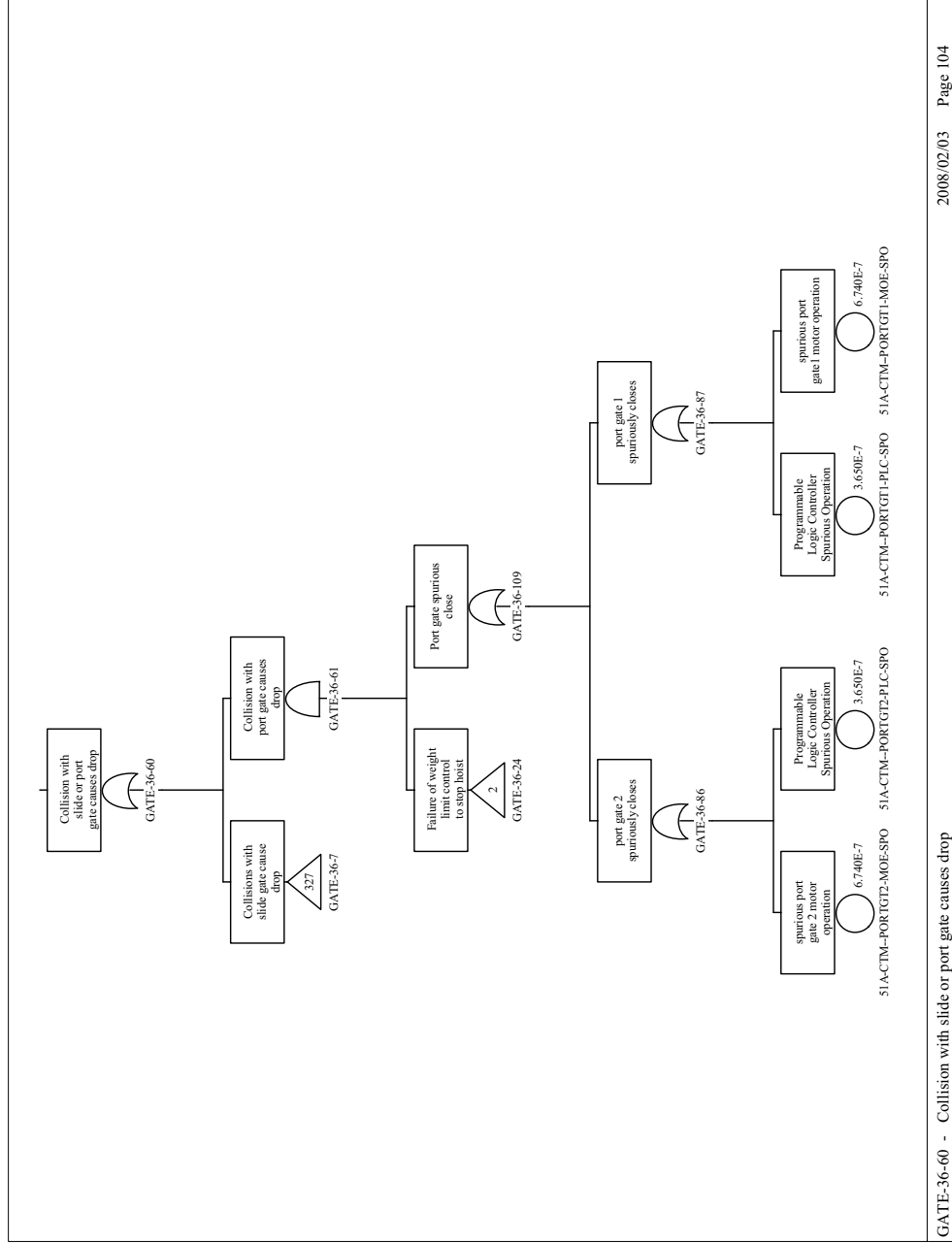
51A-CTM-EM-FAILURES - Electro-mechanical failures

Source: Original

Figure B4.4-4. CTM Drop Fault Tree Sheet 2

B4-23

March 2008

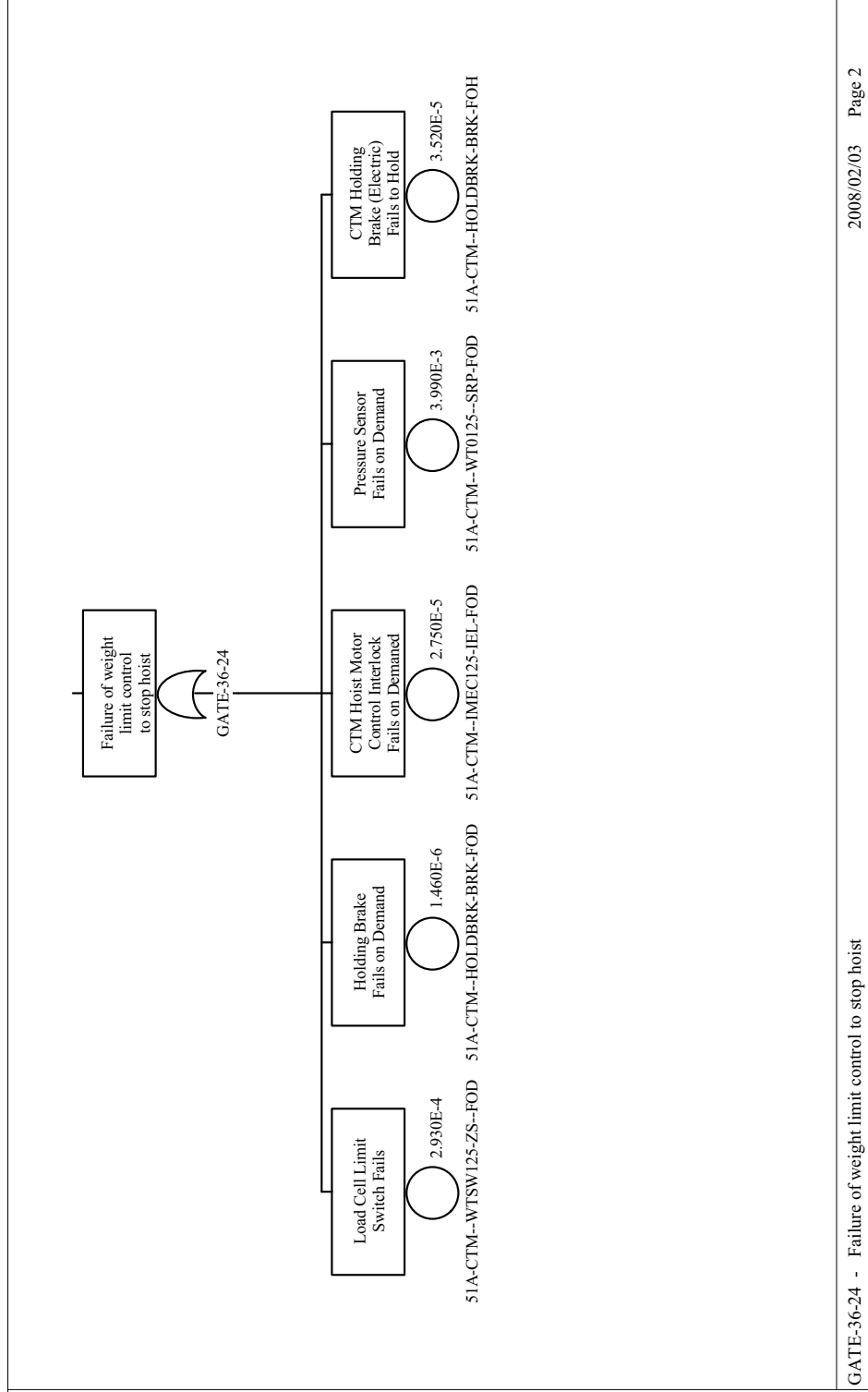


Source: Original

Figure B4.4-5 CTM Drop Fault Tree Sheet 3

B4-24

March 2008



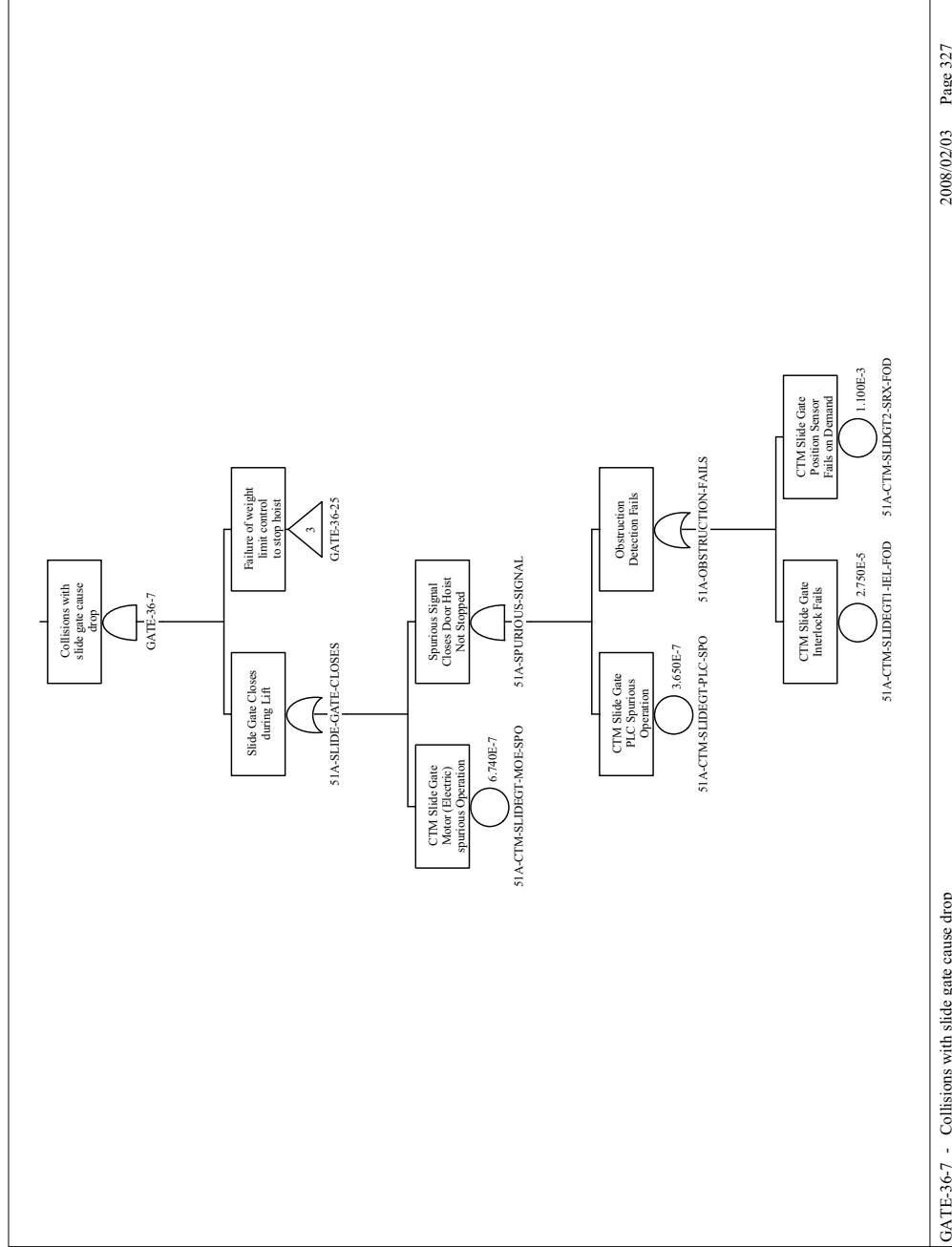
GATE-36-24 - Failure of weight limit control to stop hoist

Source: Original

Figure B4.4.6. CTM Drop Fault Tree Sheet 4

B4-25

March 2008



2008/02/03 Page 327

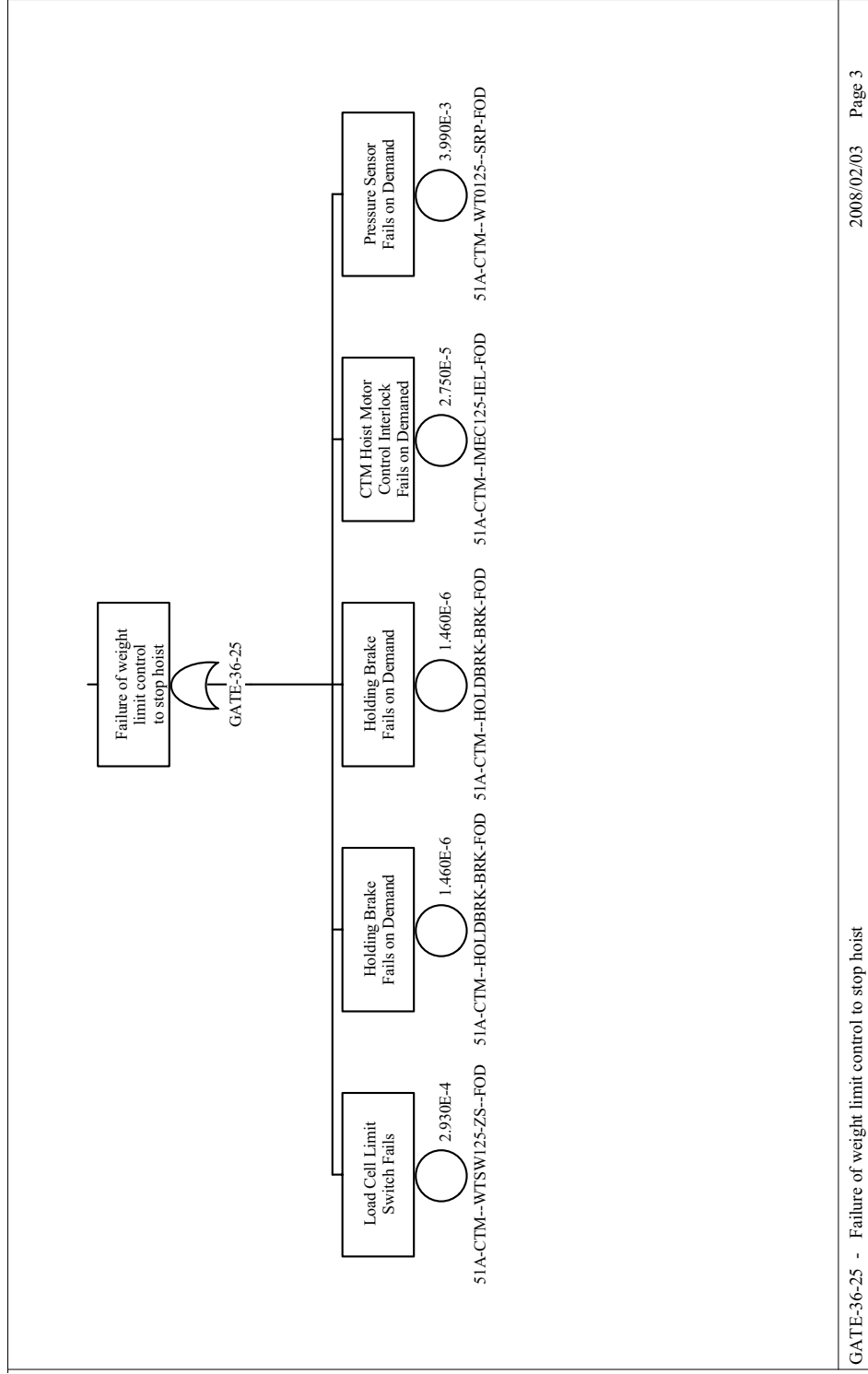
GATE-36-7 - Collisions with slide gate cause drop

Source: Original

Figure B4.4-7. CTM Drop Fault Tree Sheet 5

B4-26

March 2008



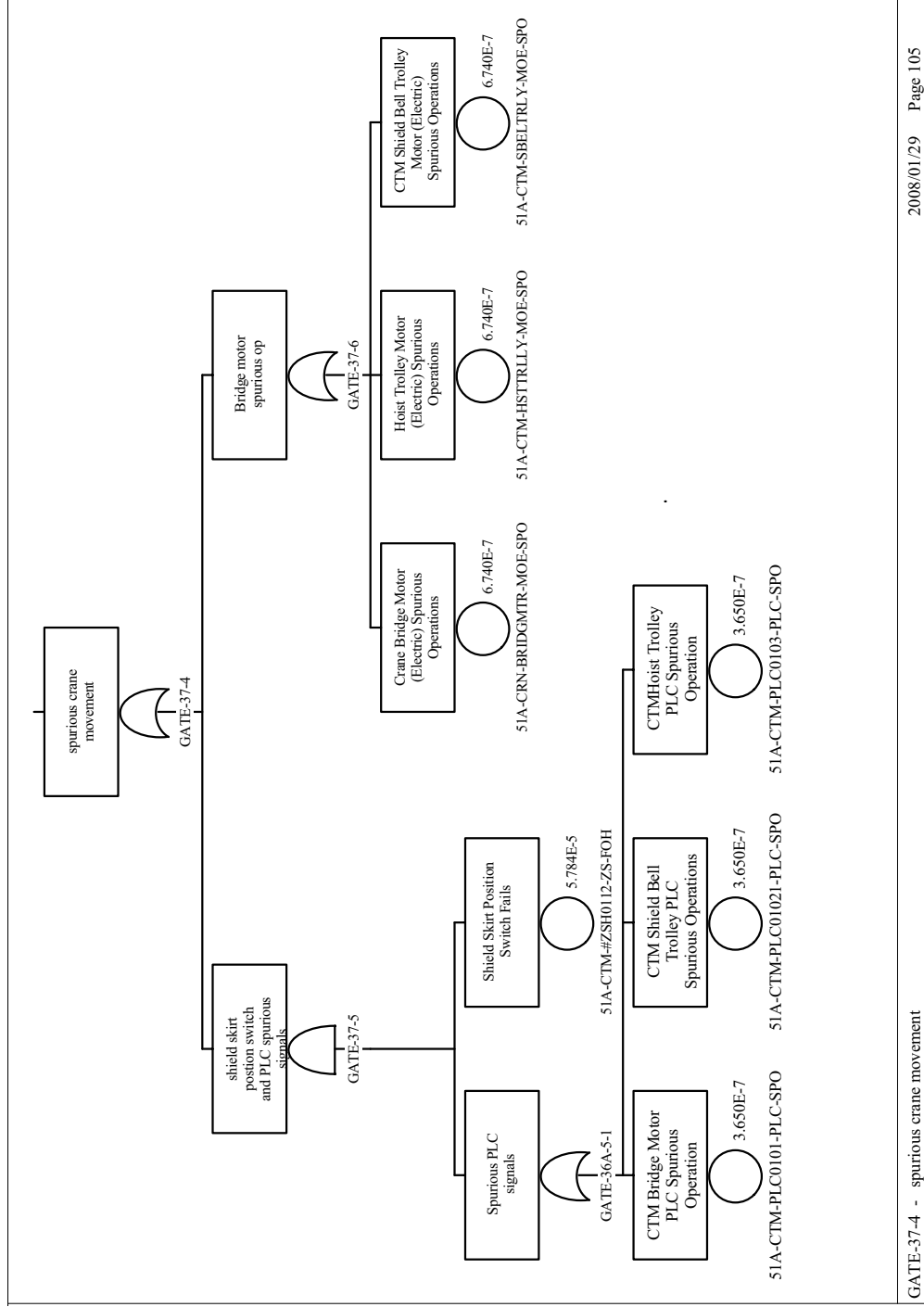
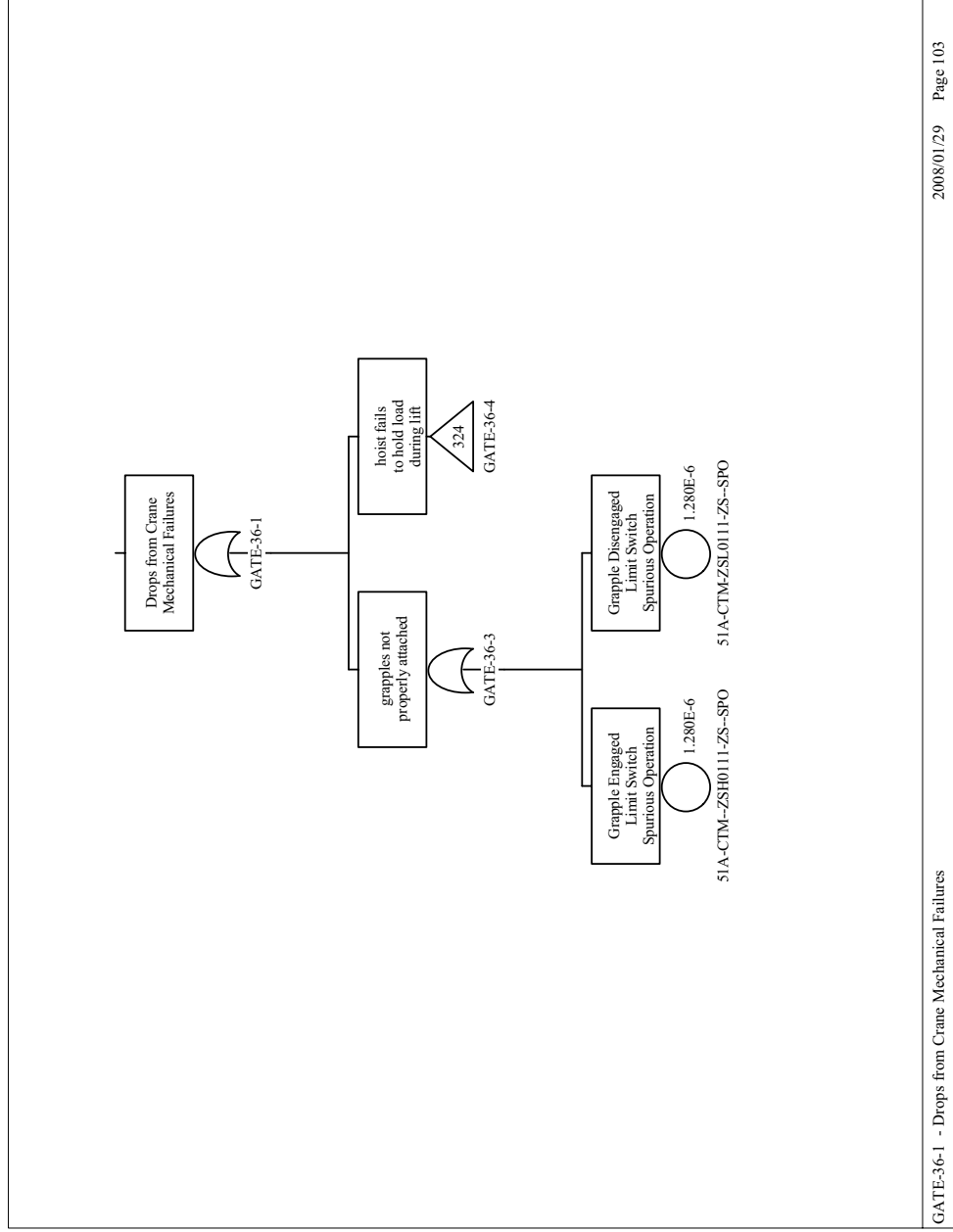


Figure B4.4-9. CTM Drop Fault Tree Sheet 7



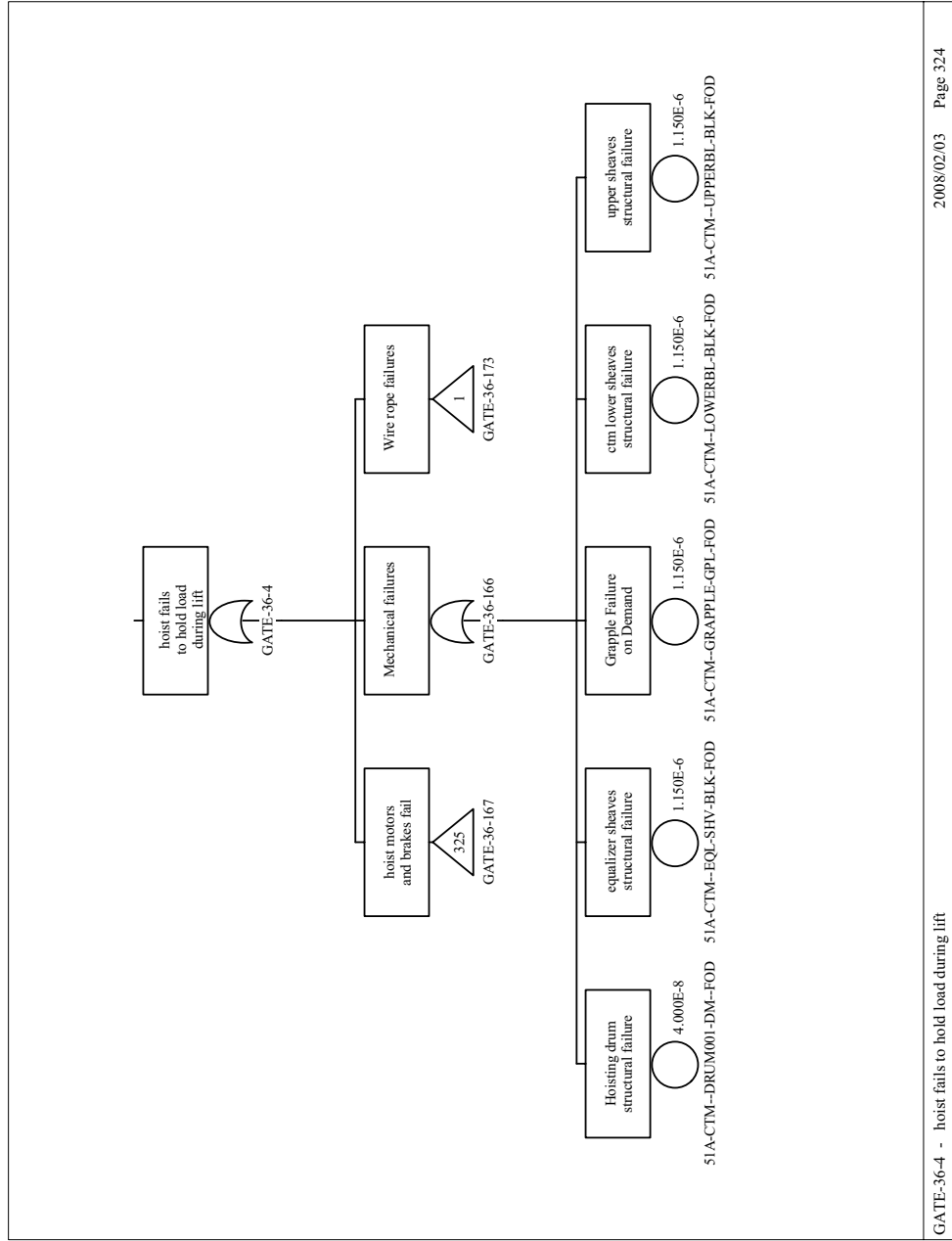
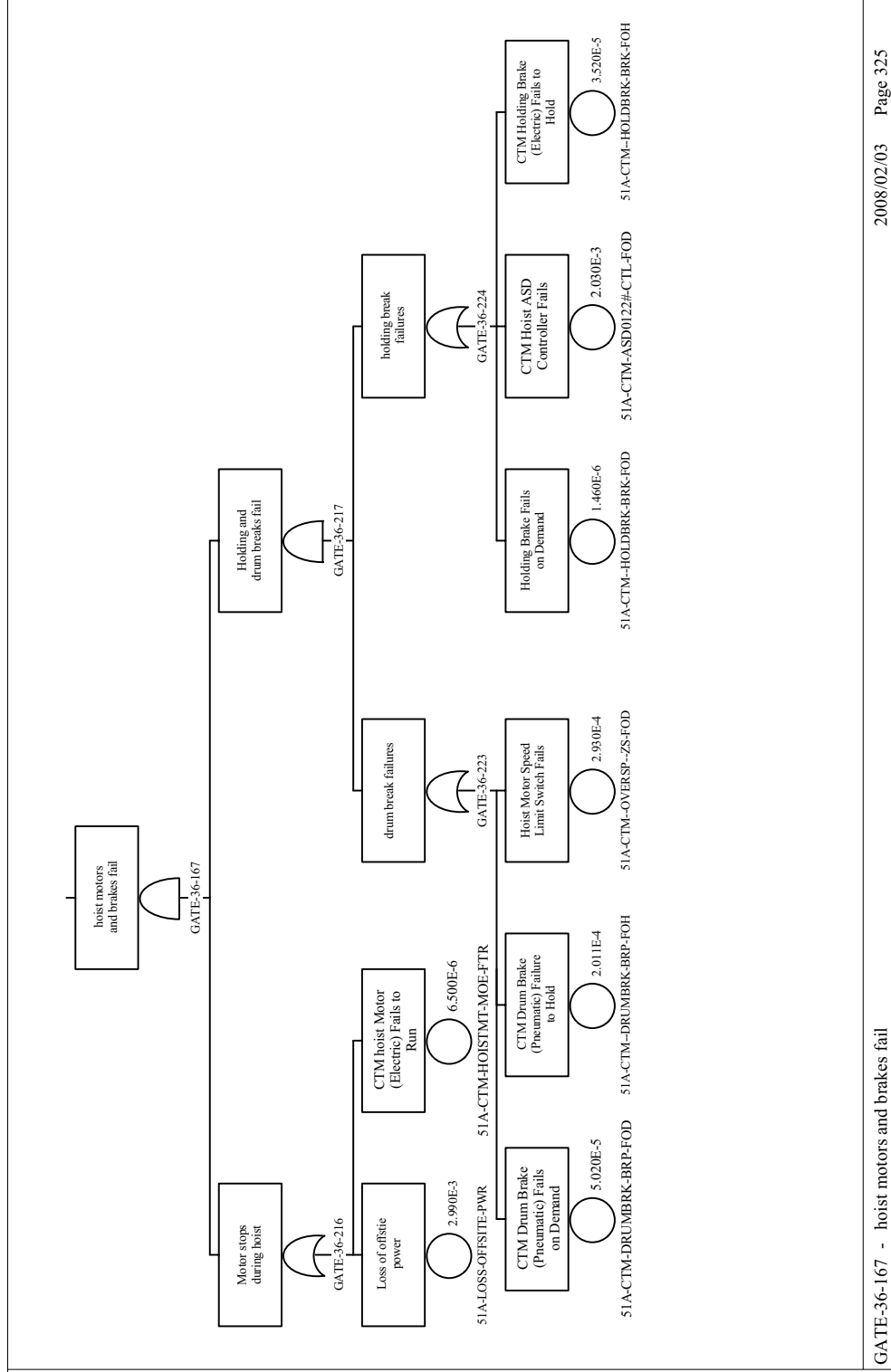


Figure B4.4-11. CTM Drop Fault Tree Sheet 9



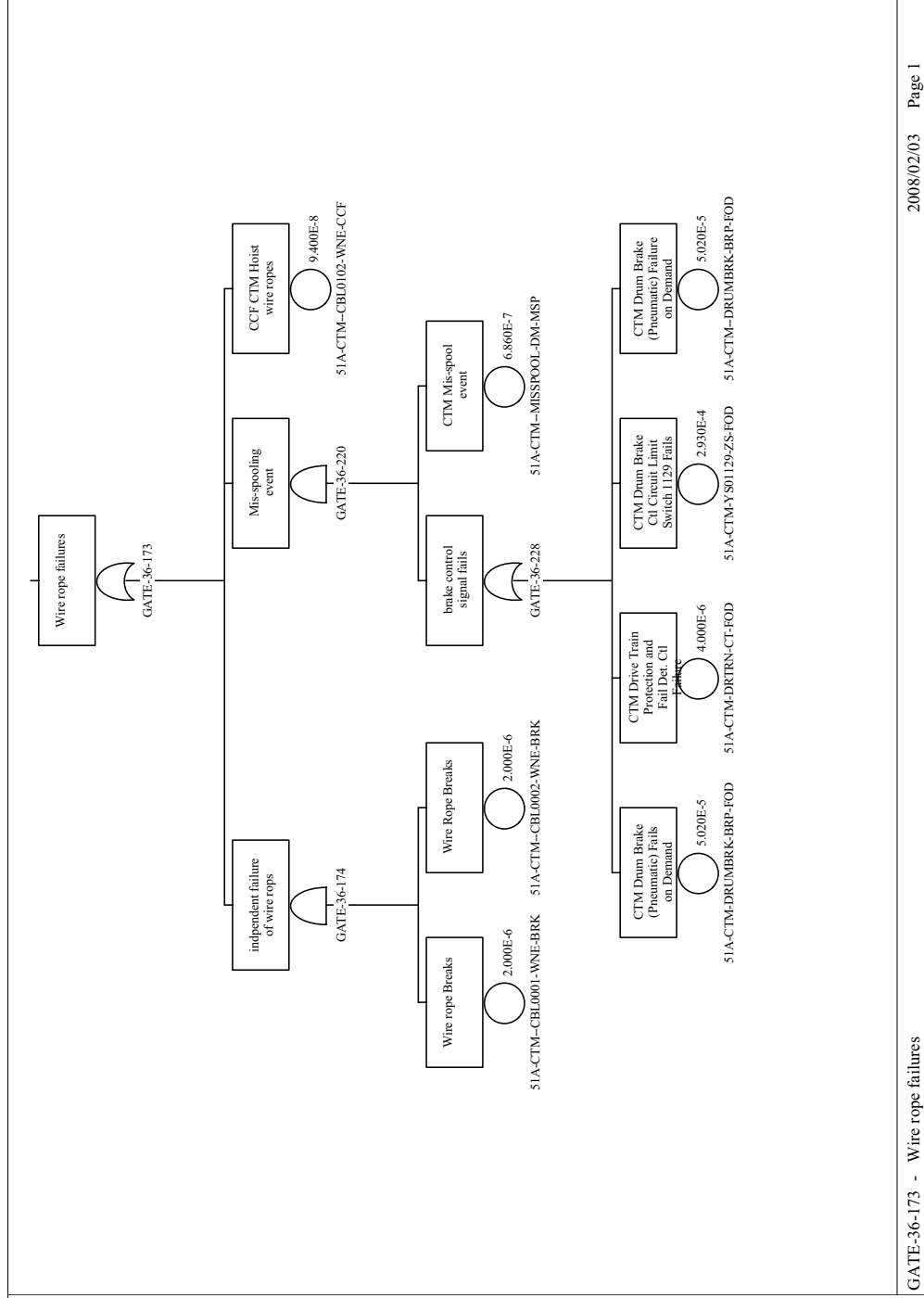
GATE-36-167 - hoist motors and brakes fail

Source: Original

Figure B4.4-12. CTM Drop Fault Tree Sheet 10

B4-31

March 2008



GATE-36-173 - Wire rope failures

2008/02/03 Page 1

Source: Original

Figure B4.4-13. CTM Drop Fault Tree Sheet 11

B4-32

March 2008

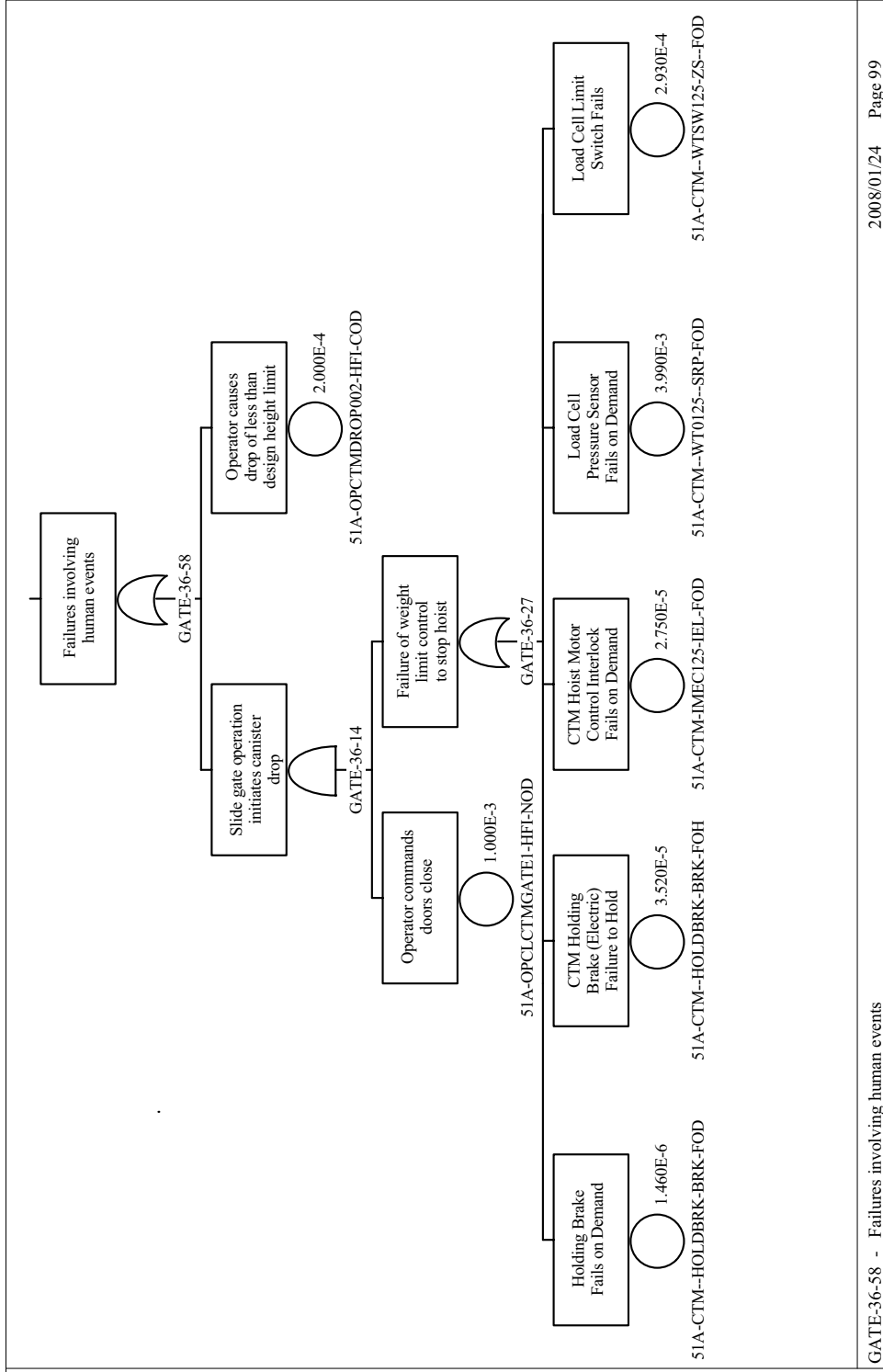


Figure B4.4-14. CTM Drop Fault Tree Sheet 12

B4.4.2 Canister Drop 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 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, stops 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 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 place 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 rely on CTM features that could allow the system to withstand a two-block event without dropping the load. That is, the model conservatively treats two-block events as drops.

B4.4.2.5 Basic Event Data

Table B4.4-4 contains a list of basic events used in the “Canister Drop from Above the Canister Design Limit Drop Height” fault tree. Included are the human failure events and the common-cause failure events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is 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 Canister Drop from Above the Canister Design Limit Drop Height Fault Tree

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1	1.377E-05	1.377E-05	0.000E+00	0.000E+00
51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00
51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	0.000E+00	4.700E-06	1.000E+00
51A-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; Calc. = calculation; CCF = common-cause failure; Ctl = control; CTM = canister transfer machine;

FAIL. = failure; Miss. = mission; PLC = programmable logic controller; Prob. = probability.

Source: Original

B4.4.2.5.1 Human Failure Events

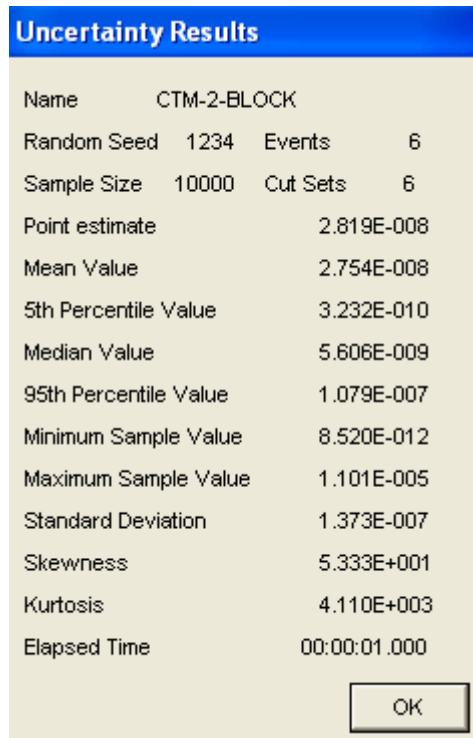
One basic event is associated with human error: 51A-OPCTMDRINT01-HFI-COD (Operator raises load too high - two block). This event models the combination of operator actions and interlock failures required to allow the operator to raise a load above design limits, and action that can lead to a two blocking failure.

B4.4.2.5.2 Common-Cause Failures

One common-cause 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 common-cause failure of these switches was considered.

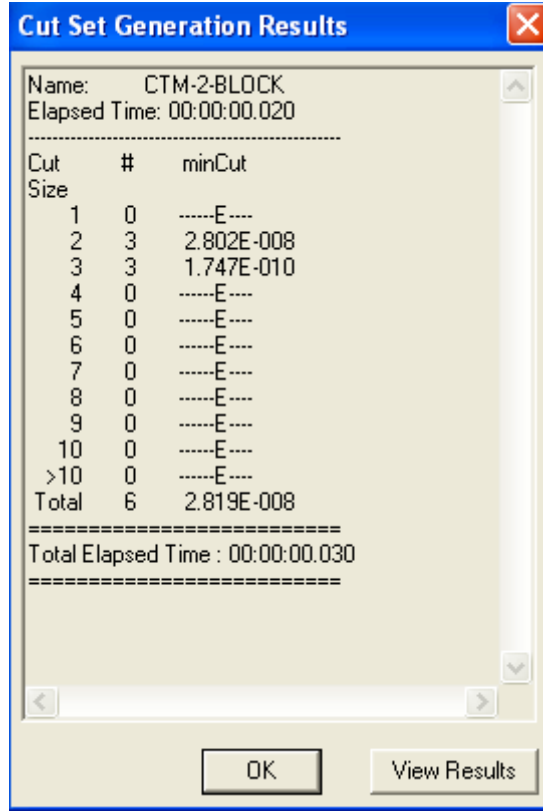
B4.4.2.6 Uncertainty and Cut Set Generation Results

Figure B4.4-15 contains the uncertainty results obtaining from running the fault tree for “Canister Drop from Above the Canister Design Limit Drop Height” with a cutoff probability of 1E-15. Figure B4.4-16 provides the cut set generation results for “Canister Drop from Above the Canister Design Limit Drop Height” fault tree.



Source: Original

Figure B4.4-15. Uncertainty Results of the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree



Source: Original

Figure B4.4-16 Cut Set Generation Results for the Canister Drop from Above the Canister Design Limit Drop Height Fault Tree

B4.4.2.7 Cut Sets

Table B4.4-5 contains the six cut sets for the “Canister Drop from Above the Canister Design Limit Drop Height” fault tree.

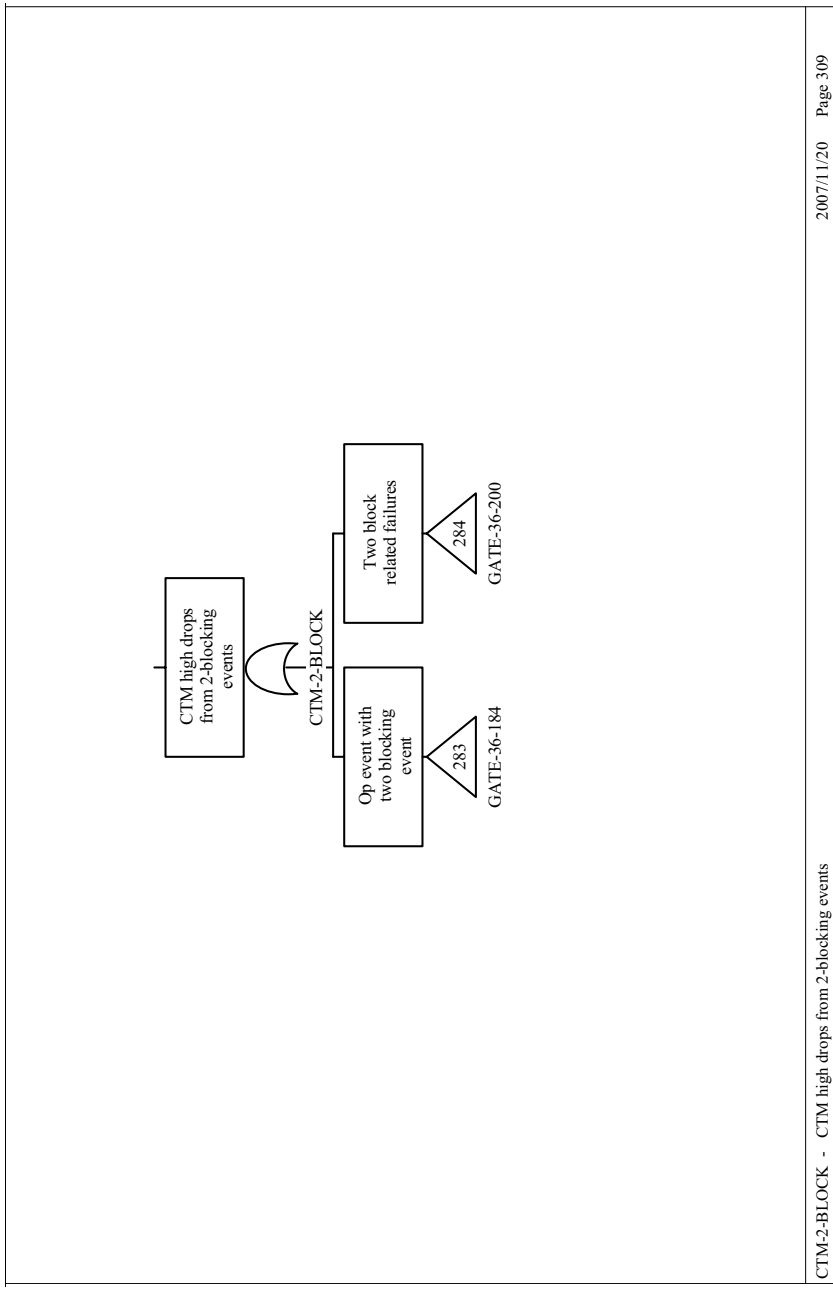
Table B4.4-5. Dominant Cut Sets for the Canister Drop from Above the Canister Design Limit Drop Height

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.15	99.15	2.795E-08	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.377E-05
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
99.77	0.62	1.743E-10	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.930E-04
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
100.00	0.23	6.472E-11	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.377E-05
			51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.700E-06
100.00	0.00	4.035E-13	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.930E-04
			51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	4.700E-06
100.00	0.00	1.859E-13	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.377E-05
			51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.350E-08
100.00	0.00	1.159E-15	51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	2.930E-04
			51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	2.930E-04
			51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	1.350E-08

NOTE: ASD = adjustable speed drive; CCF = common-cause failure; CTM = canister transfer machine.

Source: Original

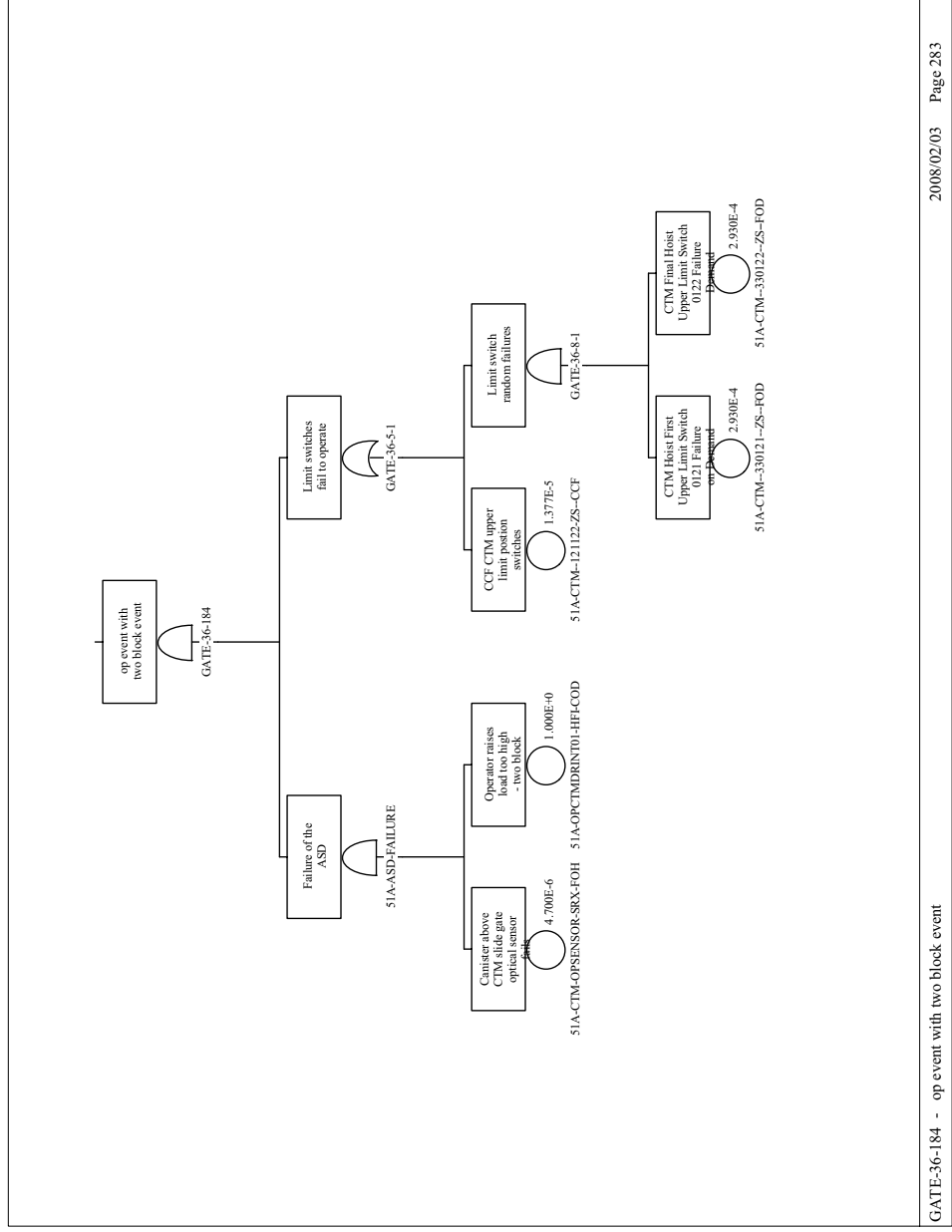
B4.4.2.8 Fault Trees



CTM-2-BLOCK - CTM high drops from 2-blocking events 2007/11/20 Page 309

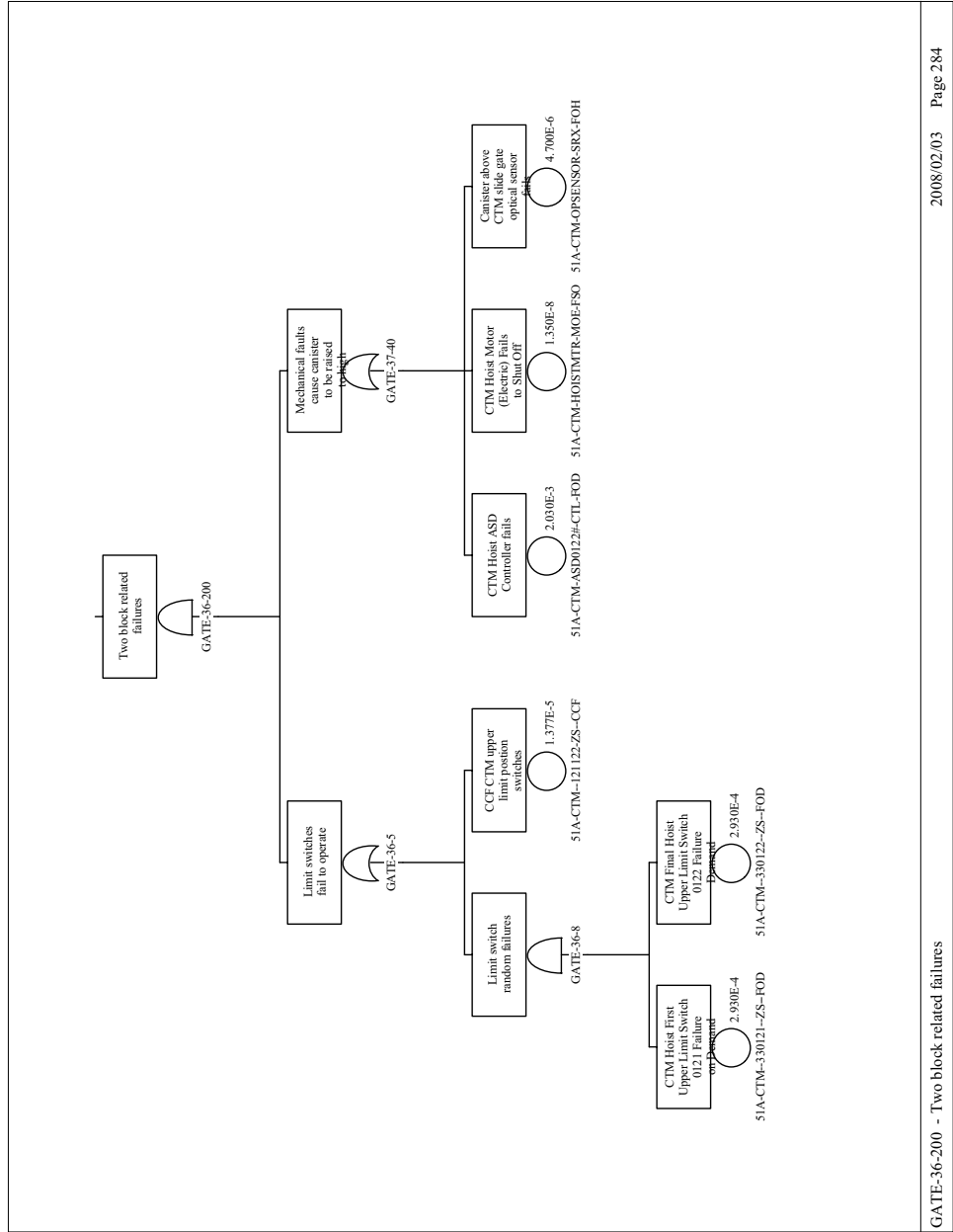
Source: Original

Figure B4.4-17. CTM High Drops from Two Blocking Event Sheet 1



Source: Original

Figure B4.4-18. CTM High Drops from Two Blocking Event Sheet 2



2008/02/03 Page 284

GATE-36-200 - Two block related failures

Source: Original

Figure B4.4-19. CTM High Drops from Two Blocking Event Sheet 3

B4-43

March 2008

B4.4.3 Drop of Object onto Canister

B4.4.3.1 Description

Transfer operations using the CTM entail the possibility of inadvertent drops of an object 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 criterion for the CTM is 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, stops 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 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 drop of object onto canister fault tree. Included are the human failure events and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is 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 Drop of Object onto Canister Fault Tree

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	3	5.784E-05	0.000E+00	7.230E-06	8.000E+00
51A-CTM-#ZSH0112-ZS-FOH	Shield Skirt Position Switch Fails	3	5.784E-05	0.000E+00	7.230E-06	8.000E+00
51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1	1.377E-05	1.377E-05	0.000E+00	1.000E+00
51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--CBL0001-WNE-BRK	Wire rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	0.000E+00
51A-CTM--CBL0002-WNE-BRK	Wire Rope Breaks	1	2.000E-06	2.000E-06	0.000E+00	0.000E+00
51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	1	9.400E-08	9.400E-08	9.400E-08	0.000E+00
51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	1	4.000E-08	4.000E-08	0.000E+00	0.000E+00
51A-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
51A-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure to Hold	3	2.011E-04	0.000E+00	8.380E-06	2.400E+01
51A-CTM--EQL-SHV-BLK-FOD	Equalizer sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--HOLDBRK-BRK-FOD	Brake Failure on Demand	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3	3.520E-05	0.000E+00	4.400E-06	8.000E+00
51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--MISSPOOL-DM-MSP	CTM Mis-spool event	3	6.860E-07	0.000E+00	6.860E-07	1.000E+00
51A-CTM--OVERSP--ZS-FOD	Hoist Motor Speed Limit Switch Fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM--PORTGT1-MOE-SPO	Spurious port gate1 motor operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM--PORTGT1-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM--PORTGT2-MOE-SPO	Spurious port gate 2 motor operation	3	6.740E-07	0.000E+00	6.740E-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	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM--UPPERBL-BLK-FOD	Upper sheaves structural failure	1	1.150E-06	1.150E-06	0.000E+00	0.000E+00
51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	1	3.990E-03	3.990E-03	0.000E+00	0.000E+00
51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	1	2.930E-04	2.930E-04	0.000E+00	3.600E+02
51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-DRTRN-CT-FOD	CTM Drive Train Protection and Fail Det. Ctl Failure	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
51A-CTM-DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Fails on Demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
51A-CTM-HOISTMT-MOE-FTR	CTM hoist Motor (Electric) Fails to Run	3	6.500E-06	0.000E+00	6.500E-06	1.000E+00
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00
51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-OPSENSOR-SRX-FOH	Canister above CTM slide gate optical sensor fails	3	4.700E-06	0.000E+00	4.700E-06	1.000E+00
51A-CTM-PLC0101-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-PLC01021-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operations	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-PLC0103-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	0.000E+00
51A-CTM-SLIDEGT-PLC-SPO	CTM Slide Gate 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	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM-SLIDEGT1-IEL-FOD	CTM Slide Gate Interlock Fails	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
51A-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.100E-03	1.100E-03	0.000E+00	0.000E+00
51A-CTM-YS01129-ZS-FOD	CTM Drum Brake Ctl Circuit Limit Switch 1129 Fails	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00
51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	3	1.280E-06	0.000E+00	1.280E-06	1.000E+00
51A-LOSS-OFFSITE-PWR	Loss of offsite power	1	2.990E-03	2.990E-03	0.000E+00	0.000E+00
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
51A-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	1	4.000E-07	4.000E-07	0.000E+00	0.000E+00
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	1.000E-03	1.000E-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.

CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

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 these events includes operator actions and the failures of interlocks intended to prevent such operator action.

Table B4.4-7. Human Failure Events

Name	Description
51A-OPCTMDRINT01-HFI-COD	Operator raises load too high - two block
51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister
51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor

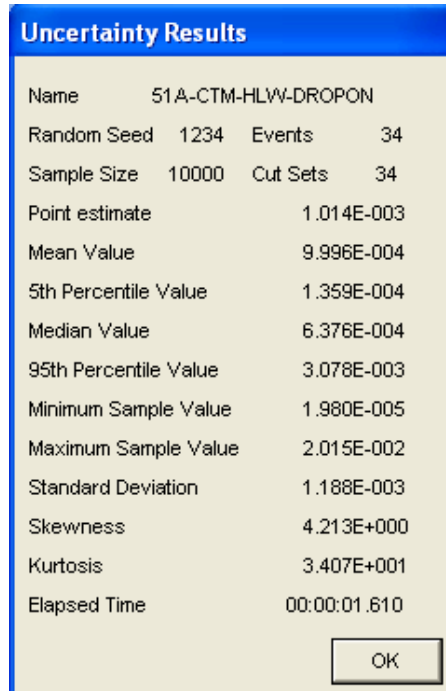
Source: Original

B4.4.3.5.2 Common-Cause Failures

Two common-cause events were considered in the evaluation of this fault tree. One is associated with pairs of sensors used to limit CTM movement. The two upper limit sensors on the hoist are used to prevent a two-block event. The second common-cause event considered is the common-cause failure of the hoist cables.

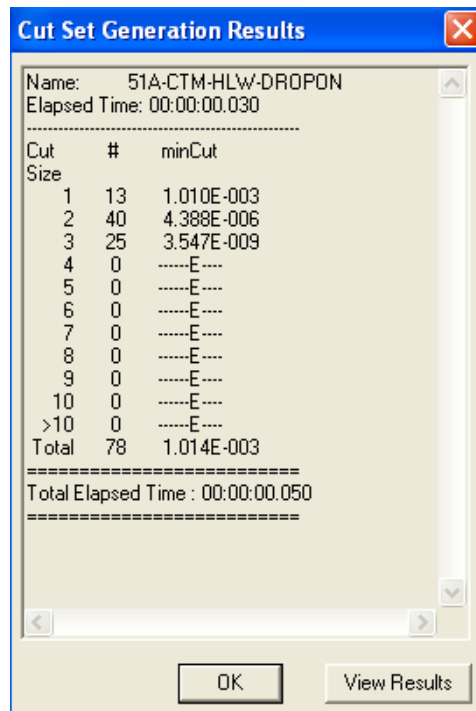
B4.4.3.6 Uncertainty and Cut Set Generation

Figure B4.4-20 contains the uncertainty results obtaining from running the fault trees for the “Drop of Object onto Canister” with a cutoff probability of 1E-15. Figure B4.4-21 provides the cut set generation results for the “Drop of Object onto Canister” fault tree.



Source: Original

Figure B4.4-20 Uncertainty Results of the Drop of Object onto Canister Fault Tree



Source: Original

Figure B4.4-21. Cut Set Generation Results for the Drop of Object onto Canister Fault Tree

B4.4.3.7 Cut Sets

Table B4.4-8 contains the top 20 cut sets for the “Drop of Object onto Canister” fault tree.

Table B4.4-8. Dominant Cut Sets for the “Drop of Object onto Canister Fault” Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.61	98.61	1.000E-03	51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
99.00	0.39	3.990E-06	51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.13	0.13	1.280E-06	51A-CTM--ZSH0111-ZS--SPO	Grapple Engaged Limit Switch Spurious Operation	1.280E-06
99.26	0.13	1.280E-06	51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	1.280E-06
99.37	0.11	1.150E-06	51A-CTM--EQL-SHV-BLK-FOD	equalizer sheaves structural failure	1.150E-06
99.48	0.11	1.150E-06	51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1.150E-06
99.59	0.11	1.150E-06	51A-CTM--LOWERBL-BLK-FOD	CTM lower sheaves structural failure	1.150E-06
99.70	0.11	1.150E-06	51A-CTM--UPPERBL-BLK-FOD	upper sheaves structural failure	1.150E-06
99.77	0.07	6.740E-07	51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	6.740E-07
99.84	0.07	6.740E-07	51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operations	6.740E-07
99.91	0.07	6.740E-07	51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	6.740E-07
99.95	0.04	4.000E-07	51A-OPCTMDROP001-HFI-COD	Operator causes drop of object onto canister	4.000E-07
99.98	0.03	2.930E-07	51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	2.930E-04
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.99	0.01	9.400E-08	51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist wire ropes	9.400E-08
99.99	0.00	4.000E-08	51A-CTM--DRUM001-DM--FOD	Hoisting drum structural failure	4.000E-08

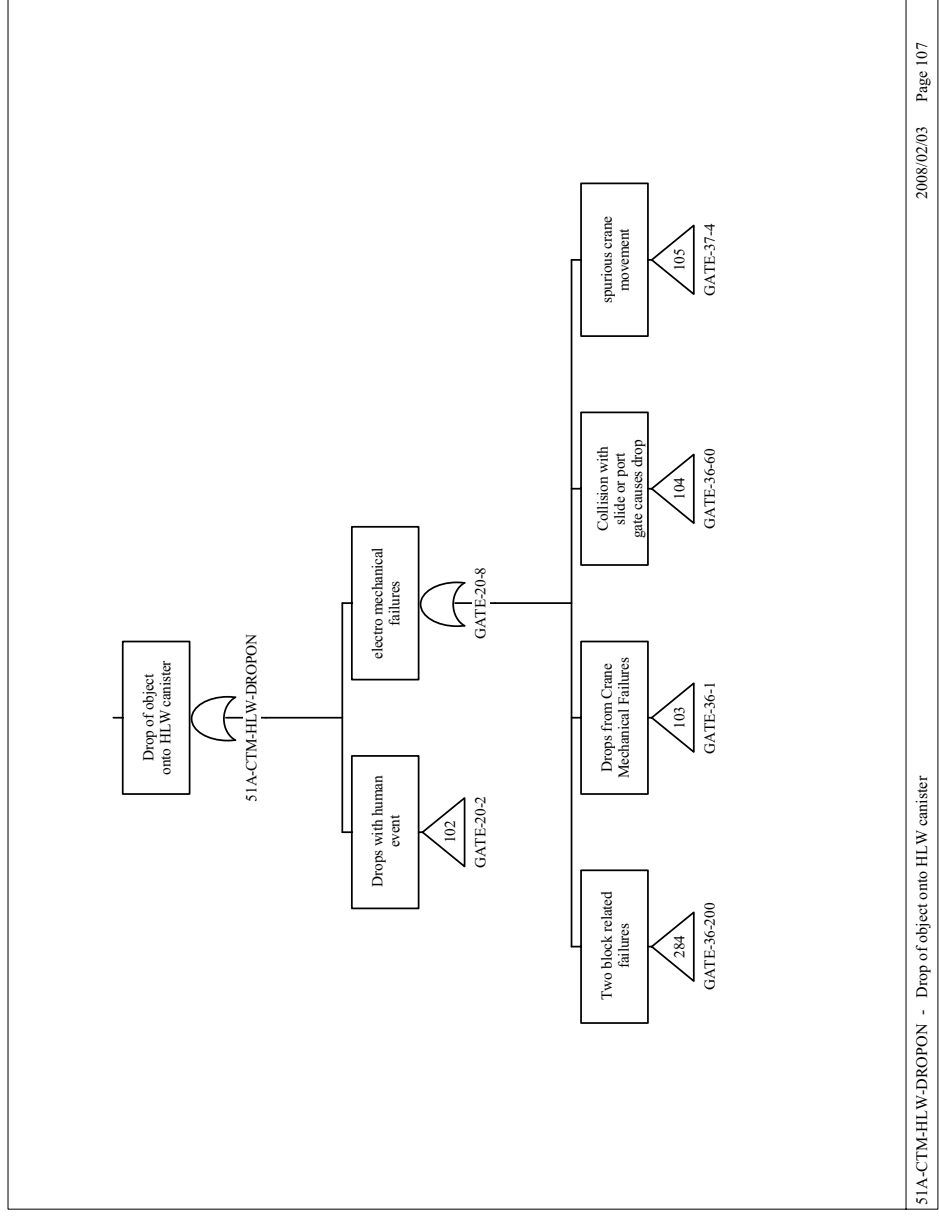
Table B4.4-8. Dominant Cut Sets for the CTM Drop onto Canister Fault Tree (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.99	0.00	3.520E-08	51A-CTM--HOLDBRK-BRK-FOH	Holding Brake (electric) Fails to Hold	3.520E-05
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.99	0.00	2.795E-08	51A-CTM--121122-ZS--CCF	CCF CTM upper limit position switches	1.377E-05
			51A-CTM-ASD0122#-CTL-FOD	CTM Hoist ASD Controller fails	2.030E-03
99.99	0.00	2.750E-08	51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	2.750E-05
			51A-OPCLCTMGATE1-HFI-NOD	Operator commands doors close	1.000E-03
99.99	0.00	2.689E-09	51A-CTM--PORTGT2-MOE-SPO	spurious port gate 2 motor operation	6.740E-07
			51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
99.99	0.00	2.689E-09	51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	3.990E-03
			51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) spurious Operation	6.740E-07

NOTE: CCF = common-cause failure; Ctl = control; CTM = canister transfer machine;
PLC = programmable logic controller.

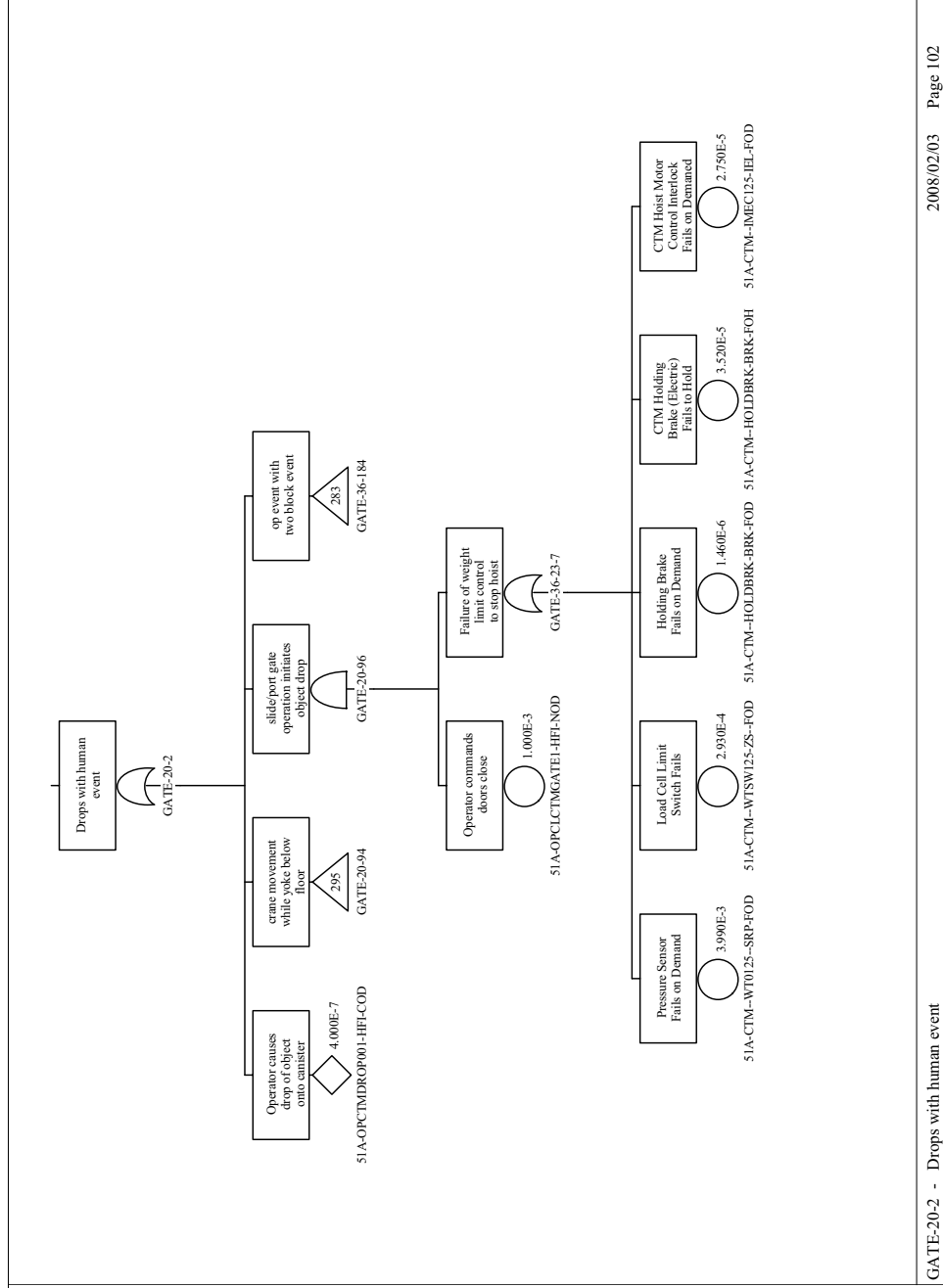
Source: Original

B4.4.3.8 Fault Trees



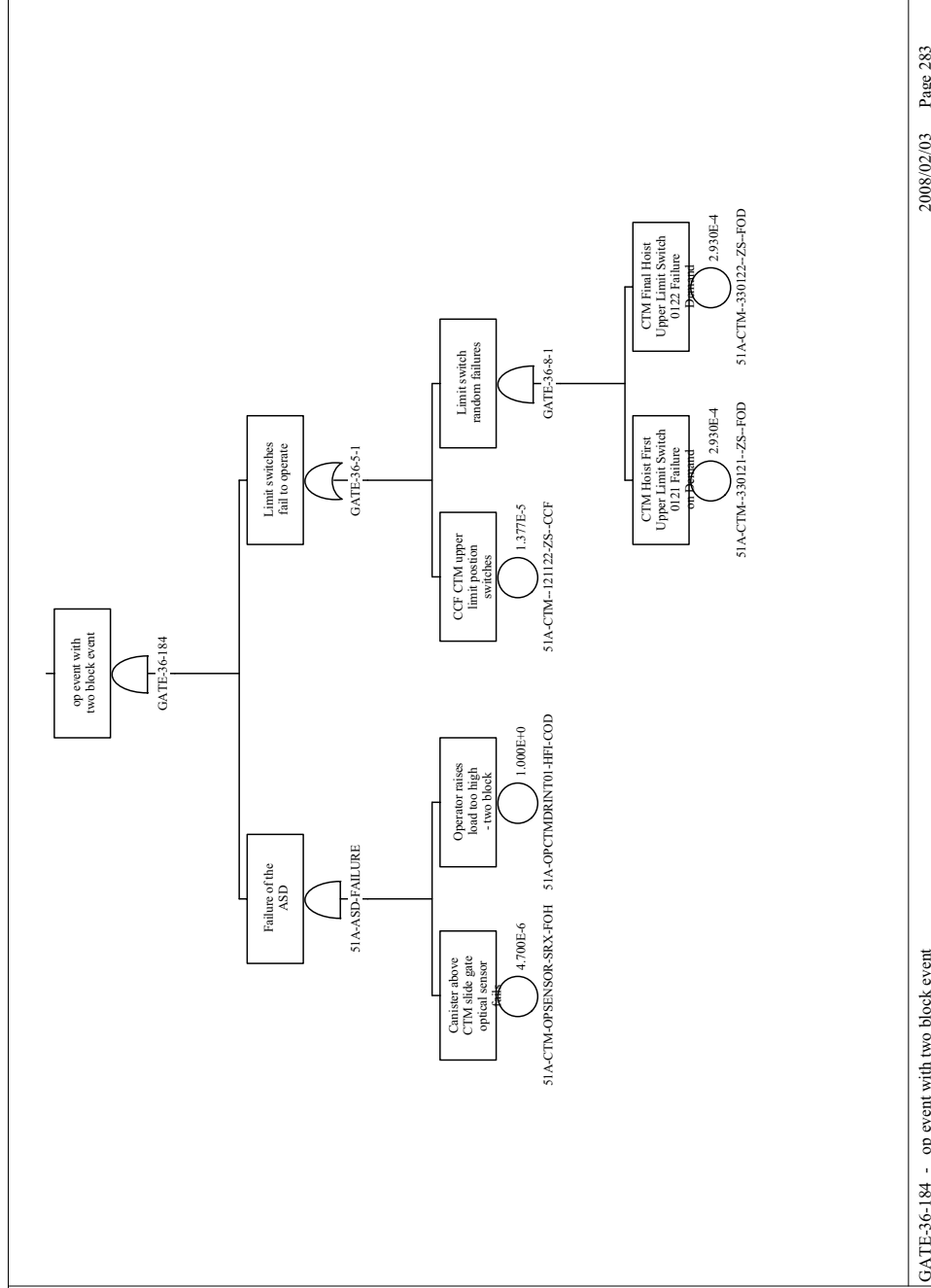
Source: Original

Figure B4.4-22. Drop of Object onto Cask
Sheet 1



Source: Original

Figure B4.4-23. Drop of Object onto Cask Sheet 2



2008/02/03 Page 283

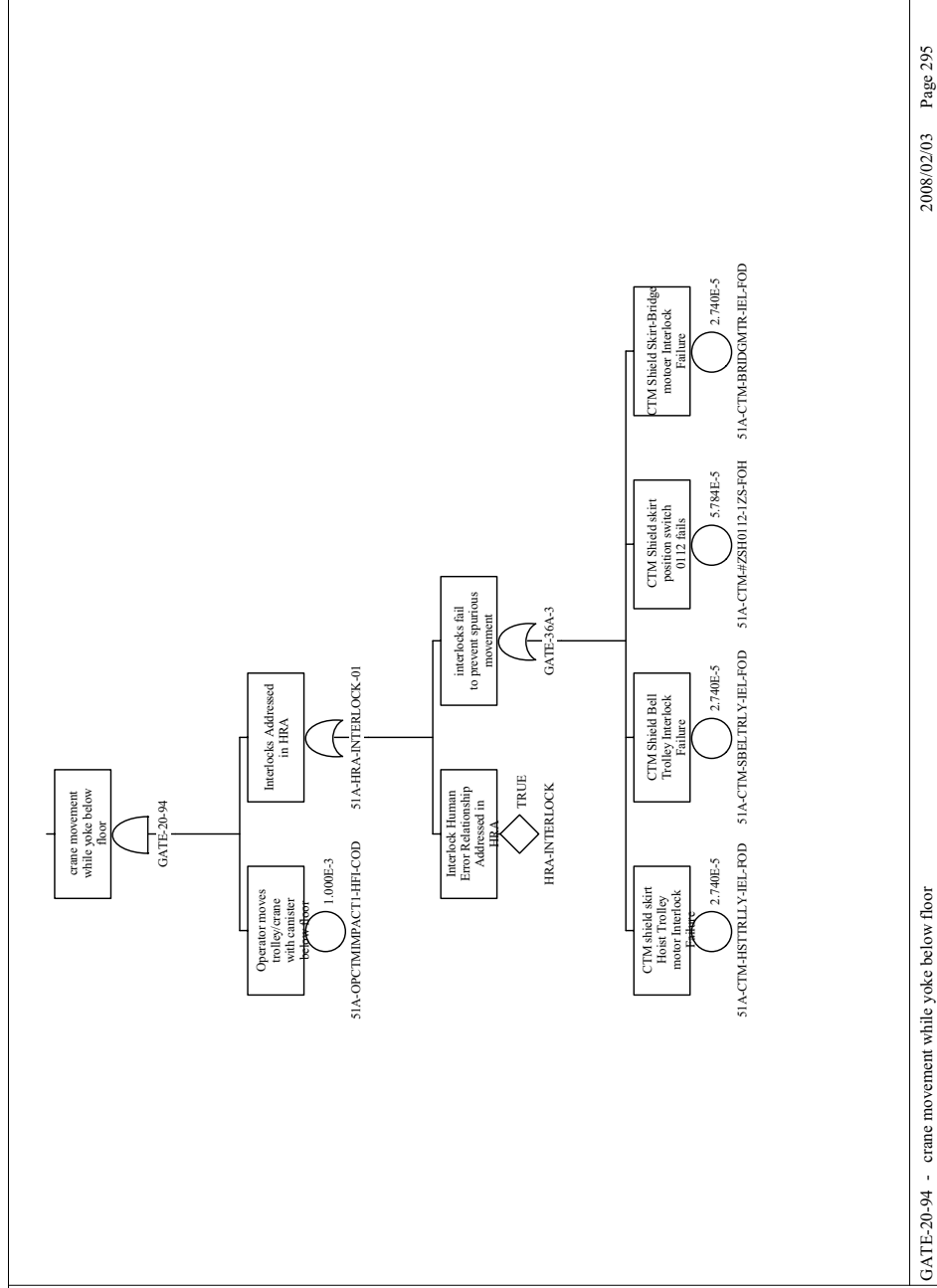
GATE-36-184 - op event with two block event

Source: Original

Figure B4.4-24. Drop of Object onto Cask Sheet 3

B4-56

March 2008



2008/02/03 Page 295

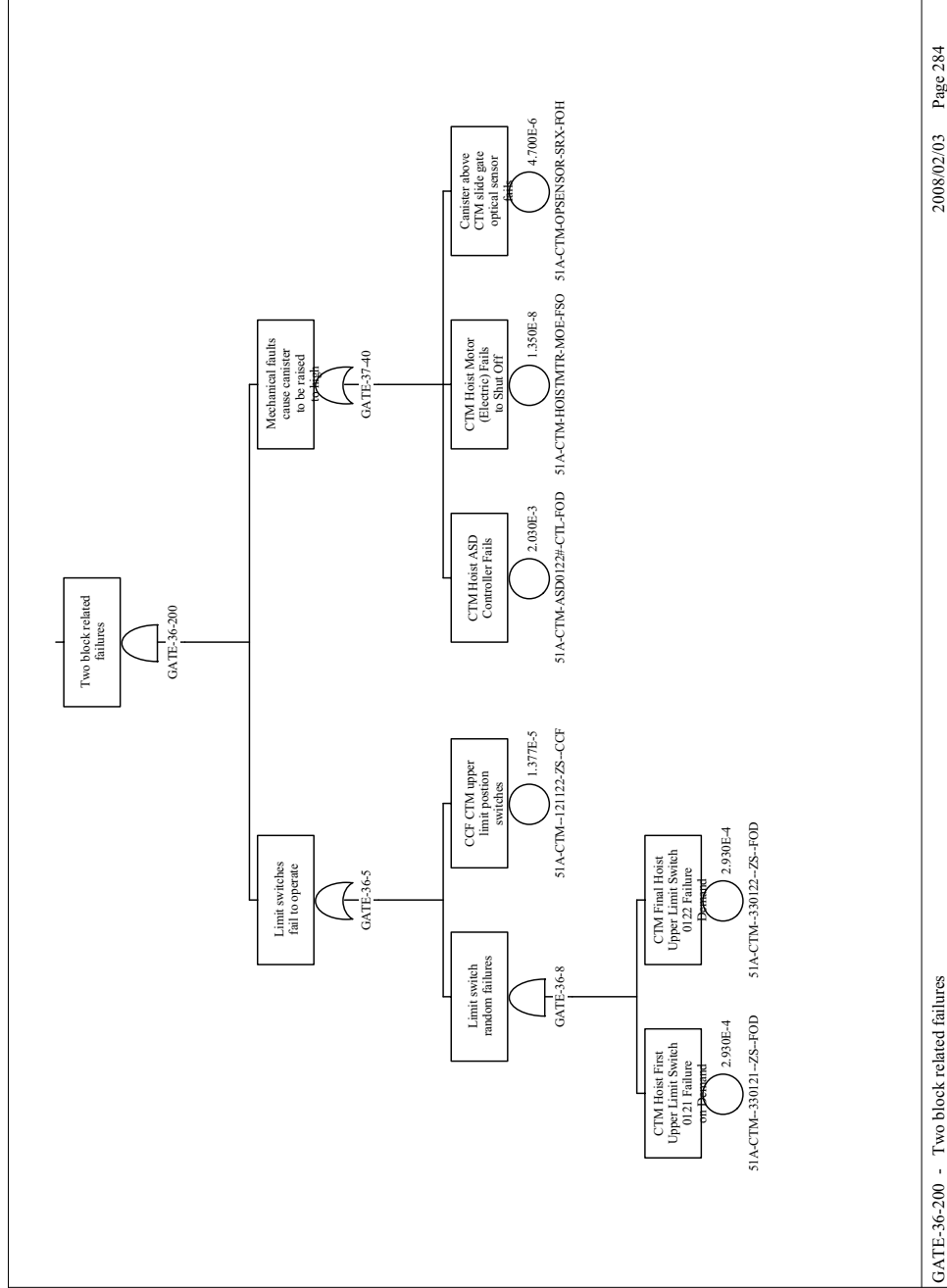
GATE-20-94 - crane movement while yoke below floor

Source: Original

Figure B4.4-25. Drop of Object onto Cask Sheet 4

B4-57

March 2008

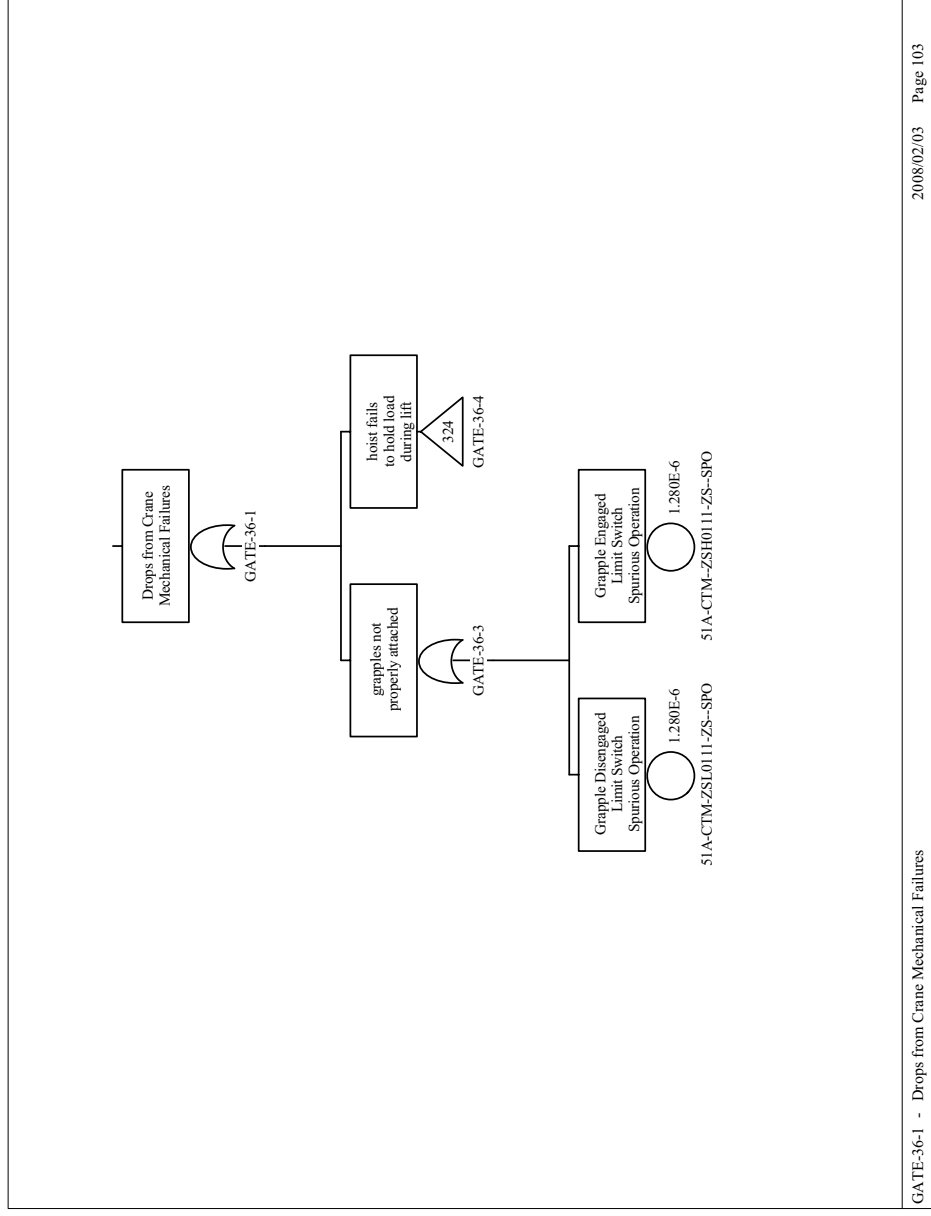


2008/02/03 Page 284

GATE-36-200 - Two block related failures

Source: Original

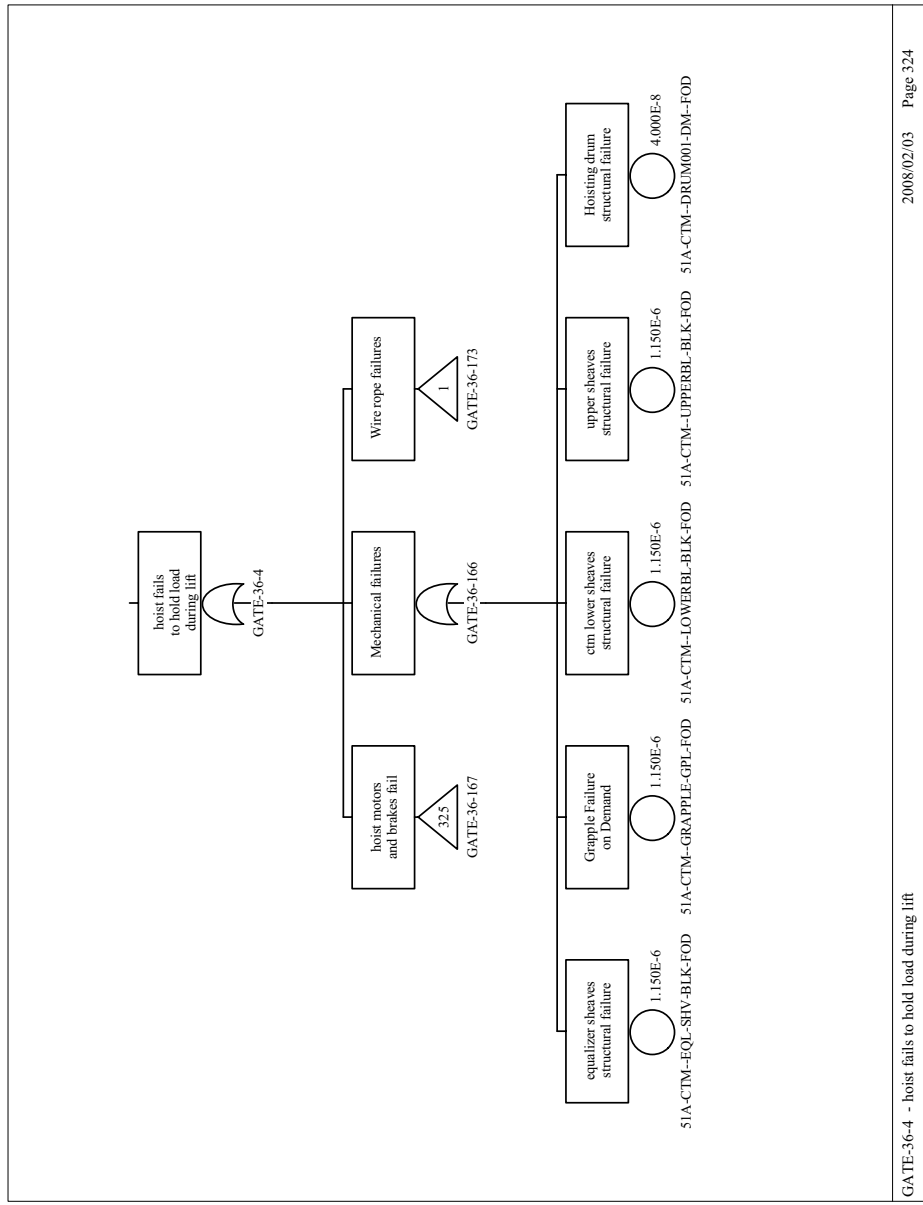
Figure B4.4-26. Drop of Object onto Cask Sheet 5



GATE-36-1 - Drops from Crane Mechanical Failures

Source: Original

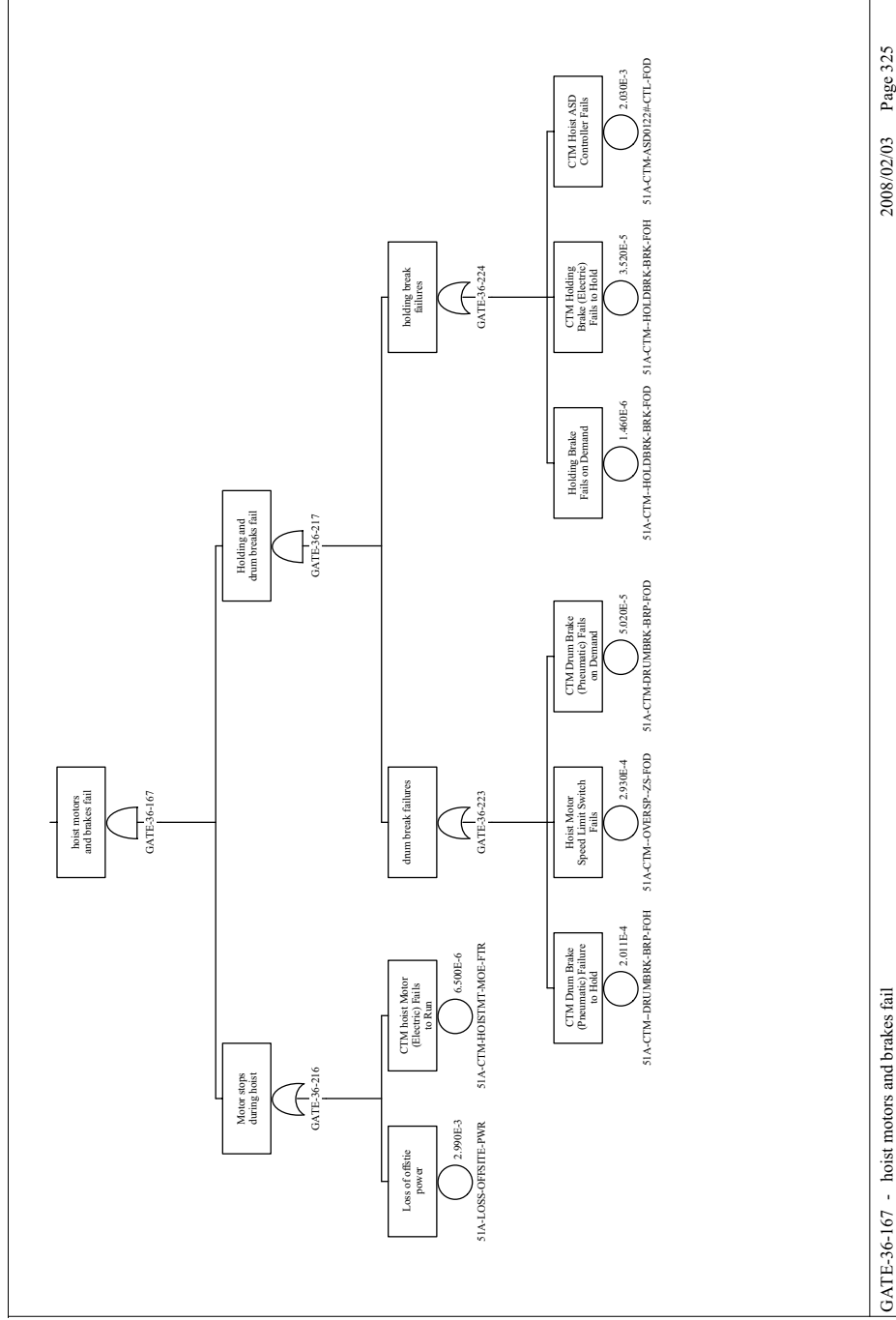
Figure B4.4-27. Drop of Object onto Cask
Sheet 6



GATE-36-4 - hoist fails to hold load during lift

Source: Original

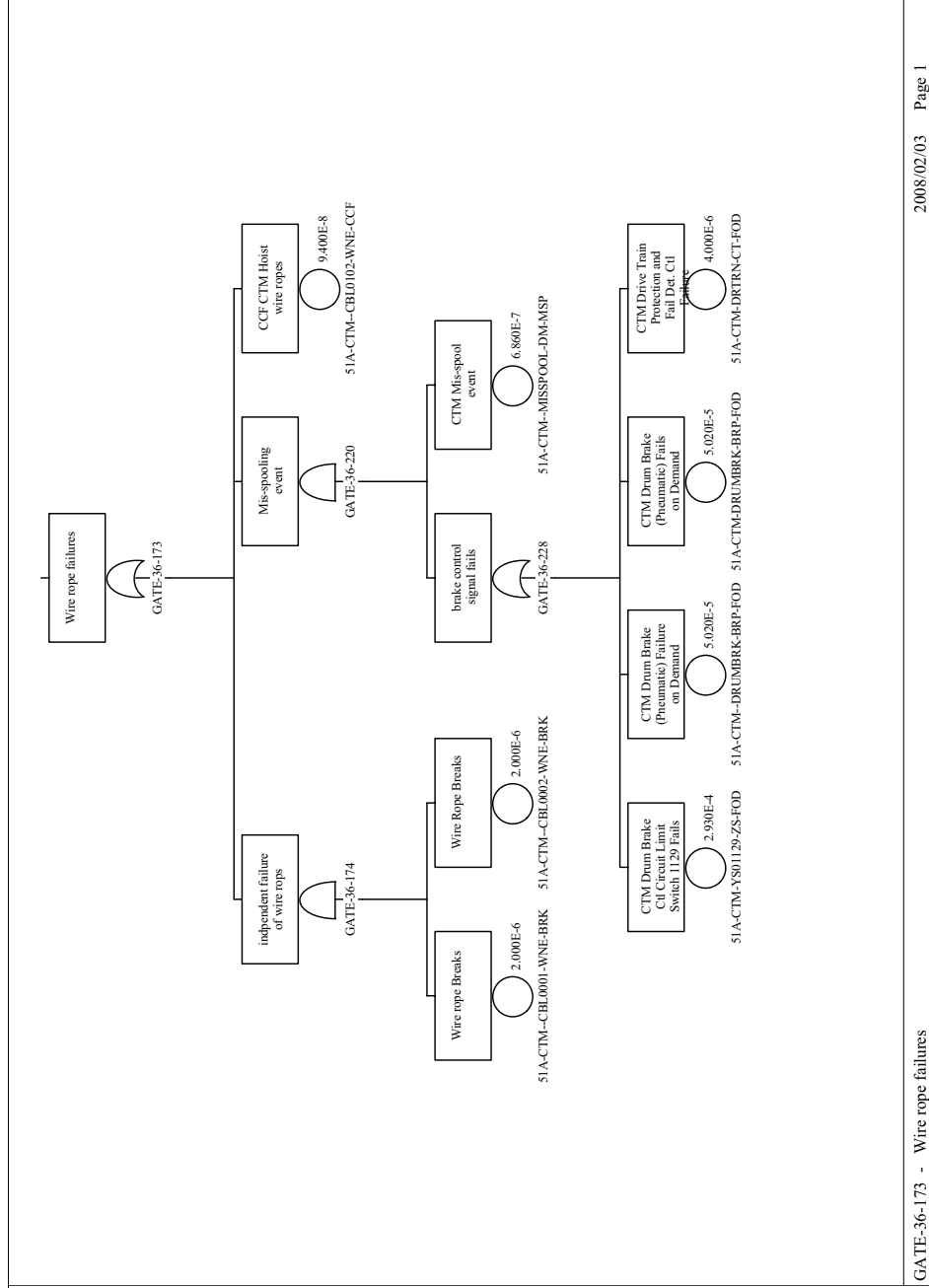
Figure B4.4-28. Drop of Object onto Cask
Sheet 7



GATE-36-167 - hoist motors and brakes fail

Source: Original

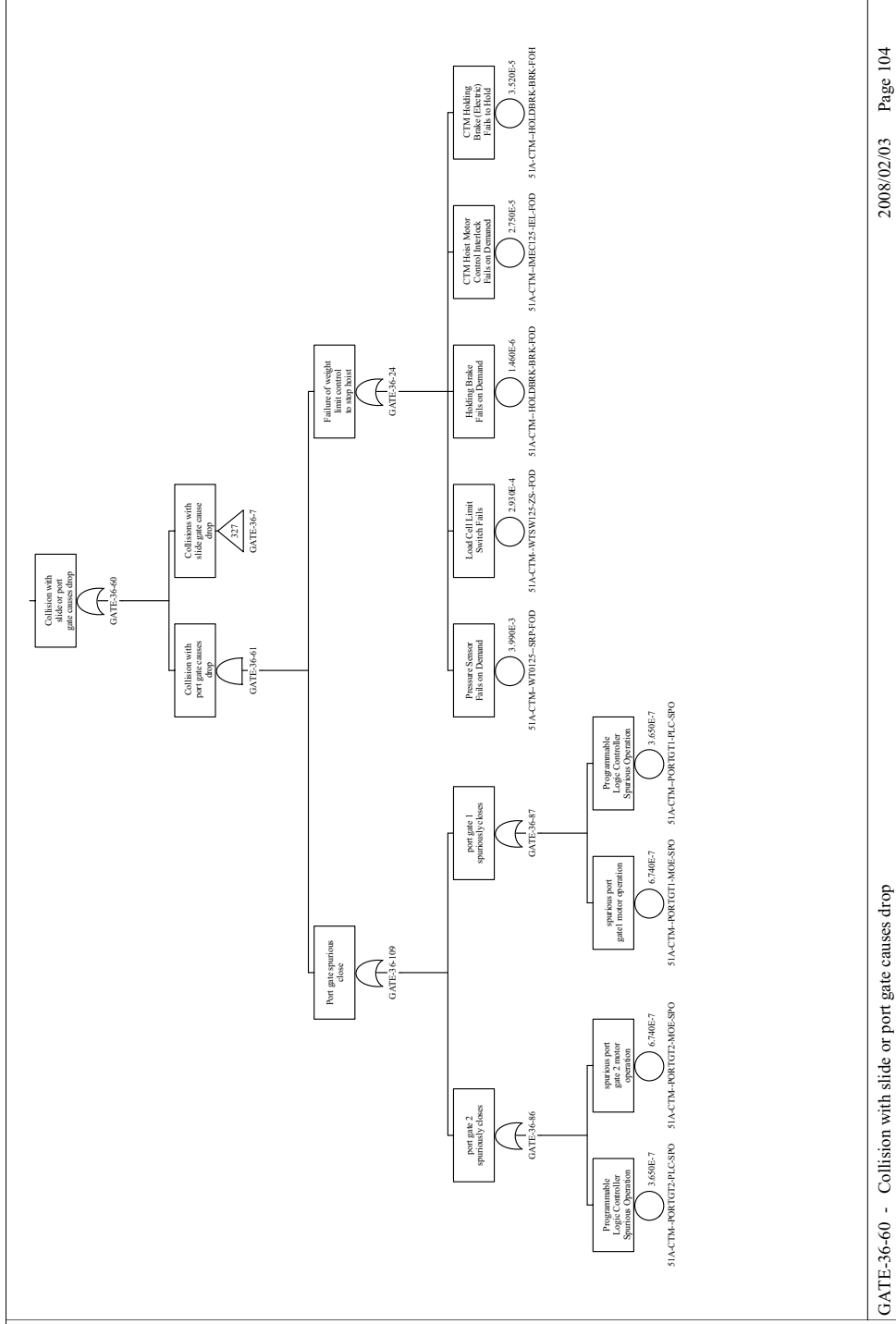
Figure B4.4-29. Drop of Object onto Cask Sheet 8



GATE-36-173 - Wire rope failures

Source: Original

Figure B4.4-30. Drop of Object onto Cask Sheet 9



2008/02/03 Page 104

GATE-36-60 - Collision with slide or port gate causes drop

Source: Original

Figure B4.4-31. Drop of Object onto Cask Sheet 10

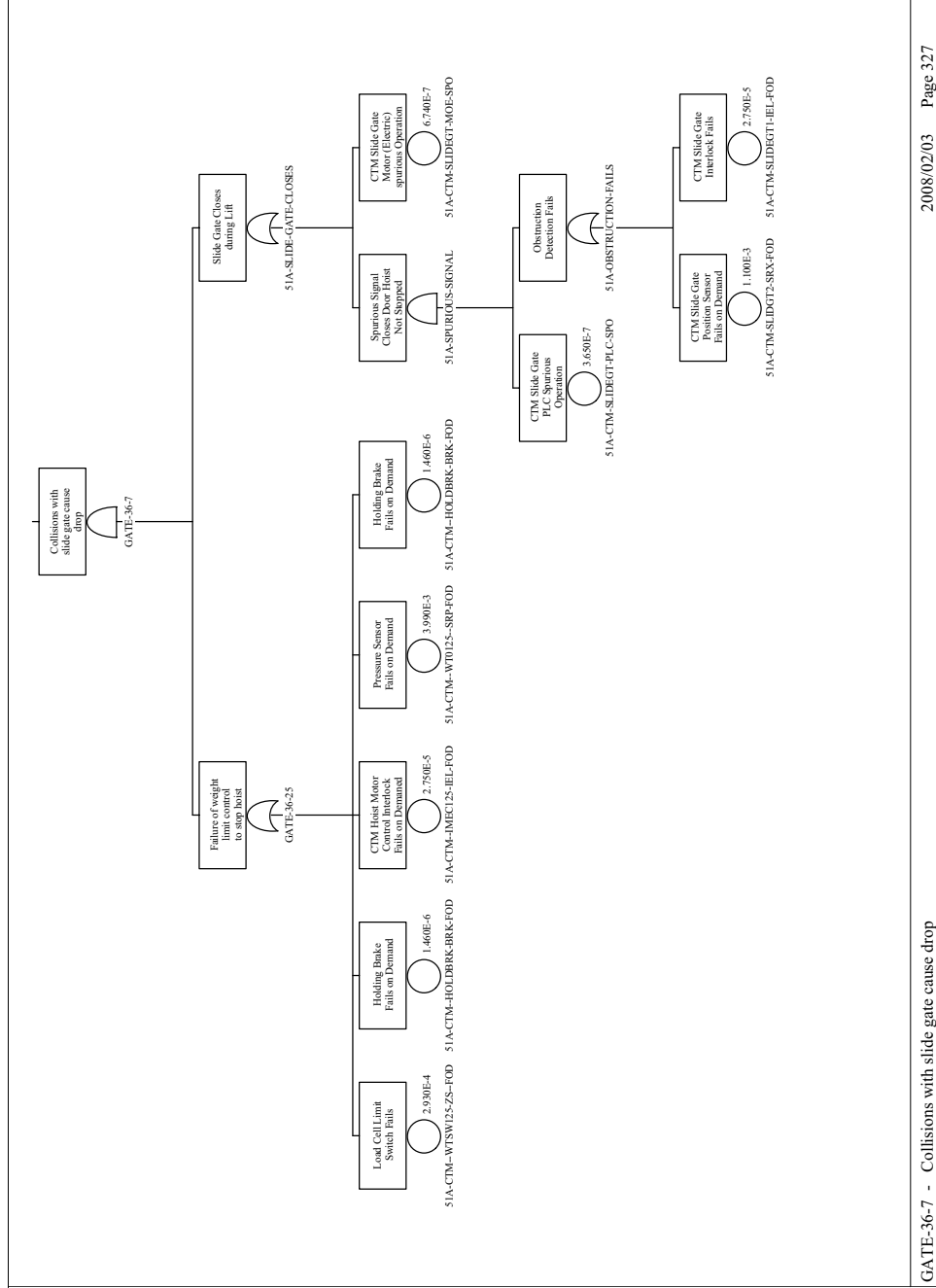
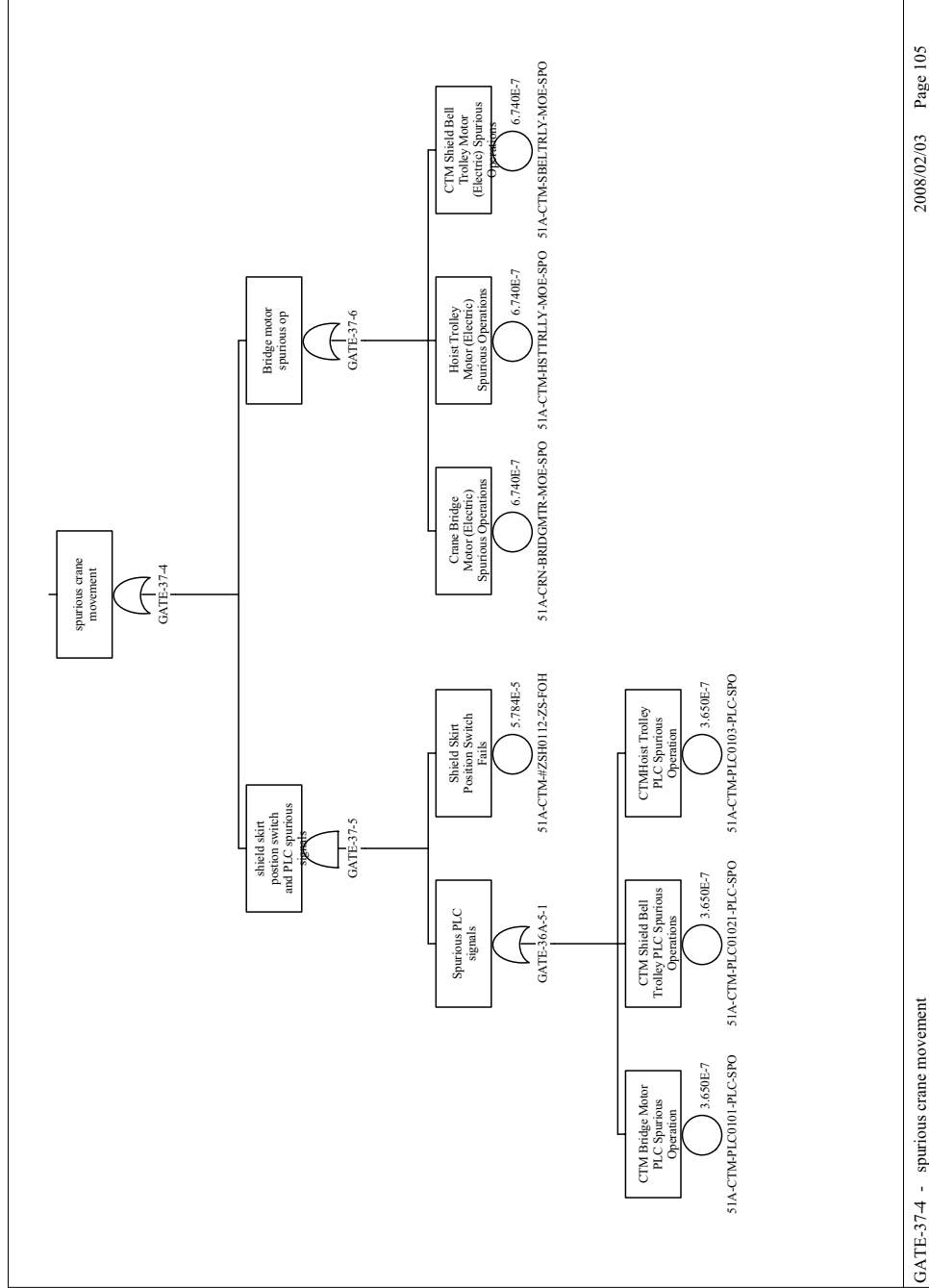


Figure B4.4-32. Drop of Object onto Cask Sheet 11



GATE-37-4 - spurious crane movement

Source: Original

Figure B4.4-33. Drop of Object onto Cask Sheet 12

B4.4.4 Canister Impact

B4.4.4.1 Description

A fault tree was developed to address the potential for impacts to the canister. Collisions between the CTM, shield bell, floor, and a permanent structure were considered.

B4.4.4.2 Success Criteria

Success criteria for the “Canister Impact” is the prevention of 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.

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, stops the hoist and erases 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 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. 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 “Canister Impact” fault tree. Included are the human failure events and the common-cause failure events identified in the previous two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is 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 Canister Impact Fault Tree

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	3	1.949E-06	0.000E+00	4.450E-10	4.380E+03
51A-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	3	1.949E-06	0.000E+00	4.450E-10	4.380E+03
51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.080E-07	0.000E+00	1.350E-08	8.000E+00
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-BRIDTR-HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	1	1.740E-03	1.740E-03	0.000E+00	0.000E+00
51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.740E-05	2.740E-05	0.000E+00	0.000E+00
51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	1	4.000E-03	4.000E-03	0.000E+00	0.000E+00
51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	3	1.080E-07	0.000E+00	1.350E-08	8.000E+00
51A-CTM-TROLLYTR-#PR-FOH	Passive restraint (bumper) Failure	3	1.949E-06	0.000E+00	4.450E-10	4.380E+03
51A-CTM-TROLLYTR--PR-FOH	CTM Trolley & Run Stop Failure	3	1.949E-06	0.000E+00	4.450E-10	4.380E+03
51A-CTM-TROLT1-HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	1	1.740E-03	1.740E-03	0.000E+00	0.000E+00
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into End stop	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.

CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

The canister 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 (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 quantification of these events includes the probability of operator actions and the failure of ITS related interlocks intended to prevent such operator actions.

Table B4.4-10. Human Failure Events

Name	Description
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor
51A-OPCTMIMPACT5-HFI-COD	Operator over runs travel - collides into end stop

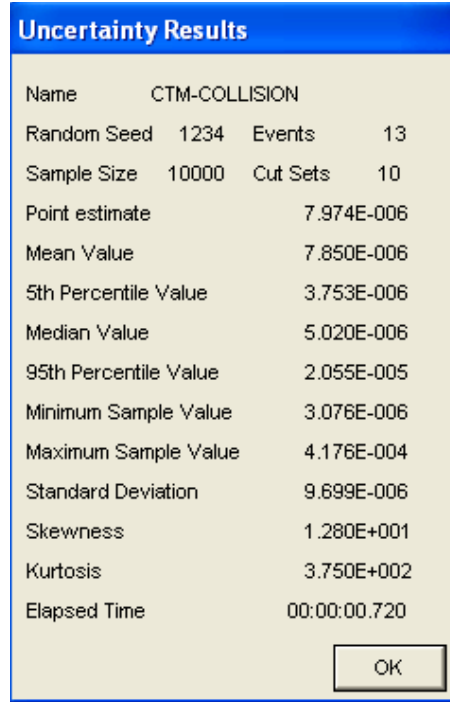
Source: Original

B4.4.4.5.2 Common-Cause Failures

There are no CCF modeled in the “Canister Impact” fault tree.

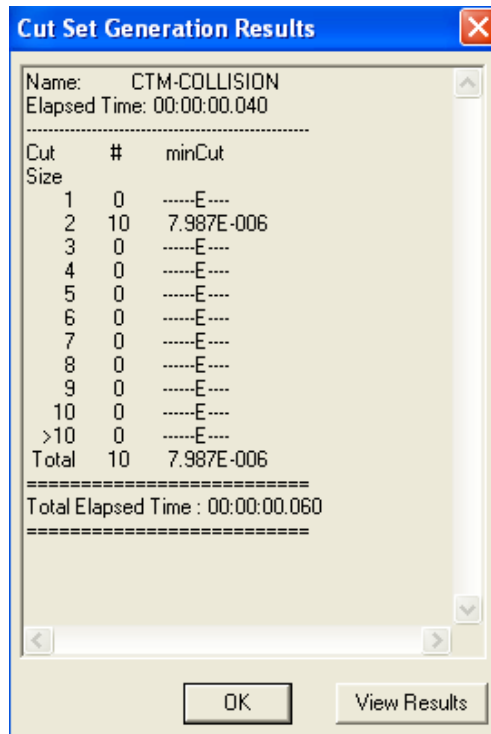
B4.4.4.6 Uncertainty and Cut Set Generation

Figures B4.4-34 contains the uncertainty results obtained from running the fault tree for “Canister Impact” using a cutoff probability of 1E-15. B4.4-35 contains the cut set generation results obtained from running the fault trees for “Canister Impact”.



Source: Original

Figure B4.4-34 Uncertainty Results of the Canister Impact Fault Tree



Source: Original

Figure B4.4-35. Cut Set Generation Results for the Canister Impact Fault Tree

B4.4.4.7 Cut Sets

Table B4.4-11 contains the cut sets for the “Canister Impact” fault tree.

Table B4.4-11. Dominant Cut Sets for the Canister Impact Fault Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
50.04	50.04	3.990E-06	51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt floor contact sensors fail	3.990E-03
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
74.48	24.44	1.949E-06	51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.949E-06
			51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into End stop	1.000E+000
98.92	24.44	1.949E-06	51A-CTM-BRIDGETR-#PR-FOH	Passive restraint (bumper) Failure	1.949E-06
			51A-OPCTMIMPACT5-HFI-COD	Operator Over Runs Travel Collides Into End stop	1.000E+000
99.26	0.34	2.740E-08	51A-CTM-HSTTRLLY-IEL-FOD	CTM shield skirt Hoist Trolley motor Interlock Failure	2.740E-05
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
99.60	0.34	2.740E-08	51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	2.740E-05
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
99.94	0.34	2.740E-08	51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge motor Interlock Failure	2.740E-05
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
99.98	0.04	3.391E-09	51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.949E-06
			51A-CTM-TROLT1-HC-FOD	Controller Failure to Stop (on Demand)	1.740E-03
99.98	0.00	7.796E-12	51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	1.949E-06
			51A-CTM-BRIDTR-CT-FOD	CTM Bridge Motor Controller Failure	4.000E-06

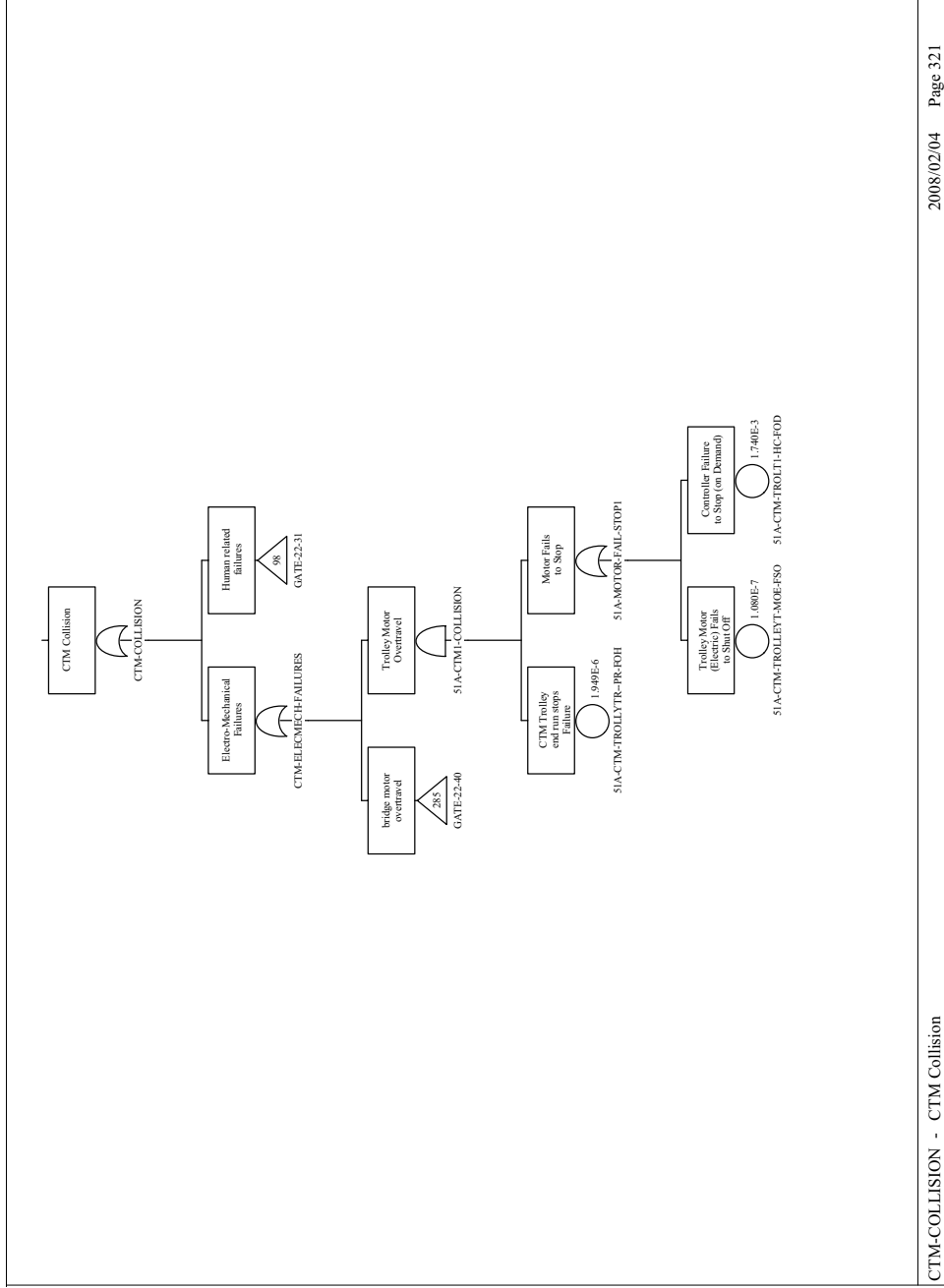
Table B4.4-11. Dominant Cut Sets for the Canister Impact Fault Tree (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.98	0.00	2.105E-13	51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	1.080E-07
			51A-CTM-TROLLYTR--PR-FOH	CTM Trolley end run stops Failure	1.949E-06
99.98	0.00	2.631E-14	51A-CTM-BREDGMTR--PR-FOH	Bridge Passive Restraints (end stops) Fail	1.949E-06
			51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	1.350E-08

NOTE: CCF = common-cause failure; Ctl = control; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

B4.4.4.8 Fault Trees



2008/02/04 Page 321

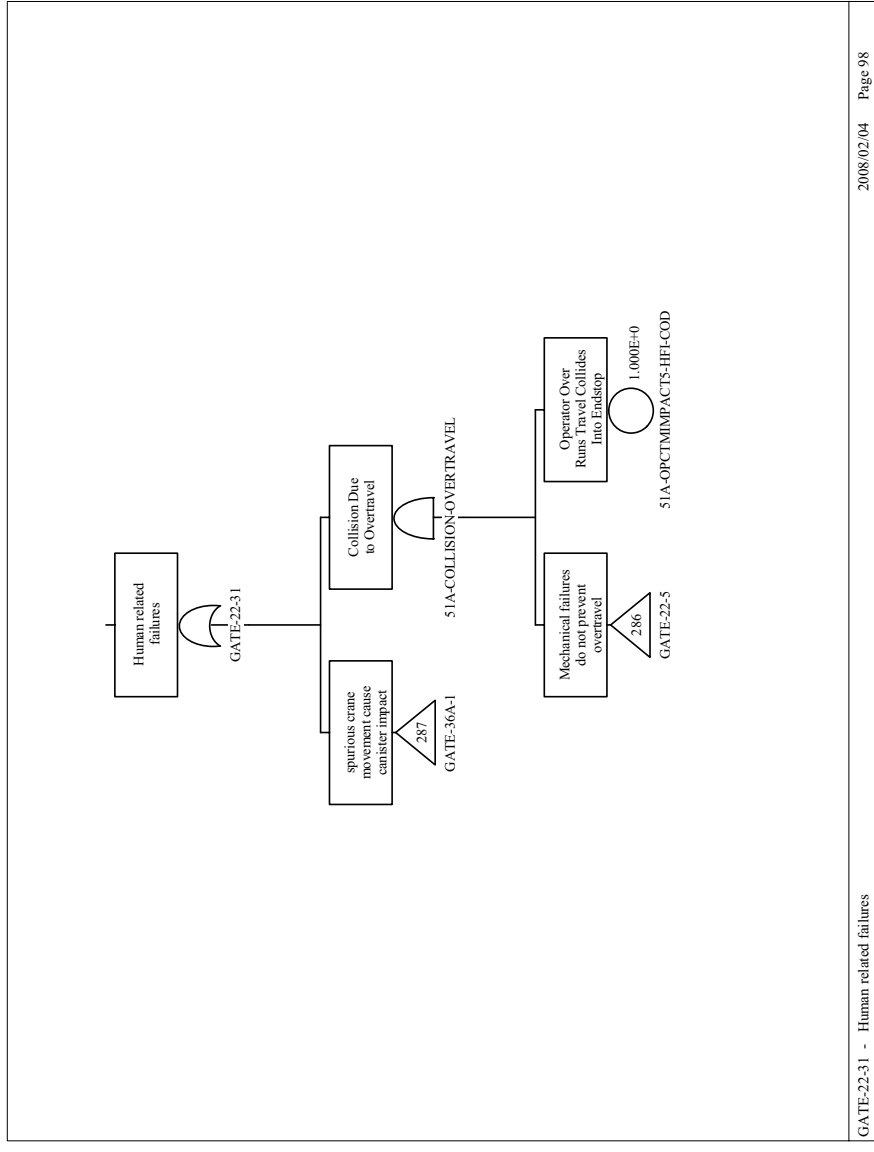
CTM-COLLISION - CTM Collision

Source: Original

Figure B4.4-36. CTM Collision Sheet 1

B4-73

March 2008



2008/02/04 Page 98

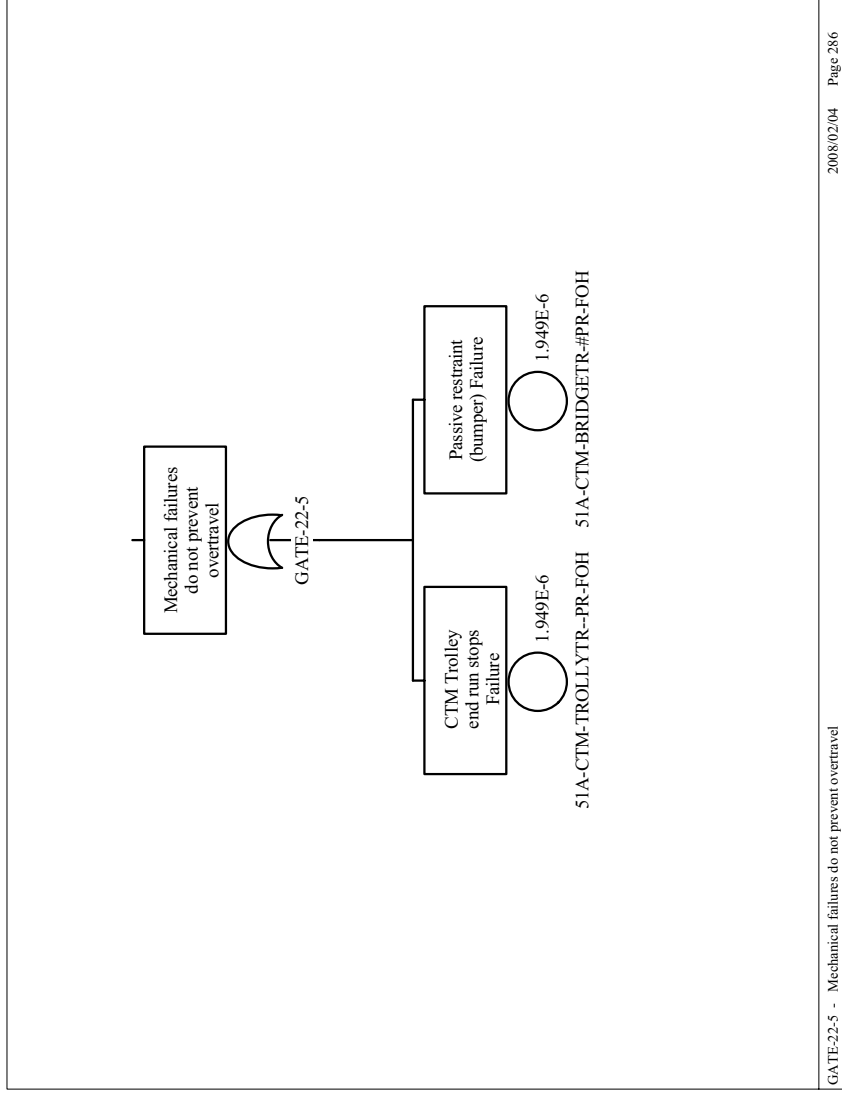
GATE-22-31 - Human related failures

Source: Original

Figure B4.4-37. CTM Collision Sheet 2

B4-74

March 2008

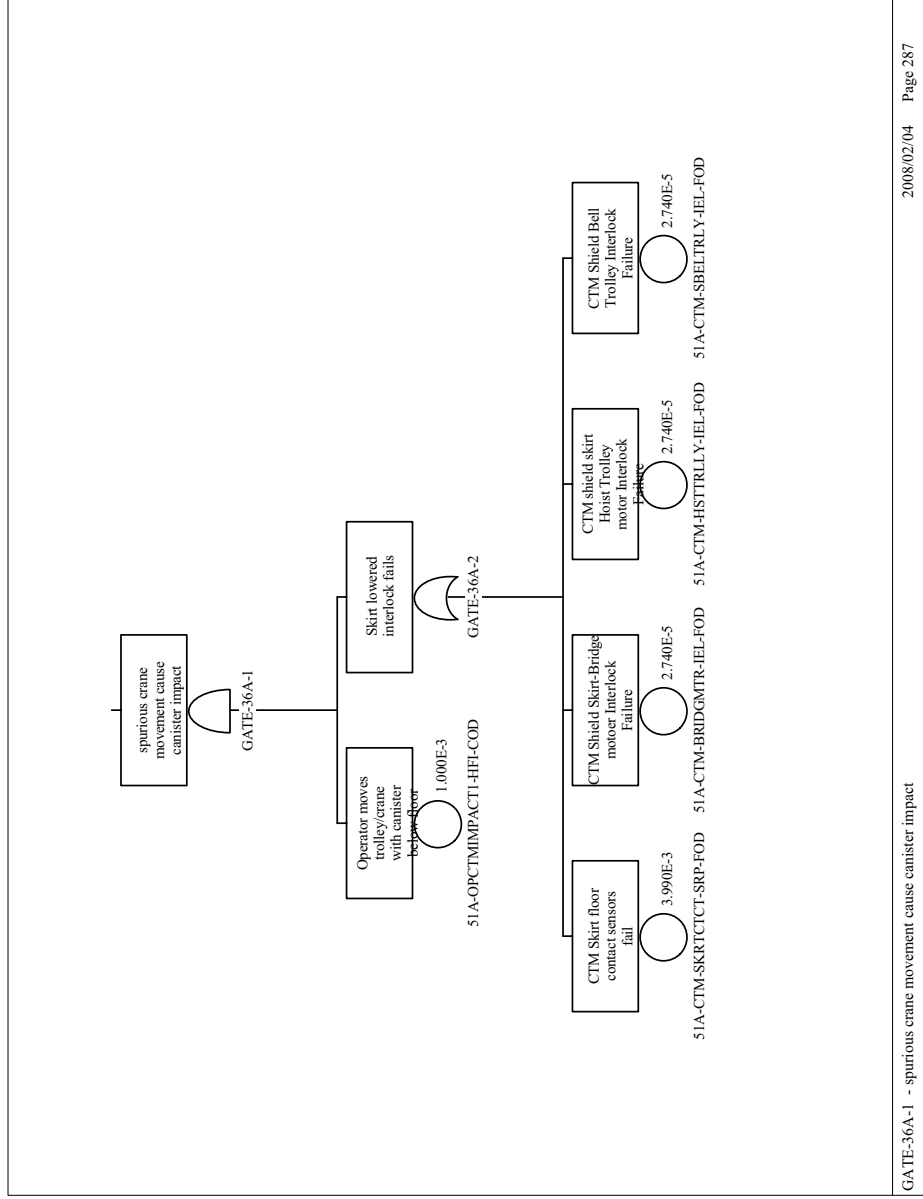


Source: Original

Figure B4.4-38. CTM Collision Sheet 3

B4-75

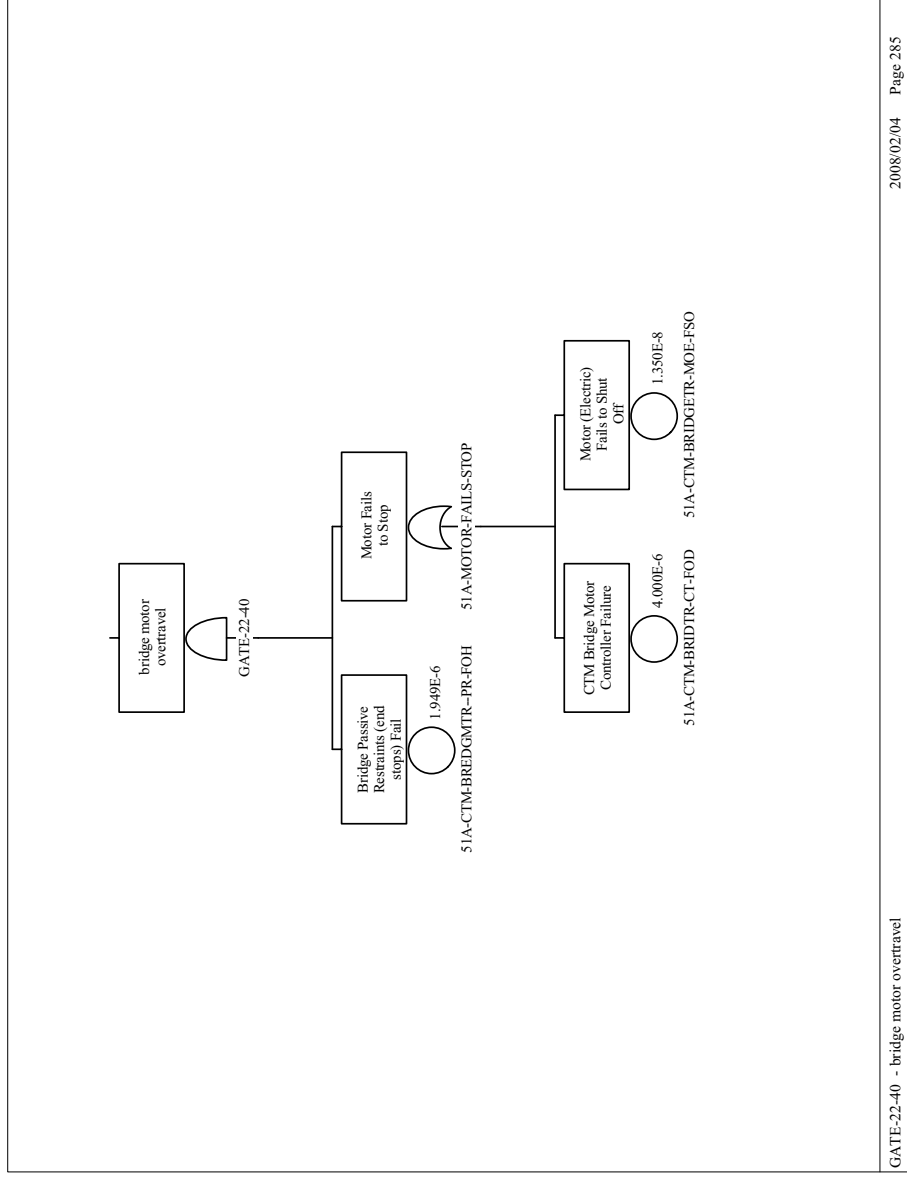
March 2008



GATE-36A-1 - spurious crane movement cause canister impact 2008/02/04 Page 287

Source: Original

Figure B4.4-39. CTM Collision Sheet 4



2008/02/04 Page 285

GATE-22-40 - bridge motor overtravel

Source: Original

Figure B4.4-40. CTM Collision Sheet 5

B4-77

March 2008

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 IHF 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 IHF 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, stops the hoist and erases 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 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 Subjects Canister to Shearing Forces.” 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 IHF.

B4.4.5.5 Basic Event Data

Table B4.4-12 contains a list of basic events used in the “CTM Movement Subjects Canister to Shearing Forces” fault tree. Included are the human failure events and the common-cause failure events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is 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 B4.4-12. Basic Event Probability for the CTM Movement Subjects Canister to Shearing Forces Fault Trees

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	3	5.784E-05	0.000E+00	7.230E-06	8.000E+00
51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
51A-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation - shear	3	6.740E-08	0.000E+00	6.740E-07	1.000E-01
51A-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
51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation - shear	3	3.650E-08	0.000E+00	3.650E-07	1.000E-01
51A-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
51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation - shear	3	3.650E-08	0.000E+00	3.650E-07	1.000E-01
51A-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
51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
51A-OPCTMIMPACT1-HFI-COD	Collision of CTT into Structure	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
	CTT Collides with Shield Door					
	Operator moves trolley/crane with canister below floor					

NOTE: ^a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

The shear impact drop 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.

B4.4.5.5.1 Human Failure Events

One basic event is associated with human error: 51A-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 IHF floors.

B4.4.5.5.2 Common-Cause Failures

No common-cause failures apply to this fault tree.

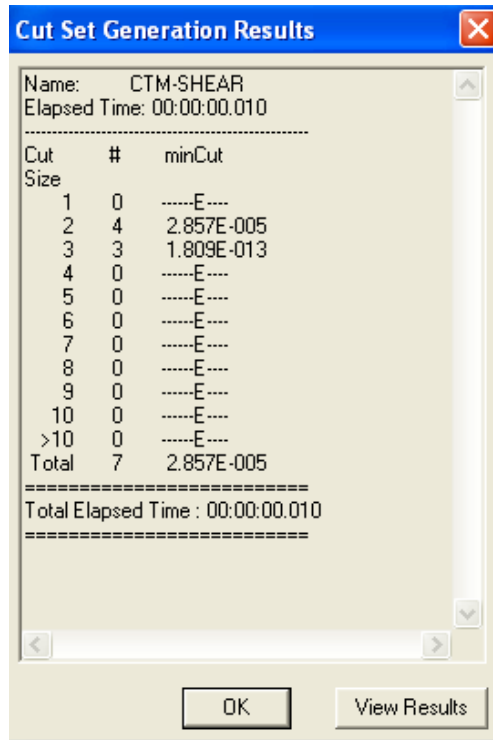
B4.4.5.6 Uncertainty and Cut Set Generation

Figure B4.4-41 contains the uncertainty results obtained from running the fault trees for “CTM Movement Subjects Canister to Shearing Forces” using a cutoff probability of 1E-15. Figure B4.4-42 provides the cut set generation results for the “CTM Movement Subjects Canister to Shearing Forces” fault tree.

Uncertainty Results			
Name	CTM-SHEAR		
Random Seed	1234	Events	11
Sample Size	10000	Cut Sets	7
Point estimate	2.857E-005		
Mean Value	2.830E-005		
5th Percentile Value	3.470E-006		
Median Value	1.742E-005		
95th Percentile Value	8.820E-005		
Minimum Sample Value	2.914E-007		
Maximum Sample Value	6.582E-004		
Standard Deviation	3.532E-005		
Skewness	4.687E+000		
Kurtosis	4.328E+001		
Elapsed Time	00:00:01.090		
OK			

Source: Original

Figure B4.4-41. Uncertainty Results of the CTM Movement Subjects Canister to Shearing Forces Fault Tree



Source: Original

Figure B4.4-42. Cut Set Generation Results for the CTM Movement Subjects Canister to Shearing Forces Fault Tree

B4.4.5.7 Cut Sets

Table B4.4-13 contains the cut sets for the “CTM Movement Subjects Canister to Shearing Forces” fault tree.

Table B4.4-13. Dominant Cut Sets for the CTM Movement Subjects Canister to Shearing Forces Fault Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.98	99.98	2.856E-05	51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1.000E-03
99.99	0.01	1.925E-09	51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			51A-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	6.740E-08
100.00	0.01	1.925E-09	51A-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	6.740E-08

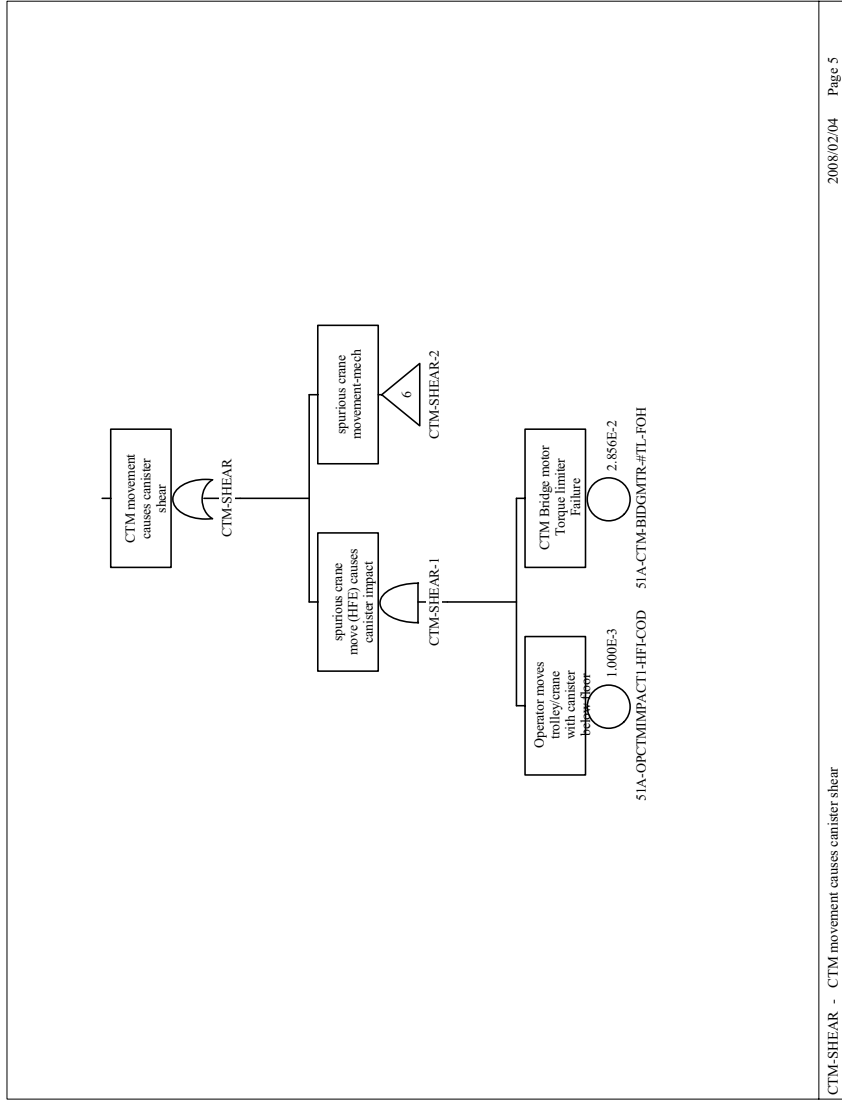
Table B4.4-13. Dominant Cut Sets for the CTM Collision Fault Tree (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
			51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor torque limiter Failure	2.856E-02
100.00	0.01	1.925E-09	51A-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	6.740E-08
			51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.856E-02
100.00	0.00	6.030E-14	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.784E-05
			51A-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3.650E-08
			51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.856E-02
100.00	0.00	6.030E-14	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.784E-05
			51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.856E-02
			51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3.650E-08
100.00	0.00	6.030E-14	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.784E-05
			51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.856E-02
			51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -shear	3.650E-08

NOTE: CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

B4.4.5.8 Fault Tree



2008/02/04 Page 5

CTM-SHEAR - CTM movement causes canister shear

Source: Original

Figure B4.4-43. CTM Shear Sheet 1

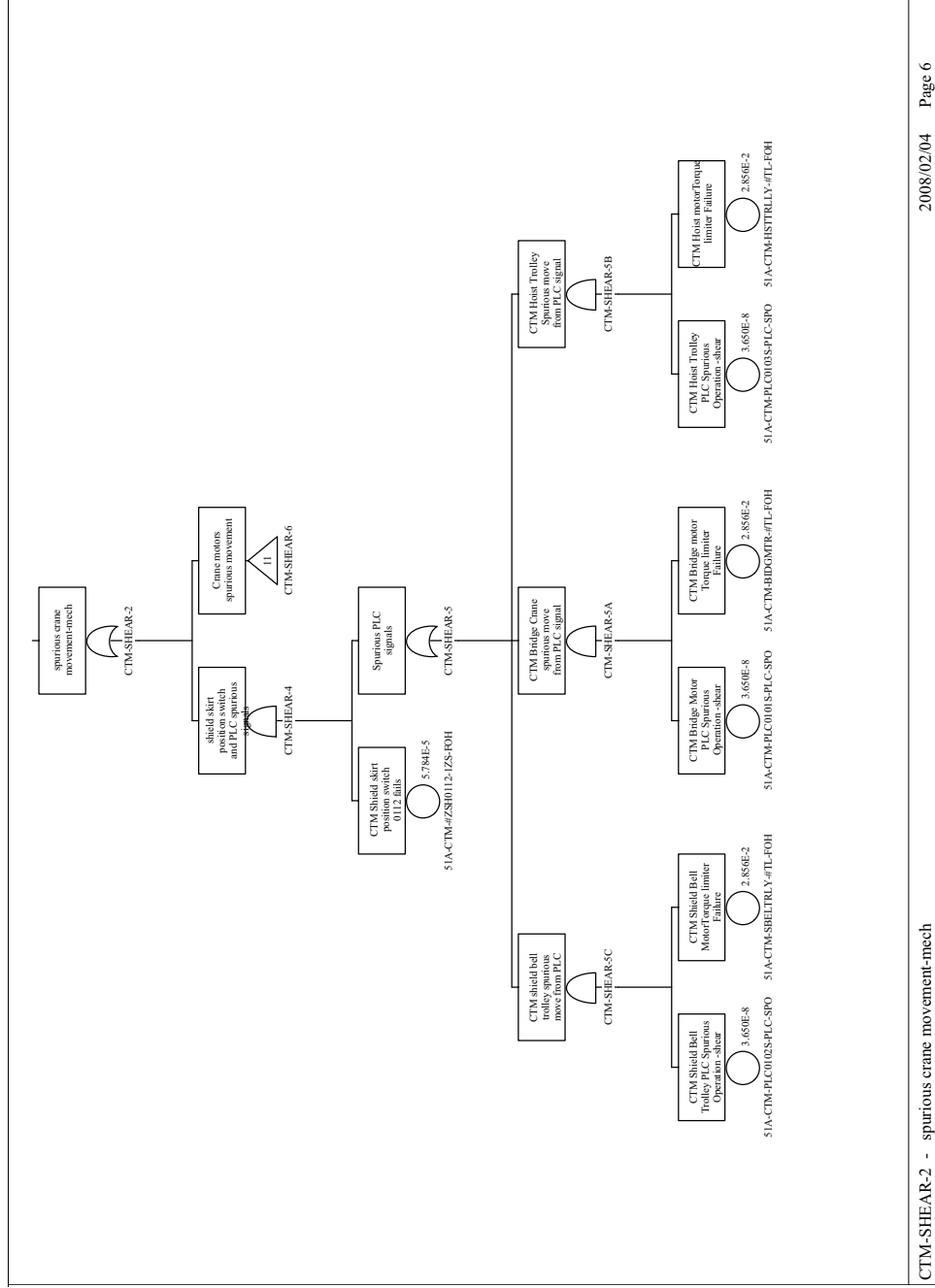
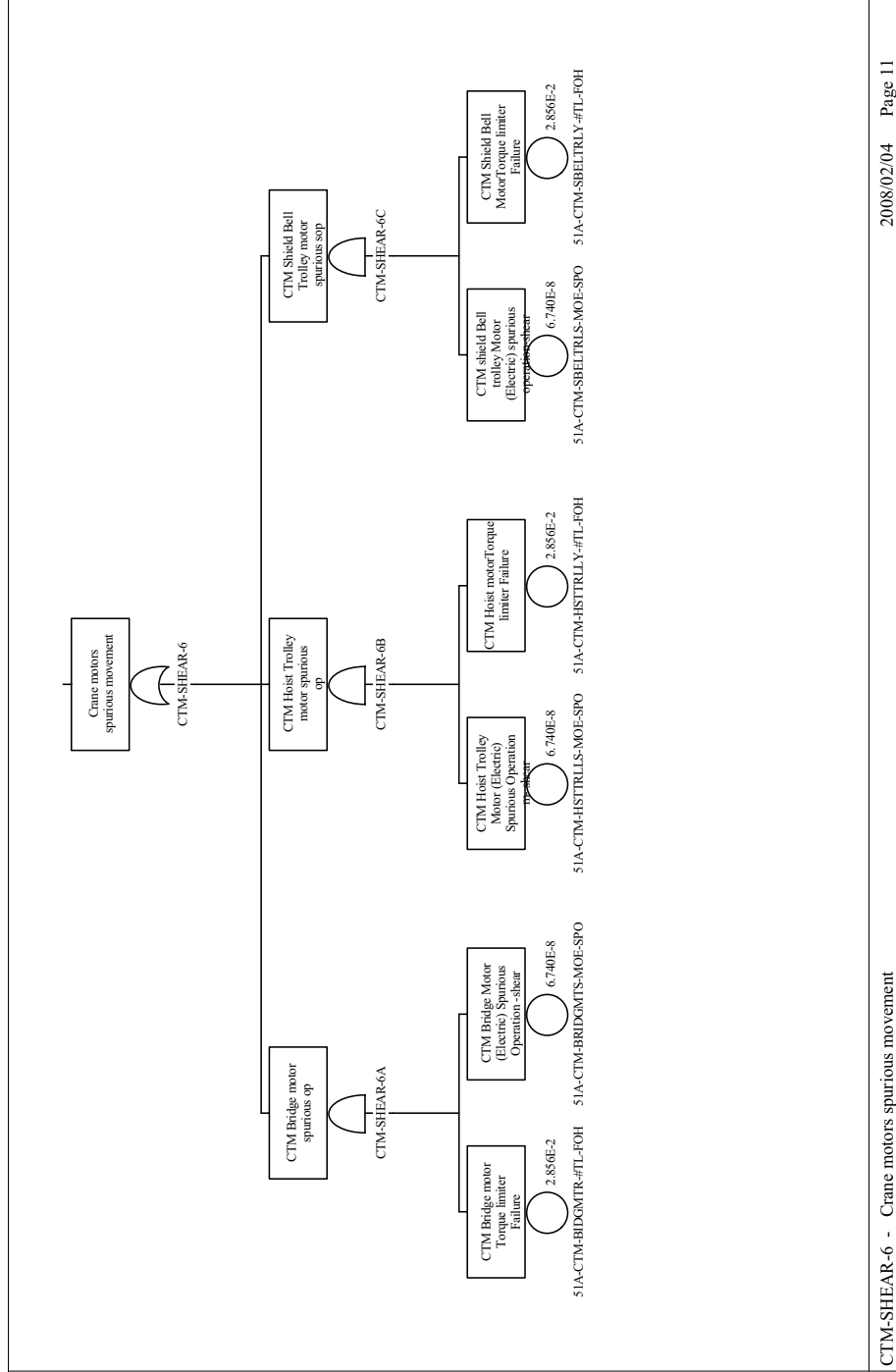


Figure B4.4-44. CTM Shear Sheet 2



Source: Original

Figure B4.4-45. CTM Shear Sheet 3

B5 WASTE PACKAGE TRANSFER TROLLEY ANALYSIS – FAULT TREES

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.

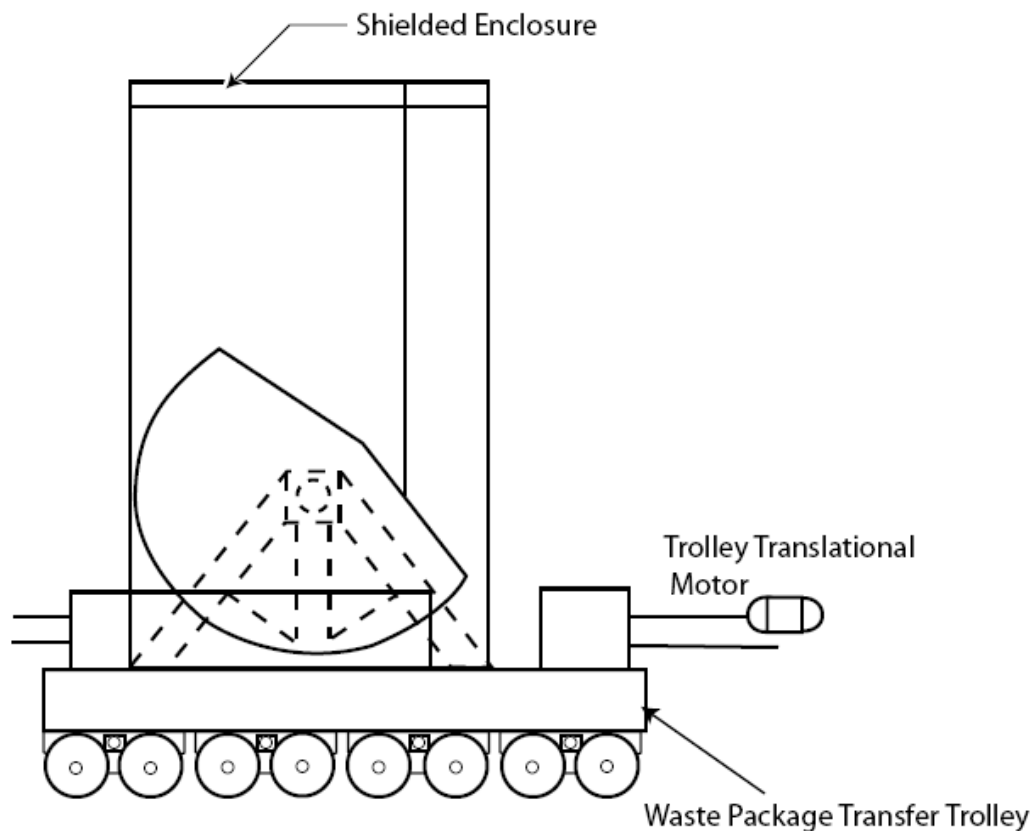
The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

- B5.1.1 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.
- B5.1.2 Not Used.
- B5.1.3 Not Used.
- B5.1.4 BSC 2007. *CRCF and IHF WP Transfer Trolley Process & Instrumentation Diagram*. 000-M60-HL00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0013.
- B5.1.5 *BSC 2007. *CRCF-1 and IHF WP XFR Carriage Docking Sta Mechanical Equipment Envelope Plan, Elevation, & Section*. 000-MJ0-HL00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0018.
- B5.1.6 *BSC 2007. *CRCF and IHF WP XFR Carriage Docking Sta Process & Instrumentation Diagram*. 000-M60-HL00-00301-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0014.
- B5.1.7 BSC 2007. *Mechanical Handling Design Report – Waste Package Transfer Trolley*. 000-30R-WHS0-01200-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0001.
- B5.1.8 *BSC 2007. *Preliminary Throughput Study for the Initial Handling Facility*. 51A-30R-IH00-00100-000. REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0021.
- B5.1.9 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.

B5.1.10 BSC 2008. *Waste Package Transfer Trolley Calculation*. 000-M0C-HL00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080207.0002.

B5.2 SYSTEM DESCRIPTION

This system description is derived from *CRCF and IHF WP XFR Carriage Docking Sta Process & Instrumentation Diagram* (Ref. B5.1.6), *CRCF-1 and IHF WP XFR Carriage Docking Sta Mechanical Equipment Envelope Plan, Elevation, & Section* (Ref. B5.1.5), *CRCF and IHF WP Transfer Trolley Process & Instrumentation Diagram* (Ref. B5.1.4), *Mechanical Handling Design Report – Waste Package Transfer Trolley* (Ref. B5.1.7) and *Waste Package Transfer Trolley Calculation* (Ref. B5.1.10). The Waste Package Transfer Trolley (WPTT), shown in Figure B5.2-1 is an electrically powered machine that is used to transport the waste package containing various waste canisters from the Waste Package Loading Room to the Waste Package Positioning Room and then to the waste package transfer carriage docking station in the Waste Package Loadout Room. The WPTT consists of the trolley and the shielded enclosure that holds the waste package, waste package pallet, waste package transfer carriage, and pedestal. The shielded enclosure acts to minimize radiation to the surroundings. The enclosure pivots between a vertical and horizontal position for waste package loading and unloading. The center of gravity of the shielded enclosure is positioned such that the vertical position is the most stable position.



Source: Derived from (Ref. B5.1.4)

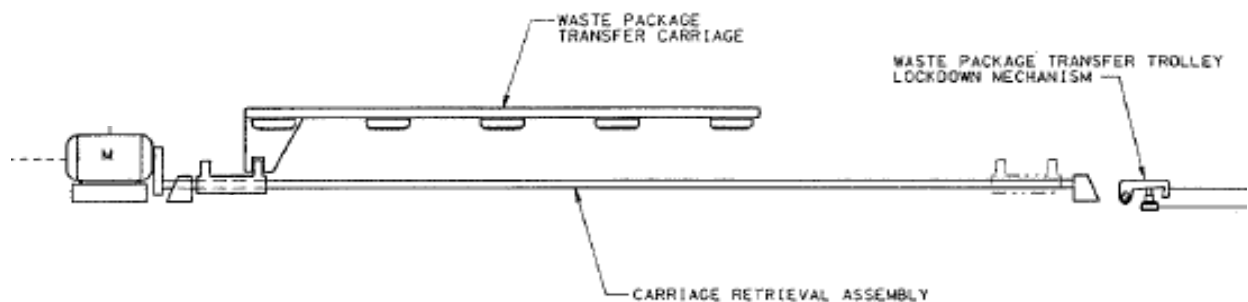
Figure B5.2-1. Waste Package Transfer Trolley

The WPTT travels on rails between the Waste Package Loading Room and the docking station using 24" double-flanged crane wheels. The total travel distance between these rooms is approximately 118 ft. Rail sweeps are used in front of each trolley wheel to brush away any object that might fall onto the trolley rails. The crane rails supporting the WPTT are gapped in multiple locations (as much as 16") to accommodate shield doors between rooms. Power is supplied to the motor by a third rail system and the maximum speed is less than 40 fpm (Ref. B5.1.7, Section 3.2.4) established by the size of the drive motor and the gear drive system. The WPTT includes seismic rail clamps and rails anchored to the floor to ensure the stability of the WPTT during a seismic event.

The rotation of the shielded enclosure, which is also powered by the third rail system, is controlled by two rotation mechanisms, each consisting of a motor and a mechanical worm gear system. Each rotation mechanism is sized to rotate at a rate of 90-degrees per hour (Ref. B5.1.10, Section 6.15), and the worm gear mechanism has the inherent property to self lock to prevent uncontrolled tilt down. Within the shielded enclosure is a pedestal where the waste package sits during transfer operations that allow the waste package to be at the correct height for loading and sealing operations. There are interchangeable pedestals of different sizes which are for the loading operations of different sized waste packages.

The motor power for the trolley and the shielded enclosure is such that the canister cannot be breached through a shear failure in the event of spurious signals during canister transfer into the waste package. Either the drive train or rotational motors trip off before the canister is breached.

The waste package transfer carriage shown in Figure B5.2-2 is a wheeled platform that carries the waste package pallet and waste package. The transfer carriage is moved by a mechanical screw driven carriage retrieval assembly which places the carriage with an empty waste package into the shielded enclosure and retrieves the carriage with a loaded waste package in the Waste Package Loadout Room after the waste package has been loaded and sealed. Once removed from the shielded enclosure, the transport and emplacement vehicle (TEV) is able to pick up the loaded waste package and pallet by lifting features on the waste package pallet.



Source: Derived from (Ref. B5.1.6)

Figure B5.2-2. Waste Package Transfer Carriage

B5.2.1 Control System

Interlocks prevent translational or rotational motion of the WPTT while a canister is being loaded into the waste package (i.e., when the waste package slide gate is open) or while the waste package is being withdrawn from the shielded enclosure on the transfer carriage (Ref. B5.1.6), (Ref. B5.1.9), and (Ref. B5.1.4). The shielded enclosure is not able to rotate in either direction unless the WPTT is locked into the waste package transfer carriage docking station and the waste package carriage retrieval assembly is completely extended or retracted. Interlocks also prevent over-travel of the trolley and travel through portals when the shield doors are closed. Manually actuated, hardwired emergency stop buttons are available at all control locations to allow power to be removed from the drive motors. However, 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. A schematic of the control system and interlocks is shown in Figure B5.2-3.

The following controls are incorporated in the design of the rotation mechanism of the shielded enclosure:

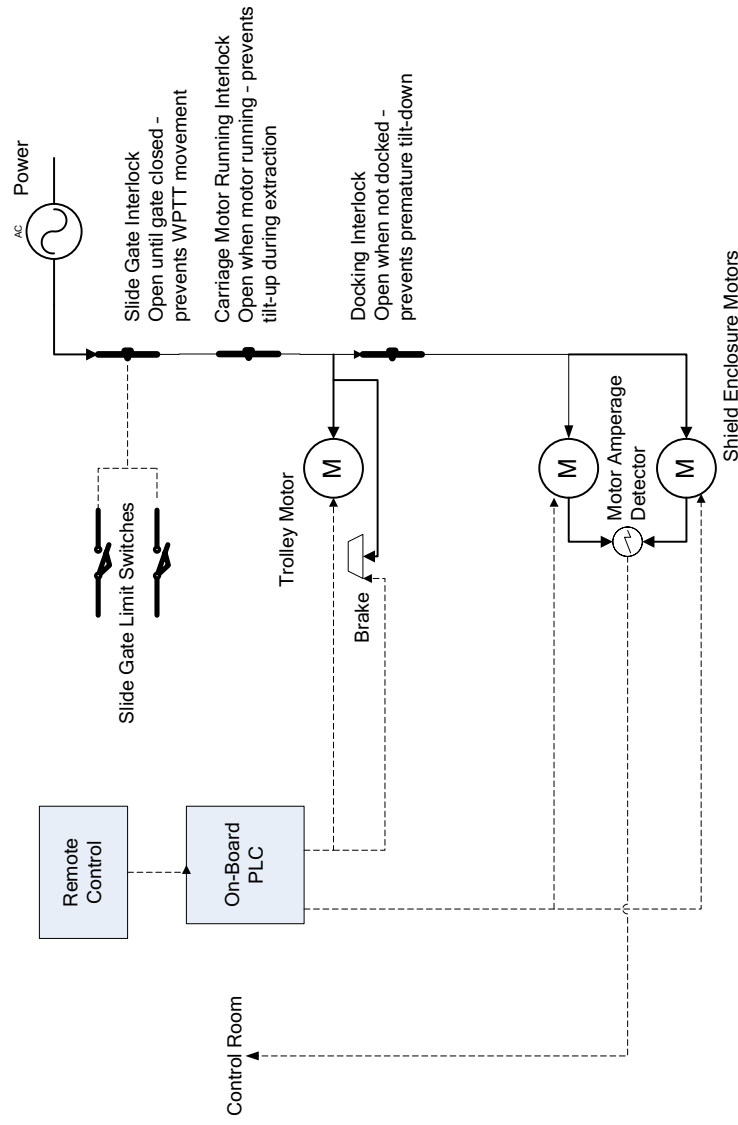
- Rotation start and stop
- End of travel limit switches
- Motor amperage readout
- Interlocks to prevent movement of the shielded enclosure unless the trolley is locked down at the docking station and the waste package carriage retrieval assembly is completely extended or retracted.

The following controls are provided for operation of the trolley system:

- Trolley start (forward and reverse) and stop
- Forward and reverse end of travel limit switches
- Motor amperage readout
- Forward and reverse range detectors, interlocked with the motors through a PLC
- Interlock to prevent movement of the trolley when the waste package slide gate is opened
- Position indication along the travel rail.

The following controls are provided for operation of the docking station system:

- Waste package retrieval system start (forward and reverse) and stop
- Raise and lower motions for the WPTT locking mechanisms
- Interlock between the locking mechanisms and the shielded enclosure to prevent unlocking the trolley from the docking station unless the enclosure is in the vertical position
- Interlock between the retrieval system and the power feed to the WPTT to prevent operation of the WPTT during waste package retrieval
- Motor amperage readout
- Position indication of the waste package as it is being retrieved from the WPTT.



NOTE: AC = alternating current; M = motor; PLC = programmable logic controller; WPTT = waste package transfer trolley.

Source: Original

Figure B5.2-3. Schematic of the Waste
Package Transfer Trolley
Control System

B5.2.2 Operation

B5.2.3 Initial Conditions

The waste package loading operation begins with an empty waste package being loaded into the WPTT on the pallet while the WPTT is locked into the waste package transfer carriage docking station and in the horizontal position. The transfer carriage with an empty waste package on the pallet is moved into the shielded enclosure of the WPTT via the waste package transfer carriage docking station's waste package retrieval assembly. Once the retrieval assembly is fully extended and the carriage and empty waste package are positioned within the WPTT, the shielded enclosure is rotated into the vertical position. A visual inspection of the waste package is then performed to ensure the positioning is correct within the shielded enclosure. When the waste package is correctly placed in the vertically oriented shielded enclosure the shield ring is lowered and locked into position on top of the shielded enclosure by the waste package handling crane equipped with the shield ring lift beam. Again a visual inspection is performed to ensure the shield ring is properly seated.

The WPTT is unlocked from the waste package transfer carriage docking station and is remotely driven into the Waste Package Loading Room. The WPTT is situated so that the empty waste package is directly beneath the center of the slide gate which separates the Waste Package Loading Room and Canister Transfer Area.

B5.2.4 Waste Package Loading

Once in position in the loading room, the slide gate is opened to allow the waste canister(s) to be lowered into the empty waste package using the canister transfer machine (CTM). The waste is contained in canisters during the entire process; these canisters are either HLW canisters or naval canisters.

B5.2.5 Waste Package Transfer

After the waste package is loaded and the slide gate closed, an operator in the control room provides power to the WPTT to move it to the Waste Package Positioning Room.

B5.2.6 Waste Package Closure

After the waste package is loaded and the slide gate closed, the WPTT moves to the Waste Package Positioning Room. The WPTT is positioned under the opening to the Waste Package Closure Room so that the top of the waste package is accessible through the opening. At this station the inner lid is placed on the waste package, welded in place, and the weld's integrity inspected. The air within the waste package is replaced by helium with a helium purging operation. Once the inner lid is inspected for leakage, the outer lid is positioned and welded in place. The welds of the outer lid are inspected to ensure the waste package is properly sealed.

B5.2.7 Waste Package Transfer Trolley Loadout

After the waste package is sealed, the WPTT is moved into the Waste Package Loadout Room where it is locked into the waste package transfer carriage docking station. The shield ring is remotely removed with the waste package handling crane and the shielded enclosure is rotated into the horizontal position. The waste package carriage retrieval assembly engages the carriage interface and retracts guiding the carriage and waste package out of the shielded enclosure. During the transfer from the WPTT to the TEV, video cameras allow operators to inspect the waste package surface for damage. The waste package is positioned such that the TEV is able to lift the waste package and pallet off the carriage. From here the TEV transports the waste package into the repository for emplacement.

Upon the WPTT reaching the loadout area, the TEV is in place and the carriage retrieval assembly is completely retracted. The WPTT links to the docking mechanism of the waste package retrieval system closing an interlock and allowing the shielded enclosure to be rotated to the horizontal position. The retrieval system links with the carriage assembly within the shielded enclosure. During extraction of the waste package carriage an interlock interrupts the power feed to the WPTT to prevent operation of the WPTT during the retrieval operation. When the carriage retrieval system is fully retracted the waste package has been removed from the shielded enclosure, an interlock is closed, and the shielded enclosure can now be raised to the vertical position. When the enclosure is vertical, the trolley can be unlocked from the docking station and moved back.

B5.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

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 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

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environmental	Spatial	Human	External Events
Electric Power	Provides motive force	—	—	—	—
Trolley motor and gear drive	Limits maximum speed	—	—	—	—
Shielded enclosure motor and gear drive	Limits rotational speed and prevents slapdown	—	—	—	—
Interlocks	Prevents spurious movement	—	—	—	Fire or explosion can cause loss of power

Table B5.3-1. Dependencies and Interactions Analysis (Continued)

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environmental	Spatial	Human	External Events
Rails	Prevents movement in wrong direction	—	—	—	—
Control room	Controls direction and speed and initiates movement	—	—	Wrong instructions	Fire or explosion can cause loss of power
Emergency stop	Stops WPTT	—	—	Fail to energize	
Structure	Constrains and supports canisters and WP	—	—		Seismic causes impact
Shield door	Opens for WPTT to pass through	—	—	Close door inadvertently	Closes on WPTT

NOTE: WP = waste package; WPTT = waste package transfer trolley.

Source: Original

B5.4 RELATED FAILURE SCENARIOS

There are five fault trees associated with the WPTT:

1. Spurious movement of the WPTT in the loading area while loading the waste package with canisters—while loading a cask onto the WPTT, and spurious movement into the Waste Package Loadout Room while extracting the waste package carriage from the shielded enclosure.
2. Impact of the WPTT with a structure—while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
3. Derailment of the WPTT—while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
4. Premature tiltdown of the WPTT—premature tiltdown of the shielded enclosure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
5. Malfunction of WPTT or waste package transfer carriage—while extracting the carriage and waste package from the shielded enclosure at the Waste Package Loadout Room.

An additional fault tree associated with damage to the waste package at the positioning and closure area satisfies ESD-09 and is also described in Attachment A and B6. These fault trees involve waste package failure due to the welding process or drop of an object on the WP.

In all cases a conservative mission time of 1 hour per canister was used for canister and waste package transfers through the process for each fault tree. The time required to lower a canister into the waste package by the CTM is approximately 20 minutes, the time required to move the trolley from the loading area to the positioning area and then to the Waste Package Loadout Room is approximately 35 minutes, and the time required to extract the carriage from the shielded enclosure is also approximately 15 minutes (Ref. B5.1.8, Appendix A). Therefore, a one hour mission time is considered a conservative value for each fault tree.

Although the time in the Waste Package Positioning Room is approximately 40 hours, there are no WPTT failures that would damage the canister in this area.

B5.4.1 Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

B5.4.1.1 Description

This fault tree describes spurious movement of the WPTT during canister loading of the waste package to satisfy ESD-07, pivotal event “Canister Impact due to Movement of CTM, CTT, or WPTT During Lift.” The top event is “Spurious Movement of the WPTT While Loading the Waste Package with Canisters” which is defined as unplanned movement of the WPTT while canisters are being loaded into the waste package. This fault tree is shown in Figures B5.4-3, B5.4-4, B5.4-5 and B5.4-6.

Spurious movement may involve movement of the trolley or the shielded enclosure and may be caused by multiple equipment failures, or by a combination of equipment failure and operator error. For equipment failures to cause spurious movement the controls (remote or on-board) must emit a spurious signal, and the gate interlocks must fail for trolley movement, or the gate and docking interlocks must fail for shielded enclosure movement. For the operator to initiate spurious movement, the interlocks must fail as described above for the trolley or shielded enclosure to move.

B5.4.1.2 Success Criteria

Success criteria for loading a canister onto the shielded enclosure of the WPTT at the loading area require that the WPTT remain stationary during these operations. Interlocks prevent rotational movement of the shielded enclosure unless the trolley is locked down at the docking station in the Waste Package Loadout Room, and port slide gate interlocks interrupt all power to the WPTT to prevent any movement of the trolley or shielded enclosure when the slide gate is opened.

B5.4.1.3 Design Requirements and Features

Design features include the interlock that interrupts all power to the WPTT when it is in the loading room, and the slide gate interlocks that interrupt all power to the WPTT while the slide gate is open during the canister loading process. The docking interlock is another feature that prevents rotation of the shielded enclosure unless the WPTT is at the docking station in the Waste Package Loadout Room.

Requirements include sizing of the motor and gearing system such that the canister cannot be breached through a shear failure in the event of spurious signals during canister transfer into the waste package. Either the drive train or rotational motors must trip before the canister is breached

B5.4.1.4 Fault Tree Model

The top event in Figure B5.4-3 is spurious movement of the WPTT during the canister loading process. This may occur due to initiation of a spurious signal due to equipment failure or operator error coupled with the failure of an interlock that interrupts all power to the WPTT while the WPTT is in the loading position. Power can be provided to the WPTT only through operator action to reset the interlock after loading is completed.

Spurious movement due to equipment failure, shown in Figures B5.4-4 and B5.4-5, may occur from initiation of spurious signals from the control system and failure of the gate and docking interlocks. Failure modes of the gate interlocks are shown in Figure B5.4-6.

B5.4.1.5 Basic Events

Basic events for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters” are shown in Table B5.4-1.

Table B5.4-1. Basic Event Probabilities for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-WPTT-IME001--IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-WPTT-ZS000---ZS--CCF	1	1.380E-005	1.380E-005	0.000E+000	0.000E+000
51A-WPTT-ZS001---ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
51A-WPTT--ZS002--ZS--FOD	1	2.930E-004	2.930E-004	0.000E+000	0.000E+000
51A-OPTILTDOWN01-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
51A-PWRPRTGATINT-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-WPTT--HC001--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-WPTT-HC002-HC-SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-WPTT-IELDK3--IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-WPTT-PLC001-PLC-SPO	3	3.650E-007	0.000E+000	3.650E-007	1.000E+000
51A-WPTT-PLC002-PLC-SPO	3	3.650E-007	0.000E+000	3.650E-007	1.000E+000
51A-OPWPTTSPUR01-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

B5.4.1.5.1 Human Failure Events

Two operator errors involve initiation of spurious movement of the trolley 51A-OPWPTTSPUR01-HFI-NOD or shielded enclosure 51A-OPTILTDOWN01-HFI-NOD which involves initiation of a tiltdown.

B5.4.1.5.2 Common-Cause Failure

One common-cause failure (CCF) was added to the tree to account for failure of both gate closed limit switches. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criteria (Table C3-1, CCCF = 2).

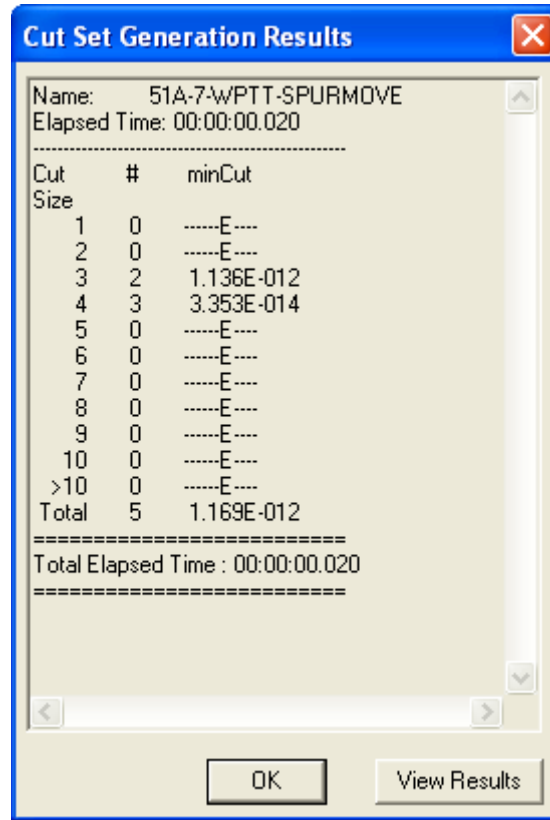
B5.4.1.6 Uncertainty and Cut Set Generation

Figure B5.4-1 contains the uncertainty results obtained from running the fault trees for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters” using a cutoff probability of 1E-15. Figure B5.4-2 provides the cut set generation results for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters”.

Uncertainty Results			
Name	51A-7-WPTT-SPURMOVE		
Random Seed	1234	Events	8
Sample Size	10000	Cut Sets	5
Point estimate	1.169E-012		
Mean Value	2.835E-012		
5th Percentile Value	1.399E-014		
Median Value	3.341E-013		
95th Percentile Value	8.902E-012		
Minimum Sample Value	2.220E-016		
Maximum Sample Value	3.417E-009		
Standard Deviation	3.673E-011		
Skewness	8.157E+001		
Kurtosis	7.485E+003		
Elapsed Time	00:00:00.820		
OK			

Source: Original

Figure B5.4-1. Uncertainty Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters



Source: Original

Figure B5.4-2. Cut Set Generation Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

B5.4.1.7 Cut Sets

Table B5.4-2 contains the cut sets for spurious movement of the WPTT during canister loading. The total probability per cask loading is 1.169E -12.

Table B5.4-2. Cut Sets for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-7-WPTT-SPURMOVE	64.68	7.563E-013	51A-OPWPTTSPUR01-HFI-NOD	Operator initiates Spurious Movement of Trolley	1.0E-003
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT-IME001--IEL-FOD	Interlock Failure on Demand	2.8E-005
	32.46	3.795E-013	51A-OPWPTTSPUR01-HFI-NOD	Operator initiates Spurious Movement of Trolley	1.0E-003

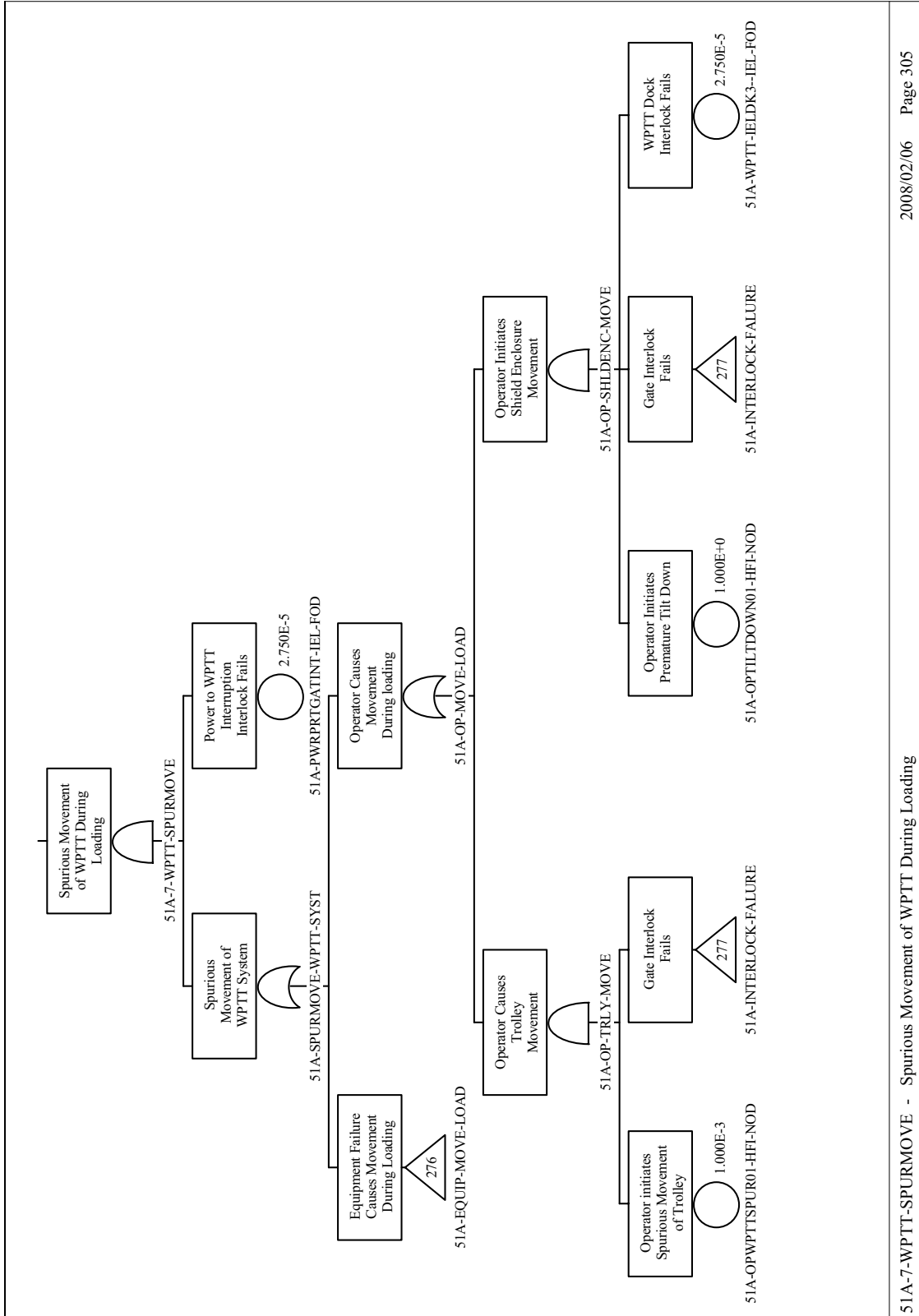
Table B5.4-2. Cut Sets for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT-ZS000---ZS--CCF	CCF of Gate Closed Limit Switches	1.4E-005
	1.78	2.080E-014	51A-OPTILTDOWN01-HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT-IELDK3--IEL-FOD	WPTT Dock Interlock Fails	2.8E-005
			51A-WPTT-IME001--IEL-FOD	Interlock Failure on Demand	2.8E-005
	0.89	1.044E-014	51A-OPTILTDOWN01-HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT-IELDK3--IEL-FOD	WPTT Dock Interlock Fails	2.8E-005
			51A-WPTT-ZS000---ZS--CCF	CCF of Gate Closed Limit Switches	1.4E-005
	0.20	2.361E-015	51A-OPWPTTSPUR01-HFI-NOD	Operator initiates Spurious Movement of Trolley	1.0E-003
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT--ZS002--ZS--FOD	Gate Closed Limit Switch #2 Spurious Transfer	2.9E-004
			51A-WPTT-ZS001---ZS--FOD	Gate Closed Limit Switch #1 Spurious Transfer	2.9E-004
		1.169E-012	= Total		

NOTE: CCF = common-cause failure; Freq. = frequency; Prob. = probability; WPTT = waste package transfer trolley.

Source: Original

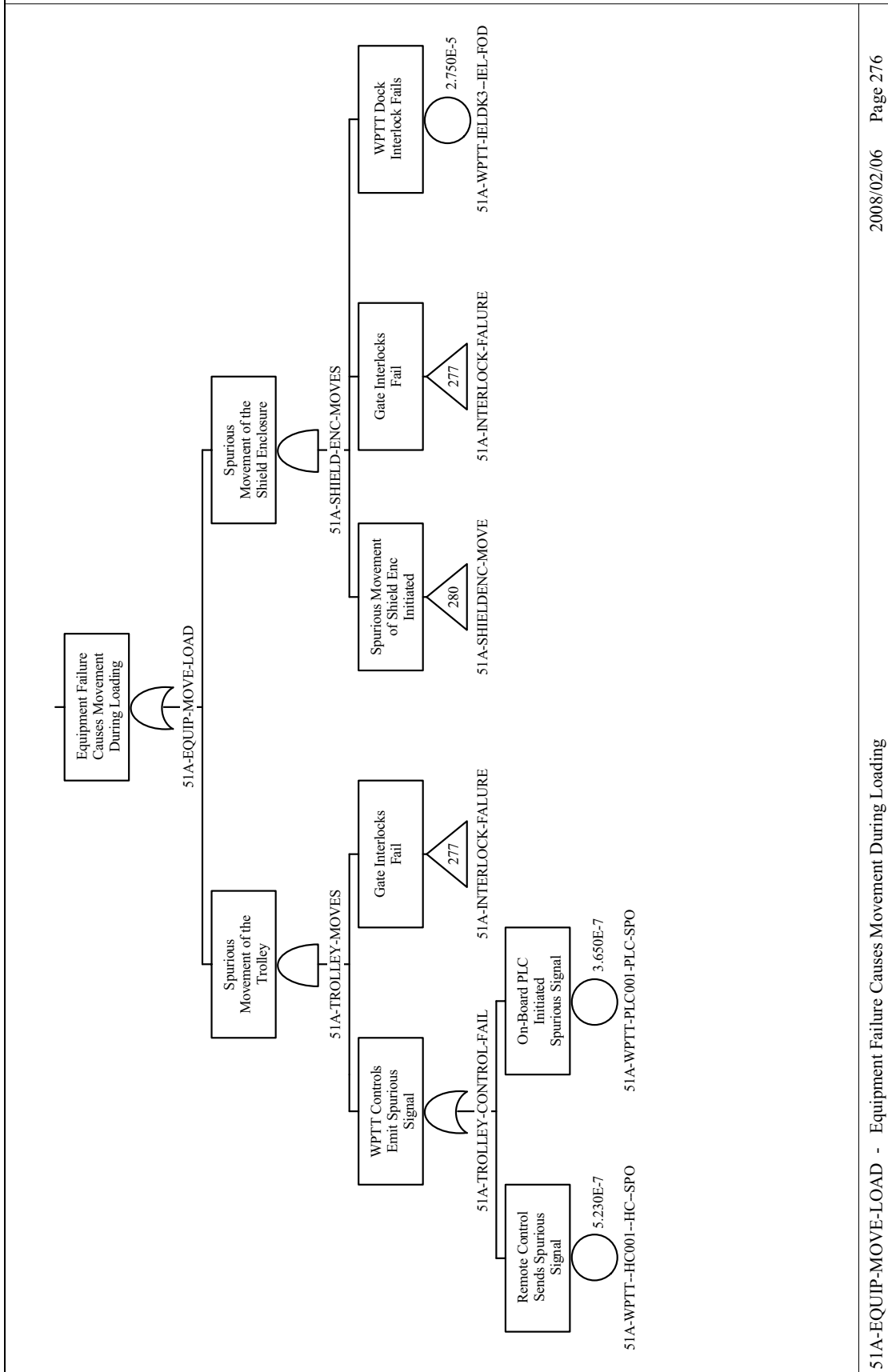
B5.4.1.8 Fault Tree



51A-7-WPTT-SPURMOVE - Spurious Movement of WPTT During Loading 2008/02/06 Page 305

Source: Original

Figure B5.4-3. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

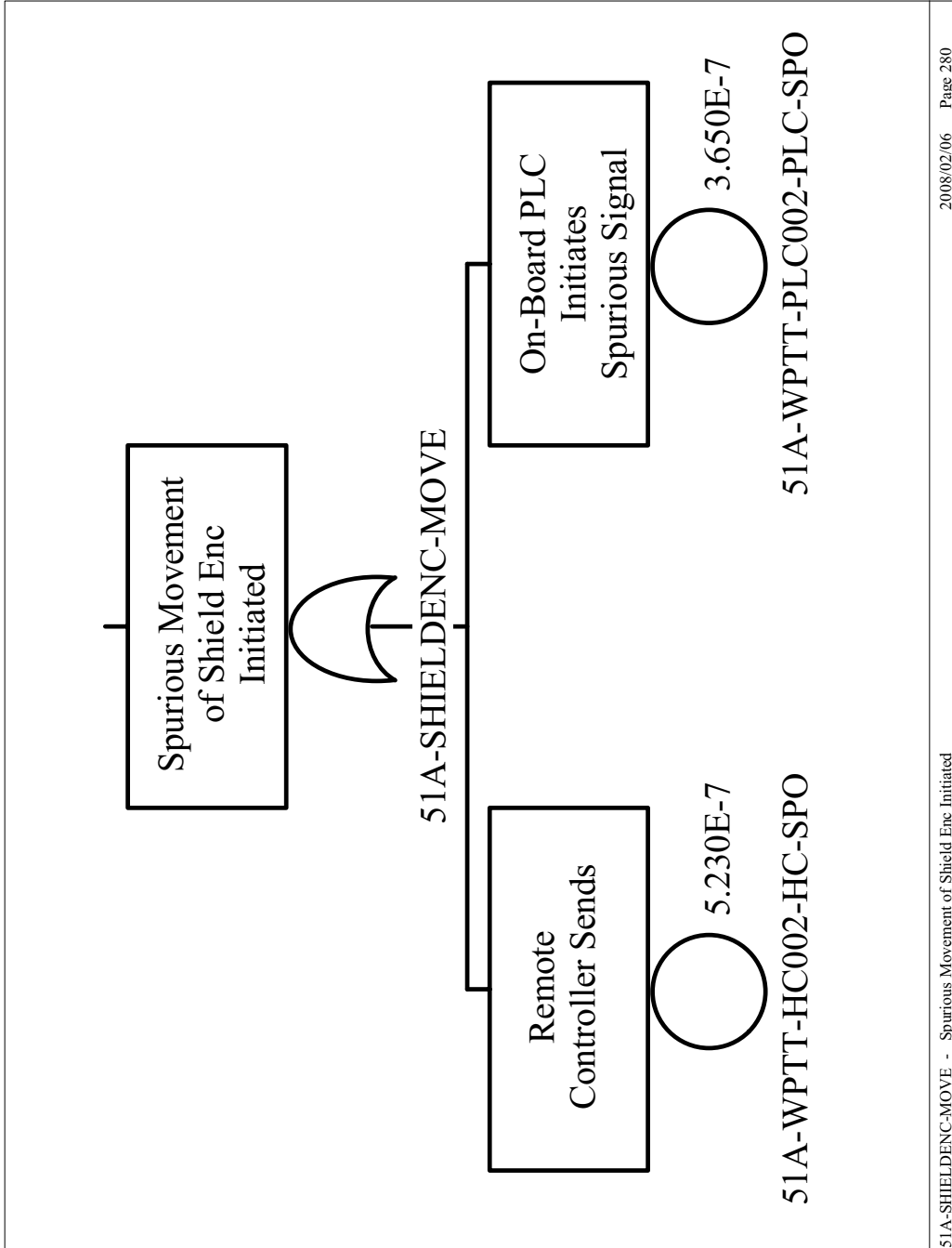


2008/02/06 Page 276

51A-EQUIP-MOVE-LOAD - Equipment Failure Causes Movement During Loading

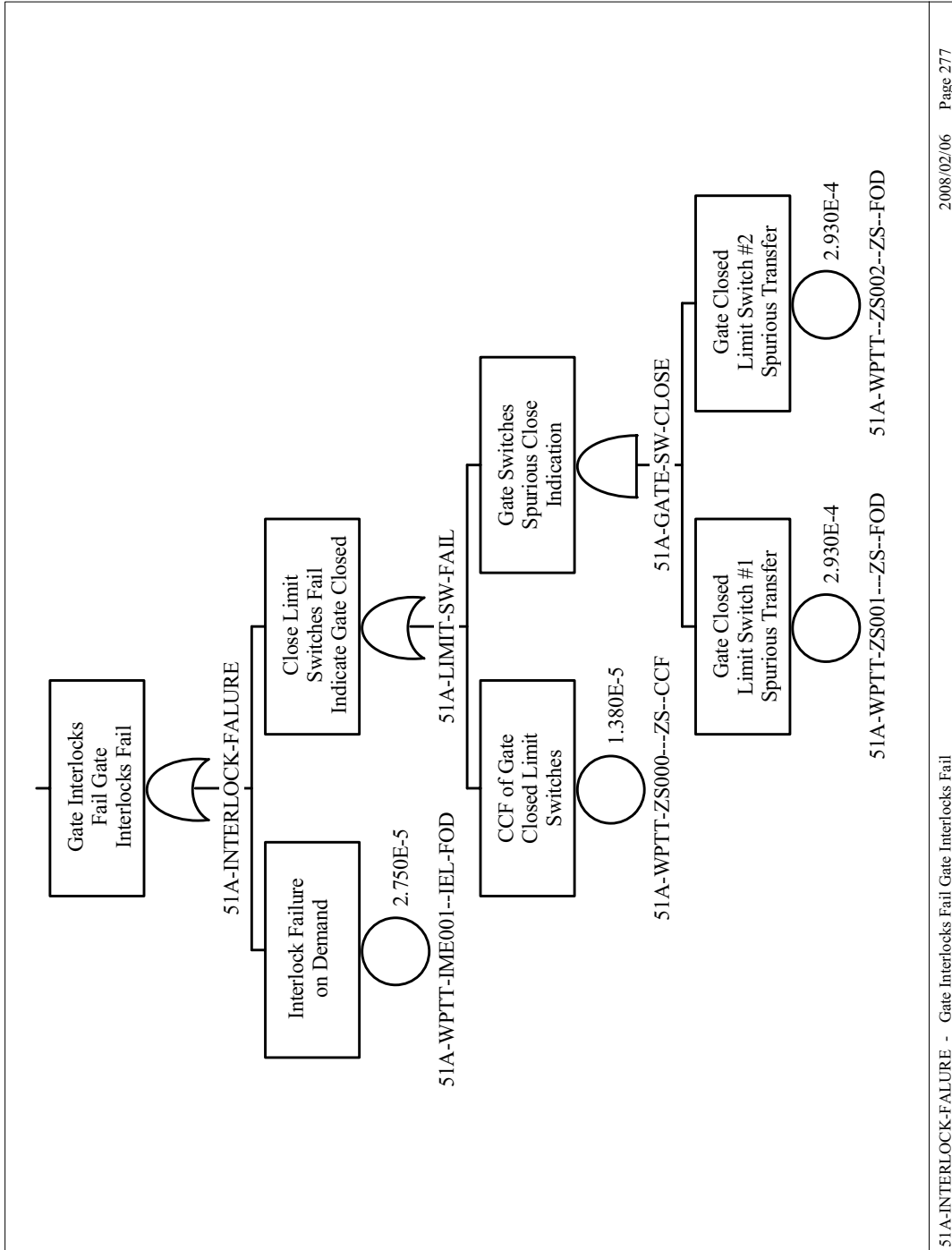
Source: Original

Figure B5.4-4. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters
(Continued)



Source: Original

Figure B5.4-5. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued)



2008/02/06 Page 277

51A-INTERLOCK-FALURE - Gate Interlocks Fail Gate Interlocks Fail

Source: Original

Figure B5.4-6. Fault Tree for Spurious Movement of the WPPT in the Loading Area While Loading the Waste Package with Canisters (Continued)

B5.4.2 Impact of the WPTT with a Structure

B5.4.2.1 Description

This fault tree considers the potential for the WPTT to collide with a structure or object while moving the waste package from the loading area to the positioning area to satisfy ESD-08 pivotal event “Collision of WPTT with facility structure or equipment.” The top event is “WPTT Collides Trip Loading Rm to Positioning RM.” This fault tree is shown in Figures B5.4-9 and B5.4-10.

The fault tree is more general than the name of the top event implies. The same fault tree considers the potential for the WPTT to collide into a structure or object while moving the waste package from the Waste Package Positioning Room to the docking station to satisfy ESD-10, pivotal event “WPTT Collision.”

Two primary causes of a collision are operator initiated (possibly through inattention) or failure of the WPTT to stop. Movement in the wrong direction as a contributing factor is negated by the use of rails forcing the WPTT to only move forward and backward. A runaway condition is prevented by the sizing of the electrical motor and drive gears to limit the speed to less than 40 fpm.

Failure to stop requires failure of the brake or failure of the motor to shut off. The emergency stop buttons in the control room 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.

B5.4.2.2 Success Criteria

Success criteria for moving the WPTT with a waste package from the loading area to the Waste Package Positioning Room and then to the Waste Package Loadout Room requires the WPTT travel at a speed no greater than 40 fpm and the operator be in control and able to stop the WPTT as required. The WPTT is stopped to prevent a collision into a closed shield door or other object by the operator speed controls in the control room, or by the emergency stop buttons in the control room that remove power to the WPTT. When moving the waste package between the loading area and the Waste Package Loadout Room, movement in the wrong direction is prevented by the rails on which the WPTT travels. This forces the WPTT to move only in a straight line forward and backward between the two areas. Runaway of the WPTT is prevented by the limited motor power and gear drive system such that the maximum speed allowable is less than 40 fpm.

B5.4.2.3 Design Requirements and Features

The design feature is the size of the motor that limits the speed of the WPTT to 40 fpm. The requirement is that the speed of the WPTT does not exceed 40 fpm.

B5.4.2.4 Fault Tree Model

The fault tree is shown in Figures B5.4-9 and B5.4-10. The top event is “WPTT Collides Trip Loading Rm to Positioning RM” and may be caused by operator error of failure to stop. Failure to stop may be caused by equipment failure shown in Figure B5.4-10.

B5.4.2.5 Basic Event Data

Table B5.4-3 contains a list of basic events used in the fault tree for an impact of the WPTT with a structure while moving the waste package from the loading area to the loadout room.

Table B5.4-3. Basic Event Probabilities for Impact of the WPTT with a Structure

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-WPTT-BRK401--BRK-FOD	1	1.460E-006	1.460E-006	0.000E+000	0.000E+000
51A-WPTT-MOE001-MOE-FSO	3	1.350E-008	0.000E+000	1.350E-008	1.000E+000
51A-OPWPCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	0.000E+000	0.000E+000

NOTE: ^aFor 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

B5.4.2.5.1 Human Failure Events

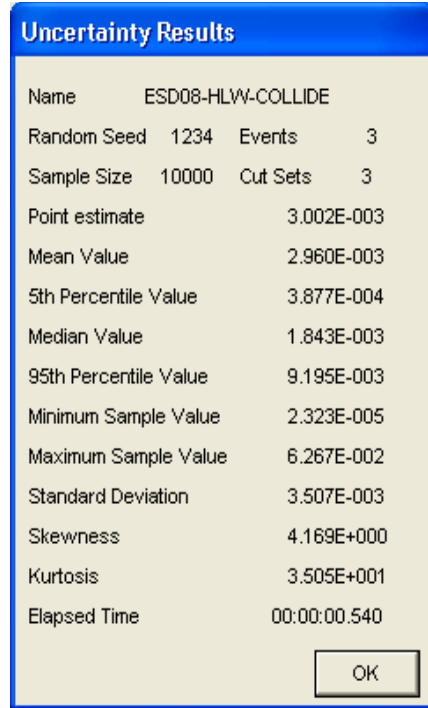
One operator error (51A-OPWPCOLLIDE1-HFI-NOD) involves causing a collision of the WPTT.

B5.4.2.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

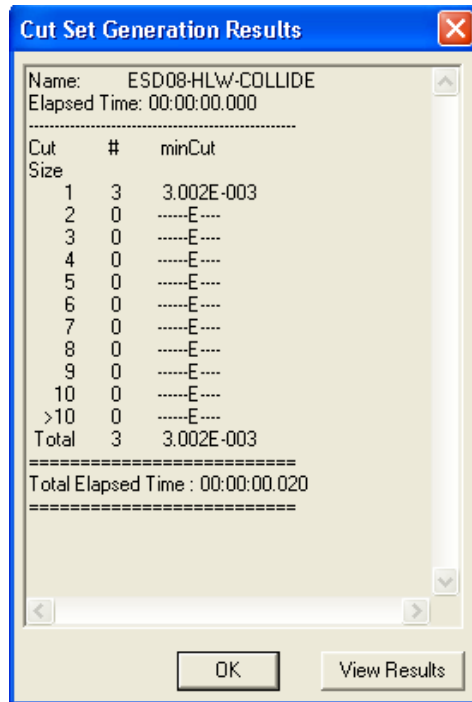
B5.4.2.6 Uncertainty and Cut Set Generation

Figure B5.4-7 contains the uncertainty results for impact of the WPTT with a structure using a cutoff probability of 1E-15. Figure B5.4-8 provides the cut set generation results for impact of the WPTT with a structure during movement.



Source: Original

Figure B5.4-7. Uncertainty Results for Impact of the WPTT with a Structure Fault Tree



Source: Original

Figure B5.4-8. Cut Set Generation Results for Impact of the WPTT with a Structure Fault Tree

B5.4.2.7 Cut Sets

Table B5.4-4 contains the cut sets for impact of the WPTT with a structure during waste package transfer. The total probability per cask is 3.002E-003 with operator error the dominant cause of collision.

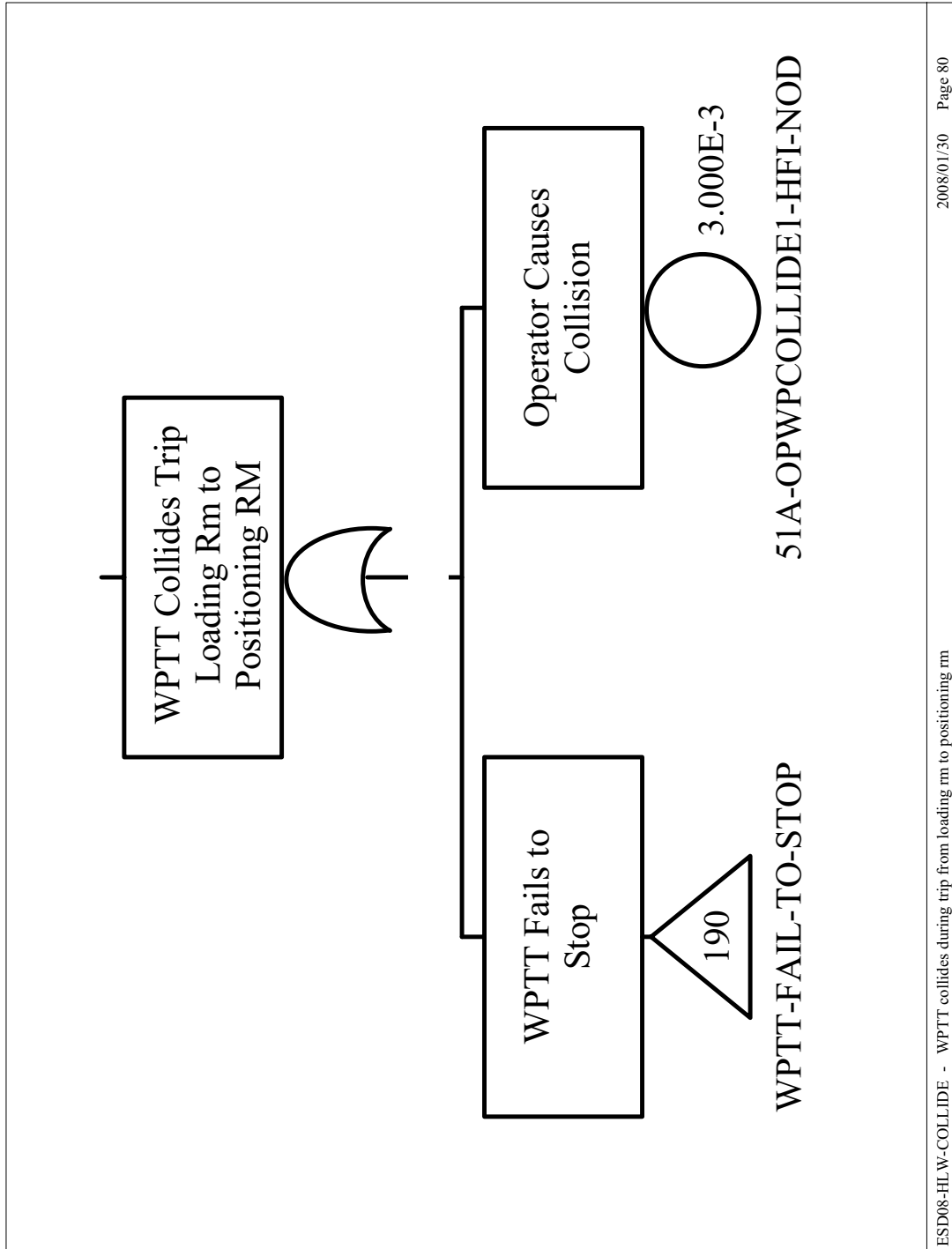
Table B5.4-4. Cut Sets for Impact of the WPTT with a Structure

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW-COLLIDE	99.95	3.000E-003	51A-OPWPCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	0.05	1.460E-006	51A-WPTT-BRK401--BRK-FOD	Brakes Fail	1.5E-006
	0.00	1.350E-008	51A-WPTT-MOE001-MOE-FSO	Motor (Electric) Fails to Shut Off	1.4E-008
		3.002E-003	= Total		

NOTE: Freq. = frequency; Prob. = probability.

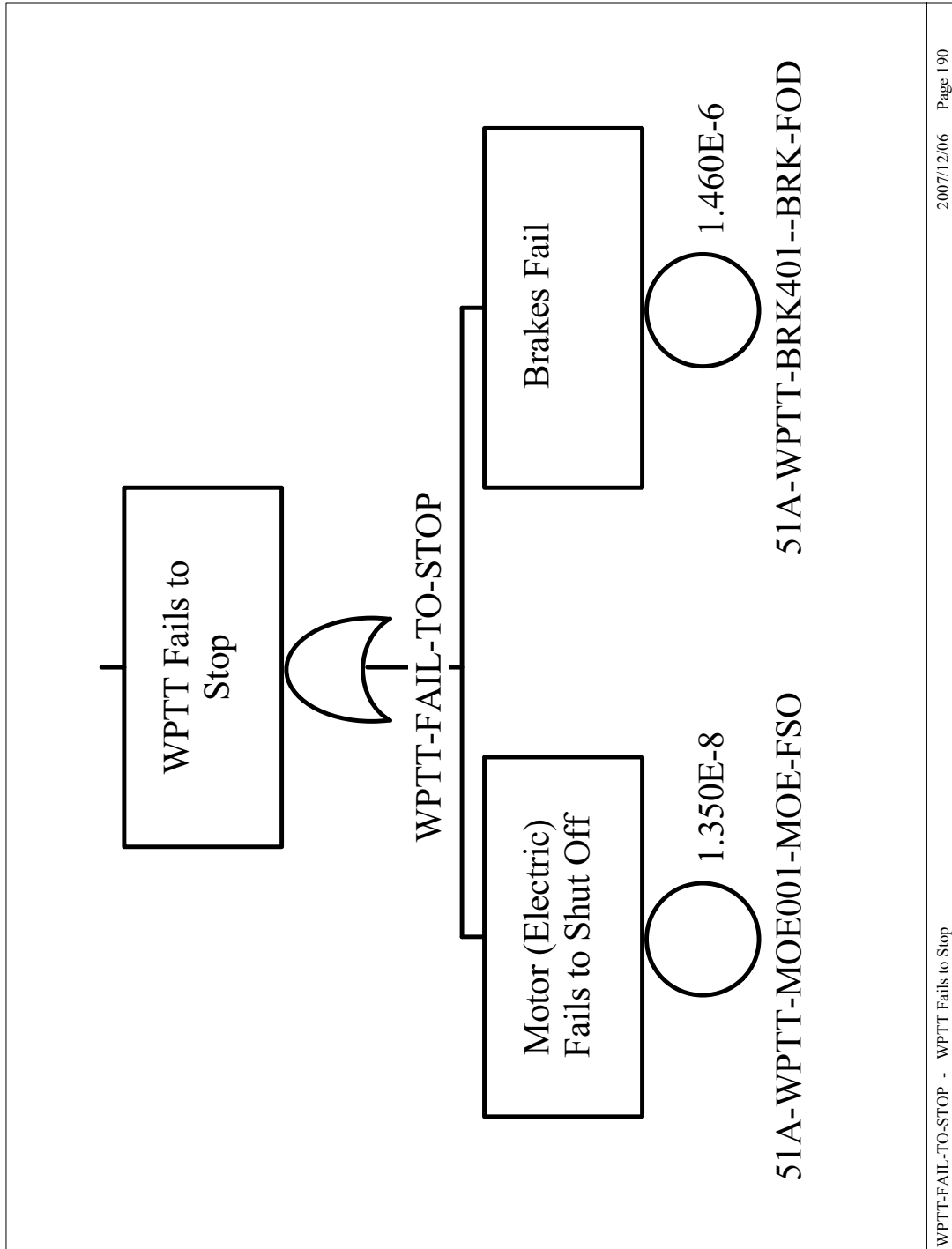
Source: Original

B5.4.2.8 Fault Tree



Source: Original

Figure B5.4-9. Fault Tree for Impact of the WPTT with a Structure



Source: Original

Figure B5.4-10. Fault Tree for Impact of the WPTT into a Structure during Waste Package Transfer (Continued)

B5.4.3 Derailment of the Waste Package Transfer Trolley

B5.4.3.1 Description

This fault tree considers the potential for the WPTT to derail during movement from loading area to the Waste Package Positioning Room (ESD-08) and during movement from the Waste Package Positioning Room) to the docking station (ESD-10). For both ESDs, the pivotal event is “Derailment of WPTT.” The top event is “WPTT Derails.” This fault tree is shown in Figure B5.4-13.

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 WPTT travels from the loading area to the Waste Package Loadout Room (approximately 4E-2 miles).

B5.4.3.2 Success Criteria

The success criterion is that the WPTT does not derail during the transport process.

B5.4.3.3 Design Features and Requirements

There are no design features or requirements.

B5.4.3.4 Fault Tree Model

The fault tree model is shown in Figure B5.4-13 with “WPTT Derails” as the top event.

B5.4.3.5 Basic Event Data

Table B5.4-5 contains a list of basic events used in the “Derailment of the WPTT” fault tree.

Table B5.4-5. Basic Event Probabilities for Derailment of the WPTT During Waste Package Transfer

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-WPTT-DERAIL-DER-FOM	3	1.180E-005	0.000E+000	1.180E-005	1.000E+000
51A-WPTT-MILES-IN-IHF	V	4.000E-002	4.000E-002	0.000E+000	0.000E+000

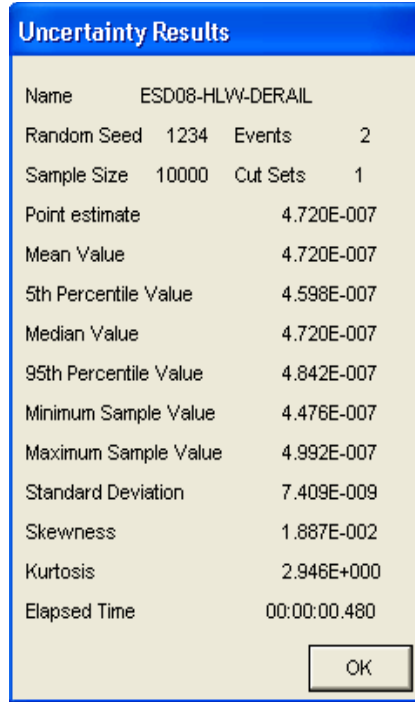
NOTE: ^aFor Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability; V = value.

Source: Original

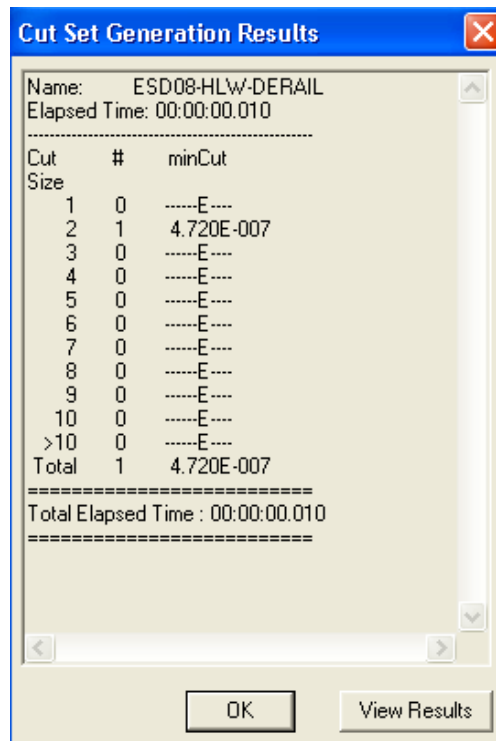
B5.4.3.6 Uncertainty and Cut Set Generation

Figure B5.4-11 contains the uncertainty results for “Derailment of the WPTT” using a cutoff probability of 1E-15. Figure B5.4-12 provides the cut set generation results obtained from running the fault trees for “Derailment of the WPTT” during waste package transfer.



Source: Original

Figure B5.4-11. Uncertainty Results for the Derailment of the WPTT Fault Tree



Source: Original

Figure B5.4-12. Cut Set Generation Results for the Derailment of the WPTT Fault Tree

B5.4.3.7 Cut Sets

Table B5.4-6 contains the cut sets for “Derailment of the WPTT” during waste package transfer. The total probability per cask is 4.720E-007.

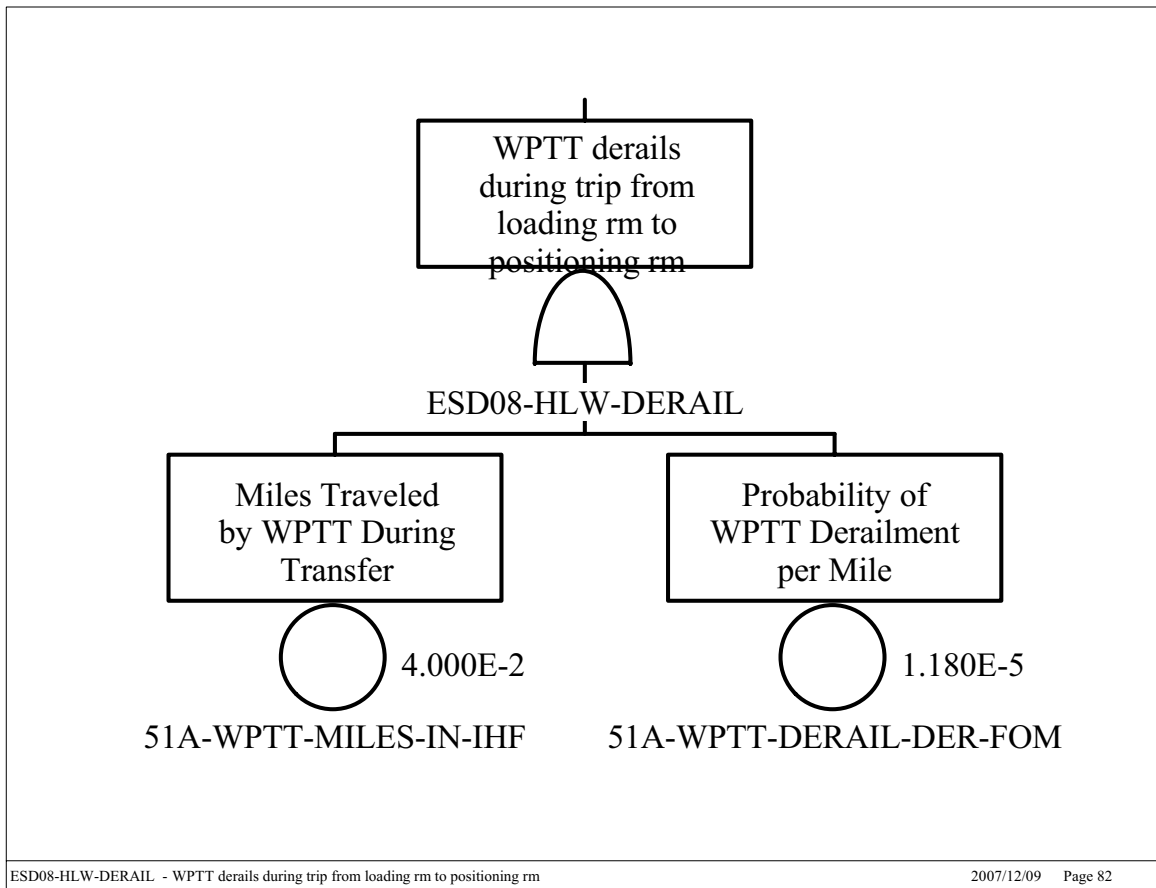
Table B5.4-6. Cut Sets for Derailment of the WPTT

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW- DERAIL	100.00	4.720E-007	51A-WPTT-DERAIL-DER-FOM	Probability of WPTT derailment per mile	1.2E-005
			51A-WPTT-MILES-IN-IHF	Miles traveled by WPTT during transfer	4.0E-002
		4.720E-007	= Total		

NOTE: Freq. = frequency; Prob. Probability; WPTT = waste package transfer trolley.

Source: Original

B5.4.3.8 Fault Trees



Source: Original

Figure B5.4-13. Fault Tree for Derailment of the WPTT

B5.4.4 Premature Tilt-down of the WPTT

B5.4.4.1 Description

This fault tree considers the potential for the shielded enclosure to prematurely tilt down during movement of the WPTT from the loading area to the Waste Package Positioning Room (ESD-8) and during movement from the Waste Package Positioning Room to the docking station (ESD-10). For both ESDs, the pivotal event is “Premature Tilt-down of WPTT.” The top event is “Premature Tilt-down of WPTT.” This fault tree is shown in Figure B5.4-16.

Premature tilt-down may occur due to operator error, failure of the control system, or structural failure of the mechanical components supporting the shielded enclosure. Operator or control system initiated tilt-down must coincide with failure of the docking interlock that must engage for power to be supplied to the shielded enclosure motors. Structural failure requires failure of either the gear box or shaft on both sides of the shielded enclosure since each side is designed to support the shielded enclosure independently. If inadvertent tilt-down does begin, the gear system on each side is designed to provide a slow tilt-down and prevent slapdown.

B5.4.4.2 Success Criteria

Premature tilt-down of the shielded enclosure is prevented during this transfer by interlocks that prevent power to the shielded enclosure motors until the WPTT is docked.

B5.4.4.3 Design Features and Requirements

The design feature is the gearing system on each side of the shielded enclosure that prevents slapdown and which can support the shielded enclosure independently. An additional design feature is the docking interlock that must be engaged for power to be provided to the shielded enclosure motors. There are no requirements.

B5.4.4.4 Fault Tree Model

The top event of the fault tree, shown in Figure B5.4-16, is premature tilt-down during movement of the WPTT from the loading area to the loadout room. Premature tilt-down may occur due to operator error or spurious signals from the control system coupled with the failure of the docking interlock.

B5.4.4.5 Basic Events

Table B5.4-7 contains a list of basic events used in the fault tree for “Premature Tilt-down of the WPTT” during waste package transfer.

Table B5.4-7. Basic Event Probabilities for Premature Tilt-down of the WPTT

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-WPTT-HC002---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-WPTT-PLC002--PLC-SPO	3	3.650E-007	0.000E+000	3.650E-007	1.000E+000
51A-WPTT-IEL001-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-OPTILTDOWN01-HFI-NOD	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.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B5.4.4.5.1 Human Failure Events

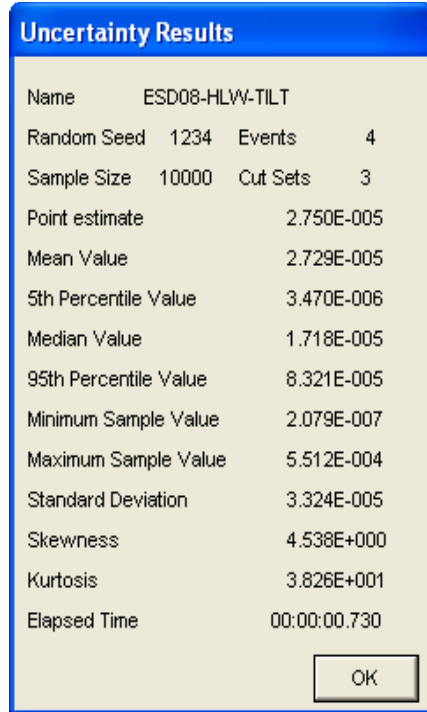
One operator error (51A-OPTILTDOWN01-HFI-NOD) involves initiation of tilt-down.

B5.4.4.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

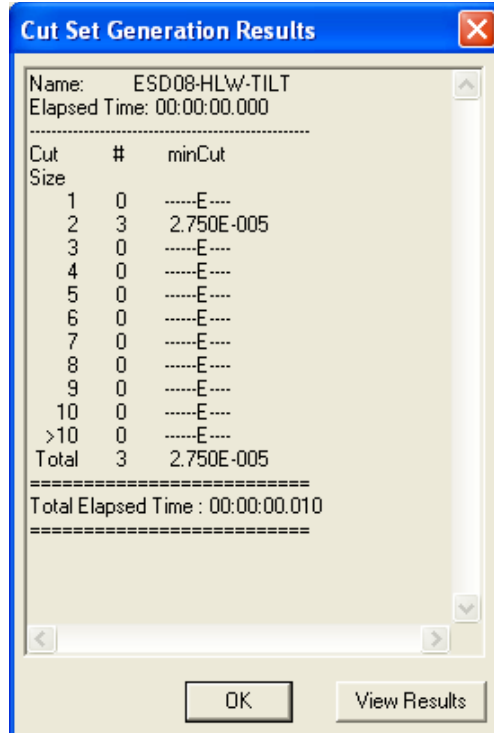
B5.4.4.6 Uncertainty and Cut Set Generation

Figure B5.4-14 contains the uncertainty results for “Premature Tilt-down of the WPTT” using a cutoff probability of 1E-15. Figure B5.4-15 provides the cut set generation results obtained from running the fault trees for “Premature Tilt-down of the WPTT” during waste package transfer.



Source: Original

Figure B5.4-14. Uncertainty Results for the Premature Tilt-down of the WPTT Fault Tree



Source: Original

Figure B5.4-15. Cut Set Generation Results for the Premature Tilt-down of the WPTT Fault Tree

B5.4.4.7 Cut Sets

Table B5.4-8 contains the cut sets for “Premature Tilt-down of the WPTT” during waste package transfer. The total probability per cask is 2.750E-005 with the major contributor being an operator initiation of premature tilt-down coinciding with the failure of the docking interlock.

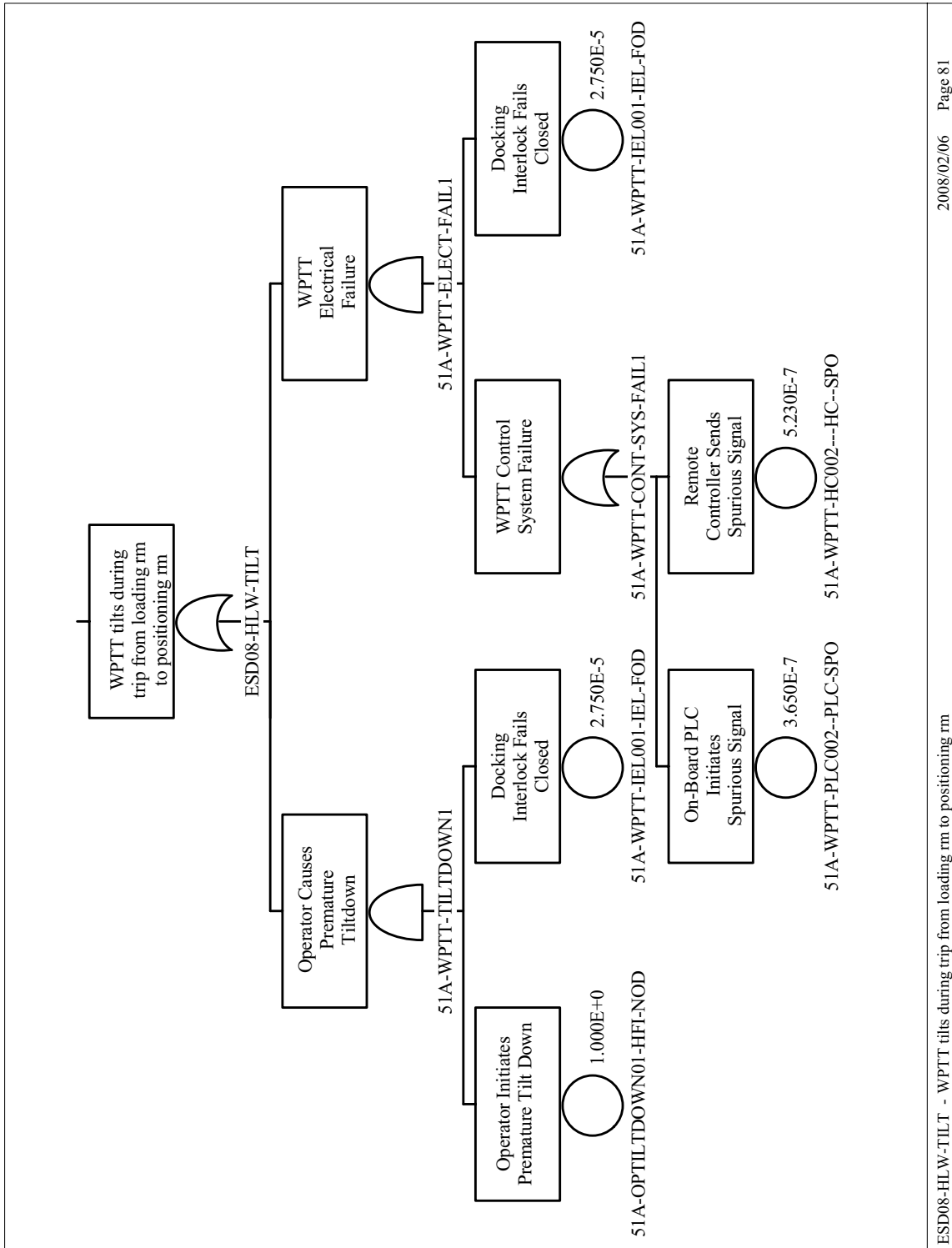
Table B5.4-8. Cut Sets for Premature Tilt-down of the WPTT

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW-TILT	100.00	2.750E-005	51A-OPTILTDOWN01-HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000
			51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
	0.00	1.438E-011	51A-WPTT-HC002---HC--SPO	Remote Controller Sends Spurious Signal	5.2E-007
			51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
	0.00	1.004E-011	51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
			51A-WPTT-PLC002--PLC-SPO	On-Board PLC Initiates Spurious Signal	3.6E-007
		2.750E-005	= Total		

NOTE: Freq. = frequency; Prob. Probability; WPTT = waste package transfer trolley.

Source: Original

B5.4.4.8 Fault Trees



ESD08-HLW-TILT - WPTT tilts during trip from loading rm to positioning rm

2008/02/06 Page 81

Source: Original

Figure B5.4-16. Fault Tree for Premature Tilt-down of the WPTT

B5.4.5 Malfunction of WPTT or Waste Package Transfer Carriage

B5.4.5.1 Description

This fault tree describes unplanned movements of the WPTT or carriage leading to impacts to the waste package during extraction of the waste package from the shielded enclosure in the Waste Package Loadout Room. This fault tree satisfies ESD-11, pivotal event “Exposure due to Malfunction of WPTT or the Waste Package Transfer Carriage.” The top event is “WPTT or Carriage Malfunction During Export.” During the waste package extraction process, damage to the waste package may occur due to premature departure of the WPTT from the docking station, tilt-up of the shielded enclosure, or operator error initiating the extraction process before the TEV door is completely open and impacting the waste package with the TEV door. This fault tree is shown in Figures B5.4-19, B5.4-20 and B5.4-21.

Several mechanical or control system failures must occur for the WPTT to prematurely leave the docking station during extraction. The control system (on-board or remote systems) must initiate a spurious signal, the locking mechanism must fail, and the docking interlock between the retrieval system and the power feed to the WPTT must fail. For the shielded enclosure to tilt-up during extraction a tilt-up signal must be initiated (either through the control system or by the operator) and the motor running interlocks that close only when the waste package carriage retrieval assembly is completely extended or retracted must fail.

B5.4.5.2 Success Criteria

The success criteria are for the WPTT to remain motionless during the extraction process, and the extraction process start only after the TEV doors are completely open.

B5.4.5.3 Design Requirements and Features

The design features include the docking interlock that interrupts power to the trolley motor while the trolley is docked to prevent premature departure, and the carriage motor interlock that prevents power to the shielded enclosure motors unless the carriage retrieval assembly is completely extended or retracted. A requirement is that the extraction process is not initiated until the TEV doors are fully open.

B5.4.5.4 Fault Tree Model

The top event of the fault trees in Figure B5.4-19 is “Malfunction of WPTT or Waste Package Transfer Carriage” during export of the waste package from the shielded enclosure. This may occur due to premature departure of the WPTT from the docking station, premature tiltup of the shielded enclosure during extraction or premature extraction of the waste package before the TEV doors are open due to operator error.

Premature departure (Figure B5.4-20) may occur due to spurious signals from the control system couples with failure of the docking interlock and the mechanical locking mechanism at the docking station. Premature tiltup (Figure B5.4-21) may occur due to spurious signals from the control system or operator initiation of tiltup couples with failure of the carriage motor interlock.

B5.4.5.5 Basic Events

Table B5.4-9 contains a list of basic events used in the fault tree for “Malfunction of WPTT or Waste Package Transfer Carriage” during waste package export”.

Table B5.4-9. Basic Event Probabilities for Malfunction of WPTT or Waste Package Transfer Carriage Malfunction during Waste Package Export

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
51A-WPTT--CAM001-CAM-FOH	3	3.190E-006	0.000E+000	3.190E-006	1.000E+000
51A-WPTT--HC001--HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-WPTT-HC002---HC--SPO	3	5.230E-007	0.000E+000	5.230E-007	1.000E+000
51A-WPTT-IEL001-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-WPTT-IEL003--IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
51A-WPTT-PLC001-PLC-SPO	3	3.650E-007	0.000E+000	3.650E-007	1.000E+000
51A-WPTT-PLC002--PLC-SPO	3	3.650E-007	0.000E+000	3.650E-007	1.000E+000
51A-OPTEVDRCLOSD-HFI-NOD	1	1.000E-003	1.000E-003	0.000E+000	0.000E+000
51A-OPWPTILTUP01-HFI-NOD	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.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B5.4.5.5.1 Human Failure Events

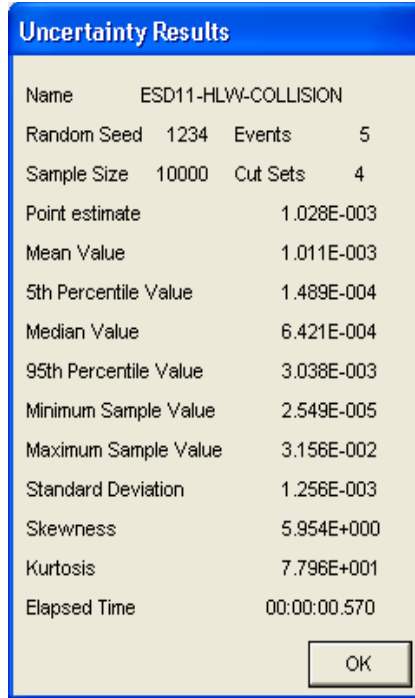
There are two operator errors; one involves initiation of tilt-up and the other extraction of the waste package with the TEV door closed.

B5.4.5.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

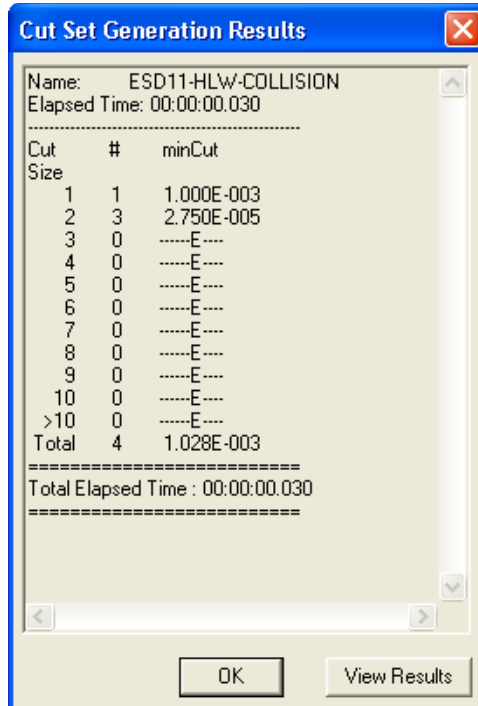
B5.4.5.6 Uncertainty and Cut Set Generation

Figure B5.4-17 contains the uncertainty results for “Malfunction of WPTT or Waste Package Transfer Carriage” using a cutoff probability of 1E-15. Figure B5.4-18 provides the cut set generation results obtained from “Malfunction of WPTT or Waste Package Transfer Carriage” malfunction during extraction of the waste package from the shielded enclosure.



Source: Original

Figure B5.4-17. Uncertainty Results for Malfunction of WPTT or Waste Package Transfer Carriage



Source: Original

Figure B5.4-18. Cut Set Generation Results for Malfunction of WPTT or Waste Package Transfer Carriage

B5.4.5.7 Cut Sets

Table B5.4-10 contains the cut sets for “Malfunction of WPTT or Waste Package Transfer Carriage” during waste package export. The total probability per cask is 1.028E-003 with operator error causing the waste package to impact the closed TEV door the primary contributor.

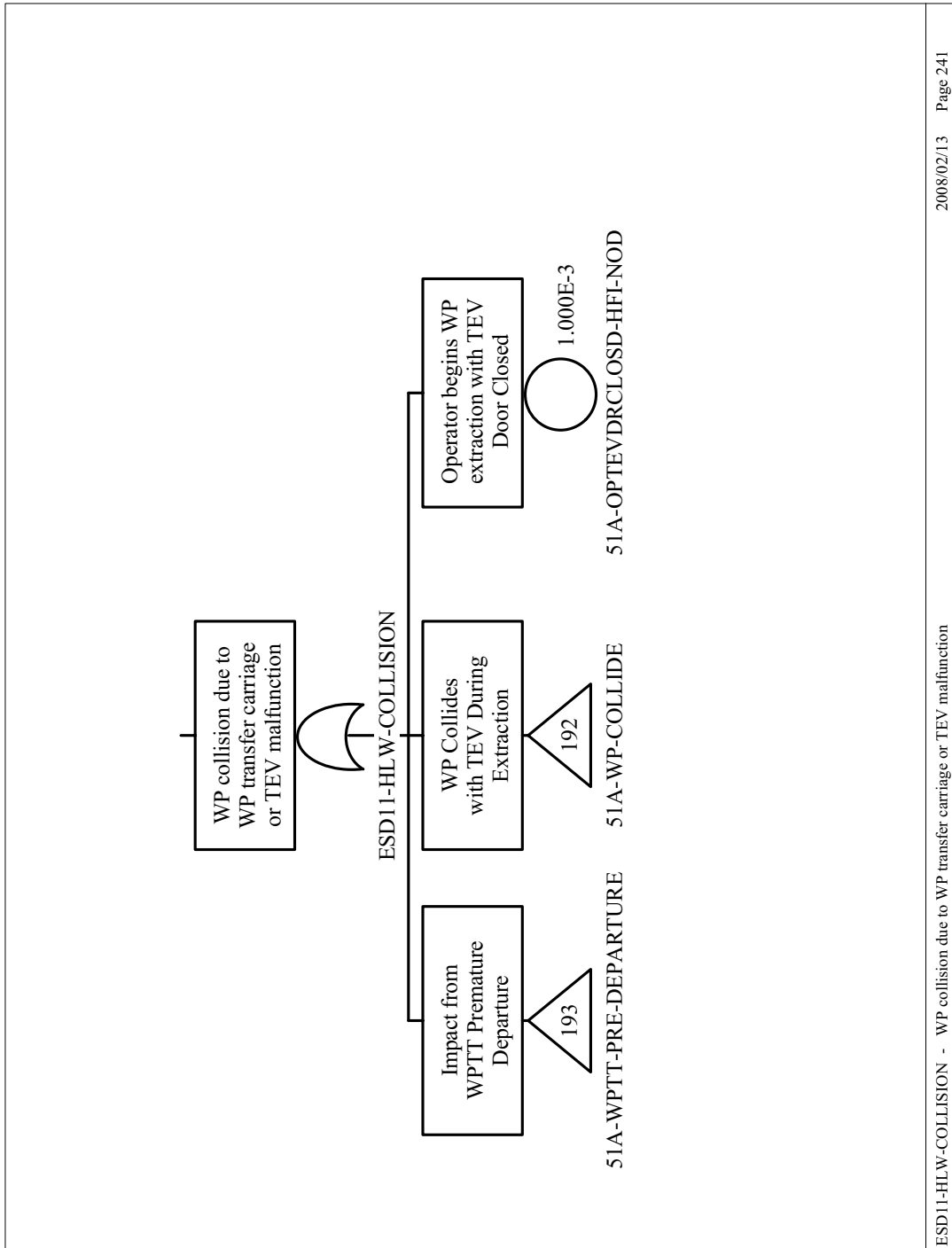
Table B5.4-10. Cut Sets for Malfunction of WPTT or Waste Package Transfer Carriage During Waste Package Export

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD11-HLW-COLLISION	97.33	1.000E-003	51A-OPTEVDRCLOSD-HFI-NOD	Operator begins WP extraction with TEV Door Closed	1.0E-003
	2.68	2.750E-005	51A-OPWPTILTUP01-HFI-NOD	Operator Initiates Tilt Up	1.0E+000
			51A-WPTT-IEL001-IEL-FOD	Carriage Motor Interlock Fails	2.8E-005
	0.00	1.438E-011	51A-WPTT-HC002---HC-SPO	Remote Controller Sends Spurious Signal	5.2E-007
			51A-WPTT-IEL001-IEL-FOD	Carriage Motor Interlock Fails	2.8E-005
	0.00	1.004E-011	51A-WPTT-IEL001-IEL-FOD	Carriage Motor Interlock Fails	2.8E-005
			51A-WPTT-PLC002--PLC-SPO	On-Board PLC Initiates Spurious Signal	3.6E-007
		1.028E-003	= Total		

NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

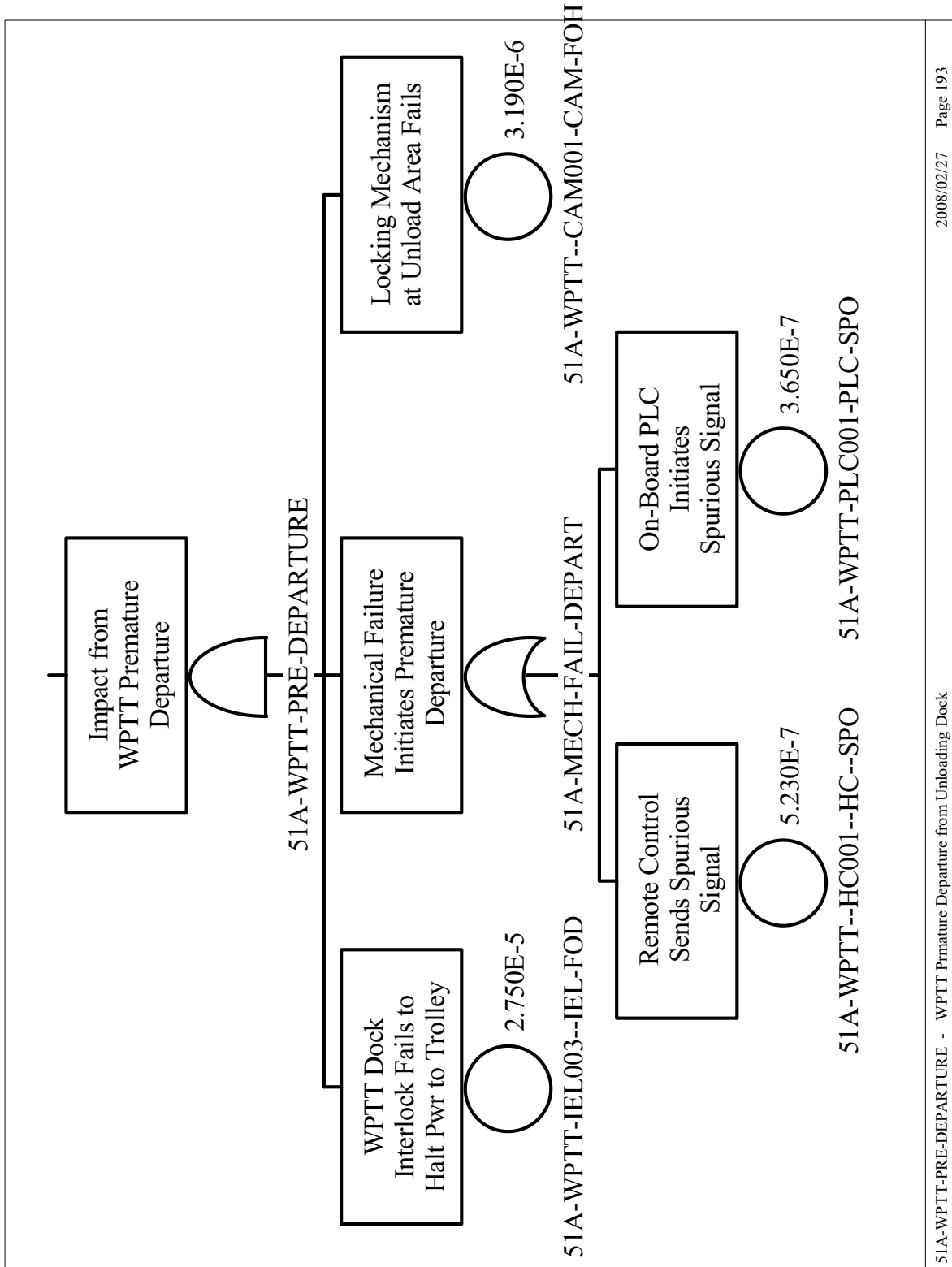
Source: Original

B5.4.5.8 Fault Trees



Source: Original

Figure B5.4-19. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage

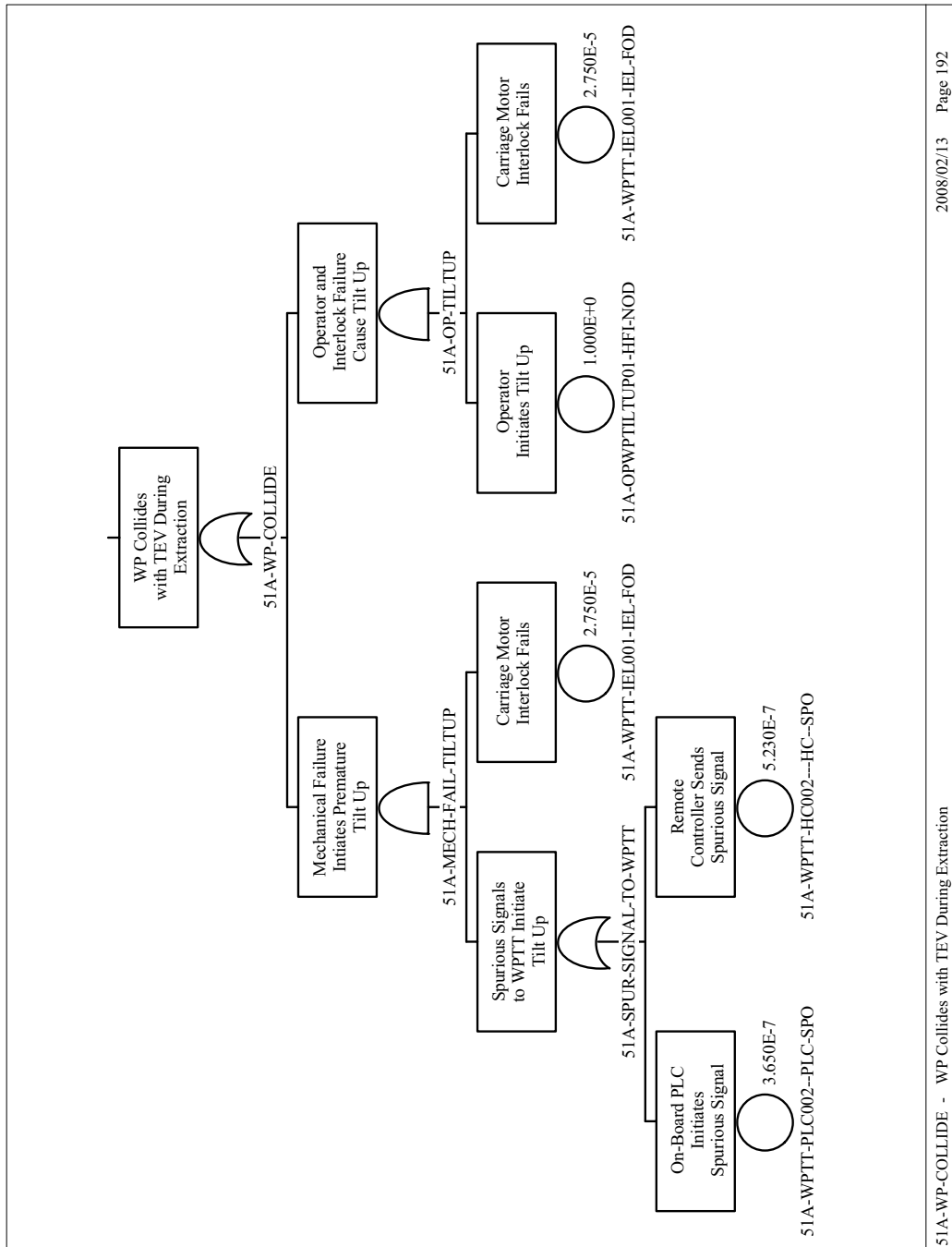


2008/02/27 Page 193

51A-WPTT-PRE-DEPARTURE - WPTT Premature Departure from Unloading Dock

Source: Original

Figure B5.4-20. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage (Continued)



Source: Original

Figure B5.4-21. Fault Tree for Malfunction of WPTT or Waste Package Transfer Carriage (Continued)

B6 PIVOTAL EVENT ANALYSIS

Miscellaneous linking fault trees that were not discussed in Attachment A are described in this section. Attachment A described 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, Sections B1 to B5. This section describes the remaining types of initiating event fault trees that do not fit into these categories.

There are four types of fault trees discussed in this section: dropping an object onto a cask or waste package, impact to a cask by another vehicle or object, spurious movement of a crane causing an impact to or a tip over of a cask, loss of shielding leading to direct exposure, and introduction of liquid moderator.

B6.1 FAULT TREES INVOLVING DROPPING AN OBJECT

These “drop-on” fault trees describe dropping an object onto a cask or a waste package and are listed in Table B6.1-1. A typical fault tree for drop of an object onto a transportation cask is shown in Figure B6.1-1, and a fault tree for dropping an object onto a waste package is shown in Figure B6.1-2.

Table B6.1-1. Drop-On Fault Trees

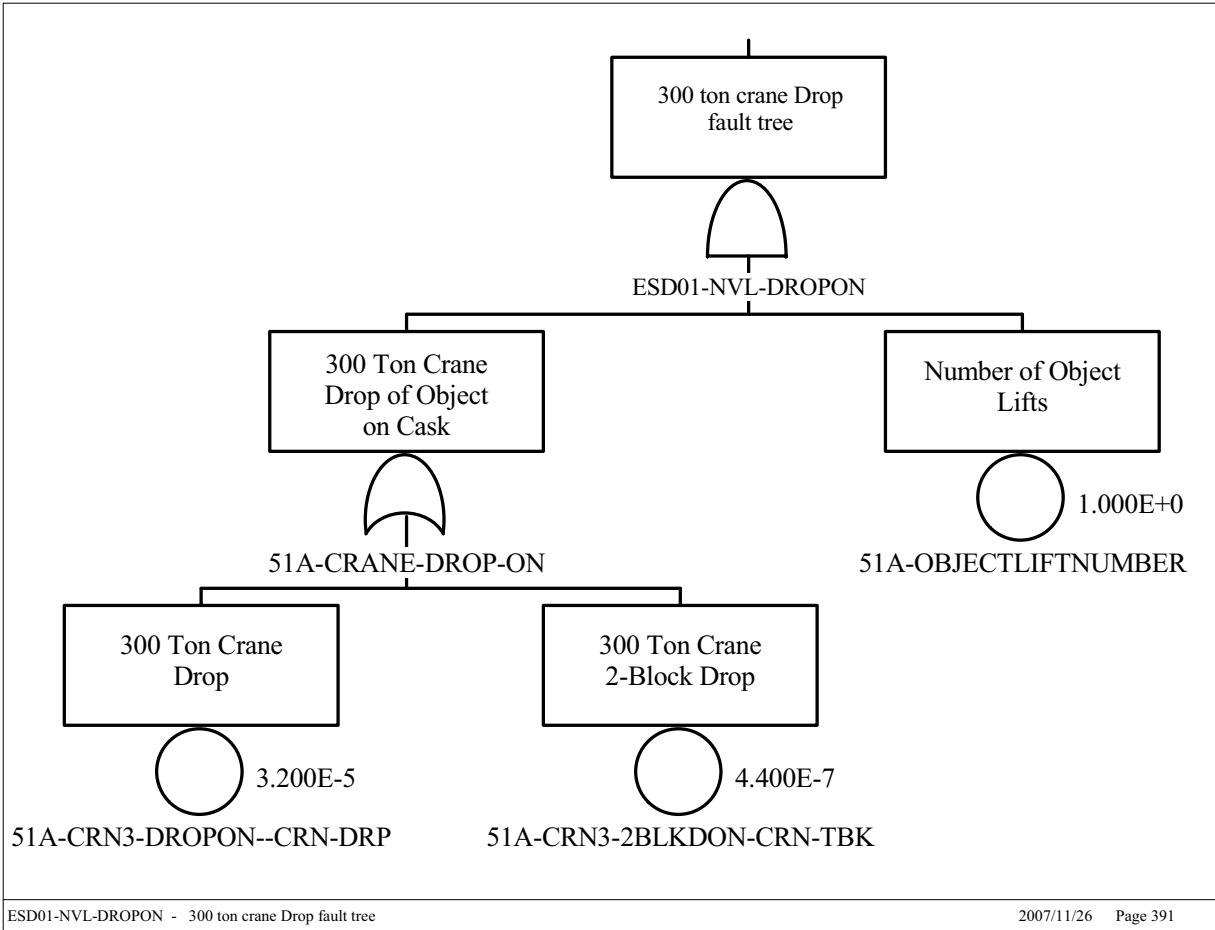
Fault Tree Name	Applies to ESD	Applies To	Number of Objects Lifted
ESD01-NVL-DROPON	ESD-01	Naval transportation cask	1
ESD02-HLW-DROPON	ESD-02	HLW transportation cask	1
ESD02-NVL-DROPON	ESD-02	Naval transportation cask	1
ESD03-HLW-DROPON	ESD-03	HLW transportation cask	1
ESD04-NVL-DROPON	ESD-04	Naval transportation cask	1
ESD07-HLW-DROPON	ESD-07	HLW canister	1
ESD07-NVL-DROPON	ESD-07	Naval canister	1
ESD09-HLW-DROPON	ESD-09	HLW waste package	2
ESD09-NVL-DROPON	ESD-09	Naval waste package	2
ESD11-HLW-DROPON	ESD-11	HLW waste package	1
ESD11-NVL-DROPON	ESD-11	Naval waste package	1

NOTE: HLW = high-level radioactive waste; NVL = naval.

Source: Original

In Figure B6.1-1 the 300-ton crane may drop a lifting fixture onto the transportation cask from a normal height or from a much higher than normal height due to a two-blocking event. The probabilities of crane drops are based on historical data discussed in Section 6.3 and Attachment C. The calculated probability of a crane dropping an object on a cask is 3.24E-005 for one object lifted.

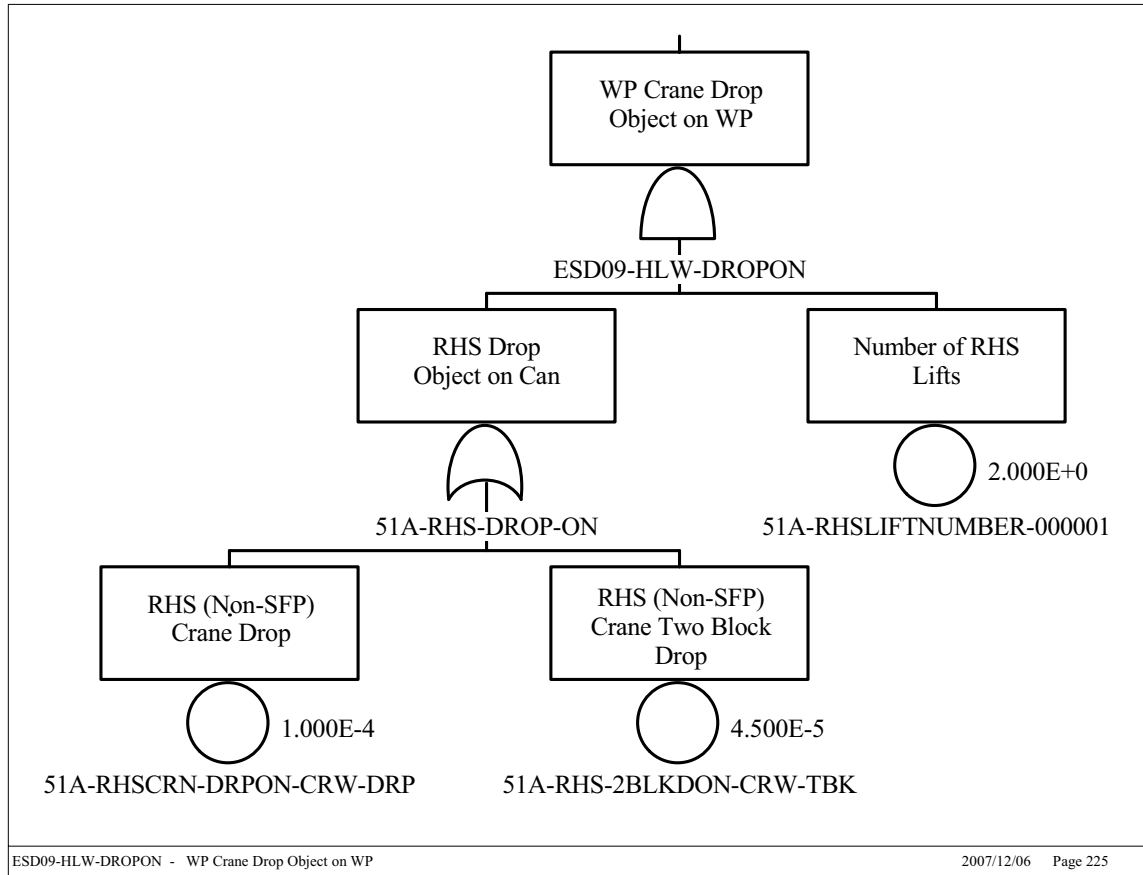
The data for the 300-ton crane is based on operational experience of cranes designed to be single failure proof (SFP).



Source: Original

Figure B6.1-1. Typical 300-Ton Crane “Drop-On” Fault Tree

In Figure B6.1-2 the remote handling system (RHS) crane may drop the inner or outer waste package lids onto the waste package from a normal height or from a much higher than normal height due to a two-blocking event. The probabilities of crane drops are based on historical data discussed in Section 6.3 and Attachment C. The calculated probability of a crane dropping an object on a cask is 3.0E-04 for the two objects lifted.



Source: Original

Figure B6.1-2. Typical RHS Crane “Drop-On” Fault Tree

B6.2 IMPACT TO A CASK BY ANOTHER VEHICLE OR OBJECT

These fault trees involve side impacts to the transportation cask by another vehicle or object. Table B6.2-1 lists the fault trees that describe these impacts.

Table B6.2-1. Transportation Cask Impact Fault Trees

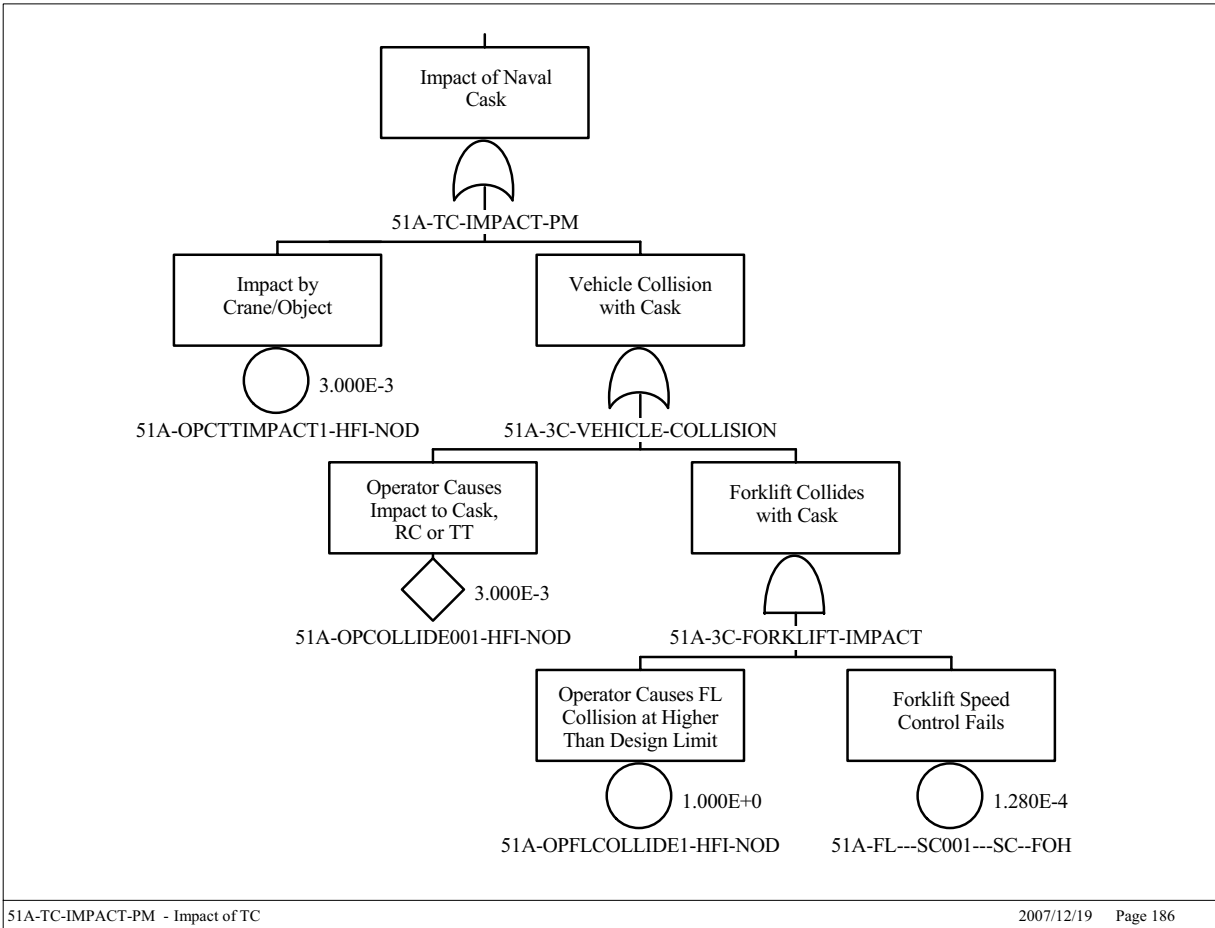
Fault Tree Name	Applies to ESD	Applies To
ESD01 NVL COL CSK (transfers to 51A-TC-IMPACT-PM)	ESD-01	Naval Transportation Cask
ESD02-HLW-SIDEIMP	ESD-02	HLW Transportation Cask
ESD02-NVL-SIDEIMP	ESD-02	Naval Transportation Cask
ESD03-HLW-SIDEIMP	ESD-03	HLW Transportation Cask
ESD03-NVL-SIDEIMP	ESD-03	Naval Transportation Cask

NOTE: ESD = event sequence diagram; HLW = high level waste; NVL = naval.

Source: Original

Figure B6.2-1 illustrates a side impact to a transportation cask that may occur due to the following operator errors:

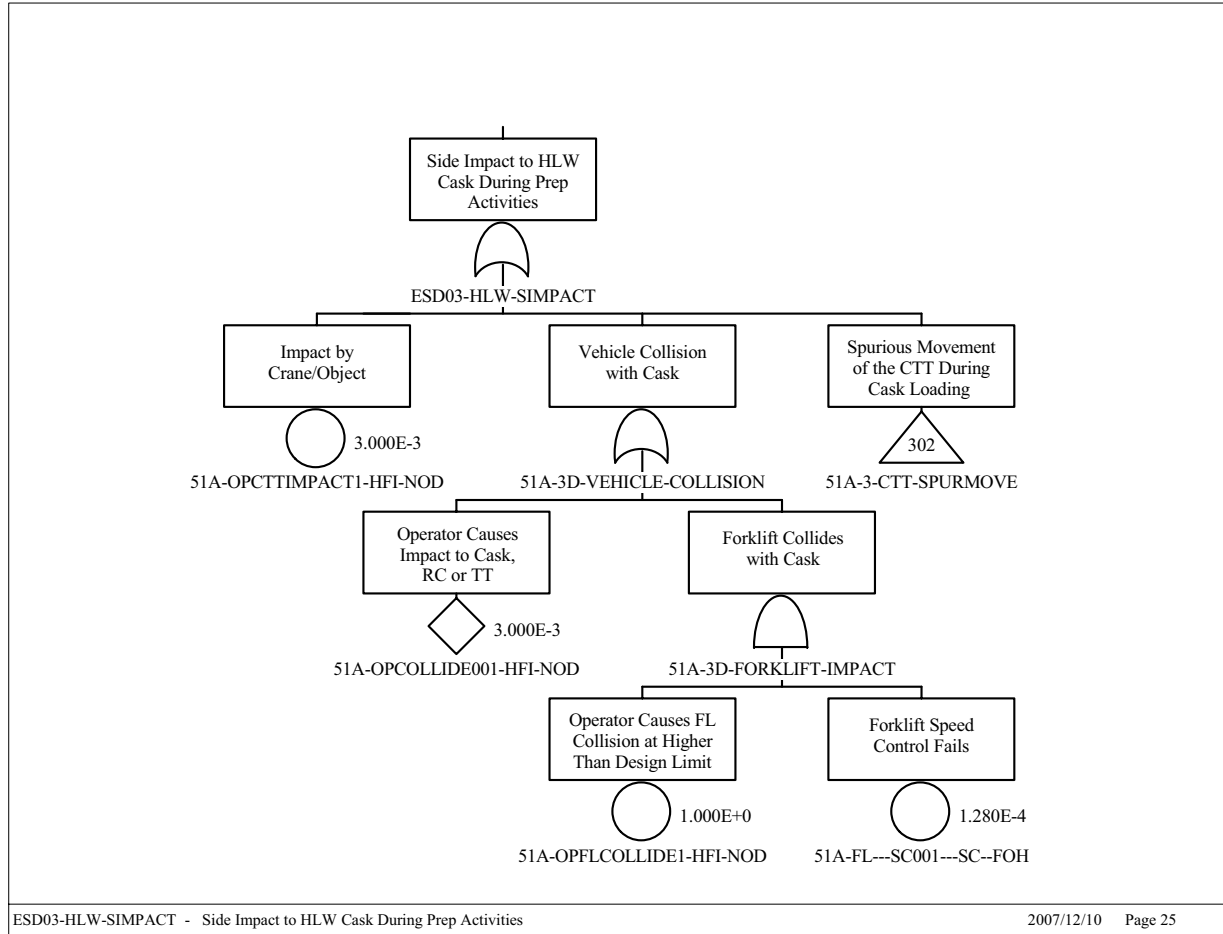
- Operator causing impact by the crane or object being carried by the crane
- Operator impacting a vehicle (such as a forklift) into the cask at the design speed
- Operator causing a forklift impact at higher than the design speed coupled with failure of the forklift speed control.



Source: Original

Figure B6.2-1. Typical Side Impact Fault Tree

Figure B6.2-2 is identical to Figure B6.2-1 except for the addition of another cause of a side impact, and the spurious movement of the CTT during cask loading which is described in Attachment B3.



Source: Original

Figure B6.2-2. Typical Side Impact with Spurious Movement of CTT Fault Tree

B6.3 IMPACT TO A CASK DUE TO SPURIOUS MOVEMENT

These trees involve impacts to or a tip over the transportation cask due to operator error or spurious movements of the crane or CTT. Table B6.3-1 lists the fault trees that describe these impacts.

Table B6.3-1. Transportation Cask Impacts or Tipover Fault Trees

Fault Tree Name	Applies to ESD	Applies To
51A Crane SPURMOVE	ESD-02	HLW Transportation Cask
	ESD-03	HLW Transportation Cask
	ESD-04	NVL Transportation Cask
51A-CTT-SPURMOVE	ESD-02	HLW Transportation Cask
*ESD01-NVL-TIPOVER	ESD-01	NVL Transportation Cask
*ESD02-HLW-TIP-CSK	ESD-02	HLW Transportation Cask

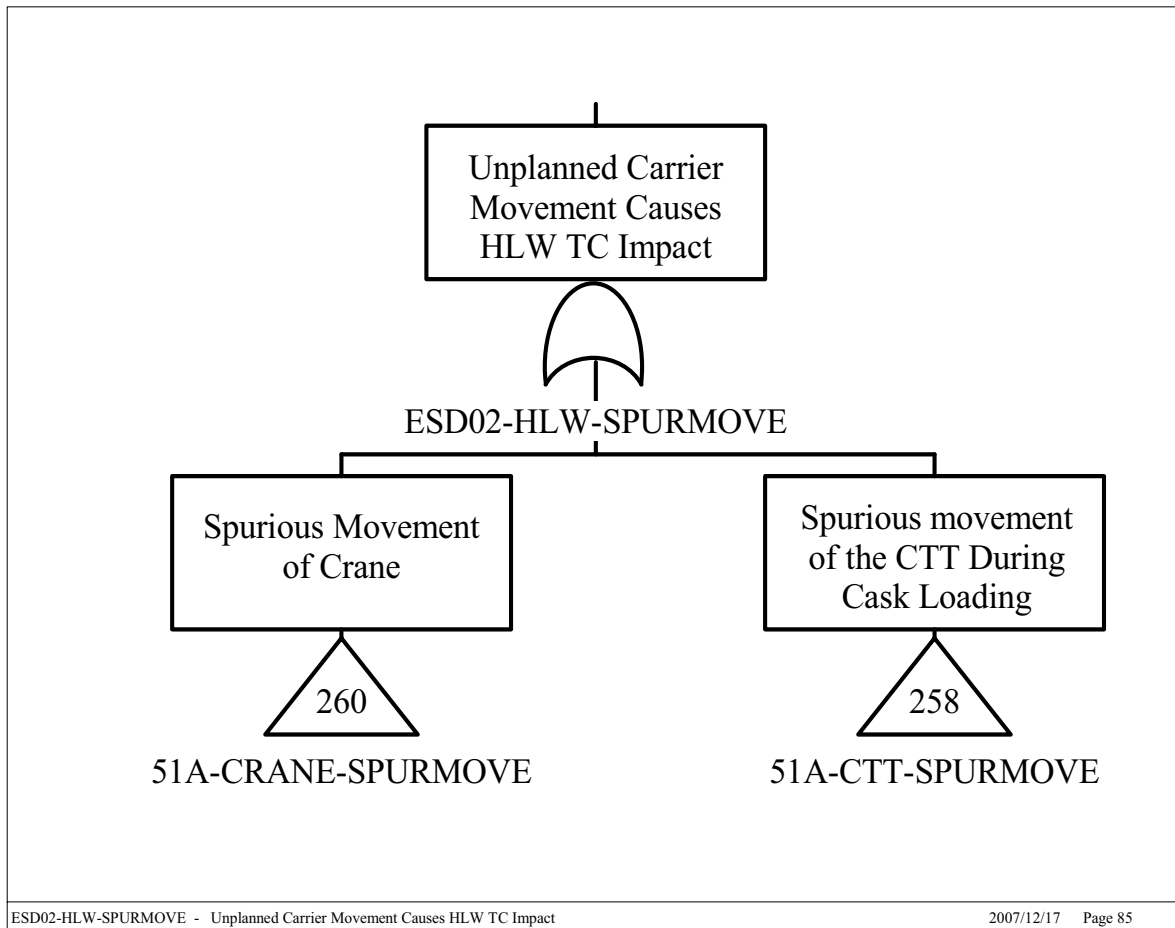
Table B6.3-1. Transportation Cask Impacts or Tipover Fault Trees (Continued)

Fault Tree Name	Applies to ESD	Applies To
ESD03-HLW-CASKTIP	ESD-03	HLW Transportation Cask
ESD04-NVL-CASKTIP	ESD-04	NVL Transportation Cask
*ESD05-HLW-CASKTIP	ESD-05	HLW Transportation Cask

NOTE: Entries marked with * are human failure events and are detailed in Section 6.4 and Attachment E.
CTT = cask transport trolley; HLW = high level waste; NVL = naval; SPURMOVE = spurious movement.

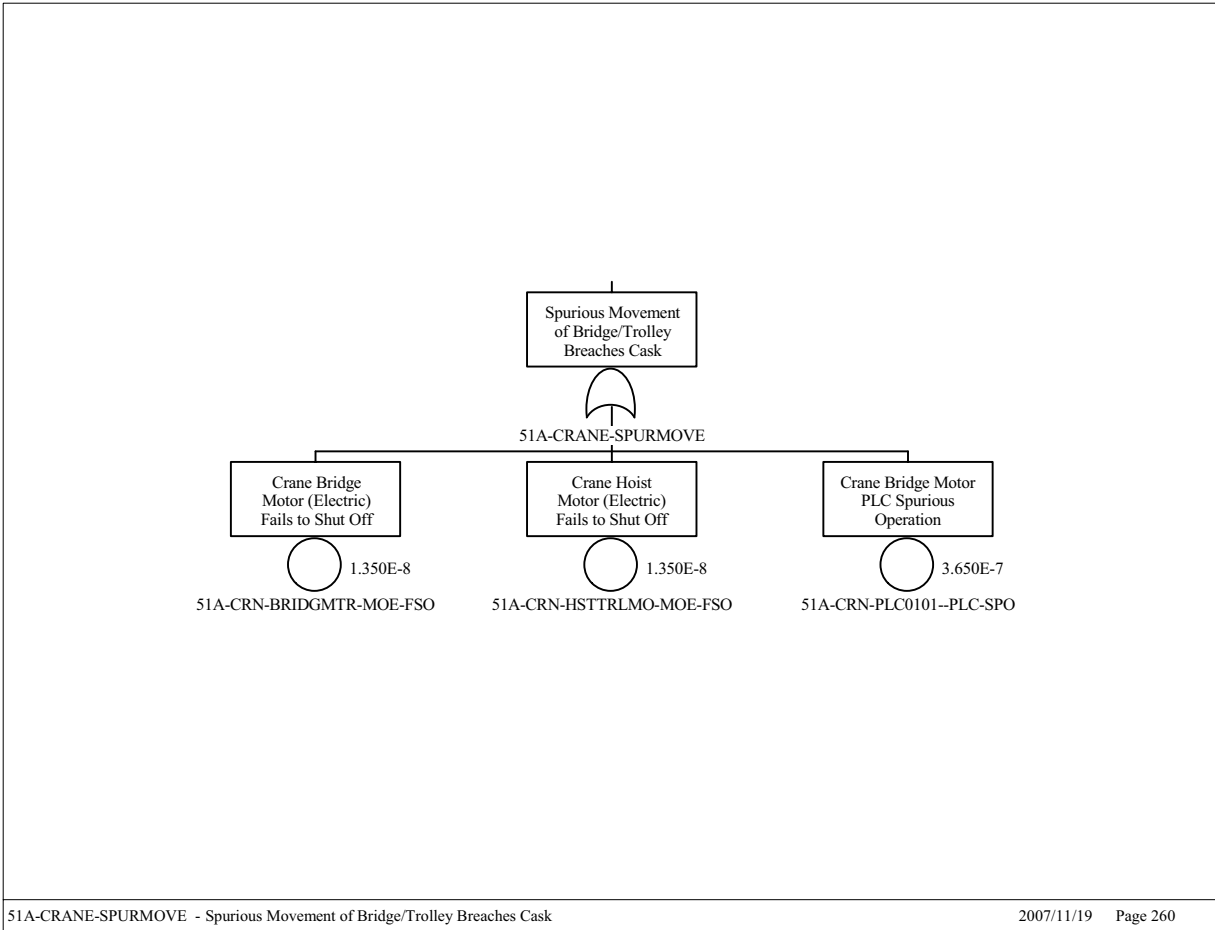
Source: Original

Figure B6.3-1 describes an impact to a cask due to spurious movement of the CTT during loading or spurious movement of the crane. The fault tree for spurious movement of the CTT is described in Attachment B. Spurious movement of the crane fault tree is shown in Figure B6.3-2. 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.



Source: Original

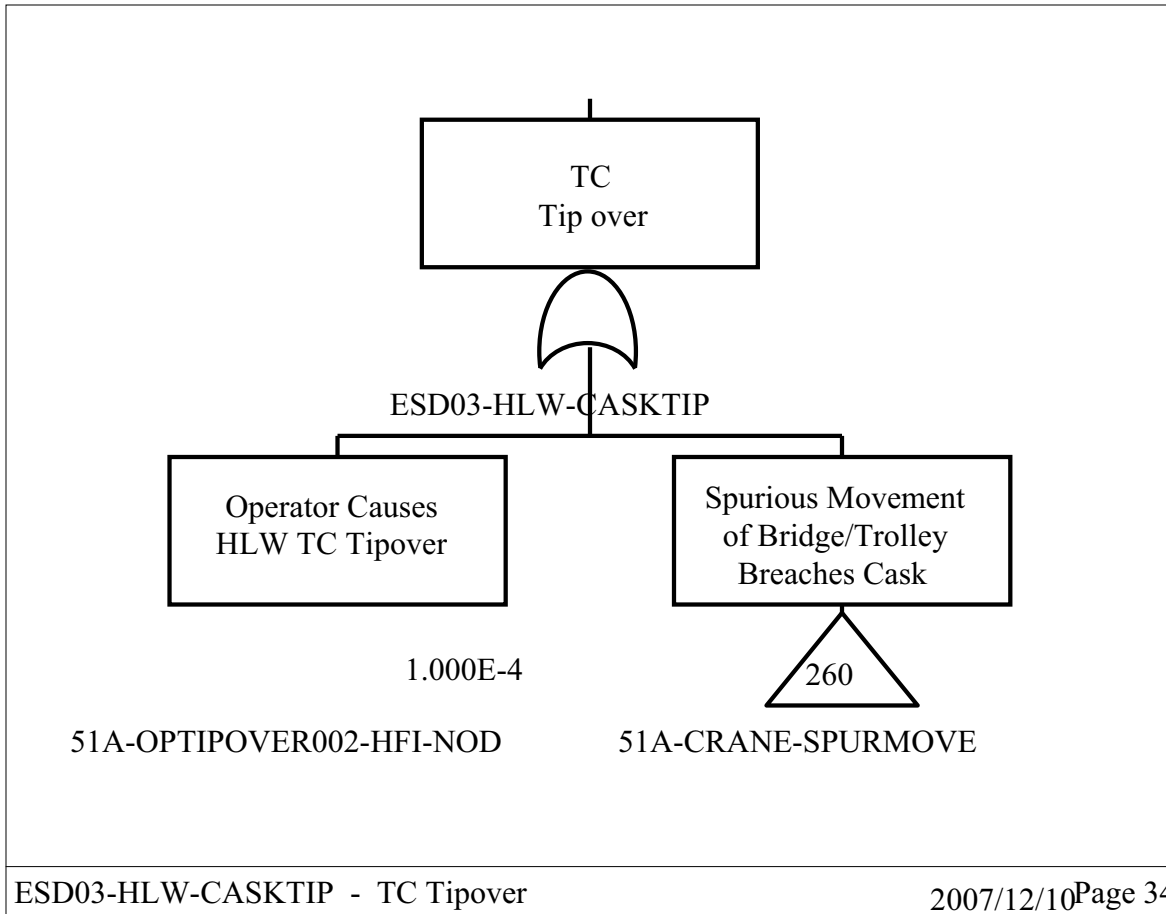
Figure B6.3-1. Spurious Movement of the Crane or CTT Fault Tree



Source: Original

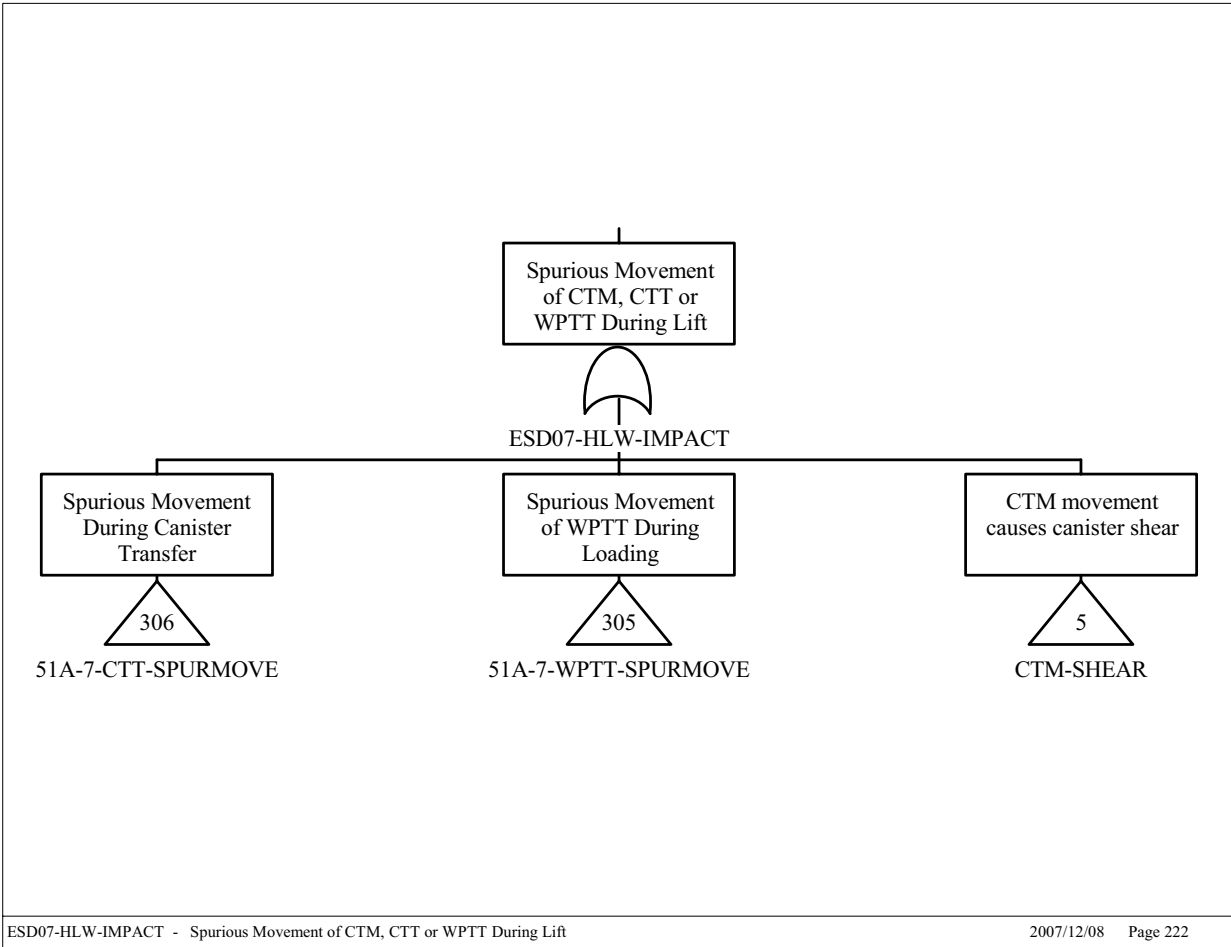
Figure B6.3-2. Spurious Movement of the Crane Fault Tree

Impacts due to a tip over may be caused by operator error or spurious movement of the crane as shown in Figure B6.3-3. The calculated probability of a tipover is 1.004E-04 due to the overriding influence of operator error causing the tipover.



Source: Original

Figure B6.3-3. Typical Tipover Fault Tree



Source: Original

Figure B6.3-4. Fault Tree for Spurious Movement CTM, CTT or WPTT during Lift

Figure B6.3-4 illustrates the fault tree for impact to a canister caused by spurious movement of the CTT during unloading of the transportation cask, the WPTT during loading of the WP, or the CTM during transfer of the canister. The calculated probability of an impact due to spurious movement of the carriers is 2.857E-05. Fault trees for the various spurious movements are addressed in their respective sections in Attachment B.

B6.4 LOSS OF SHIELDING LEADING TO DIRECT EXPOSURE

These fault trees describe direct exposure during canister transfer or while closing the waste package. Table B6.4-1 lists the fault trees that describe these direct exposures.

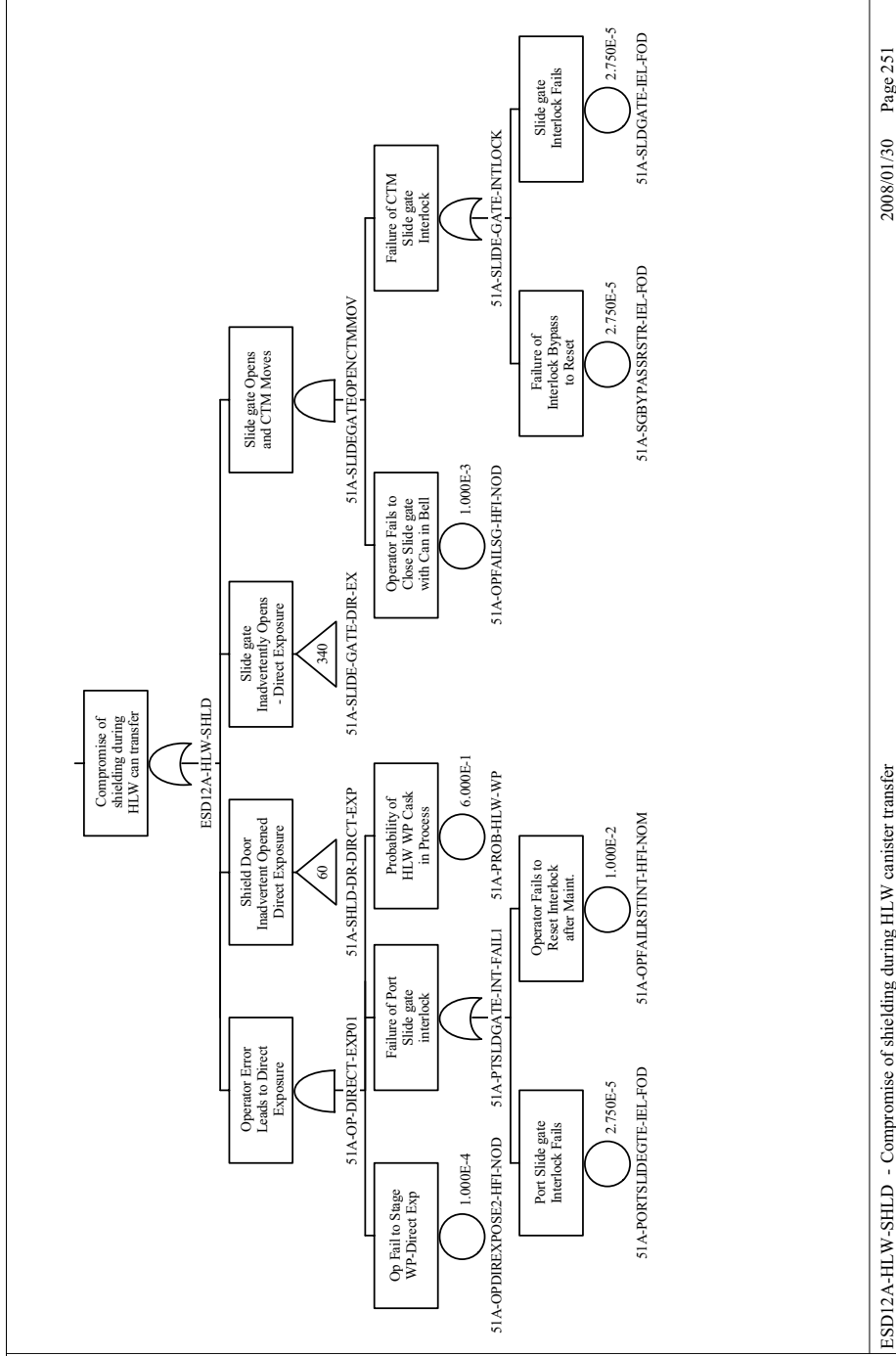
Table B6.4-1. Direct Exposure Fault Trees

Fault Tree Name	Applies To
ESD12A-HLW-SHLD	HLW canister
ESD12A-NVL-SHLD	Naval canister
ESD12B-HLW-SHLD	HLW canister in WP
ESD12B-NVL-SHLD	Naval canister in WP

NOTE: HLW = high level waste; NVL = naval; SHLD = shielding; WP = waste package.

Source: Original

Figure B6.4-1 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 B. The calculated probability of a direct exposure during this canister transfer is 1.954E-06.



2008/01/30 Page 251

ESD12A-HLW-SHLD - Compromise of shielding during HLW canister transfer

Source: Original

Figure B6.4-1. Typical Direct Exposure Fault Tree due to Shield Door or Slide Gate Opening

Figure B6.4-2 is a fault tree for direct exposure from a HLW waste package that has been improperly closed or shielded. The causes are improper installation of the waste package shield ring due to operator error (Figure B6.4-3), failure to properly install the shield ring or improper installation of the inner lid during closure (Figure B6.4-4). The calculated probability of a direct exposure from improper shield ring installation is 1.01E-04.

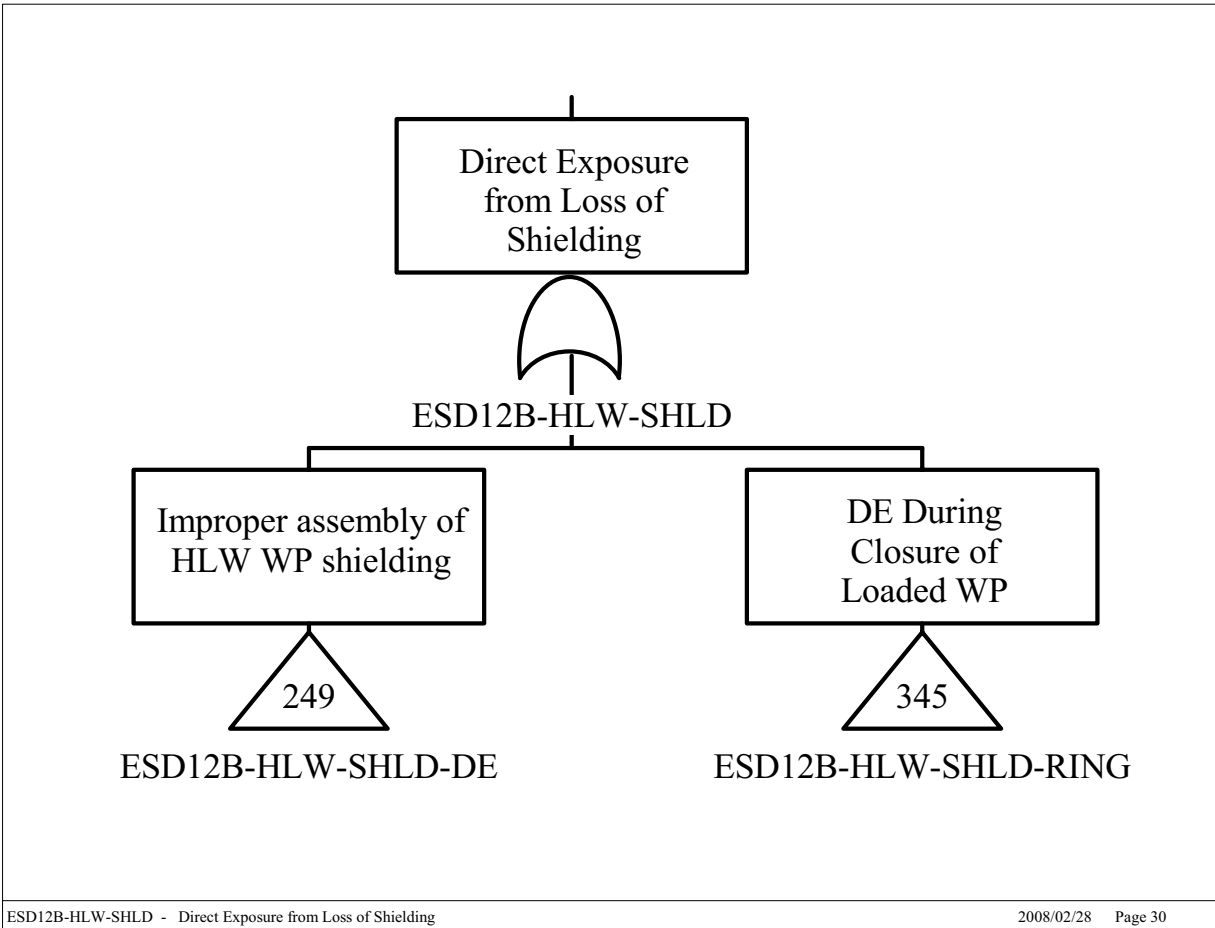
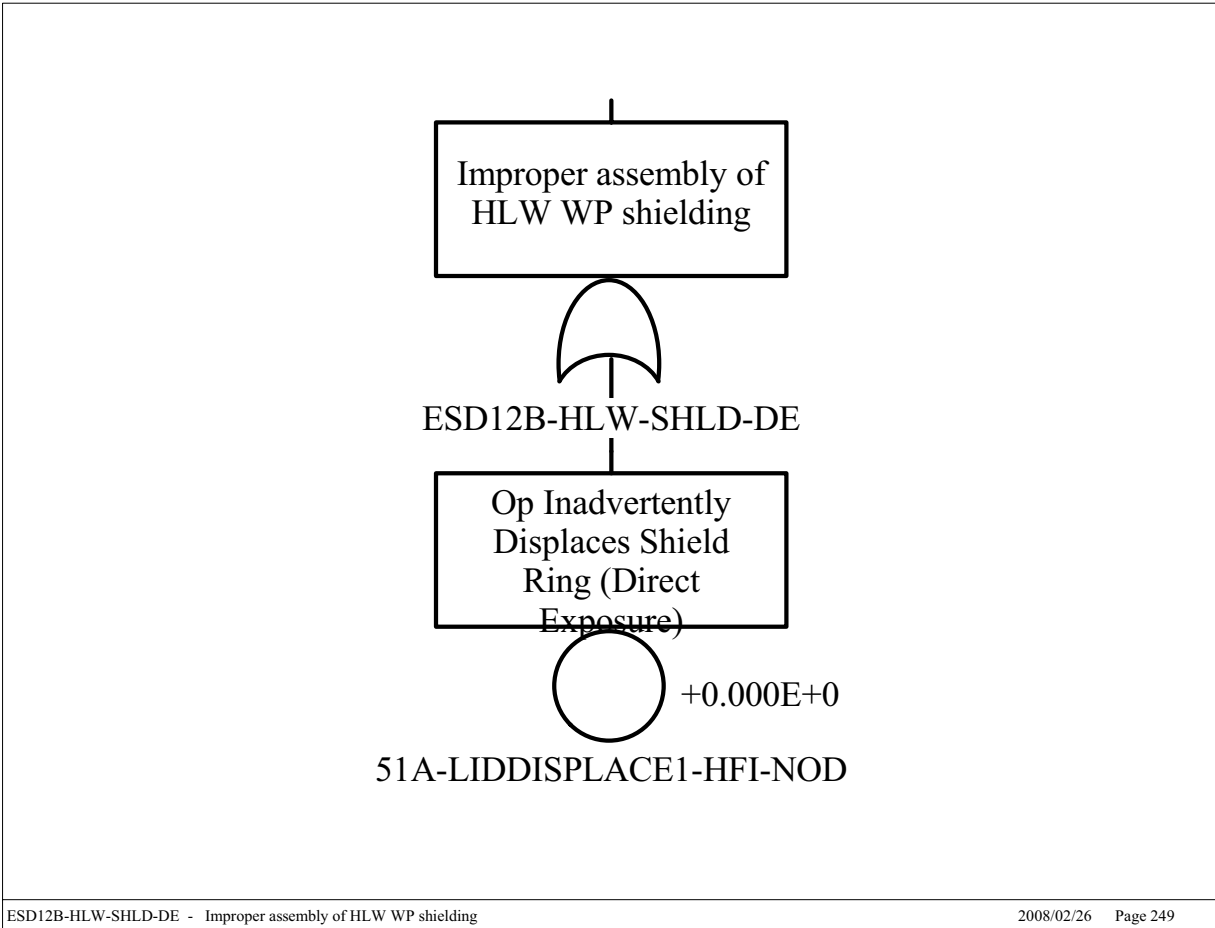


Figure B6.4-2. Direct Exposure from HLW due to Loss of Shielding



ESD12B-HLW-SHLD-DE - Improper assembly of HLW WP shielding

2008/02/26 Page 249

Figure B6.4-3. Direct Exposure from HLW due to Improper Assembly of Shield Ring

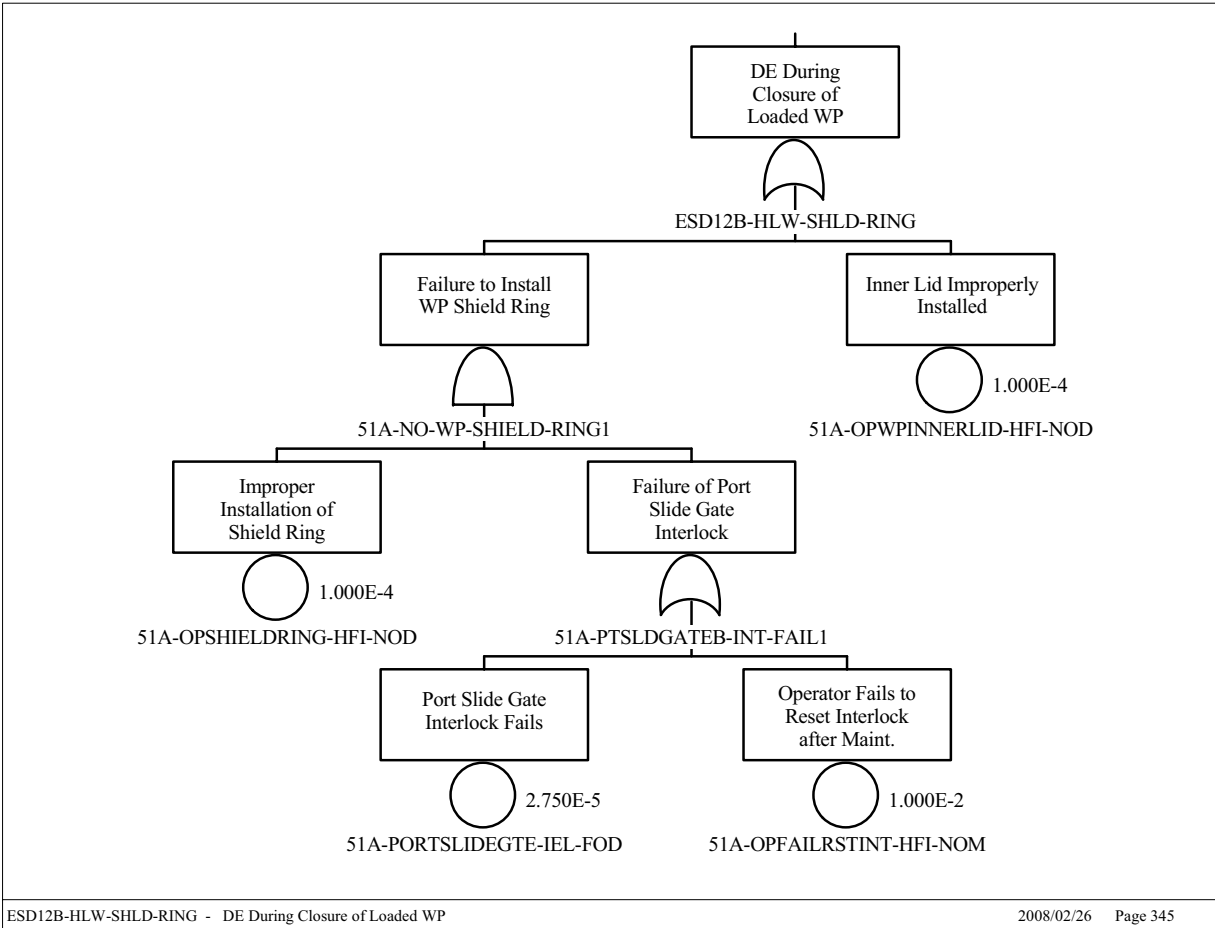


Figure B6.4-4. Direct Exposure from HLW during Closure of the WP

Figure B6.4-5 is a fault tree for direct exposure from a NVL waste package that has been improperly closed or shielded. Direct exposure results from improper assembly of the waste package shield ring or inadvertently displacement of the shield ring due to operator error (Figure B6.4-6). Direct exposure will also result from failure to properly install the shield ring or the improper installation of the inner lid during closure (Figure B6.4-4). The calculated probability of a direct exposure from improper shield ring installation is 4.01E-04.

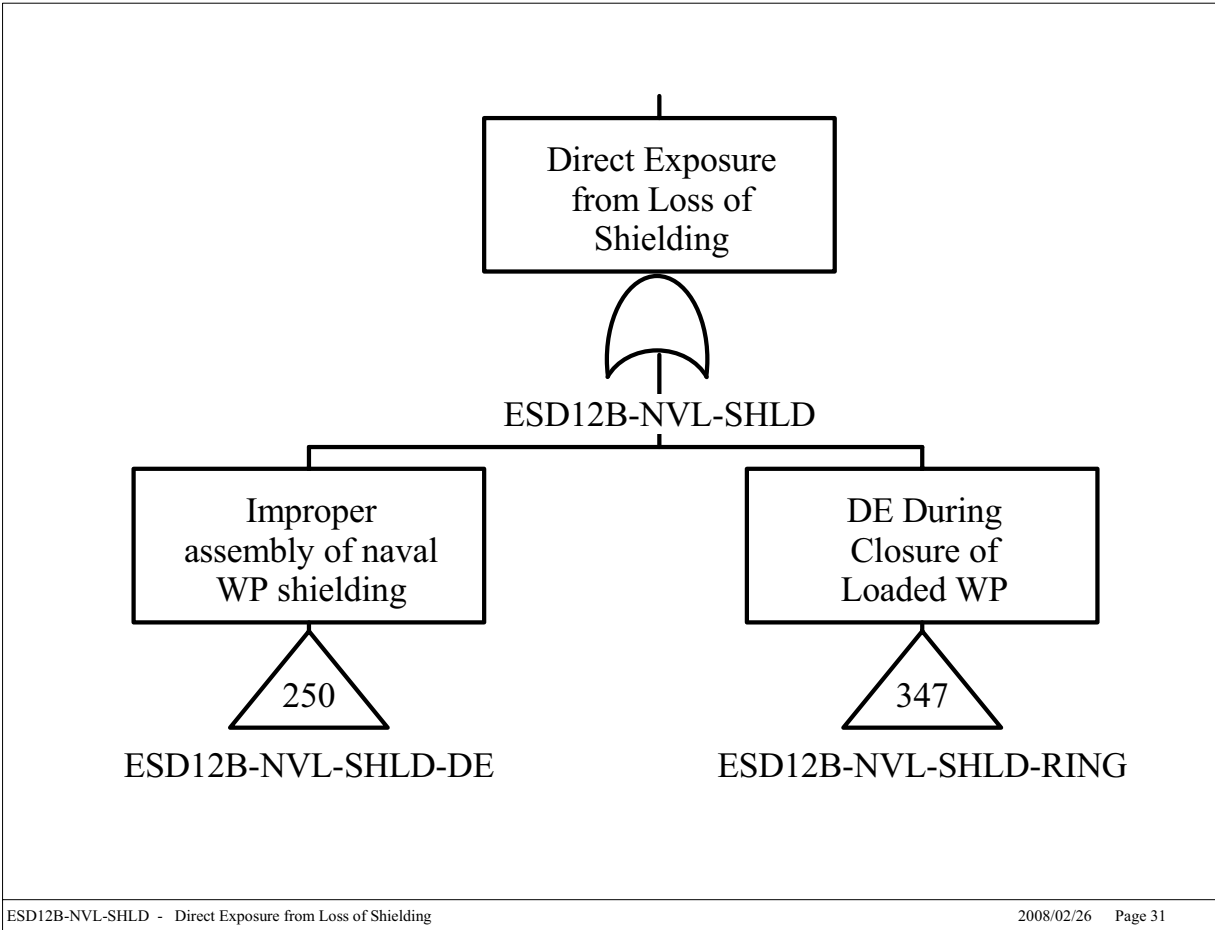


Figure B6.4-5. Direct Exposure from NVL Canister due to Loss of Shielding

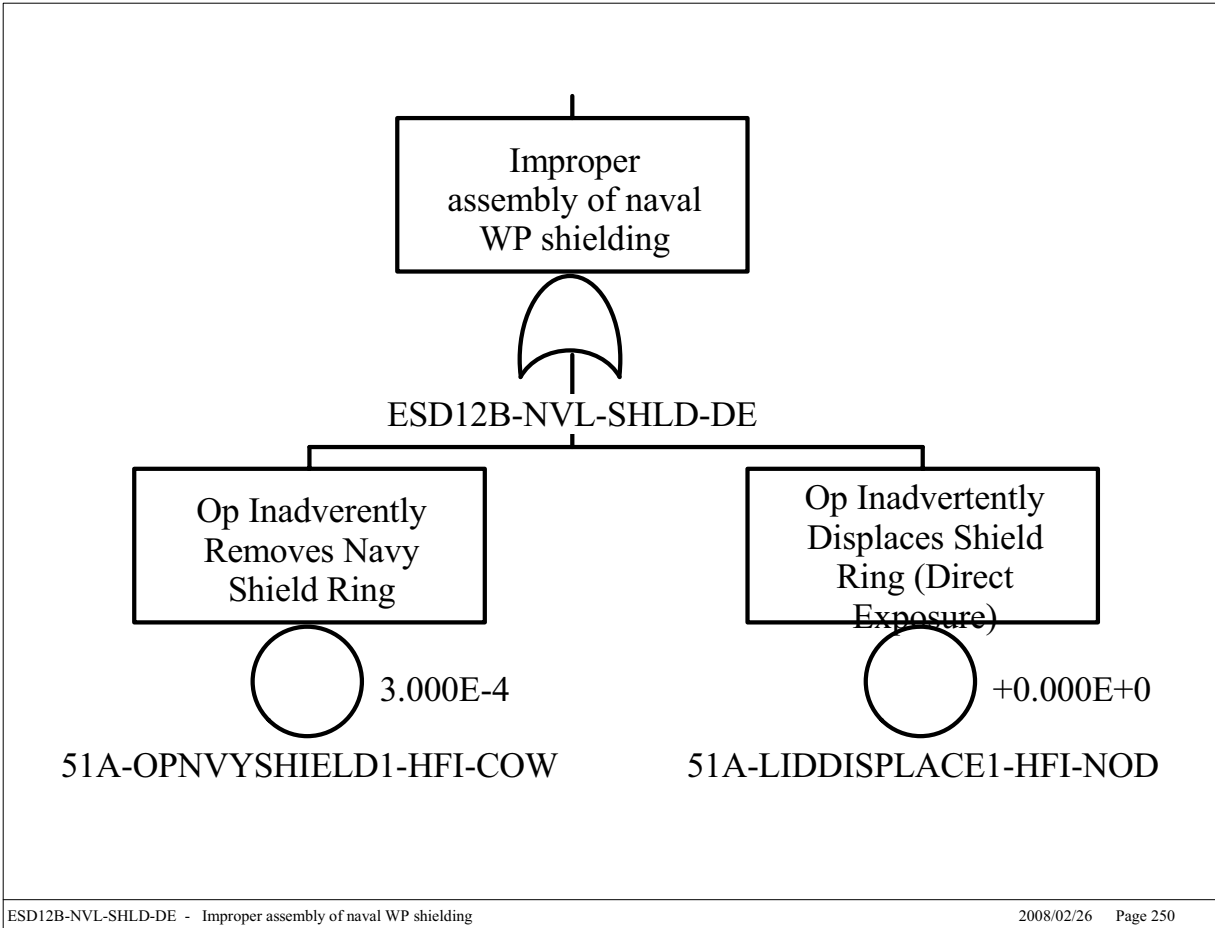


Figure B6.4-6. Direct Exposure from NVL Canister due to Improper Assembly of Shield Ring

B6.5 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 intrusion into a canister can occur following a breach of the canister and a subsequent internal flooded. Table B6.5-1 lists the fault trees that describe the moderator events during IHF operations. It should be noted that HLW criticality is not affected by the presence of a moderator source; therefore, the moderator value for HLW sequences dealing with radiological releases important to criticality are set to “0.00E+00.”

Table B6.5-1 Moderator Events during IHF Operations

Fault Tree Name	Applies To
MOD-NOFIRE	Transportation casks, canisters, and waste packages
MOD-FIRE	Transportation casks, canisters, and waste packages

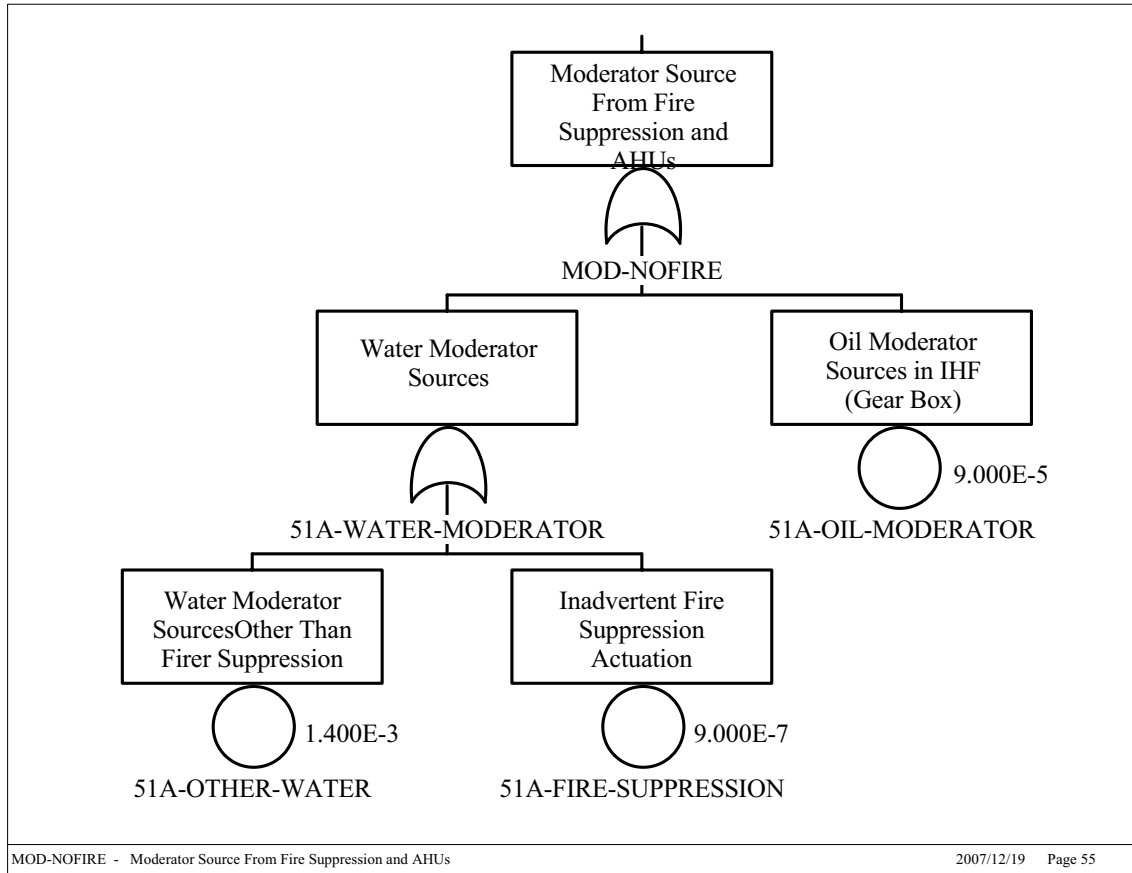
NOTE: MOD: = moderator.

Source: Original

Figure B6.5-1 illustrates the possibility of a moderator source during normal operations in the IHF. Potential sources are:

- Oil from the 300-ton crane gear box
- Water from an inadvertent activation of the fire suppression system or air handling unit (AHU)
- Water from other sources in the facility (i.e., water pipe).

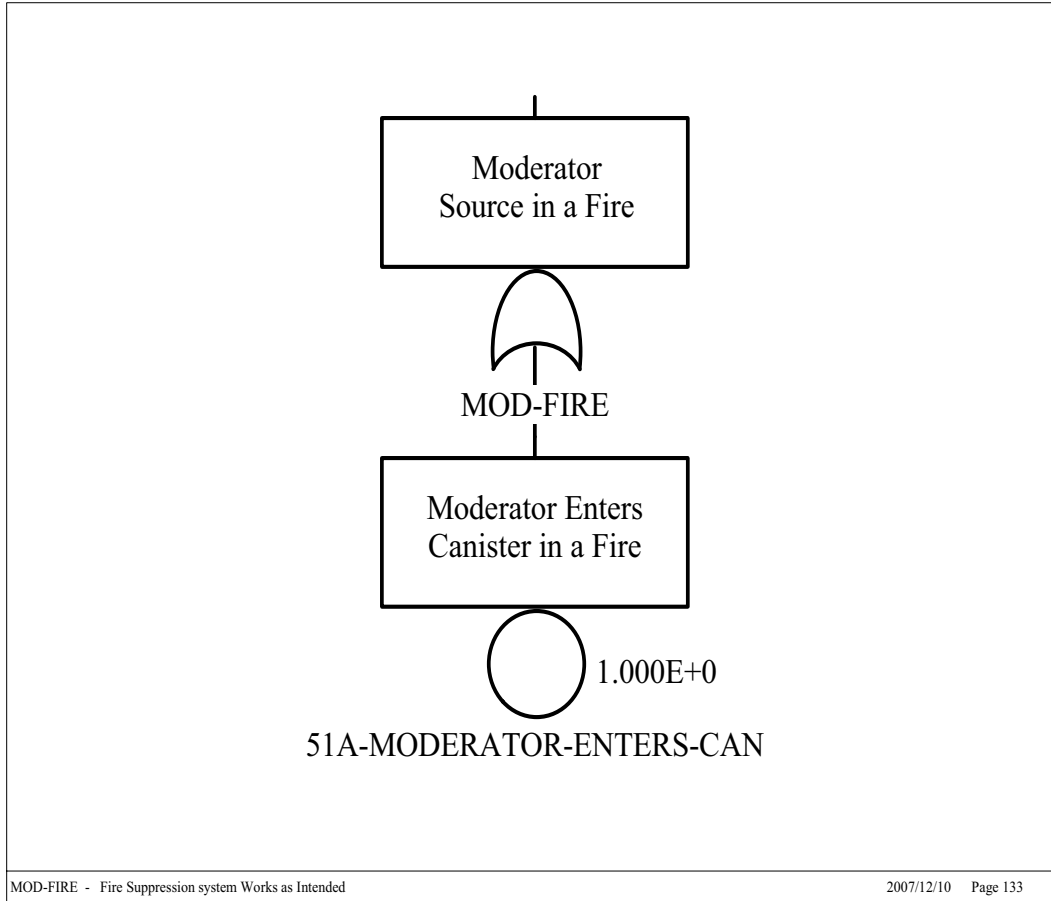
Details on moderator source failures are addressed in Section 6.2.2.6. The calculated probability of a moderator being present when there is no facility fire is 1.493E-03.



Source: Original

Figure B6.5-1. Moderator Source from Fire Suppression and AHUs

Figure B6.5-2 addresses the possibility of a moderator entering a breached transportation cask, canister, or waste package during a facility fire in the IHF. A conservative conditional probability, given a breach, of 1.00E+00 has been established for this event.



Source: Original

Figure B6.5-2. Moderator Source in a Fire

ATTACHMENT C
ACTIVE COMPONENT RELIABILITY DATA ANALYSIS

CONTENTS

	Page
ACRONYMS AND ABBREVIATIONS	C-5
C1 INDUSTRY-WIDE COMPONENT RELIABILITY DATA	C-6
C1.1 COMPONENT DEFINITION	C-6
C1.2 INDUSTRY-WIDE RELIABILITY DATA.....	C-13
C1.3 CRANE AND SPENT FUEL TRANSFER MACHINE DROP ESTIMATES	C-18
C2 BAYESIAN DATA COMBINATION	C-21
C2.1 PARAMETER ESTIMATION USING DATA FROM DIFFERENT SOURCES.....	C-23
C2.2 PARAMETER ESTIMATION IN CASE ONLY ONE DATA SOURCE IS AVAILABLE.....	C-31
C3 COMMON CAUSE FAILURE DATA	C-32
C4 ACTIVE COMPONENT RELIABILITY ESTIMATES INPUT TO SAPHIRE	C-35
C5 REFERENCES; DESIGN INPUTS	C-48

FIGURES

	Page
C2.1-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)	C-31
C3-1. Alpha Factor.....	C-33

TABLES

	Page
C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM).....	C-9
C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database	C-13
C1.2-2. Data Source Comparison for Check Valve	C-16
C1.2-3. Failure Rates Extracted from Various Data Sources for Check Valve.....	C-17
C1.2-4. Guidelines for Industry-wide Data Selection.....	C-17
C2.1-1. Comparison of Results of Parametric Empirical Bayes and Results Reported by Lopez Droguett et al.....	C-26
C3-1. Alpha Factor Table	C-34
C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models	C-37

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 codes (FM) were developed using prior database conventions or abbreviations that would be as intuitively obvious as possible.

Both type (TYP) and failure mode 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 & 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 & 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 Misspooling (Hourly)
DMP-FOH	Damper (Manual) Fails to Operate

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)
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

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
PMD-FTR	Pump (Motor Driven) Fails to Run
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand
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

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
TDA-FOH	Transducer (Air Flow) Failure
TDP-FOH	Transducer (Pressure) Fails
TDT-FOH	Transducer (Temperature) Fails
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; TYP-FM = component type and failure mode; 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
<i>Guidelines for Process Equipment Reliability Data with Data Tables.</i> [CCPS] (Ref. C5.1)
<i>Savannah River Site, Generic Data Base Development (U)</i> [SRS Reactors] (Ref. C5.5)
<i>The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve Component.</i> NUREG/CR-3154 (Ref. C5.6)
<i>Waste Form Throughputs for Preclosure Safety Analysis.</i> [BSC 2007](Ref. C5.7)
<i>Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.</i> [EPRI PRA] (Ref. C5.8)

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
<i>Component Failure and Repair Data for Coal-Fired Power Units.</i> EPRI AP-2071 [EPRI Pipe Failure Study] (Ref. C5.10)
<i>Mechanical Reliability: Theory, Models and Applications.</i> [AIAA] (Ref. C5.11)
<i>Military Handbook, Reliability Prediction of Electronic Equipment.</i> MIL-HDBK-217F [MIL-HDBK-217F] (Ref. C5.12)
<i>The In-Plant Reliability Data Base for Nuclear Power Plant Components - Pump Component.</i> NUREG/CR-2886. (Ref. C5.13)
<i>Some Published and Estimated Failure Rates for Use in Fault Tree Analysis</i> [DuPont] (Ref. C5.14)
<i>Analysis of Station Blackout Risk. Volume 2 of Reevaluation of Station Blackout Risk at Nuclear Power Plants.</i> NUREG/CR-6890 (Ref. C5.15)
<i>Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.</i> NUREG/CR-6928. (Ref. C5.16)
"Train Accidents by Cause from Form FRA F 6180.54." [Federal Railroad Administration] (Ref. C5.17)
<i>Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999.</i> [McKenna] (Ref. C5.20)
Ruggedized Card Reader/Ruggedized Keypad Card Reader. [HID] (Ref. C5.21)
<i>IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems.</i> [IEEE-493] (Ref. C5.22)
<i>IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.</i> [IEEE-500] (Ref. C5.23)
<i>The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report- Diesel Generators, Batteries, Chargers and Inverters.</i> NUREG/CR-3831 (Ref. C5.24)
Instruments and Software Solutions (for Emergency Response and Health Physics [LAURUS] (Ref. C5.25)
<i>A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.</i> NUREG-1774. (Ref. C5.26)
<i>Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980.</i> NUREG/CR-1363 (Ref. C5.28)
<i>The Reliability Data Handbook.</i> [Moss] (Ref. C5.32)
<i>Control of Heavy Loads at Nuclear Power Plants.</i> NUREG-0612. (Ref. C5.35)
<i>Handbook of Reliability Prediction Procedures for Mechanical Equipment</i> [NSWC-98-LE1] (Ref. C5.37)
"Using the EDA to Gain Insight into Failure Rates" [Rand] (Ref. C5.38)
<i>Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data.</i> NUREG/CR-4639, (Ref. C5.39)

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
<i>Nonelectronic Parts Reliability Data 1995.</i> NPRD-95. [NPRD -95] (Ref. C5.40)
<i>Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.</i> [SAIC Umatilla] (Ref. C5.41)
<i>Offshore Reliability Data Handbook.</i> 2nd Edition [OREDA-92] (Ref. C5.42)
<i>Offshore Reliability Data Handbook.</i> 4th Edition. [OREDA-2002] (Ref. C5.43)
<i>Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1972-April 30, 1980.</i> NUREG/CR-1205. (Ref. C5.45)
<i>N-Reactor Level 1 Probabilistic Risk Assessment: Final Report.</i> [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 failure mode (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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 – 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% – 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 $79,914.87 \times 17$ 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 λ_j 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:

$$P(\lambda_j | E) = \frac{P(\lambda_j)L(E | \lambda_j)}{\sum_j P(\lambda_j)P(E | \lambda_j)} \quad (\text{Eq. C-1})$$

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 or 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 be 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:

$$L_i(\nu, \tau) = \int_0^1 \text{Binom}(x, r, n) \times g(x, \nu, \tau) dx \quad (\text{Eq. C-2})$$

where $\text{Binom}(x, r, n)$ 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}
1 st percentile	1.32×10^{-7}	3.16×10^{-7}
5 th percentile	4.75×10^{-7}	1.38×10^{-6}
10 th percentile	9.38×10^{-7}	2.67×10^{-6}
50 th percentile (median)	1.04×10^{-5}	1.61×10^{-5}
90 th percentile	1.14×10^{-4}	7.79×10^{-5}
95 th percentile	2.26×10^{-4}	1.36×10^{-4}
99 th 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 $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$. 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 $\exp(v)$, where v 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 $10^{-8}/\text{hr}$ to $10^{-2}/\text{hr}$. Thus, the likelihood functions, unconditional on x , for each of the data source in the matrix A , are calculated as follows:

$$a := 1..4 \quad fe(a, x) := dlnorm\left(x, \ln(A_{a,1}), \frac{\ln(A_{a,2})}{1.645}\right) \quad (\text{Eq. C-3})$$

$$LA(a, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fe(a, x) \cdot dlnorm(x, \nu, \tau) dx \quad (\text{Eq. C-4})$$

(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:

$$b := 1..8 \qquad fd(b, x) := dpois(Bb, 1, Bb, 2 \cdot x) \qquad \text{(Eq. C-5)}$$

$$LB(b, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fd(b, x) \cdot dlnorm(x, \nu, \tau) dx \qquad \text{(Eq. C-6)}$$

(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:

$$\underline{\underline{L}}(\nu, \tau) := \sum_{a=1}^4 \ln(LA(a, \nu, \tau)) + \sum_{b=1}^8 \ln(LB(b, \nu, \tau)) \qquad \text{(Eq. C-7)}$$

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:

$$\nu := \ln(10^{-6}) \qquad \nu = -13.8$$

Based on a typical error factor value of 10, a guess value for τ is:

$$\tau := \frac{\ln(10)}{1.645} \qquad \tau = 1.4$$

A reasonable range over which to perform the likelihood maximization is as follows:

<i>Given</i>	$\nu > -20$	$\nu < -1$
	$\tau > 0.01$	$\tau < 5$

The maximum likelihood estimators for ν and τ are:

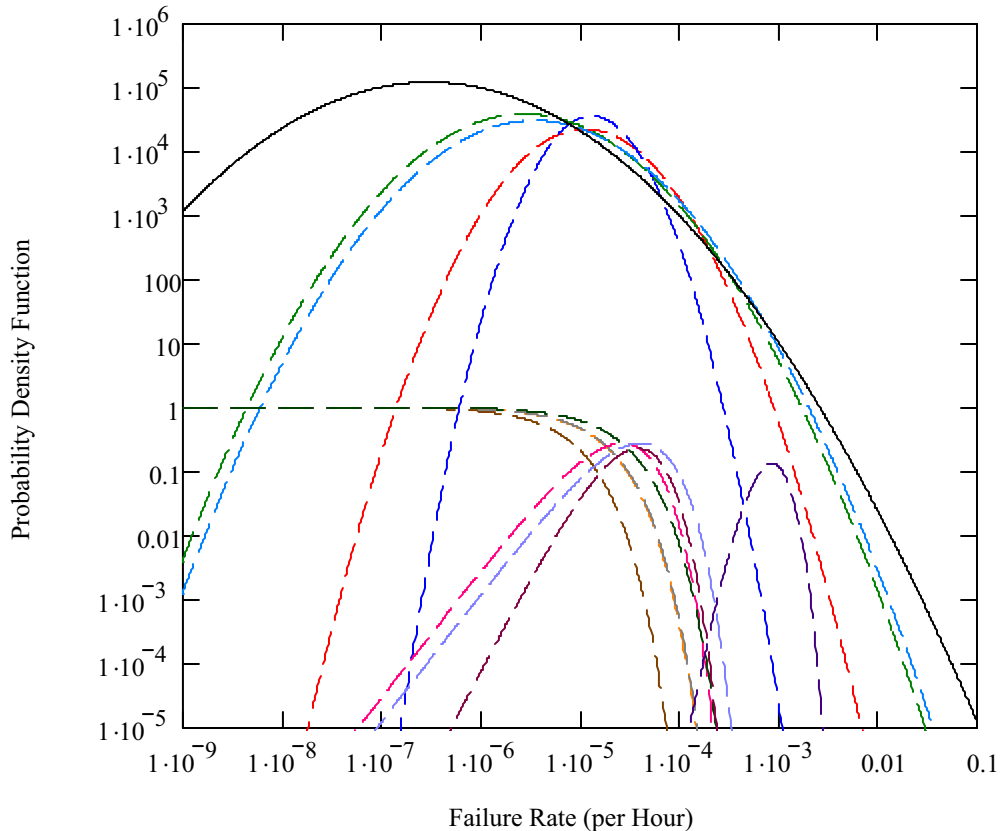
$$\begin{aligned} \underline{\nu} &:= \text{Maximize}(L, \nu, \tau) & \underline{\nu} &:= L1 & \nu &= -11.478 \\ \underline{\tau} &:= L2 & \tau &= 1.874 \end{aligned}$$

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)):

$$\begin{aligned} \underline{m} &:= \exp\left(\nu + \frac{\tau}{2}\right) & m &= 6.00 \times 10^{-5} & \text{per hour} \\ EF &:= \exp(1.645 \cdot \tau) & EF &= 21.8 \end{aligned}$$

Notable percentiles of the population-variability distribution are as follows (expressed as hourly failure rates) and shown in Figure C2.1-1:

1 st percentile:	$qlnorm(0.01, \nu, \tau) = 1.32 \times 10^{-7}$
5 th percentile:	$qlnorm(0.05, \nu, \tau) = 4.75 \times 10^{-7}$
10 th percentile:	$qlnorm(0.10, \nu, \tau) = 9.38 \times 10^{-7}$
50 th percentile:	$qlnorm(0.50, \nu, \tau) = 1.04 \times 10^{-5}$
90 th percentile:	$qlnorm(0.90, \nu, \tau) = 1.14 \times 10^{-4}$
95 th percentile:	$qlnorm(0.95, \nu, \tau) = 2.26 \times 10^{-4}$
99 th percentile:	$qlnorm(0.99, \nu, \tau) = 8.10 \times 10^{-4}$



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 U.S. 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.

$$\alpha_k^m = \frac{n_k}{\sum_{j=1}^m n_j} \quad k = 1, \dots, m$$

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 CCF size, based on all CCF events in their database. Events were mapped to a given CCF 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 ₁₀	P ₅₀	P ₉₀	
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 within 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 & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	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 & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
CRJ-DRP	Jib Crane Drop	B	9.72E+04	2.60E-05		1 source; N/D	NUREG-1774 (Ref. C5.26)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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 Misspooling (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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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	OverSpeed 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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncertainty Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources ^a
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)
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; Dist Type = Distribution Type; EF = Lognormal Error Factor; G = Gamma Distribution; L = Lognormal Distribution;

N/D = Numerator/Denominator; TYP-FM = Component Type and Failure Mode.

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/b196002.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. (DIRS 184293)
- C5.14 *E.I. DuPont de Nemours & Company (Inc.) 1981. *Some Published and Estimated Failure Rates for Use in Fault Tree Analysis*. Washington, DE: 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, New York: 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
ACRONYMS AND ABBREVIATIONS	D-5
D1 LOSS OF CONTAINMENT DUE TO DROPS AND IMPACTS	D-7
D1.1 LAWRENCE LIVERMORE NATIONAL LABORATORY ANALYSIS OF CANISTERS AND CASKS.....	D-8
D1.2 IDAHO NATIONAL LABORATORY ANALYSIS OF SPENT NUCLEAR FUEL CANISTERS AND MULTICANISTER OVERPACKS.....	D-12
D1.3 PROBABILITIES OF FAILURE OF HIGH LEVEL WASTE CANISTERS DUE TO DROPS.....	D-19
D1.4 PROBABILITIES OF FAILURE OF WASTE PACKAGES DUE TO DROPS AND IMPACTS	D-21
D1.5 PREDICTING OUTCOMES OF OTHER SITUATIONS BY EXTRAPOLATING STRAINS FOR MODELED SCENARIOS	D-26
D1.6 MISCELLANEOUS SCENARIOS	D-28
D2 PASSIVE FAILURE DUE TO FIRE.....	D-29
D2.1 ANALYSIS OF CANISTER FAILURE DUE TO FIRE	D-30
D2.2 SHIELDING DEGRADATION IN A FIRE.....	D-69
D3 SHIELDING DEGRADATION DUE TO IMPACTS.....	D-72
D3.1 DAMAGE THRESHOLDS FOR LOS	D-74
D3.2 SEVERITY OF DAMAGE VERSUS IMPACT VELOCITY	D-75
D3.3 ESTIMATE OF THRESHOLD SPEEDS FOR LOSS OF SHIELDING DUE TO IMPACTS	D-79
D3.4 PROBABILITY OF LOSS OF SHIELDING	D-81
D4 REFERENCES.....	D-87
D4.1 DESIGN INPUTS	D-87
D4.2 DESIGN CONSTRAINTS.....	D-93

FIGURES

	Page
D1.1-1. Original and Shifted Cumulative Distribution Functions (CDF) for Capacity (or Fragility) Plotted as a Function of True Strain.....	D-9
D2.1-1. Comparison Between Results Calculated Using the Simplified Heat Transfer Model and ANSYS – Fire Engulfing a TAD Canister in a Waste Package	D-43
D2.1-2. Plot of Larson-Miller Parameter for Type 316 Stainless Steel	D-54
D2.1-3. Yield, Ultimate, and Flow Stress for Type 316 Stainless Steel	D-55
D2.1-4. Probability Distribution for the Failure Temperature of Thin-Walled Canisters ...	D-59
D2.1-5. Probability Distribution for the Failure Temperature of Thick-Walled Canisters.....	D-60
D2.1-6. Probability Distribution for Maximum Canister Temperature – Thin-Walled Canister in a Waste Package	D-62
D2.1-7. Distribution of Radiation Energy from Fire.....	D-68
D3.2-1. Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph	D-77
D3.2-2. Truck Steel/Lead/Steel Inner Shell Strain versus Impact Speed	D-78
D3.2-3. Rail Steel/Lead/Steel Strain versus Impact Speed	D-79
D3.4-1. Summary Event Tree Showing Model Logic for Canisters and Aging Overpacks	D-82

TABLES

	Page
D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1	D-9
D1.2-1. Container Configurations and Loading Conditions	D-13
D1.2-2. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for Representative Canister within an Aging Overpack.....	D-14
D1.2-3. Failure Probabilities with and without Triaxiality Factor, with and without Fragility Curve Adjustment, for Representative Canister.....	D-14
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	D-16
D1.2-5. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Transportation Cask	D-17
D1.2-6. Strains at Various Canister Locations Due to Drops	D-18
D1.2-7. Failure Probabilities for the DOE Spent Nuclear Fuel (DSNF) Canisters and Multicanister Overpack (MCO).....	D-19
D1.4-1. Waste Package Probabilities of Failure for Various Drop and Impact Events	D-23
D1.5-1. Calculated Strains and Failure Probabilities for Given Side Impact Velocities	D-27
D2.1-1. Probability Distribution for Fire Duration - Without Automatic Fire Suppression.....	D-33
D2.1-2. Probability Distribution for Fire Duration - With Automatic Fire Suppression.....	D-35
D2.1-3. Effective Thermal Properties for 21-PWR Fuel in a TAD	D-39
D2.1-4. Model Inputs – Bare Canister	D-46
D2.1-5. Model Inputs – Canister in a Waste Package.....	D-47
D2.1-6. Model Inputs – Canister in Transportation Cask	D-48
D2.1-7. Model Inputs – Canister in a Shielded Bell	D-49
D2.1-8. Summary of Canister Failure Probabilities in Fire	D-63
D2.1-9. Model Inputs – Bare Fuel Cask	D-65
D2.1-10. Summary of Fuel Failure Probabilities	D-67
D2.1-11. Probabilities that Radiation Input Exceeds Failure Energy for Cask	D-69
D3.2-1. Maximum Plastic Strain in Inner Shell of Sandwich Wall Casks	D-76
D3.3-1. Drop Height to Reach a Given Impact Speed.....	D-81
D3.3-2. Impact Speeds on Real Target for Equivalent Damage for Unyielding Targets	D-81
D3.4-1. Probabilities of Degradation or Loss of Shielding.....	D-86

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
SDU	steel-depleted uranium-steel
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	watts per meter Kelvin
W/m ² K	watts 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.

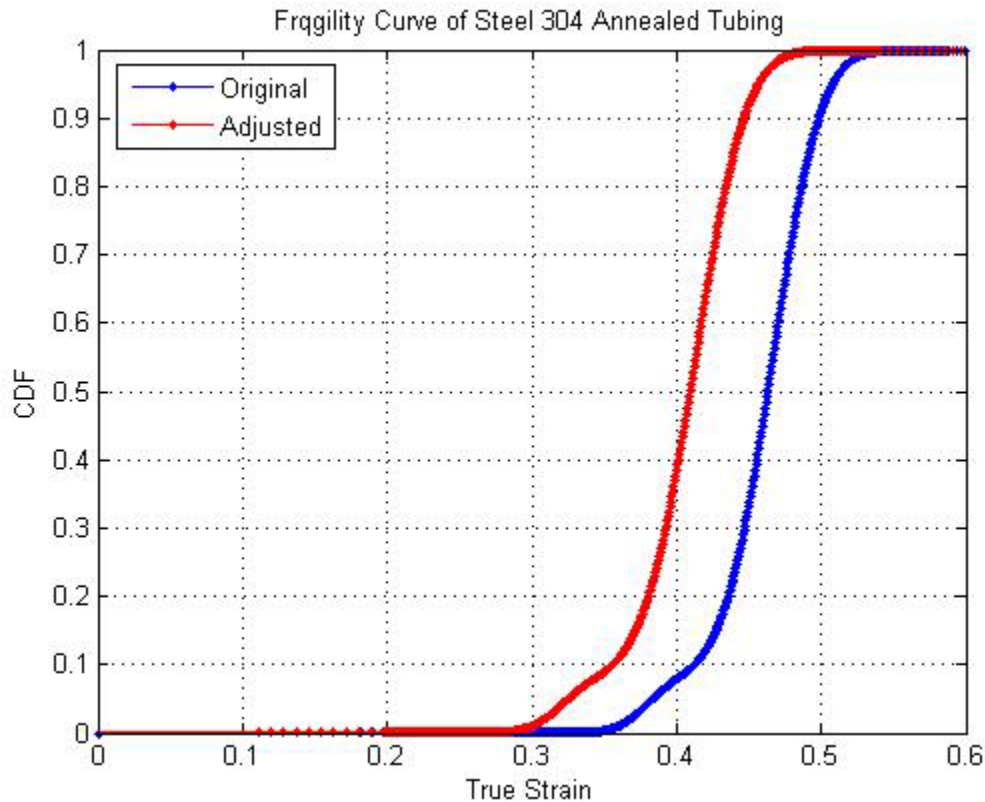
The maximum strain for each scenario was compared with the capacity distribution based on material properties to obtain containment failure probabilities using the methodology described in Section 4.3.2.2. For simplicity and consistency in interpreting results, the impact-surface conditions, including 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-inch-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
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	w/ Triaxiality	w/o Triaxiality	w/ 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.
^bValues 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	w/ Triaxiality	w/o Triaxiality	w/ 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	w/ Triaxiality	w/o Triaxiality	w/ 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.

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.

^bValues 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)

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	w/ Triaxiality	w/o Triaxiality	w/ 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.

^bValues 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	w/ 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.
^bValues 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 Minimum 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 Bernoulli 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:

$$r' = r + n \quad \text{and} \quad s' = s + N - n \quad (\text{Eq. D-1})$$

The mean, μ , and standard deviation, σ , of the posterior distribution are determined using the following equations:

$$\mu = r' / (r' + s') \quad \text{and} \quad \sigma = \{r's' / [(r' + s' + 1)(r' + s')^2]\}^{1/2} \quad (\text{Eq. D-2})$$

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:

$$P = \int_{-\infty}^x N(t) dt \quad \text{and} \quad x = \frac{ETF - 1}{COV} \quad (\text{Eq. D-3})$$

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 triaxiality 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, p. 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: ^aA 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 cm³/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.

$$\tau_i = \tau_{ref} \left(\frac{v_i}{v_{ref}} \right)^2 \quad (\text{Eq. D-4})$$

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		% strain	Probability of failure
(ft/sec)	(ft/min)		
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 $< 1 \times 10^{-8}$. 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 $1/90^{\text{th}}$ 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 $1/7^{\text{th}}$ 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 minutes, the median (50th percentile) is approximately 24 min, and the error factor (i.e., the ratio of the 95th 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 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 is 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:

$$T_c = \frac{q_{c,net} \Delta t}{m_c c_{p,c}} + T_{c,i} \quad (\text{Eq. D-5})$$

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:

$$q_{c,net} = q_{r,fire} + q_{c,fire} - q_{r,f} \quad (\text{Eq. D-6})$$

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:

$$q_{r,fire} = \epsilon_c A_c F_{c-fire} F_s \sigma (T_{fire}^4 - T_c^4) \quad (\text{Eq. D-7})$$

where

ϵ_c =emissivity of the canister surface

A_c =surface area of the canister

F_{c-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:

$$q_{c,fire} = A_c F_s h_{conv} (T_{fire} - T_c) \quad (\text{Eq. D-8})$$

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:

$$q_{r,f} = \frac{A_c F_{c-f} \sigma (T_c^4 - T_f^4)}{1/\epsilon_c + 1/\epsilon_f - 1} \quad (\text{Eq. D-9})$$

where F_{c-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:

$$T_f = \frac{(q_{r,f} + q_{DH})\Delta t}{m_f c_{p,f}} + T_{fi} \quad (\text{Eq. D-10})$$

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:

$$\delta = \sqrt{\alpha t} \quad (\text{Eq. D-11})$$

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:

$$T_{ob} = \frac{(q_{ob} - q_{ib})\Delta t}{m_{ob}c_{p,ob}} + T_{ob,i} \quad (\text{Eq. D-12})$$

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:

$$q_{ob} = \epsilon_{ob} A_{ob} F_{fc} F_s \sigma (T_f^4 - T_{ob}^4) \quad (\text{Eq. D-13})$$

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:

$$q_{ib} = \frac{A_{ob} F_{oi} \sigma (T_{ob}^4 - T_{ib}^4)}{1/\epsilon_{ib} + 1/\epsilon_{ob} - 1} \quad (\text{Eq. D-14})$$

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:

$$T_c = \frac{(q_{ib} + q_{DH})\Delta t}{m_c c_{p,c}} + T_{c,i} \quad (\text{Eq. D-15})$$

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.

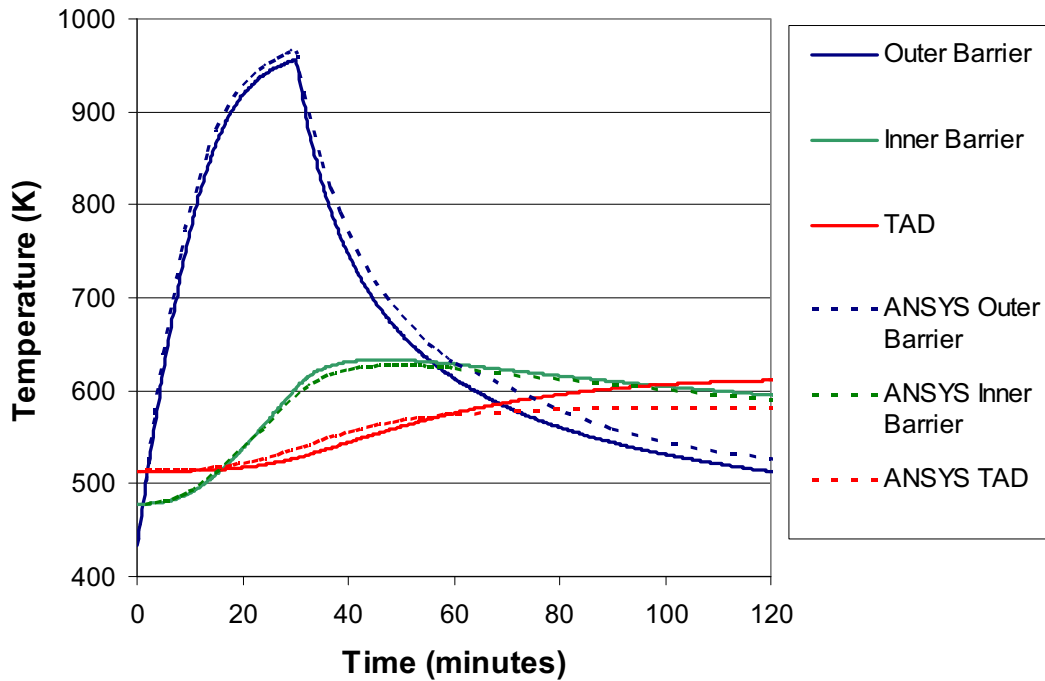
Unlike the bare canister case in which heating of the canister ends when the fire ends, heating of a canister that is inside other containers will increase after the fire ends as heat is transmitted from the heated outer and inner barrier. After the fire has been extinguished, heat will be lost by the 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/m² 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 $30 \text{ W/m}^2 \text{ K}$ have been measured in vigorously burning pool fires (Ref. D4.1.51, pp. 19-21), although values on the order of $20 \text{ W/m}^2 \text{ K}$ 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 $5 \text{ W/m}^2 \text{ K}$ 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 $17.5 \text{ W/m}^2 \text{ K}$ and $4.2 \text{ W/m}^2 \text{ K}$, respectively. This distribution yields practical upper and lower bound values (0.1 and 99.9th percentiles) of approximately 5 and $30 \text{ W/m}^2 \text{ K}$.

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 inches (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 inch 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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Table 17)
Initial Temperature (K)	543	Estimated from <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
Outer Barrier of Waste Package		
Outer Diameter (m)	1.8816	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0254	Listed in <i>TAD Waste Package Configuration</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
Inner Barrier of Waste Package		
Outer Diameter (m)	1.8212	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0508	Listed in <i>TAD Waste Package Configuration</i> (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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (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 <i>Introduction to Heat Transfer</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (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

Table D2.1-6. Model Inputs – Canister in Transportation Cask (Continued)

Model Parameter	Value	Basis/Rationale
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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (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 <i>Introduction to Heat Transfer</i> (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 <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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

Table D2.1-7. Model Inputs – Canister in a Shielded Bell (Continued)

Model Parameter	Value	Basis/Rationale
Length (m)	5.4	Typical length of TAD canister listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (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 <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
Shielded Bell		
Outer Diameter (m)	2.388	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (Ref. D4.1.11)
Wall Thickness (m)	0.273	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (Ref. D4.1.11)
Length (m)	7.62	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (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 <i>Introduction to Heat Transfer</i> (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:

$$\int_0^{t_f} \frac{dt}{t_R(T, \sigma)} = 1 \quad (\text{Eq. D-16})$$

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

$$t_R = 10^{\frac{P_{LM}-20}{T}} \quad (\text{Eq. D-17})$$

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:

$$\sigma = \frac{Pr_c}{h} \quad (\text{Eq. D-18})$$

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):

$$\bar{\sigma} = k(\sigma_y + \sigma_u) \quad (\text{Eq. D-19})$$

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:

$$P_{LM} = T[C + \log(t_f)] \quad (\text{Eq. D-20})$$

where

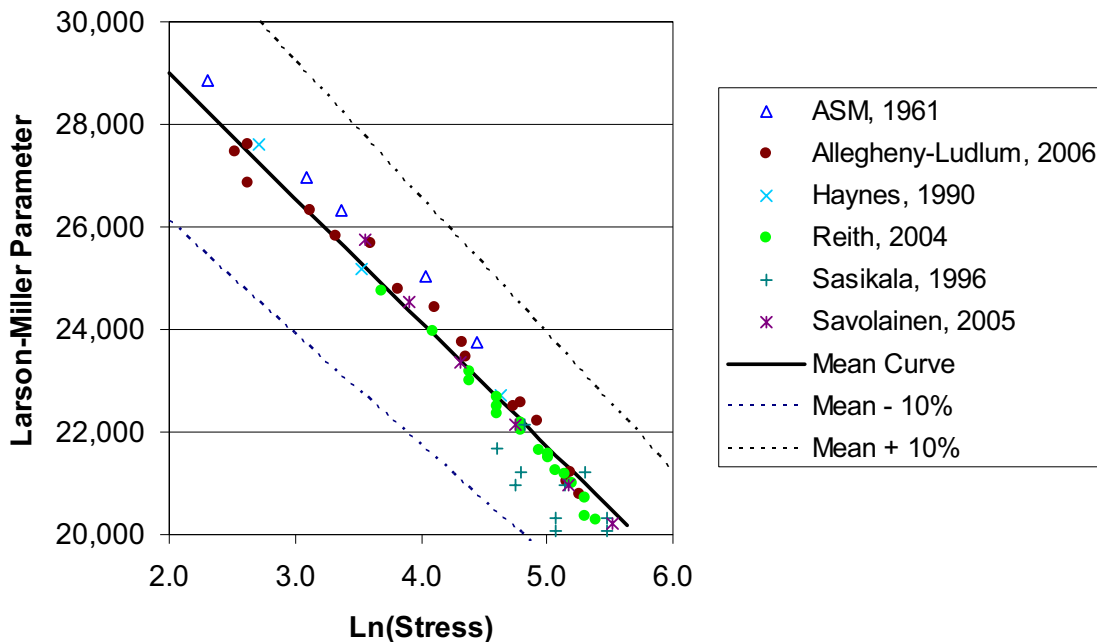
- T = temperature (K)
- t_f = failure time (hours) determined in testing
- C = a constant that is approximately 20 for most stainless steels

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:

$$P_{LM} = 33,845 - 2,423 \ln(\sigma) \quad (\text{Eq. D-21})$$

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.

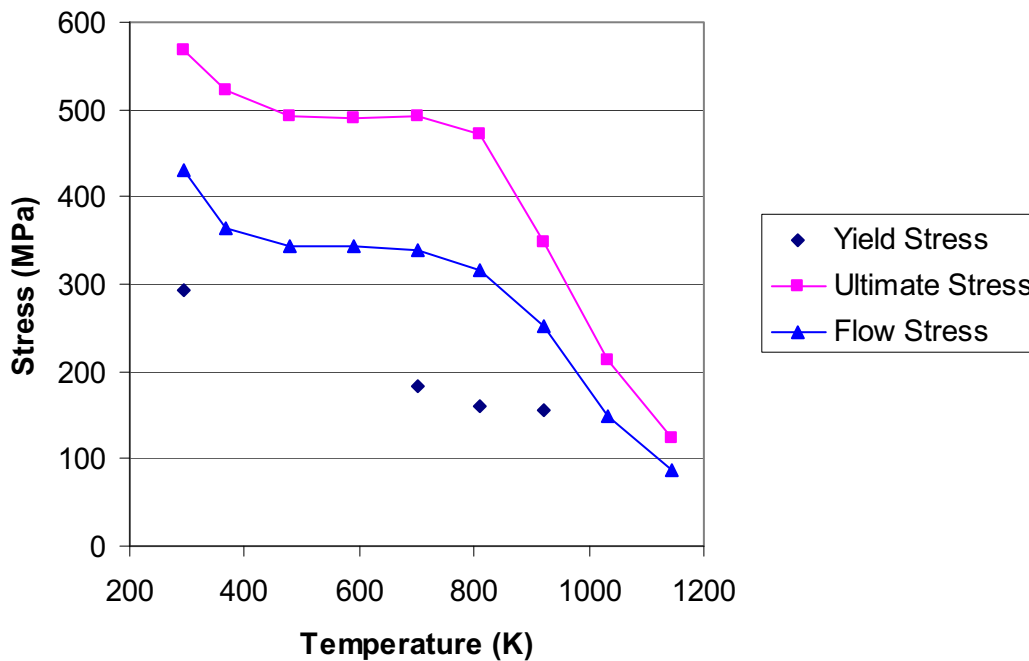
Figure D2.1-2. Plot of Larson-Miller Parameter for Type 316 Stainless Steel

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:

$$\bar{\sigma} = 395.9 - 0.0925T \quad \text{for } T < 800 \text{ K} \quad (R^2 = 0.889) \quad (\text{Eq. D-22a})$$

$$\bar{\sigma} = 899.1 - 0.7139T \quad \text{for } T \geq 800 \text{ K} \quad (R^2 = 0.989) \quad (\text{Eq. D-22b})$$

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 as 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:

$$P = P_0 \left[1 + C \left(\frac{T_{\text{can}} - T_{\text{can},0}}{T_{\text{can},0}} \right) \right] \quad (\text{Eq. D-23})$$

where

- P_0 = initial pressure inside the canister (including potential fuel failures)
- $T_{\text{can},0}$ = 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.

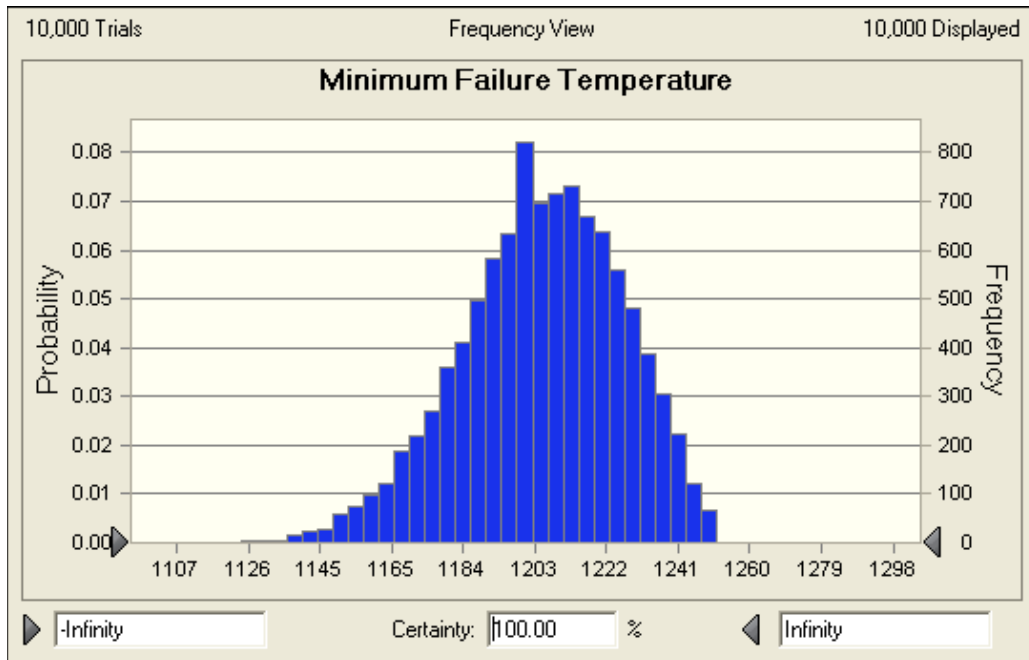
D2.1.5.1 Probabilistic Analysis of Canister Failure Temperature

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.

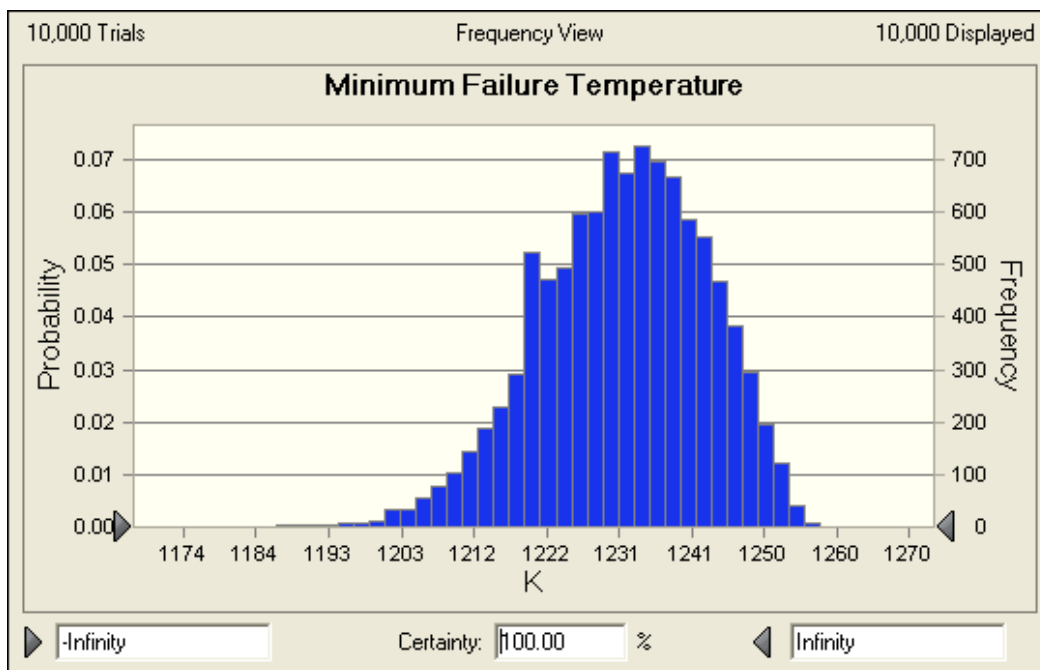
A similar analysis was performed for bare canisters. This calculation used the higher heating rate discussed in Section D2.1.4.5.3.3. The resulting probability distribution was nearly identical to the one shown in Figure D2.1-4. The reason for this is that canister failure was nearly always due to limit 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} , 100,000 (10^5) samples were needed. The maximum number of samples for any run was set at 1 million. If no failures were calculated for 1 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:

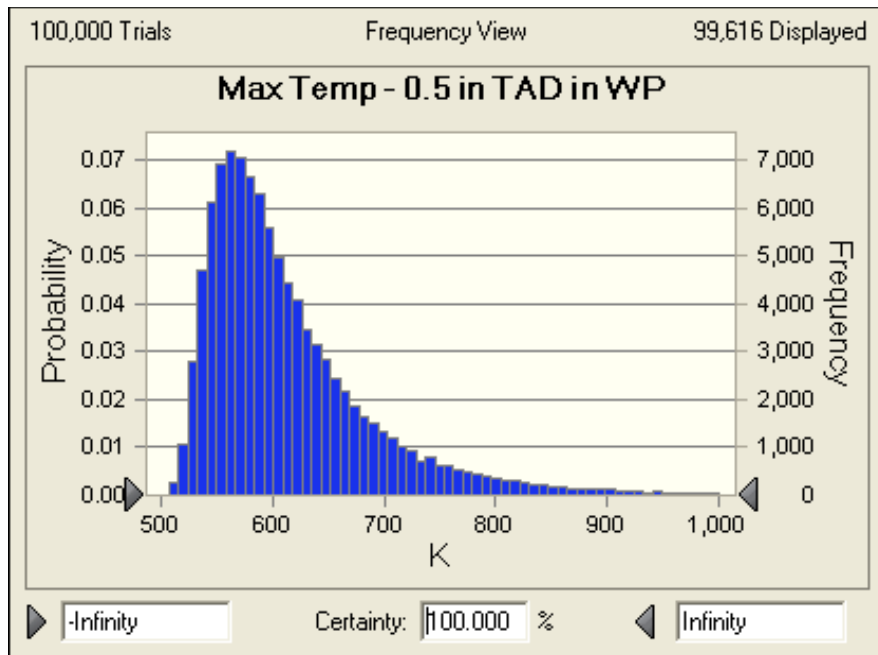
$$\sigma = \sqrt{\frac{\frac{n_{\text{fail}}}{N} \left(\frac{N - n_{\text{fail}}}{N} \right)}{N}} \quad (\text{Eq. D-24})$$

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: ^aFor 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.

^bConfigurations 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 only¹), 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 average properties: thermal conductivity = 1.2 W/m K; density = 2,200 kg/m³; 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

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.

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/m³ 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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident</i> (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 <i>Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident</i> (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)

Table D2.1-9. Model Inputs – Bare Fuel Cask (Continued)

Model Parameter	Value	Basis/Rationale
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)
Post-Fire Conditions		
Ambient Temperature (K)	361	Post-fire temperature of 190°F from <i>Discipline Design Guide and Standards for Surface Facilities HVAC Systems</i> 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 (SDU) 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.

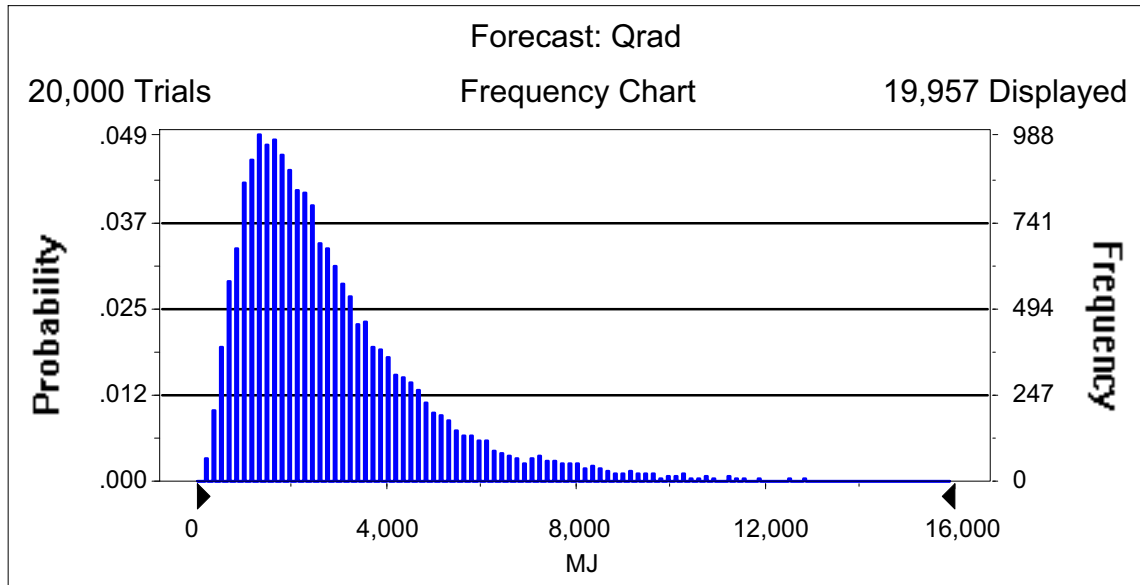
The probability distributions for fire temperature and fire duration discussed in section D2.1.1 can be used to determine the probability that the fire conditions listed in the preceding paragraph would be exceeded. This is accomplished by first determining the probability distribution (using Crystal Ball) for the maximum thermal radiation energy from the fire using the following equation:

$$Q_{\text{rad}} = \sigma A T_{\text{fire}}^4 t_{\text{fire}} \quad (\text{Eq. D-25})$$

where:

- σ = the Stefan-Boltzmann constant ($5.668 \times 10^{-8} \text{ W/m}^2 \text{ K}^4$)
- 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 expand, 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 $0.058 \text{ cm}^2/\text{g}$ 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 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 concrete², 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 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

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).

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 principal 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 than 120 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) provide 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.

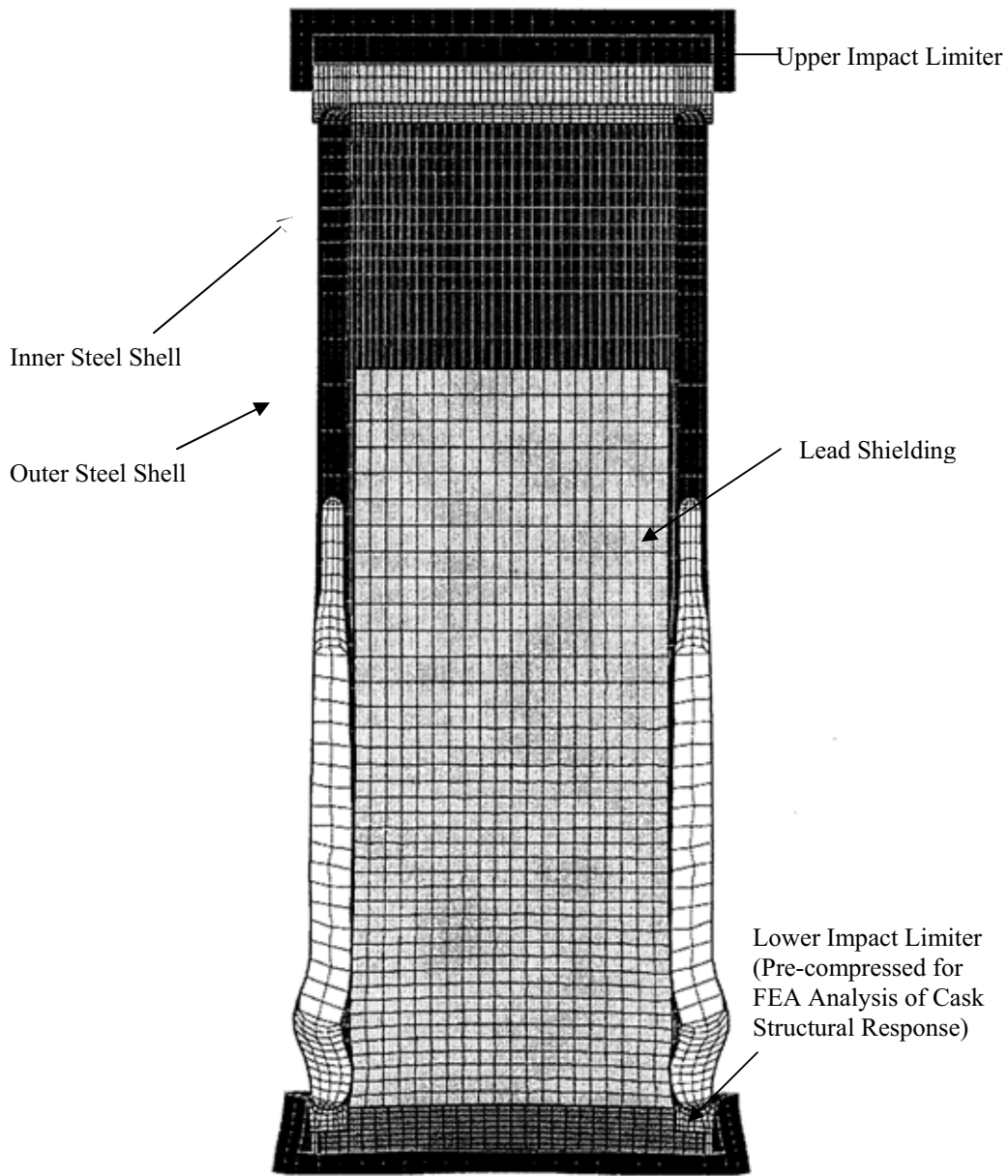
Two horizontal lines were superimposed on Figures D3.2-2 and D3.2-3 to plot the 0.2% and 2.0% strain to represent the respective S2 and S3 thresholds for inner shell strain. The intersections of the strain curves with the respective threshold values indicate the minimum impact speed at which the respective 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

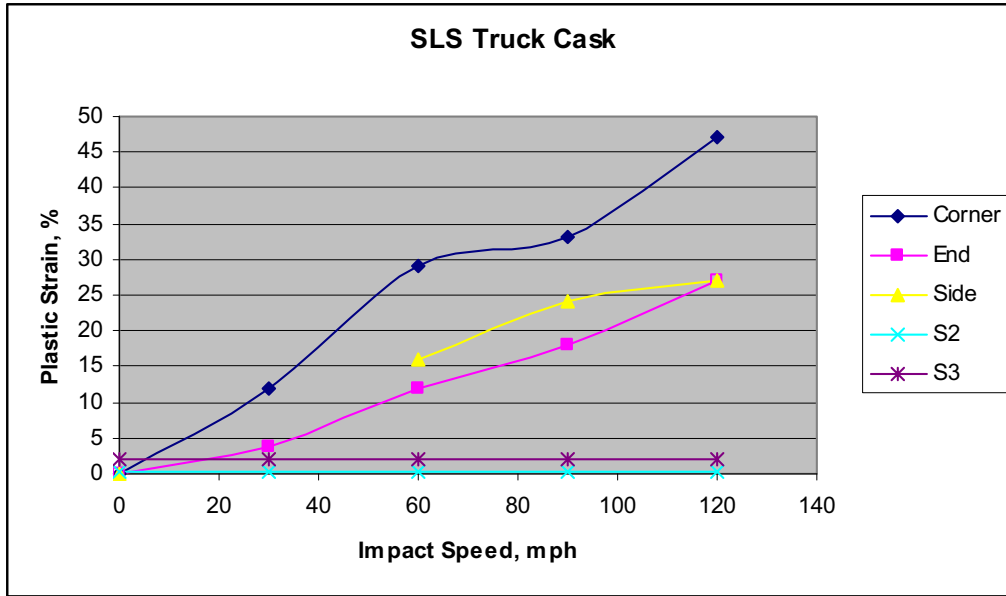
NOTE: SDU = steel-depleted uranium-steel; SLS = steel-lead-steel.

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

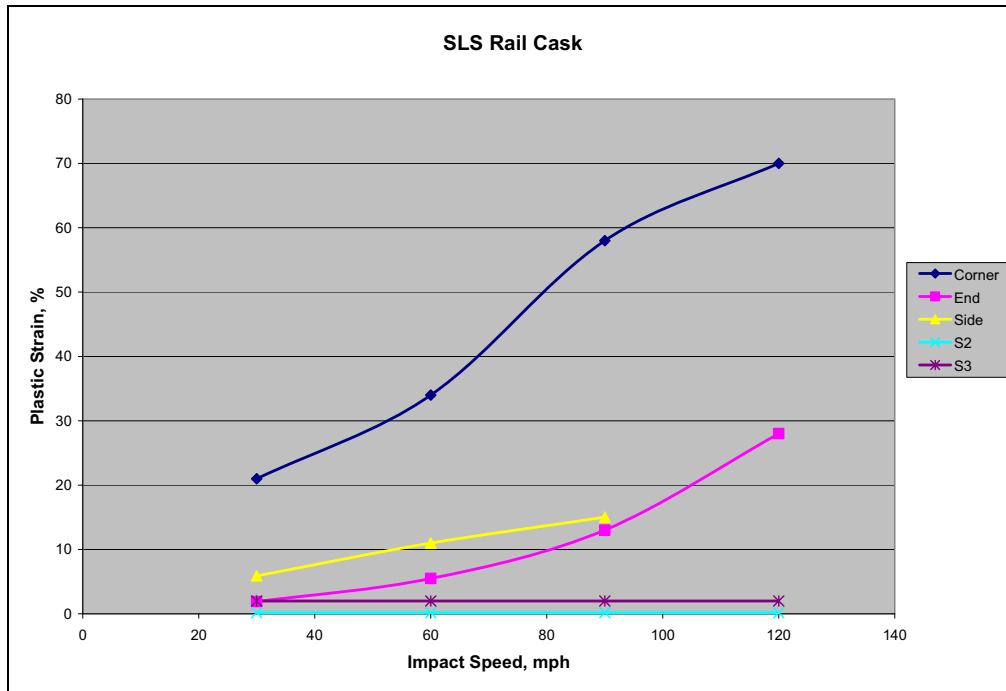


NOTE: ¹ Data points for strain versus speeds greater than 30 mph taken directly from NUREG/CR-6672, Table 5.3: plots extended to origin (0,0) to determine crossover for S2 and S3 threshold strains.

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

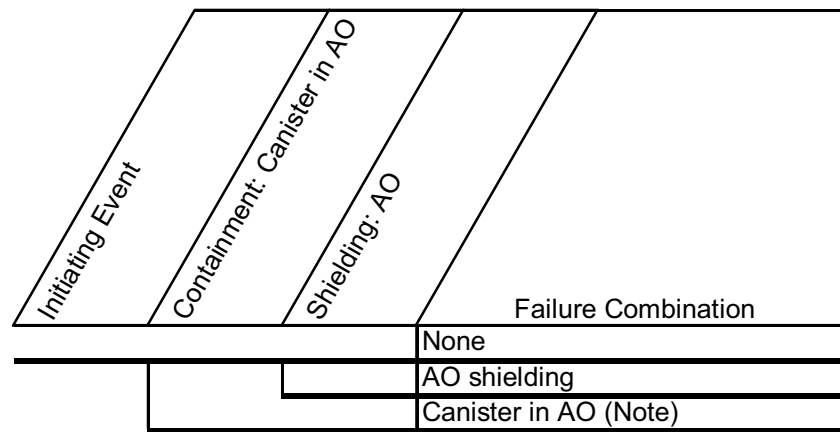
NUREG/CR-6672 (Ref. D4.1.65) do not have any direct relevance to event sequences for waste handling operations. However, the basic approach that breaks down the overall probability of an event sequence involving LOS into conditional probabilities for occurrence of various physical conditions that lead 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: Implies shielding is ineffective because of radionuclide release

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:

$$p_{AO}(C) = p_{AO}(C | O)p_{AO}(O) + p_{AO}(C | \bar{O})p_{AO}(\bar{O}), \quad (\text{Eq. D-26})$$

where

$p_{AO}(C)$ = probability of canister success within an AO.

$p_{AO}(C | O)$ = probability of canister success given AO shielding does not fail.

$p_{AO}(O)$ = probability that AO shielding does not fail.

$p_{AO}(C | \bar{O})$ = probability of canister success given AO shielding fails.

$p_{AO}(\bar{O})$ = 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: $p_{AO}(C | O) \gg p_{AO}(C | \bar{O})$. Furthermore, the probability of aging overpack breach is much less than probability of aging overpack success at the above drop and speed conditions. Therefore: $p_{AO}(O) \gg p_{AO}(\bar{O})$. 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

$$p_{AO}(C) \cong p_{AO}(C | O)p_{AO}(O) \quad (\text{Eq. D-27})$$

Note that

$$p_{AO}(C) = 1 - p_{AO}(\bar{C}) \quad \text{and}$$

$$p_{AO}(O) = 1 - p_{AO}(\bar{O}) \quad \text{and}$$

$$p_{AO}(C | O) = 1 - p_{AO}(\bar{C} | O) \quad (\text{Eq. D-28})$$

Substituting Equations D-28 into D-27 and rearranging yields:

$$p_{AO}(\bar{O}) \cong 1 - \frac{1 - p_{AO}(\bar{C})}{1 - p_{AO}(\bar{C} | O)} \quad (\text{Eq. D-29})$$

LLNL has developed a mean probability of failure for a canister within an aging overpack, $p_{AO}(\bar{C})$, 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, $p_{AO}(\bar{C} | O)$, must be less than the overall probability of canister failure within an aging overpack, $p_{AO}(\bar{C})$. 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 $p_{AO}(\bar{C} | O)$ and also substituting the aforementioned value for $p_{AO}(\bar{C})$ into Equation D-29, there obtains:

$$p_{AO}(\bar{O}) \cong 1 - \frac{1 - p_{AO}(\bar{C})}{1 - p_{AO}(\bar{C} | O)} = 1 - \frac{1 - 10^{-5}}{1 - 5 \times 10^{-6}} = 5 \times 10^{-6} \quad (\text{Eq. D-30})$$

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: ^aIn 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-MGR0-02100-000-00A. Rev. 00A. Las Vegas, Nevada: 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*. V0-CY05-QHC4-00459-00018-001-004. Oak Creek, Wisconsin: Morris Material Handling. 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.; Jäntschi, 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), 591-611. Cary, North Carolina: Oxford University Press. 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.

D4.2.2 10 CFR 71. 2007. Energy: Packaging and Transportation of Radioactive Material.

ATTACHMENT E
HUMAN RELIABILITY ANALYSIS

CONTENTS

	Page
ACRONYMS AND ABBREVIATIONS	E-9
E1 INTRODUCTION	E-11
E1.1 SUMMARY	E-11
E2 SCOPE AND BOUNDARY CONDITIONS	E-14
E2.1 SCOPE	E-14
E2.2 BOUNDARY CONDITIONS	E-14
E3 METHODOLOGY	E-16
E3.1 METHODOLOGY BASES	E-16
E3.2 GENERAL APPROACH.....	E-16
E3.2.1 Step 1: Define the Scope of the Analysis	E-16
E3.2.2 Step 2: Describe Base Case Scenarios	E-16
E3.2.3 Step 3: Identify and Define Human Failure Events of Concern	E-17
E3.2.3.1 Identifying Pre-initiator HFEs	E-18
E3.2.3.2 Identifying Human-Induced Initiator HFEs.....	E-18
E3.2.3.3 Identifying Non-recovery Post-initiator HFEs.....	E-18
E3.2.3.4 Identifying Recovery Post-initiator HFEs	E-18
E3.2.4 Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis.....	E-19
E3.2.5 Step 5: Identify Potential Vulnerabilities.....	E-20
E3.2.6 Step 6: Search for HFE Scenarios.....	E-21
E3.2.7 Step 7: Quantify Probabilities of HFEs	E-21
E3.2.7.1 Qualitative Analysis.....	E-22
E3.2.7.2 Selection of Quantification Model.....	E-22
E3.2.7.3 Quantification	E-23
E3.2.7.4 Verification of Human Error Probabilities	E-23
E3.2.8 Step 8: Incorporate Human Failure Events into PCSA.....	E-24
E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design.....	E-24
E3.3 DEPENDENCY	E-25
E3.3.1 Capturing Dependency	E-25
E3.3.2 Sources of Dependency	E-26
E3.4 UNCERTAINTY	E-26
E3.5 DOCUMENTATION OF RESULTS.....	E-27
E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT	E-28
E4.1 FACILITY FAMILIARIZATION AND INFORMATION COLLECTION	E-28
E4.1.1 General Information Sources	E-28
E4.1.2 Industry Data Reviewed by the HRA Team	E-30
E4.2 USE OF EXPERTS AND ENGINEERING JUDGMENT IN THE HRA.....	E-30
E4.2.1 Role of HRA Team Judgment	E-31
E4.2.1.1 HRA Team.....	E-32
E4.2.2 Role of Subject Matter Experts Judgment	E-33

CONTENTS (Continued)

	Page
E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES.....	E-34
E5.1 TERMINOLOGY	E-35
E5.1.1 Classification of Human Failure Events	E-35
E5.1.1.1 Temporal Phases of HFEs.....	E-36
E5.1.1.2 Error Modes	E-36
E5.1.1.3 Human Failure Type	E-37
E5.1.1.4 Informational Processing Failures	E-37
E5.1.2 Personnel Involved in IHF Operations	E-38
E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES	E-39
E6 ANALYSIS	E-40
E6.0 BACKGROUND	E-40
E6.0.1 Reader’s Guide to the HRA Analysis	E-40
E6.0.2 Topics Common to Multiple HFE Groups	E-44
E6.0.2.1 Interlocks.....	E-44
E6.0.2.2 Crane Drops: Drop of Cask or Drop of Object onto Cask....	E-45
E6.0.2.3 Preliminary Analysis of Cross-Cutting HFEs.....	E-45
E6.1 ANALYSIS OF HUMAN FAILURE EVENT GROUP #1: RECEIPT AND MOVEMENT OF WASTE INTO THE CASK PREPARATION AREA	E-48
E6.1.1 Group #1 Base Case Scenario.....	E-48
E6.1.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-48
E6.1.1.2 Prejob Plan	E-49
E6.1.1.3 Loaded Transportation Cask Receipt in the Cask Preparation Area	E-49
E6.1.1.4 Positioning the Mobile Access Platform Movement over the Conveyance.....	E-49
E6.1.2 HFE Descriptions and Preliminary Analysis	E-49
E6.1.3 Detailed Analysis.....	E-51
E6.2 ANALYSIS OF HUMAN FAILURE EVENT GROUP #2: CASK UPENDING AND REMOVAL FROM CONVEYANCE.....	E-52
E6.2.1 Group #2 Base Case Scenario.....	E-52
E6.2.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-52
E6.2.1.2 Personnel Barrier Removal and Storage (if required).....	E-54
E6.2.1.3 Cask Inspection.....	E-55
E6.2.1.4 HLW Preparation for Unloading (HLW Cask Only).....	E-55
E6.2.1.5 Naval Cask Preparation for Unloading (Naval Cask Only)	E-57
E6.2.1.6 Tie-down Removal (All Casks)	E-58
E6.2.1.7 Cask Upending (on Conveyance)	E-58
E6.2.1.8 Cask Unbolting from Constraints and Movement from Cask Receipt Area to CTT	E-58

CONTENTS (Continued)

	Page
E6.2.2 HFE Descriptions and Preliminary Analysis	E-59
E6.2.3 Detailed Analysis	E-62
E6.3 ANALYSIS OF HUMAN FAILURE EVENT GROUP #3: CASK PREPARATION AND MOVEMENT TO CASK UNLOADING ROOM	E-63
E6.3.1 Group #3 Base Case Scenario.....	E-63
E6.3.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-63
E6.3.1.2 Preparation of HLW Cask for Transfer to Cask Unloading Room (HLW Only).....	E-65
E6.3.1.3 Preparation of Naval Cask for Transfer to Cask Unloading Room (Naval Cask Only).....	E-66
E6.3.1.4 Moving Transportation Cask on CTT into Cask Unloading Room (All Casks).....	E-68
E6.3.2 HFE Descriptions and Preliminary Analysis	E-68
E6.3.3 Detailed Analysis	E-72
E6.4 ANALYSIS OF HUMAN FAILURE EVENT GROUP #4: CTM ACTIVITIES: TRANSFER OF A CANISTER FROM A TRANSPORTAION CASK TO A WASTE PACKAGE WITH THE CTM.....	E-72
E6.4.1 Group #4 Base Case Scenario.....	E-72
E6.4.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-73
E6.4.1.2 HLW Cask Lid Removal	E-77
E6.4.1.3 Grapple Exchange and Installation	E-78
E6.4.1.4 Canister Transfer to Waste Package	E-78
E6.4.1.5 Naval Lift Adapter and Shield Ring Removal.....	E-79
E6.4.1.6 Waste Package Preparation for Loading Room Departure....	E-79
E6.4.2 HFE Descriptions and Preliminary Analysis	E-80
E6.4.3 Detailed Analysis for HFE Group #4	E-85
E6.4.3.1 Human Failure Events Requiring Detailed Analysis.....	E-86
E6.4.3.2 Assessment of Potential Vulnerabilities (Step 5).....	E-86
E6.4.3.3 HFE Scenarios and Expected Human Failures (Step 6)	E-89
E6.4.3.4 Quantitative Analysis (Step 7).....	E-91
E6.4.4 Results of Detailed HRA for HFE Group #4.....	E-121
E6.5 ANALYSIS OF HUMAN FAILURE EVENT GROUP #5: WASTE PACKAGE ASSEMBLY AND CLOSURE	E-122
E6.5.1 Group #5 Base Case Scenario.....	E-122
E6.5.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-122
E6.5.1.2 Moving the WPTT with Loaded Waste Package under Waste Package Closure Room.....	E-123
E6.5.1.3 Initiating Closure Process (Loaded Waste Package with HLW or Naval Waste)	E-123
E6.5.1.4 Waste Package Welding	E-123

CONTENTS (Continued)

	Page
E6.5.2 HFE Descriptions and Preliminary Analysis	E-125
E6.5.3 Detailed Analysis	E-127
E6.6 ANALYSIS OF HUMAN FAILURE EVENT GROUP #6: WASTE PACKAGE EXPORT	E-128
E6.6.1 Group #6 Base Case Scenario.....	E-128
E6.6.1.1 Initial Conditions and Design Considerations Affecting the Analysis.....	E-128
E6.6.1.2 Loaded and Sealed Waste Package Movement to Waste Package Loadout Room and WPTT Docking Station Engagement.....	E-129
E6.6.1.3 Waste Package Shield Ring Removal and Movement of Shield Ring to Waste Package Shield Ring Stand	E-129
E6.6.1.4 WPTT Horizontal Rotation.....	E-129
E6.6.1.5 Waste Package Inspection and Loading into TEV	E-130
E6.6.2 HFE Descriptions and Preliminary Analysis	E-130
E6.6.3 Detailed Analysis for HFE Group #6	E-133
E6.6.3.1 Human Failure Events Requiring Detailed Analysis	E-134
E6.6.3.2 Assessment of Potential Vulnerabilities (Step 5).....	E-134
E6.6.3.3 HFE Scenarios and Expected Human Failures (Step 6)	E-138
E6.6.3.4 Quantitative Analysis (Step 7).....	E-139
E6.6.4 Results of Detailed HRA for HFE Group #6.....	E-147
E7 RESULTS: HUMAN RELIABILITY ANALYSIS DATABASE	E-148
E8 REFERENCES	E-152
E8.1 DESIGN INPUTS.....	E-152
E8.2 DESIGN CONSTRAINTS	E-154
APPENDIX E.I RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA.....	E-155
APPENDIX E.II GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS	E-156
APPENDIX E.III PRELIMINARY (Screening) Quantification PROCESS for Human Failure Events.....	E-157
APPENDIX E.IV SELECTION OF METHODS FOR DETAILED QUANTIFICATION.....	E-162
APPENDIX E.V HUMAN FAILURE EVENTS NAMING CONVENTION.....	E-166

FIGURES

	Page
E6.0-1. HFE Groups Associated with Facility Operations.....	E-41
E6.1-1. Activities Associated with HFE Group #1.....	E-48
E6.2-1. Activities Associated with HFE Group #2.....	E-52
E6.3-1. Activities Associated with HFE Group #3.....	E-63
E6.4-1. Activities Associated with HFE Group #4.....	E-72
E6.4-2. Canister Transfer Machine—Side View.....	E-76
E6.4-3. Canister Transfer Machine—End View.....	E-77
E6.5-1. Activities Associated with HFE Group #5.....	E-122
E6.6-1. Activities Associated with HFE Group #6.....	E-128
E6.6-2. Waste Package Positioning Room and Waste Package Loadout Room Conceptual Configuration.....	E-137
E.I-1. Modeling Strategy for HFE Types.....	E-155
E.II-1. Post Initiator Operator Action Event Tree.....	E-156
E.V-1. Basic Event Naming Convention.....	E-166

TABLES

	Page
E3.2-1. Human Performance Limiting Values	E-24
E3.3-1. Formulae for Addressing HFE Dependencies	E-26
E3.4-1. Lognormal Error Factor Values	E-27
E6.0-1. Correlation of HFE Groups to ESDs and HAZOP Evaluation (PFD) Nodes.....	E-43
E6.0-2. Summary of Preliminary Values for the Cross-group Generic HFEs.....	E-47
E6.1-1. HFE Group #1 Descriptions and Preliminary Analysis.....	E-50
E6.2-1. HFE Group #2 Descriptions and Preliminary Analysis.....	E-60
E6.3-1. HFE Group #3 Descriptions and Preliminary Analysis.....	E-69
E6.4-1. HFE Group #4 Descriptions and Preliminary Analysis.....	E-81
E6.4-2. Group #4 HFEs Requiring Detailed Analysis.....	E-86
E6.4-3. HFE Scenarios and Expected Human Failures for Group #4	E-90
E6.4-4. HEP Model for Group #4 Scenario 1(a) for 51A-OpCTMdrop001-HFI-COD.....	E-96
E6.4-5. HEP Model for Group #4 Scenario 1(b) for 51A-OpCTMdrop001-HFI-COD.....	E-99
E6.4-6. HEP Model for Group #4 Scenario 1(c) for 51A-OpCTMdrop001-HFI-COD.....	E-103
E6.4-7. HEP Model for Group #4 Scenario 1(d) for 51A-OpCTMdrop001-HFI-COD.....	E-106
E6.4-8. HEP Model for Group #4 Scenario 1(e) for 51A-OpCTMdrop001-HFI-COD.....	E-108
E6.4-9. HEP Model for HFE Group #4 Scenario 2(a) for 51A-OpCTMdrop002-HFI-COD	E-112
E6.4-10. HEP Model for HFE Group #4 Scenario 2(b) for 51A-OpCTMdrop002-HFI-COD	E-114
E6.4-11. HEP Model for HFE Group #4 Scenario 2(c) for 51A-OpCTMdrop002-HFI-COD	E-118
E6.4-12. HEP Model for HFE Group #4 Scenario 2(d) for 51A-OpCTMdrop002-HFI-COD	E-121
E6.4-13. Summary of HFE Detailed Analysis for HFE Group #4	E-121
E6.5-1. HFE Group #5 Descriptions and Preliminary Analysis.....	E-126
E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis.....	E-131
E6.6-2. Group #6 HFE Requiring Detailed Analysis	E-134
E6.6-3. HFE Scenarios and Expected Human Failures for Group #6	E-139
E6.6-4. HEP Model for HFE Group #6 Scenario 1(a) for 51A-OpDirExpose3-HFI-NOD	E-144

TABLES (Continued)

	Page
E6.6-5. HEP Model for HFE Group #6 Scenario 1(b) for 51A-OpDirExpose3-HFI-NOD	E-145
E6.6-6. HEP Model for HFE Group #6 Scenario 1(c) for 51A-OpDirExpose3-HFI-NOD	E-146
E6.6-7. Summary of HFE Detailed Analysis for HFE Group #6	E-147
E7-1. HFE Data Summary	E-148
E.III-1. Examples of Information Useful to HFE Quantification	E-157
E.III-2. Types of HFES	E-160
E.IV-1. Comparison between NPP and YMP Operations	E-162
E.V-1. Human Failure Event Type Codes and Failure Mode Codes	E-167

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
BSC	Bechtel SAIC Company, LLC
CBDT	Cause-Based Decision Tree
CFE	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
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
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HVAC	heating, ventilation, and air conditioning
IHF	Initial Handling Facility
INPO	Institute of Nuclear Power Operations
ISFSI	independent spent fuel storage installation
ITS	important to safety
LIS	Licensing Information Service

ACRONYMS AND ABBREVIATIONS (Continued)

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
PFD	process flow diagram
PIC	person in charge
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSF	performance-shaping factor
RHS	remote handling system
SHARP	Systematic Human Action Reliability Procedure
SLIM	Success Likelihood Index Method
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SPM	site prime mover
SSCs	structures, systems, and components
TEV	transport and emplacement vehicle
THERP	Technique for Human Error Rate Prediction
TRC	Time-Reliability Correlations
UT/ET	ultrasonic testing/eddy current testing
WPTT	waste package transfer trolley
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 Initial Handling Facility (IHF) 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 (mean 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. 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 human reliability 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 event sequence diagram (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 Room during 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 are absolute. The remaining conditions apply unless there is reason to believe that they do not apply. The analyst determines whether those conditions apply 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 the plant. 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. The only available substitute is similar operations involving similar hazards and equipment. Examples 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, as part of the assessment of performance, documents 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 model¹
- 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 Human Failure Events 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 HFEs²:
 - 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

¹ATHEANA (Ref. E8.1.22), Section 9.3.1 defines 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.”

²Terminology 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, described and documented in *Initial 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 IHF 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 traps³ 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.

³A "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 the 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). 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 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) and *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).

⁴Extended 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 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 Human Failure Events 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/LIS data on ISFSI events (1994 through 2007) Scientech LIS 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 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 *Initial 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.

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 Novovoronezh 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. (Nuclear)—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 Experts 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), 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)
- 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)
- General facility (including aging pad and drifts) layout and time line of operations
- Interlocks (general)
- Waste package welding equipment and process
- Waste package transfer trolley (WPTT) design and operations (including interface with the CTM and the transport and emplacement vehicle (TEV))
- TEV design and operations
- Naval cask design (shielding)
- 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 Human Failure Events

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

The four classification schemes are based on the following:

1. The three temporal phases used in PRA modeling:
 - A. Pre-initiator
 - B. 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.

⁵There 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 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.

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 HFE⁶—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.
 - 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 equipment⁷) 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

⁶ The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

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.

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:

- 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 IHF Operations

A list of personnel involved in IHF operations with a brief description of their duties is provided below:

Arm operator—The person who is designated to operate one of the robotic arms that are used to weld the waste package. This person welds the canister from a remote location.

Crane operator—The person who is designated to operate the crane for a given operation (i.e., the cask handling crane, the cask preparation crane, or the waste package handling crane).

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 IHF Control Room and controls the CTM remotely.

Level 2 and 3 NDE personnel—The person(s) who is certified to inspect the waste package 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., tracking the bar codes on the waste package and documenting the waste form identification with the bar code).

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.

RHS operator—The person who is designated to operate the remote handling system (RHS) and who is specifically trained to aid in the welding process. This person controls the RHS remotely.

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 (HLW) *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)* (Ref. E8.1.12).

SPM operator—The person who is designated to operate the SPM to bring a railcar or truck trailer into 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).

TEV operator—The person who is designated to operate the TEV. This person is in charge of ensuring that the TEV is in the appropriate configuration for waste package loading prior to the WPTT being moved into the Waste Package Loadout Room. This person is located in the Central Control Center and controls the TEV remotely.

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.

WPTT operator—The person who is designated to operate the WPTT. The WPTT is semiautonomous with all safety functions carried onboard. This person is located in the IHF Control Room and controls the WPTT remotely.

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 IHF 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 IHF 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 IHF 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

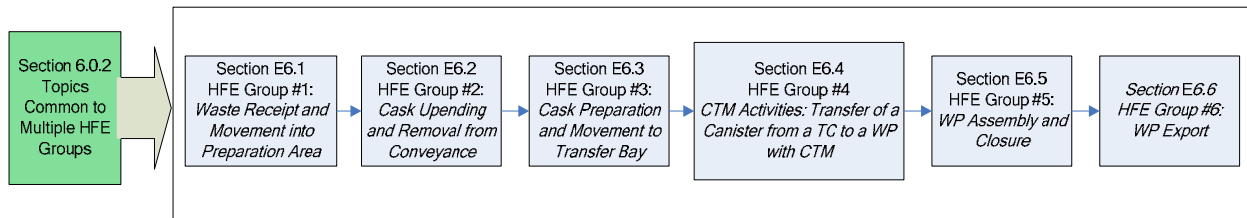
E6.0.1 Reader's Guide to the HRA Analysis

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 IHF 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 IHF, there are six HFE groups analyzed, with each presented in a separate subsection of Section E6.



NOTE: CTM = canister transfer machine; HFE = human failure event; TC = transportation cask; WP = waste package.

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 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.

⁸ HAZOP nodes are defined by the PFD in the PCSA *Initial Handling Facility Event Sequence Development Analysis* (Ref. E8.1.10).

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 Receipt and Movement into Cask Preparation Room		
Move RC/truck into Cask Preparation Room	1	1
Disengage and remove SPM from facility		
HFE Group #2: Cask Upending and Removal from Conveyance		
Remove personnel barriers	1	1, 2
Remove impact limiters (HLW)	2	
Cask upending, removal from conveyance, and placement into CTT	3-5	
HFE Group #3: Cask Preparation and Movement to Transfer Bay		
Preparation activities—HLW (gas sampling and cask lid lift fixture installation)	6	2, 3, 4
Preparation activities—naval (impact limiter and cask lid removal; restraint removal and canister lift fixture installation)	7	
Move CTT to Cask Unloading Room	8	5, 6
HFE Group #4: CTM Activities		
Remove cask lid (HLW)	9	7, 12A
Transfer canister into WP	9-11	
Install WP inner lid (and, for the navy, remove lifting adapter and naval shield ring)	12	
HFE Group #5: WP Assembly and Closure		
Move WP to WP Positioning Room	12	8
Close WP	13	9
HFE Group #6: WP Export		
Move WP to WP Loadout Room and remove shield ring	14	10
Transfer WP to TEV		11, 12C

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HAZOP = hazard and operability; HFE = human failure event; HLW = high-level (radioactive) waste; PFD = process flow diagram; RC = railcar; SPM = site prime mover; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

The following ESDs refer to actions that fall under several HFE groups and PFD nodes:

- ESD 12B: Event Sequences for Activities Associated with Direct Exposure during Various Activities – Inadvertent displacement of naval cask shield ring from cask or waste package or improper installation of waste package shield ring on waste package (HFE groups 3, 4, and 5)
- ESD 13: Event Sequences for Fire Occurring in the IHF (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 human reliability analysis, interlocks were generally modeled explicitly in the fault tree instead of being embedded in the HRA for the preliminary analysis. The approach chosen by the HRA 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 its HFE. Therefore, the analysis relies 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 HRA 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 HRA 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 screening approach was not adequate to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1), a more realistic preliminary value was applied and justified. That is, the HRA 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. These factors were 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 controllers (PLCs) were not credited in this analysis since they are not declared important to safety (ITS).

E6.0.2.2 Crane Drops: Drop of Cask or Drop of Object onto Cask

There are several lifts in the IHF operations, including lifts with the cask handling crane, the cask preparation crane, the CTM, the RHS crane, and the Waste Package Loadout Room crane. 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 cranes seen in industry to warrant a separate analysis.

E6.0.2.3 Preliminary Analysis of Cross-Cutting HFES

E6.0.2.3.1 Operator Introduces Moderator Source into Moderator-Controlled Areas of the IHF

The analysts have not found any way for operators to introduce significant quantities of moderator in the moderator-controlled areas of the IHF; therefore, this failure was omitted from analysis.

E6.0.2.3.2 Load Lifted too Heavy for Crane

There are several lifts in the IHF operations that may potentially result in the operator attempting to lift a load that is too heavy for the crane. Some of these opportunities include the following:

- Attempting to remove the cask lid with the CTM or cask preparation crane when all the lid bolts have not been removed
- Attempting to remove the impact limiters with the cask preparation 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 or 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 railcar or truck trailer carrying a cask moves into the Cask Preparation Area.
- The CTT carrying a cask moves from the Cask Preparation Area into the Cask Unloading Room.
- The WPTT carrying a waste package moves from the Waste Package Positioning Room to the Waste Package Loadout Room.
- The TEV, carrying a waste package, leaves the facility.

Each time a conveyance moves through a set of shield doors, an operator can close the shield door on the conveyance. This collision was considered separately from collision of the conveyance directly into the shield door or 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 7: Event Sequences Associated with Collision of CTT, Site Transporter, or WPTT with IHF Shield Door. Each transfer was assessed separately for these failures, but the operations were considered sufficiently similar to allow for a common preliminary value to be applied to all transfers. The preliminary value is described below:

51A-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. This interlock is never bypassed during normal operations or maintenance. To be conservative, a preliminary HEP value of 1.0 has been assigned to this HFE because it requires an equipment failure in addition to one or more unsafe actions to cause an initiating event.

E6.0.2.3.4 Heating, Ventilation, and Air Conditioning (HVAC) and Electrical Systems

There are no ITS HVAC or electrical functions associated with this facility.

E6.0.2.3.5 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. Summary of Preliminary Values for the Cross-group Generic HFEs

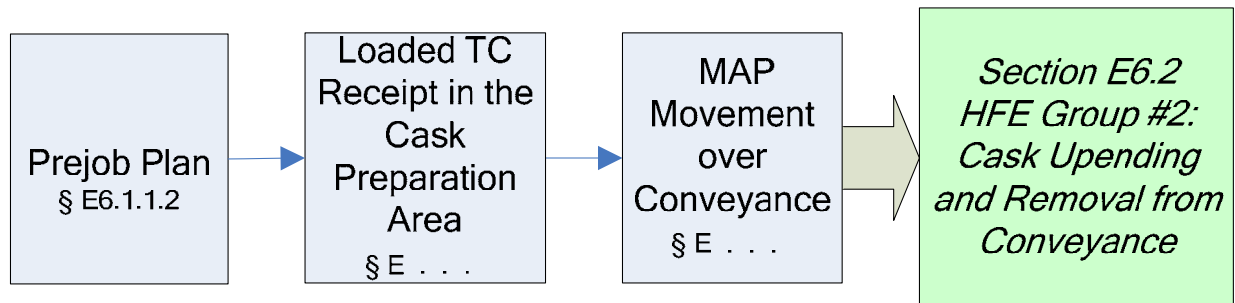
HFE ID	HFE Brief Description	Preliminary Value
Moderator	Operator introduces moderator source into moderator-controlled areas of the IHF	N/A
Load too Heavy	Operator causes drop of cask by attempting to lift a load that is too heavy for the crane	N/A
51A-OpSDClose001-HFI-NOD	Operator closes shield door on conveyance	1.0
HVAC or Electrical	Operator causes failure of HVAC or electrical system	N/A

NOTE: HFE = human failure event; HVAC = heating, ventilation, and air conditioning;
ID = identification; IHF = Initial Handling Facility; N/A = not applicable.

Source: Original

E6.1 ANALYSIS OF HUMAN FAILURE EVENT GROUP #1: RECEIPT AND MOVEMENT OF WASTE 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 railcar or truck trailer containing the transportation cask (naval or HLW) is just outside the door to the Cask Preparation Area, just before the 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 SPM, pulling a railcar or truck trailer, arrives at the door of the Cask Preparation Area loaded with a transportation cask containing an HLW canister or loaded with a naval cask containing a naval canister (railcar only).
2. The cask is secured to the conveyance by tie-downs and has impact limiters surrounding the cask and, possibly, a personnel barrier in place.
3. There are no speed governors or interlocks on the railcar or truck trailer; however, there is a speed governor on the SPM.
4. There are wheel blocks at the end of the rail.

The following personnel are involved in this set of operations:

- Crew members (two people)

- Person in charge (PIC)
- SPM operator
- Radiation protection worker⁹.

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 cask and conveyance reach the IHF, 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 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 pre-lift safety checklist (Ref. E8.1.12) verifying that the equipment is in proper operational condition. All crew members are properly trained and abide by the procedures of the facility.

E6.1.1.3 Loaded Transportation Cask Receipt in the Cask Preparation Area

Two crew members are located at the entrance. Both the railcar and truck trailer are moved by the SPM, which runs on rail or road. When the conveyance approaches the IHF, it is visually inspected. Then one crew member opens the overhead door, and the other crew member uses hand signals to direct the conveyance into the Cask Preparation Area, ensuring that there are no vehicles or obstructions in the path. The SPM operator follows all relevant restrictions and procedures regarding conveyance speed and direction of travel. When stopped, the crew members set the conveyance brakes and chock the wheels. The SPM detaches from the railcar or truck trailer and leaves the facility. The overhead door is closed by a crew member. A checklist is signed to indicate that the door has been closed and that the brakes are set.

Railcar Lowering and Securing (Naval Cask Only)—For naval casks, after the railcar is parked, the hydraulic leveling jacks are lowered and the tie-downs secured.

E6.1.1.4 Positioning the Mobile Access Platform Movement over the Conveyance

A crew member raises the MAP and moves it over the conveyance, in position 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 or truck trailer 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.

⁹The 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 E6.1-1. HFE Group #1 Descriptions and Preliminary Analysis

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-OpRCColli1-HFI-NOD	Operator Causes Low-Speed Collision between Railcar or Truck Trailer and Facility SSCs: operator causes collision of railcar or truck trailer with facility structure or equipment while moving through the Entrance Vestibule to the Cask Preparation Area or operator of an auxiliary vehicle causes collision with the conveyance while the conveyance is parked in the Cask Preparation Area.	1	3E-3	In this step, the railcar or truck trailer moves into the Cask Preparation Area, passing through two doors. The railcar and truck trailer have the same 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 (i.e., railcar or truck trailer) 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 are limited and include the following: <ul style="list-style-type: none"> Improper motion (i.e., backward motion beyond the limit) could result in collision with the end stops, wall, or vestibule doors. An improperly attached railcar or truck trailer could continue moving when the SPM stops, resulting in collision with the end stops, wall, or vestibule doors. A forklift or other auxiliary vehicle could collide into the conveyance. <p>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 (x3). Also, in general, collisions were considered relatively more likely than drop events. The dominant contributor to this failure was assessed to be collision of a forklift into the conveyance.</p>
51A-OpTTColli1-HFI-NOD	Operator Causes High-Speed Collision between Railcar or Truck Trailer and Facility SSCs: operator causes a collision of the railcar or truck trailer at a speed higher than design requirements, if the speed governor of the SPM fails, the railcar or truck trailer could collide into an SSC.	1	3E-3	The operator can cause the SPM to overspeed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, all unsafe actions that require an equipment failure to cause an initiating event were assigned an HEP of 1.0.
51A-OpRCInCol01-HFI-NOD	Operator Causes Mobile Access Platform to Collide into Railcar or Truck Trailer: when the railcar or truck trailer 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 anticollision interlock that prevents movement of the platform if there is an obstruction in its path.	1	1.0	The operator can cause the MAP to collide into the railcar or truck trailer 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, all unsafe actions that require an equipment failure to cause an initiating event were assigned an HEP of 1.0.
51A-OpTTInCol2-HFI-NOD	Operator Causes Truck Trailer to Roll over while Moving into the Cask Preparation Area: operator drives over a significantly uneven surface or jackknifes while moving the truck trailer into the Cask Preparation Area, causing the truck trailer to roll over.	1	1.0	For a truck trailer 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 IHF Entrance Vestibule/Cask Preparation Area; it is incredible for the truck to run over an object large enough to shift its center of mass. The other mode of failure considered here is jackknifing the truck trailer. This failure mode was also seen as incredible because there is not enough room in the Entrance Vestibule/Cask Preparation Area to physically cause the truck trailer to jackknife. The truck is going very slowly; there are three observers; and if the truck trailer were significantly out of alignment, the truck trailer might impact the building, but it would not jackknife and roll over. Therefore, this HFE was omitted from analysis.
51A-OpTRollover-HFI-NOD	Operator Causes Railcar to Derail while Moving the Railcar into the Cask Preparation Area.	1	N/A ^a	In this step, the railcar moves from outside the facility through the Entrance 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.
51A-OpSDClose001-HFI-NOD	Operator Closes Shield Door on Conveyance: the railcar or truck trailer passes through shield doors as it enters the Cask Preparation Area. During this transfer, the operator can close the shield door on the railcar or truck trailer.	6	1.0	The railcar or truck trailer passes through shield doors as it enters the Cask Preparation Area. During this transfer, the operator can close the shield door on the railcar or truck trailer. Cross-cutting HFE "Operator Causes Collision between Shield Door and Waste Conveyance" (Section E6.0.2.3.3) provides a justification of this preliminary value.

NOTE: ^a HRA value replaced by use of historic data. Attachment C provides additional information on active component reliability data. HEP = human error probability; HFE = human failure event; ID = identification; IHF = Initial Handling Facility; MAP = mobile access platform; RC = railcar; SPM = site prime mover; SSC = structure, system, or component; SSCs = structures, systems, and components.

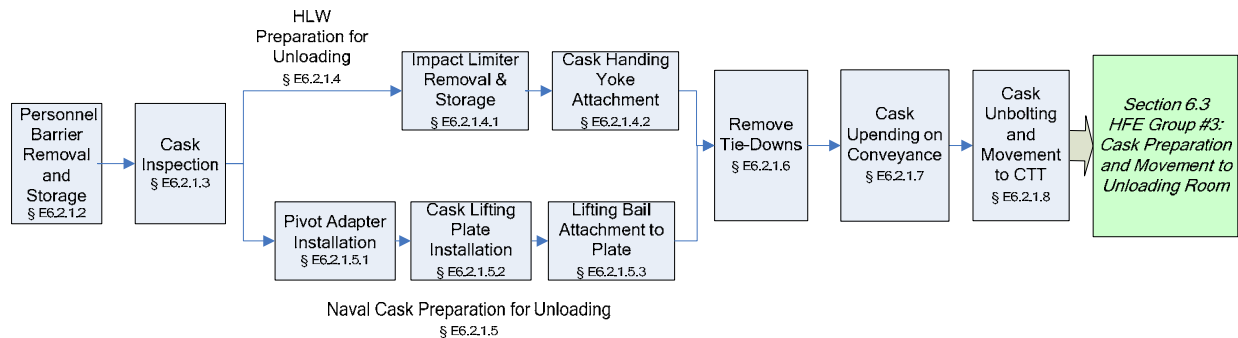
Source: Original

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 evaluation nodes listed in Table E6.0-1, covering upending and transfer of the transportation cask to the CTT. This process is shown in Figure E6.2-1. There are two variations of this step: one for HLW and one for naval canisters. Both transportation casks are upended on the conveyance and moved to the CTT.



NOTE: §= section; CTT = cask transfer trolley; HFE = human failure event; HLW = high-level radioactive waste.

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 or truck trailer (detached from the SPM) is parked in the Cask Preparation Area.
2. The cask is secured to the conveyance by tie-downs, there are impact limiters surrounding the cask, and there may be a personnel barrier in place.
3. The CTT with proper cask pedestal is pre-staged in the Cask Preparation Area.
4. The cask handling crane (300-ton crane) and cask preparation crane 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 equipment is available for upending and transferring the cask:

1. Cranes, including the following:
 - A. Cask handling crane (300-ton)
 - B. Cask preparation crane.
2. Lift fixtures, including the following:
 - A. Uneven sling (for impact limiters)
 - B. Sling
 - C. Yoke.
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 worker¹⁰
- Supervisor.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

¹⁰The 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.

E6.2.1.2 Personnel Barrier Removal and Storage (if required)

The personnel barrier is removed and stored using the cask handling crane with standard rigging, common tools, and the MAP. There is no formal checkoff list for this operation.

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 barrier as follows:

Crane Alignment to Personnel Barrier—The crane operator lowers the 20-ton auxiliary crane into position over the personnel barrier. The crane operator is positioned on the floor in view of the crew members on either side of the personnel barrier. There is a signaling crew member next to the personnel barrier 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 personnel barrier, 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 personnel barrier using the personnel barrier lifting device (i.e., 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 the load is level when lifted. If the sling is not positioned correctly 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.

Personnel Barrier Vertical Lifting—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, the crane operator stops raising the personnel barrier. The crane operator visually determines that the personnel barrier is raised roughly 6 in. above the highest obstacle, which is the proper height for movement. The crane operator clears the railcar or truck trailer and lowers the personnel barrier to the movement height. Each step of this operation is confirmed by hand signals from the signaling crew member.

Personnel Barrier Positioning for Lowering—The crane operator maneuvers the cask preparation crane so that the personnel barrier is positioned above where it is lowered in the staging area. The crane operator visually follows the indicated safe load path marked on the floor and 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.

Personnel Barrier Lowering and Disengaging the Sling—When the personnel barrier is properly positioned and the placement area is clear, the signaling crew member signals the crane operator to lower the personnel barrier. The crane operator lowers the personnel barrier at or below the maximum allowable speed. Once the personnel barrier is stable on its resting place (i.e., the floor of the staging area), the crew member disengages the sling, and 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 HLW Preparation for Unloading (HLW Cask Only)

As illustrated in Figure E6.2-1, the upending process for HLW and naval casks are very similar but not identical. At this point the processes for preparing the two types of casks for upending diverge. The HLW is discussed first, followed by a similar discussion for the naval cask in Section E6.2.1.5.

E6.2.1.4.1 Impact Limiter Removal and Storage

In preparation for this step, the crew member and crane operator attach the uneven sling to the cask preparation crane.

The impact limiters are removed and staged using the cask preparation crane with standard rigging, common tools, and the MAP. This step is performed twice since each cask has two impact limiters.

Once the personnel barrier is removed, the crew removes and stores the impact limiters. This operation is done on the railcar according to training 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 checks off bolt removal from the checklist. Once bolt removal is verified, the crane operator (using the cask preparation crane) removes and stores the impact limiters.

Crane Positioning over Impact Limiter—The crane operator positions the crane over the impact limiter. The crane operator uses visual cues to follow the indicated safe load path marked on the floor 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 over 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.

Vertically Lifting the Impact Limiter—Upon signal from the signaling crew member that all is well, 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 raises the impact limiter. Once the impact limiter has been raised (i.e., is hanging free) such that it has cleared the railcar, the

crane operator stops raising the impact limiters. The crane operator visually determines when the impact limiter has cleared the railcar, and the signaling crew member confirms this with a hand signal. Once past the railcar, the crane operator lowers the crane to the proper height for movement, based on visual inspection confirmed by a hand signal from the signaling crew member. The proper height for movement is roughly 6 in. above the highest obstacle in the movement path.

Impact Limiter Positioning for Lowering—The crane operator maneuvers the crane to position the impact limiter over the staging area. The crane operator uses visual cues to follow the indicated safe load path marked on the floor 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 of the Sling—When the impact limiter is properly positioned and the placement area is clear, the signaling crew member signals the crane operator to lower the impact limiter. The crane operator proceeds to lower the impact limiter at or below the maximum allowable speed. Once the impact limiter is lowered, the crew member disengages the sling, and the crane lifts to the maximum height in preparation for the next operation.

E6.2.1.4.2 Cask Handling Yoke Attachment to the Transportation Cask

For HLW canisters, prior to attempting to upend the transportation cask, the crew members must properly attach the yoke to the 300-ton cask handling crane.

Crane Positioning over Transportation Cask—The crane operator positions the crane over the transportation cask. The operator visually follows the indicated safe load path marked on the floor 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 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 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 verification crew member can only signal the crane operator to stop.

Yoke Arm Engagement on Trunnions—Once the yoke is aligned, the signaling crew member signals the crane 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 (i.e., the minimum distance from the edge of the trunnion to the edge of the yoke arm). The indicator on the crane's controller lets the crane operator know if the arms are sufficiently engaged on both sides, 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 crane 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, one

of the crew members 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 movement of the crane (again with hand signals) to attempt again to engage the yoke arms, and then signals the operator to close the yoke arms.

This ends the discussion of preparing an HLW cask for upending. HLW cask tie-downs are removed in Section E6.2.1.6, and the cask is upended in Section E6.2.1.7. Section E6.2.1.5 discusses the process of preparing a naval cask for upending, which includes intermediate steps to install a pivot adapter, lifting plate, and lifting bail.

E6.2.1.5 Naval Cask Preparation for Unloading (Naval Cask Only)

As illustrated in Figure E6.2-1, the upending process for HLW and naval casks are very similar but not identical. The preparation process for a naval cask is described here.

E6.2.1.5.1 Pivot Adapter Installation (if required)

Using standard crane operations for the cask handling crane (300-ton) with hook, the crew installs the pivot adapter and places the pivot pin into the lifting plate. This step is verified by quality control.

E6.2.1.5.2 Cask Lifting Plate Installation

Using the cask preparation crane with hook, the crew positions and replaces the cask lifting plate on the impact limiter. The crew then bolts (torques) the lifting plate in place. This step is verified by quality control.

Cask Lifting Plate Retrieval—The crane operator lowers the cask preparation crane into position over the lifting plate in the staging area, engages the hook, and lifts the plate to proper height for movement. The crane operator performs this operation based on visual inspection of the surroundings with confirmation of proper alignment provided 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.

Cask Lifting Plate Movement to Cask—The crane operator maneuvers the cask preparation crane to position the plate over the cask in the preparation area. The crane operator uses visual cues to follow the indicated safe load path marked on the floor and also receives confirmatory hand signals from the signaling crew member. A verification crew member, opposite the signaling crew member, can hand signal the crane operator to stop at anytime. The crane operator can roughly align the plate over the cask, but final alignment is directed by the signaling crew member.

Lowering of Lifting Plate—When the crane is properly positioned over the cask, the signaling crew member signals the crane operator to lower the plate into place. The crane operator proceeds to lower the plate at or below the maximum allowable speed. The plate is installed vertically since the cask is horizontal.

A crew member uses the MAP and common tools to emplace and tighten all the lifting plate bolts according to training procedures and then verifies via a checklist that all the bolts are properly installed.

E6.2.1.5.3 Lifting Bail Attachment to Lifting Plate

Using the cask preparation crane with hook, the lifting bail is attached to the lifting plate with a pin.

NOTE: This ends the discussion of preparing a naval cask for upending. Naval cask tie-downs are removed in Section E6.2.1.6, and the cask is upended in Section E6.2.1.7.

E6.2.1.6 Tie-down Removal (All Casks)

The crew removes the cask tie-downs in preparation for upending the cask. Using the MAP, the crew removes all the bolts of the tie-downs, 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. For naval casks, the clamps also need to be removed.

E6.2.1.7 Cask Upending (on Conveyance)

The transportation cask is upended using the 300-ton cask handling crane with yoke (HLW) or hook (navy).

The cask handling crane is already attached to the cask.

Raising Cask to Vertical Position—Upon signal from the signaling crew member that all is well, the operator begins to raise the cask. Since the bottom of the cask remains stationary, the operator positions the crane directly above the upper trunnions (i.e., to keep the cables straight). The crane operator performs this task visually with a clear view. The signaling crew member provides hand signal confirmation that the cask is “upending” properly. Once the cask is fully upright, the crane operator stops raising the cask. The crane operator determines when to stop lifting the crane based on visual inspection, confirmed by hand signals from the signaling crew member.

E6.2.1.8 Cask Unbolting from Constraints and Movement from Cask Receipt Area to CTT

Free Cask from Pivot Point—Using common tools and the MAP, the crew members unbolt the constraints on the bottom half of the cask so the cask can be lifted. This step is verified.

Lifting of Cask—Once the cask is upright 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. The crane operator determines proper height based on a visual inspection, and proper height 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.

Movement of Cask to CTT—The cask is moved onto the CTT using the cask handling crane and the cask handling yoke.

The preparation platform is open, the CTT door is open, and the crane operator maneuvers the crane to position the cask over the CTT floor. The crane operator follows the indicated safe load path marked on the floor using visual cues and 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 bottom of 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/hook and lifts the crane to the proper moving height.

Cask Securing to CTT—The cask is secured to the CTT using common tools, the cask handling crane, the cask yoke, and the cask preparation platform.

Once the cask is properly loaded, the crew member secures the cask to the CTT, which is similar to a cage that locks into position. Bumpers may be installed prior to closing the CTT door. This step is defined in training and must be signed off via a checklist prior to continuing operations. The crew closes the platform for preparation activities.

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 of this analysis. 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 Description	Applicable ESD	Preliminary Value	Justification
Cranes drops	<p>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. Both waste forms require only one lift using the cask preparation crane to upend the cask and move it to the CTT. During this lift, the operator can cause the cask to drop by improperly installing the lifting fixture (navy), improperly engaging the yoke (HLW), two-blocking the cask, or other such failures.</p> <p>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. For HLW, these objects include the personnel barrier and the two impact limiters. For naval waste, these objects include the upending adapter, the lifting plate, and the lifting ball. 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.</p>	1, 2	N/A ^a	<p>In this step the operator uses the cask handling crane to move the cask and other heavy objects. Both waste forms require only one lift using the cask preparation crane to upend the cask and move it to the CTT. For naval waste, this lift is done with a lifting ball and hook; for HLW, the cask handling yoke is used. There are three heavy-object lifts (i.e., a personnel barrier and two impact limiters for HLW; an upending adapter, lifting plate, and lifting ball for naval waste) 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.</p>
51A-OpCTTImpact1-HFI-NOD	<p>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:</p> <ul style="list-style-type: none"> • Impact cask while moving object with crane • Impact cask with crane hook • Collide cask into SSC while moving cask with crane • MAP lowers into cask • Bridge or trolley impacts end stop. 	1, 2	3E-03	<p>In this step the cask is moved from the conveyance ultimately to the CTT. 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 crew performs the CTT 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:</p> <ul style="list-style-type: none"> • Crane moved outside its safe load path (i.e., operators cut corners). • Crane moved in 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. <p>The crane operator, with the help of a signaling crew member and a verification crew member, must manually maintain movement within the safe load path. It is not unlikely that the crane operator could 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. This failure is "highly unlikely" (one in a thousand or 0.001) but is adjusted because there are several ways for an impact to occur (x3). The likelihood of impacting a cask was assessed to be comparable to the railcar collision HFE (51A-OpRCollide1-HFI-NOD, Section E6.1, HFE Group #1) and was accordingly assigned the same preliminary value.</p>
51A-OpSpurMove01-HFI-NOD	<p>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.</p>	1, 2	1E-04	<p>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 (i.e., the crane operator, two crew members, and 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 pendant and signal the CTT to move.</p>

Table E6.2-1. HFE Group #2 Descriptions and
Preliminary Analysis
(Continued)

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-OpTipover001-HF1-NOD	Operator Causes Cask to Tip over. If the crane rigging is attached to the cask, railcar, truck trailer, or CTT (either accidentally or purposefully) and the crane or conveyance moves, then the cask can potentially be tipped over.	1, 2	1E-04	<p>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 short, the crane speed is slow, the crew is well trained, and the crew is 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 the following:</p> <ul style="list-style-type: none"> • Crane hook, grapple, or rigging catches conveyance/cask • Horizontal movement with hook lowered and attached to cask • Crane travels in wrong direction • Cask is not lifted high enough to clear conveyance. <p>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 in an open area with direct observation, and tipover is a slow process; therefore, the value was adjusted by a further 0.1.</p>
51A-OpCollide001-HF1-NOD	Operator Causes Low-Speed Collision with Railcar, Truck Trailer, or CTT. Operator can cause an auxiliary vehicle to collide into a loaded railcar, truck trailer, or CTT while the conveyance is parked in the Cask Preparation Area. If speed governor of the auxiliary vehicle is properly functioning, then this is a low-speed collision.	1, 2	3E-03	<p>In this step the cask is in several positions that are vulnerable to impact via collision:</p> <ul style="list-style-type: none"> • The railcar or truck trailer is parked in the Cask Preparation Area, loaded with a cask. • The CTT is parked in the Cask Preparation Area, loaded with a cask. • The TTC is on the cask stand or tilting frame on the floor of the Cask Preparation Area. <p>Throughout this scenario there are three observers with clear visibility, the speed of auxiliary vehicles is low, the conveyance or cask is stationary and very visible. Procedural controls are expected to limit the number of other vehicles in the Cask Preparation Area during cask operations. The railcar and truck trailer have their brakes set, and the CTT is deflated, so these conveyances cannot move to collide into something; however, if the operators failed to set the brakes of the railcar or truck trailer or failed to deflate the CTT, it is unlikely that 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 failure was assessed to be "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 auxiliary vehicles (e.g., forklifts) that can collide into the cask/conveyance (x 3). This HEP was assigned the same preliminary value as railcar collision HFE (51A-OpRCollide1-HF1-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/truck trailer collision HFE has additional failure modes associated with movement of the SPM that are not applicable here.</p>
51A-OpFLCollide1-HF1-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 railcar, truck trailer or CTT while the conveyance is parked in the Cask Preparation Area. If the collision is due to the auxiliary vehicle speed governor malfunctioning, then this is a high-speed collision.	1, 2	1.0	<p>The operator can cause an auxiliary vehicle (e.g., a forklift) to overspeed, resulting in collision with the railcar, truck trailer, or CTT. In order to accomplish this, the speed governor of the colliding vehicle must fail. To be conservative, all unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.</p>

NOTE: ^aHRA value replaced by use of historic data (Attachment C).
 CTT = canister transfer machine; ESD = event sequence diagram; HEP = human error probability; HFE = high-level radioactive waste;
 ID = identification; MAP = mobile access platform; N/A = not applicable; SPM = site prime mover; SSC = structure, system, or component; SSCs = structures, systems, and components;
 TTC = a transportation cask that is upended using a tilt frame.

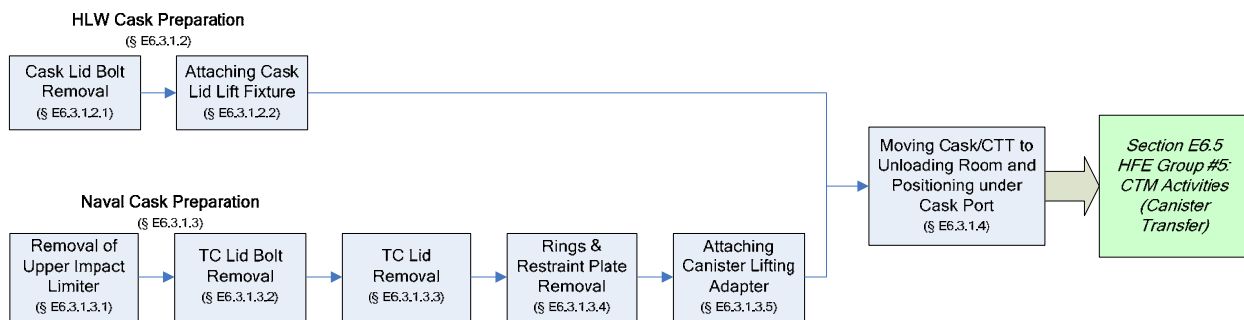
Source: Original

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: CASK PREPARATION AND MOVEMENT TO CASK UNLOADING ROOM

HFE group #3 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering cask preparation activities and movement of the cask to the Cask Unloading Room. The operations covered in this HFE group are shown in Figure E6.3-1. This operation starts with the transportation cask upright and secured in the CTT. During this operation the cask undergoes preparation activities necessary to leave the preparation area. All casks have their lid bolts removed; HLW has a lid lift fixture installed; and naval casks have the impact limiter, cask lid, and canister restraints removed and a canister lift fixture installed. Once the preparation activities are complete, the crew moves the transportation cask from the preparation area to the Cask Unloading Room and positions the cask under the cask port, ready for CTM operations. This operation ends at this point, prior to any CTM activities.



NOTE: § = Section; CTM = canister transfer machine; CTT = cask transfer trolley; HFE = human failure event; HLW = high-level radioactive waste; TC = transportation cask.

Source: Original

Figure E6.3-1. Activities Associated with HFE Group #3

E6.3.1 Group #3 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 cask is sitting in the CTT, secured, with the lid bolted on.
2. The HLW impact limiters have been removed, but naval casks still have the impact limiter on.
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 pendant stowed, during preparation activities.

4. The cask preparation crane 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 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.

5. The following equipment is utilized during preparation activities:
 - A. Cask preparation crane
 - B. Lift fixtures:
 - 1) Sling
 - 2) Hook
 - 3) Grapple
 - C. Common tools and preparation platform.

The following personnel are involved in this set of operations:

- Crane operator
- Signaling crew member
- Verification crew member
- Radiation protection worker¹¹
- Supervisor.

¹¹The 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.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.3.1.2 Preparation of HLW Cask for Transfer to Cask Unloading Room (HLW Only)

As illustrated in Figure E6.2-1, the preparation activities for HLW and naval casks are different. The HLW is discussed first, followed by a similar discussion for the naval cask in Section E6.3.1.3.

E6.3.1.2.1 Transportation Cask Lid Bolt Removal

The crew uses common tools and the preparation platform to remove all the cask lid bolts. Once removed, the bolts are counted, and the crew supervisor checks off bolt removal before the lid is removed or the lid lift fixture is attached.

E6.3.1.2.2 Attaching Cask Lid Lift Fixture

The crane operator uses the cask preparation platform; common tools; and the cask preparation crane, with hook, to retrieve and emplace the proper lid lifting fixture. Once in place, the crew members attach the fixture to the lid with bolts. This step is verified with a checklist. There are two lid lift fixtures available: one for a rail cask and the other for a truck cask.

Lid Lift Fixture Retrieval—The crane operator lowers the cask preparation crane into position over the lid lift fixture in the staging area, engages the hook, 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.

Movement of Lid Lift Fixture to Cask—The crane operator moves the cask preparation crane so as to locate the fixture over the cask in the preparation area. The crane operator then follows the indicated safe load path marked on the floor using 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. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lowering and Disengaging Lid Lift Fixture—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 crew member disengages the hook, and the crane lifts to its maximum height in preparation for the next operation.

A crew member then uses the cask preparation platform and common tools to emplace and tighten all the lid fixture bolts according to training and then verifies (i.e., via a checklist) that all the bolts have been properly installed.

Installation of the lid lift fixture marks the end of preparation activities for HLW. The HLW cask is ready to be transferred to the Cask Unloading Room for transfer of the canister to a waste

package. Movement of the HLW cask to the Cask Unloading Room is covered in Section E6.3.1.4.

E6.3.1.3 Preparation of Naval Cask for Transfer to Cask Unloading Room (Naval Cask Only)

As illustrated in Figure E6.2-1, the preparation activities for HLW and naval casks are different. Preparation of the naval casks is presented here.

E6.3.1.3.1 Removal of Upper Impact Limiter with Lifting Plate and Stage on Conveyance

Without detaching the crane from the lifting plate, the crew unbolts the impact limiter (56 bolts) and removes the upper impact limiter, along with the lifting plate. The crew verifies (i.e., via a checklist) that all the bolts are removed before attempting to lift.

E6.3.1.3.2 Transportation Cask Lid Bolt Removal

The crew uses common tools and the preparation platform to remove all the cask lid bolts. Once removed, the bolts are counted, and the crew supervisor checks off bolt removal before the lid is removed or the lid lift fixture is attached.

E6.3.1.3.3 Transportation Cask Lid Removal and Placement on Cask Lid Stand

Using the cask preparation crane and bayonet grapple, the crew removes the transportation cask lid and stores it on the lid stand.

Crane to Cask Alignment—The crane operator lowers the cask preparation crane 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. Next to the personnel barrier is a signaling crew member 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 bayonet grapple to the cask lid (i.e., places and twists manually or connects with a rotating hook). There is an indicator to verify proper engagement.

Lifting the Lid 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 lower 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.

Moving the Lid to the Staging Area—The crane operator moves the cask preparation crane so as to locate the lid over the lid stand in the staging area. The crane operator follows the indicated safe load path marked on the floor by using visual cues and confirmatory hand signals from the signaling crew member. The crane operator then sets the lid down and disengages the grapple.

E6.3.1.3.4 Cask Shear Ring, Backing Ring, Closure Shear Ring, and Spent Fuel Canister Restraint Plate Removal and Staging

Canister Restraint Removal—Using common tools and the cask preparation platform, the crew removes the canister restraint in the following manner:

1. Retracting all shear ring jack bolts
2. Disengaging all backing ring fasteners
3. Removing all backing ring segments
4. For each shear ring segment (3 or 4), starting with the middle segment, sliding the segment radially inward and removing the segment with the cask preparation crane.

Restraint Segment Removal—The crane operator lowers the cask preparation crane into position over the restraint segment and engages the sling. In order to accomplish this task, a crew member must attach the sling to the crane; secure the sling around the object; and ensure that, when lifted, the load is level. If the sling is not positioned and the load is not level, either crew member signals the crane operator to stop and lower the object so that the sling can be repositioned. Once the sling is engaged properly, the crane operator lifts the segment to clear the cask. Once the restraint segment is moved clear of the cask, the crane operator lowers it 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.

Moving Restraint Segment to Staging Area—The crane operator moves the cask preparation crane so as to locate the segment back in the staging area. The crane operator follows the indicated safe load path marked on the floor by following 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. The crane operator places the segment in its proper location and disengages the sling.

E6.3.1.3.5 Attaching Naval Canister Lifting Adapter to Canister and Shield Ring (Shield Ring Preinstalled)

The crew uses the cask preparation crane and hook to retrieve and emplace the naval canister lifting device. Once emplaced, the crew bolts (torques) the device to the naval canister, verifies (i.e., via a checklist) that it is properly attached, and removes the canister restraints. These operations are done on the cask preparation platform.

Naval Canister Lift Fixture Retrieval—The crane operator lowers the cask preparation crane into position over the naval lift fixture in the staging area, engages the hook, and lifts the fixture 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.

Moving Naval Canister Lift Fixture to Cask—The crane operator moves the cask preparation crane so as to locate the fixture over the cask in the preparation area. The crane operator follows the indicated safe load path marked on the floor by following 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. The crane operator can roughly align the crane, but final alignment is directed by the signaling crew member.

Lowering and Disengaging Naval Canister Lift Fixture—When properly positioned over the naval canister, 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 crew member disengages the hook, and the crane lifts to its maximum height in preparation for the next operation.

Then, a crew member uses the cask preparation platform and common tools to emplace and tighten (torque) all the lid fixture bolts according to training and then verifies (i.e., via a checklist) that all the bolts have been properly installed. The fixture is bolted to the canister and to the shield ring; there is a checkoff item for this operation.

Installation of the canister lift fixture marks the end of preparation activities for naval casks. The naval cask is ready to be transferred to the Cask Unloading Room for transfer of the canister to a waste package. Movement of the cask to the Cask Unloading Room is covered in the next section; this marks the end of the deviation between HLW and naval casks in this scenario.

E6.3.1.4 Moving Transportation Cask on CTT into Cask Unloading Room (All Casks)

Using the CTT, the crew moves the transportation cask to the Cask Unloading Room and positions the cask under the cask port. To do this, the crew moves the CTT to the Cask Preparation Room door, opens the door, moves the CTT through the door in position under the cask port, disconnects the air hoses, and closes the door.

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 of the HFEs of concern during cask preparation and movement to the Cask Unloading Room 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
51A-OpCaskDrop01-HF1-NOD	<i>Operator Drops Cask during Preparation Activities:</i> The cask is not lifted in this step, and no plausible scenarios that would lead to cask drop could be identified.	N/A	N/A	The cask is not lifted in this step, and the 300-ton crane is not used in this operation. For HLW, there is no possible configuration that can result in a cask drop. For naval waste, 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 lid, causing the cask to lift. 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 analysis.
Crane drop	<i>Operator Drops Object on Cask during Preparation Activities:</i> Preparation of a cask entails moving several heavy objects over the cask using the cask handling crane auxiliary hook. These objects include the lid lift fixture for HLW. For naval waste they include the impact limiter, cask lid, canister restraints, 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.	2, 3, 4	N/A ^a	In this step the operator uses the cask handling crane auxiliary hook to move objects over the cask. For HLW, there is one heavy-object lift (i.e., the lid lift fixture) using the cask preparation crane. For HLW there are seven lifts using the cask preparation crane: impact limiter, cask lid, canister restraint segments (times four), and the canister lift fixture. The lid lift and canister lift fixtures are moved with a grapple or hook, the impact limiter and canister restraints are moved with a sling, and the cask lid is moved with a sling or grapple. 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.
51A-OpCollide001-HF1-NOD	<i>Operator Causes Low-Speed Collision of Auxiliary Vehicle with CTT:</i> During cask preparation, the CTT is loaded 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.	3, 4	3E-03	In this step, the CTT is loaded and parked under the 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 preparation area during cask operations. This failure was assessed to be "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 auxiliary vehicles (e.g., forklifts) that can collide into the cask or conveyance (x3). This HEP was assigned the same preliminary value as railcar collision HFE (51A-OpRCCollide1-HF1-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-truck trailer collision HFE has additional failure modes associated with movement of the SPM that are not applicable here.
51A-OpFLCollide1-HF1-NOD	<i>Operator Causes High-Speed Collision of Auxiliary Vehicle with CTT:</i> During cask preparation, the CTT is loaded 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 is due to the auxiliary vehicle speed governor malfunctioning, this failure would be a high-speed collision.	3, 4	1.0	The operator can cause the auxiliary vehicle to overspeed, resulting in collision. In order to accomplish this failure, the speed governor of the vehicle must fail. To be conservative, all unsafe actions that require an equipment failure to cause an initiating event an HEP of 1.0 have been assigned.
51A-OpSpurMove01-HF1-NOD	<i>Operator Causes Spurious Movement of CTT during Preparation Activities:</i> 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 cask preparation, the operator can inadvertently cause the CTT to move. This spurious movement can cause the CTT to collide into the preparation platform.	3, 4	1E-04	In this step the CTT is parked under the preparation platform; the CTT is deflated, 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 CTT to be left inflated, 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 and deflate the CTT, and an operator would have to access the pendant and signal the CTT to move.
51A-OpCTTImpact1-HF1-NOD	<i>Operator Causes an Impact between SSC and Loaded CTT due to Crane Operations:</i> While performing crane operations, the operator can potentially impact the cask if the crane is moved with the hook lowered below the platform.	3, 4	3E-03	In this step the CTT is stationed under the preparation station while several objects are moved to the cask. For crane operations in this step there are three observers with clear visibility, the operators 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 CTT (containing a 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 CTT. The crane hook can also be improperly stowed such that the CTT, when moving to the Cask Unloading Room, collides with the crane hook. However, the CTT travels under the platform to the Cask Unloading Room, and the last preparation activity for both HLW and naval waste requires the shield plate to be closed, so it is unlikely in this case that, if the crane is improperly stored, the hook would be in the path of the CTT. 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 (x3). The likelihood of impacting a cask was considered comparable to the "Crane Impact during Unloading and Removal" HFE (51A-OpCTTImpact1-HF1-NOD; Section E6.2, HFE Group #2) and was accordingly assigned the same preliminary value. This assessment is considered conservative because, in comparison with unloading and removal, there are fewer crane movements in this operation, and there is a platform around the CTT that makes it harder to impact the CTT.

Table E6.3-1. HFE Group #3 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
51A-OpTipover002-HFI-NOD	<i>Operator Causes Cask to Tip over during Cask Preparation Activities:</i> The operator can improperly slow the crane rigging, and it can catch the CTT or cask. If this failure happens, movement of the crane or the CTT can cause the cask and CTT to tip over.	3, 4	1E-04	In this step the CTT is stationed under the preparation station, the lid lift fixture is attached to the cask lid, and the CTT is then moved to the Cask Unloading Room. In order to get a tipover of the cask or CTT, the crane must be attached to the cask or CTT, and the crane or CTT must also move. To be conservative, the cask preparation crane is considered capable of physically tipping over the cask underneath the platform. At no point in the operations is the crane attached to the cask; for preparation of naval canisters, 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, which 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 attempting to move the crane. It is also unlikely that, when the CTT begins movement to the Cask Unloading Room, the CTT operator and observers would not notice that the rigging is attached to the CTT. 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 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 Unloading and Removal" HFE (51A-OpTipover001-HFI-NOD; Section E6.2; HFE Group #2) because it is a very similar operation (i.e., movement with the 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, there is no platform, and there are more failure modes during unloading and removal; therefore, there would be more opportunities for tipover in that scenario.
51A-OpImpact000-HFI-NOD	<i>Operator Causes Impact of Cask during Transfer from Preparation Station to Cask Unloading Room:</i> While moving from the Preparation Station to the Cask Unloading Room, the CTT can impact the crane hook or rigging if it is improperly slowed.	5	N/A	While moving from the preparation station to the Cask Unloading Room, the CTT can impact the crane hook or rigging if it is improperly slowed. The last step in preparation activities for both HLW and naval waste 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 would impact the ST while it is moving out of the Cask Unloading Room; it is more likely that rigging would impact the cask while the crane is actually in use. Therefore, any crane interference with the CTT is already covered by 51A-OpCTTImpact1-HFI-NOD ("Operator Causes Impact between CTT and SSC during Cask Preparation with Lid On") and 51A-OpTipover002-HFI-NOD ("Operator Causes Cask to Tip over during Cask Preparation Activities").
51A-OpCTCollide2-HFI-NOD	<i>Operator Causes Low-Speed Collision of CTT during Transfer from Preparation Station to the Cask Unloading Room:</i> Once the preparation activities are over, an operator inflates the CTT and moves the cask from the preparation area to the Cask 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 overspeed; therefore, all CTT collisions are below the designed speed.	5	1E-03	In this step the CTT moves from the preparation station to the Cask Unloading Room; 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 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 an auxiliary vehicle or a facility structure (e.g., the preparation station platform, the shield door). This failure could happen if the guide rails were not installed properly or if the three crew members were distracted. This operation is simple, is 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 be less likely than a railcar-truck collision because of the guide rail, number of observers, and short travel distance.
51A-OpSDClose001-HFI-NOD	<i>Operator Closes Shield Door on Conveyance:</i> Once the preparation activities are over, an operator inflates the CTT and moves the cask from the preparation area to the Cask Unloading Room. There is a shield door between the 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.	6	1.0	The CTT passes through shield doors as it enters the Cask Unloading Room. During this transfer, an operator can close the shield door on the CTT. Section E6.0.2.3.3 provides a justification of this preliminary value.

Table E6.3-1. HFE Group #3 Descriptions and
Preliminary Analysis
(Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
51A-OpNVYShield1-HF-COW	<i>Operator Improperly Removes Naval Shield Ring:</i> The naval shield ring comes preinstalled in the naval cask and shields the crew during installation of the canister lift fixture. Before installation, however, the crew removes the shear ring, the closure shear ring, and the SFC restraint plate from the naval cask. This failure arises if, while removing the other components, the crew inadvertently removes the shield ring.	12	3E-04	In this step, the naval shield ring is preinstalled in the naval cask, and has to stay in place during installation of the canister lift fixture. Before installation, however, the crew removes the shear ring, the backing ring, the closure shear ring, and the SFC restraint plate from the naval cask. These components are lifted off in three or four segments. This failure arises if, while removing the other components, the crew also removes the shield ring. Although this operation is not performed very regularly and is somewhat complex, the crew is well trained, and the process involved in removing the shear ring, backing ring, closure shear ring, and SFC restraint plate is sufficiently different from the procedure for removing the shield ring that it would be very difficult to accomplish this error by accident. Also, the crew is sensitive to the consequences of radiation exposure and would be expected to be aware during this operation. Finally, if the shield ring is removed, the radiation protection worker would get a high radiation readout and would notify the crew right away. Overall this failure is classified as an "extremely unlikely" event and is given the preliminary value of 0.001 for failure of the crew and 0.1 for failure of the radiation protection worker. While the radiation protection worker is supposed to be entirely independent from the crew performing the action, the preliminary value was adjusted (x3) to account for a possible dependency.
51A-LidDisplace1-HF-NOD	<i>Operator Inadvertently Displaces Lid:</i> In this step the lid is unbolled and crane activities take place. 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.	12	N/A	Due to design changes to the preparation platform, improperly stowed rigging during this operation would not plausibly 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. This failure was omitted from analysis.

NOTE: ¹HRA preliminary value replaced by use of historic data (Attachment C).

CIT = cask transfer trolley; ESD = event sequence diagram; EOC = error of omission; EOO = error of commission; HEP = human error probability;

HFE = human failure event; HLW = human failure event; ID = identification; N/A = not applicable; SFC = spent fuel canister; SPM = site prime mover; ST = site transporter.

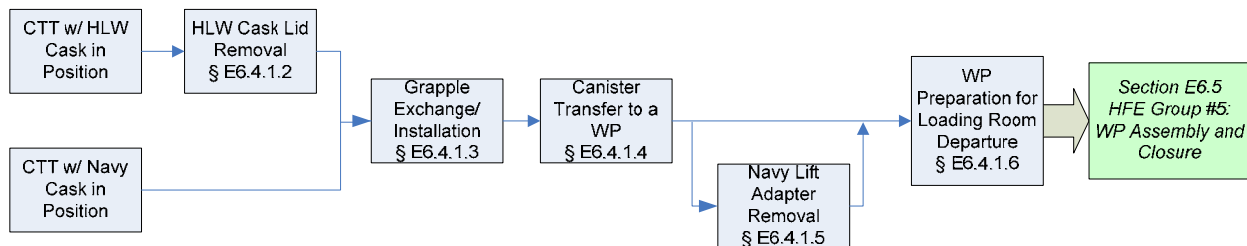
Source: Original

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 (Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada) performance objectives; therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (Ref. E8.2.1)).

E6.4 ANALYSIS OF HUMAN FAILURE EVENT GROUP #4: CTM ACTIVITIES: TRANSFER OF A CANISTER FROM A TRANSPORTATION CASK TO A WASTE PACKAGE WITH THE CTM

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 CTM operations. The overall process associated with these operations is graphically depicted in Figure 6.4-1. This operation begins with a CTT carrying a naval or HLW cask in position below the unloading port. For HLW, the cask lid is removed by the CTM and stored. For naval casks the lid is removed prior to movement of the CTT into the Cask Unloading Room. The canisters are transferred to a waste package, and the waste package inner lid is emplaced on the waste package. This operation ends when the waste package is ready to be transferred for closure.



NOTE: § = Section; CTT = cask transfer trolley; HFE = human failure event; HLW = high-level radioactive waste; WP = waste package.

Source: Original

Figure E6.4-1. Activities Associated with HFE Group #4

E6.4.1 Group #4 Base Case Scenario

There are two variations with three waste package loading possibilities for the Group #4 base case scenario:

1. Move naval canister from transportation cask to waste package
 - A. Full waste package contains one naval canister
2. Move HLW canister from transportation cask to waste package
 - A. Full waste package contains 5 HLW long canisters

B. Full waste package contains 5 HLW short canisters.

E6.4.1.1 Initial Conditions and Design Considerations Affecting the Analysis

1. The transportation cask is secure in the CTT, positioned and secured under the cask port in the Transfer Room. For HLW, the cask lid is sitting on the cask unbolted. The cask has a lid lift fixture attached. For a naval canister, the cask lid is removed, the shield ring is in place, and there is a canister lift fixture attached to the naval canister and shield ring.
2. The waste package is in a WPTT and has a waste package shield ring in place. The WPTT is stationed under the waste package port and secured with the lid removed. Some waste packages take several canisters; some waste packages may be partially full.
3. CTM operations are performed remotely from the IHF Control Room unless otherwise specified.
4. 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 (i.e., 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 (above the slide gate) that, once it is cleared, stops the hoist and erases the lift command (i.e., the CTM can only lower the hoist).
 - 2) For the object mode, the ASD automatically stops the hoist once the object clears the slide gate. There is also an optical sensor at the bottom of the bell (above the slide gate) that, once cleared, stops the hoist and erases the lift command (i.e., the CTM can only lower the hoist).
 - 3) The maintenance mode is fully manual; the ASD does not stop the lift. The maintenance mode is password protected to prevent inadvertent selection of this mode.

Above the ASD stop point is an upper limit switch which, 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 (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist.

- B. Horizontal movement/port alignment: There is some visually based system that aligns the CTM with the canister to enable the grapple to properly engage the canister. The form of this system may use a scheme of a 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, waste package, and staging ports is potentially a highly automated process. However, to be conservative, a manual horizontal movement process, generically relying on a visual alignment system and camera for alignment confirmation, is analyzed here.
- C. There is an interlock between the shield skirt and port gate that requires the shield skirt to be lowered in order for the port gate to open. For a manual process, 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/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered.
- E. There is an interlock between the CTM slide gate and shield skirt. The shield skirt cannot be raised unless the slide gate is closed. This interlock cannot be bypassed, even for maintenance. Likewise, the CTM slide gate cannot be opened unless the skirt is lowered.
- 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 and end stops on the trolley and bridge.
- I. There is a weight interlock that cuts off power to the hoist when the crane capacity is exceeded.
- J. There is an interlock that prevents CTM canister grapple (primary grapple) operation if the grapple is not properly connected to the hoist.
- K. 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.
- L. The CTM is mechanically or electrically prevented from inadvertent canister disengagement.

5. The shield door to the Cask Unloading Room is closed. There is an interlock between the port slide gates and the shield doors. The port slide gate cannot be open while the shield doors are also open.
6. There are interlocks between the waste package port slide gate and the WPTT. The gate cannot open unless the WPTT is properly aligned under the port and the waste package shield ring is in place. The power to the WPTT is removed when the waste package port gate is open. The WPTT reenergizes when the gate closes.

The following equipment is available to support Group # 4 activities:

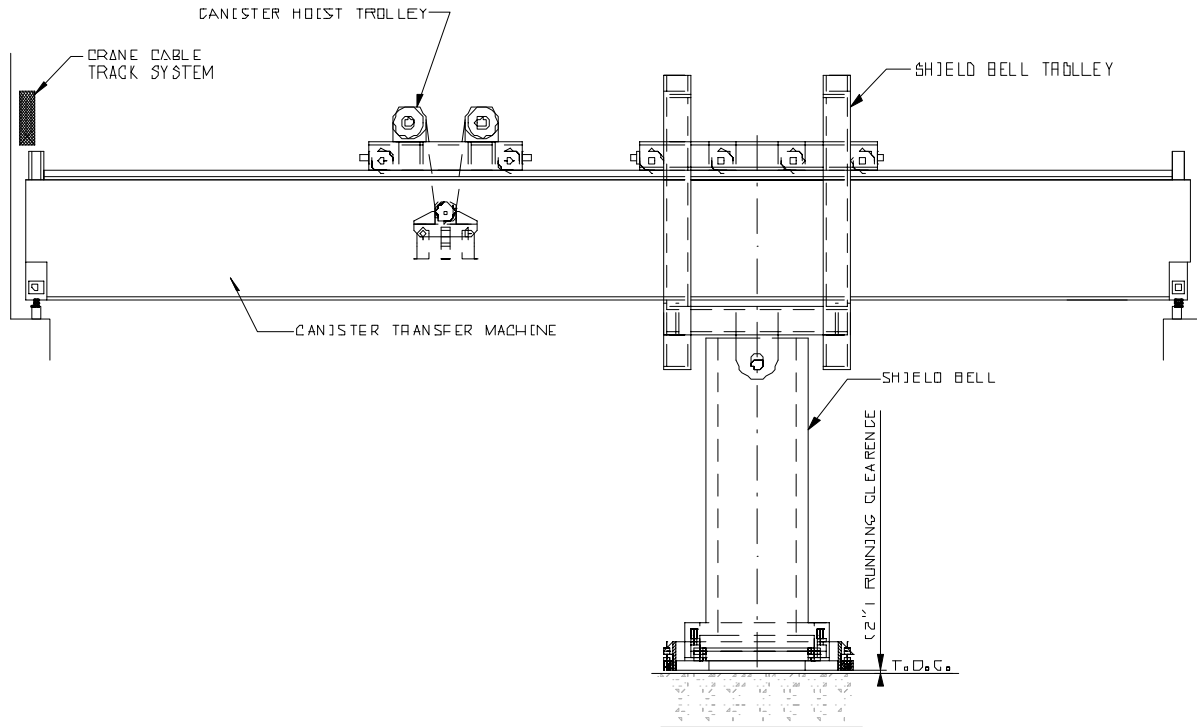
1. CTM
2. Grapples:
 - A. Lid grapple (for transportation cask and waste package lid)
 - B. Shield plug grapple (for waste package inner lid and spread ring)
 - C. HLW canister grapple (there are two types of HLW canister grapples: West Valley Demonstration Project/Hanford and Defense Waste Processing Facility/Idaho National Laboratory)
 - D. Naval canister grapple
 - E. If the wrong grapple is used, the grapple design precludes partial/full engagement (i.e., the wrong grapple is too big or small or otherwise mechanically incompatible with the fixture).

The following personnel are involved in this set of operations:

- CTM operator
- Crew members (two people)
- Supervisor.

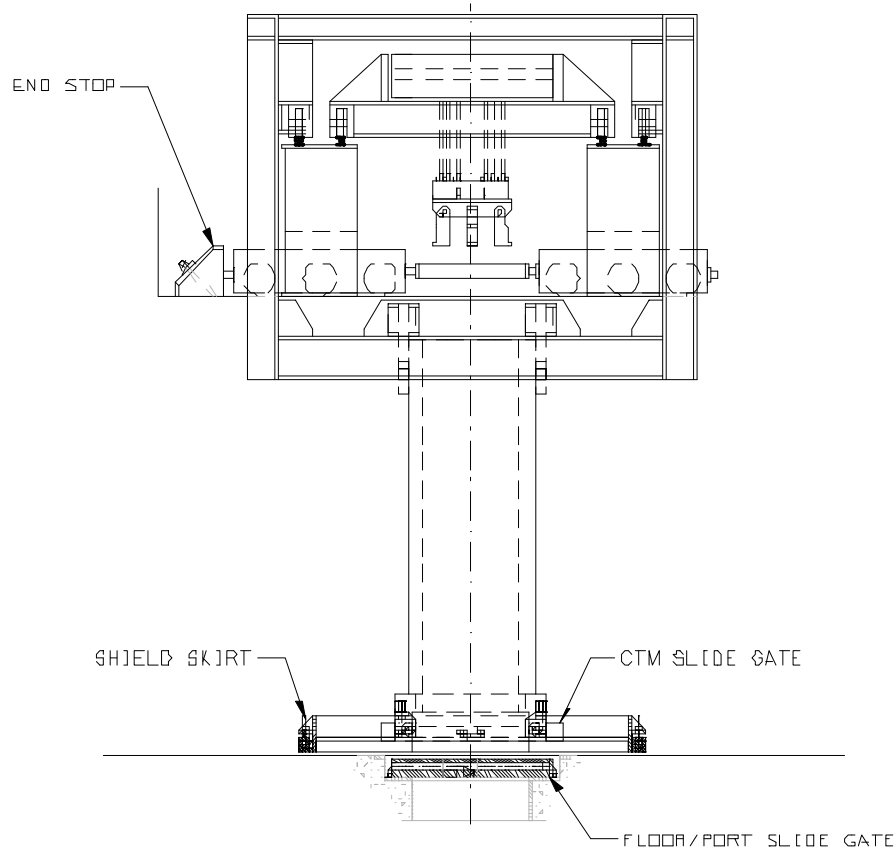
Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

Figure E6.4-2 and Figure E6.4-3 are simple diagrams illustrating the CTM.



Source: Modified from *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. 8.1.6)

Figure E6.4-2. Canister Transfer Machine—Side View



Source: Modified from *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope* (Ref. E8.1.6)

Figure E6.4-3. Canister Transfer Machine—End View

E6.4.1.2 HLW Cask Lid Removal

CTM Movement to the Cask Port—The CTM operator uses a visual alignment system and camera to position the CTM, with lid grapple, over the cask port (or staging area). There is a position indicator, along with a camera view, for the operator to know when the CTM is in position.

CTM Slide Gate and Port Slide Gate Opening—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.

Cask Lid Lifting into the CTM and Slide Gates Closing—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 via 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.

CTM Movement to the Lid Station and Lid Lowering to Lid Station—The CTM operator lifts the CTM skirt and moves the CTM with its 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 the lid is staged in the proper location.

E6.4.1.3 Grapple Exchange and Installation

Grapple Exchange (HLW)—The CTM operator moves the CTM from the lid station to the CTM Maintenance Area (Canister Transfer Room floor), where a crew member manually takes off and stores the lid grapple and attaches the appropriate canister grapple (West Valley Demonstration Project/Hanford or Defense Waste Processing Facility/Idaho National Laboratory grapple).¹²

Canister Grapple Installation (Naval)—The CTM operator moves the CTM to the CTM Maintenance Area, where a crew member manually attaches the appropriate canister grapple to the CTM. The CTM operator also ensures that the ASD is set to the appropriate setting to lift the canister.¹³

E6.4.1.4 Canister Transfer to Waste Package

CTM Movement to the Port—The CTM operator moves the CTM from the Maintenance Area and positions the CTM over the cask port. The CTM operator uses a visual alignment system in conjunction with a camera view to ensure alignment with the port. Once positioned, the operator lowers the skirt of the CTM.

CTM Slide Gate and Port Slide Gate Opening—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.

Canister Lifting into the CTM—The CTM operator looks at the relative canister/hoist position and adjusts the alignment if necessary to ensure that the CTM is over the canister (some casks have several canisters). This final adjustment is done with the alignment system in conjunction with viewing the camera. Once the CTM is appropriately aligned to the canister, the operator lowers the canister grapple and engages the grapple. Grapple engagement is automatic but is verified visually via camera and via an indicator. The operator lifts the canister by holding down a controller (i.e., joystick) until the ASD automatically stops the lift.

CTM Slide Gate and Port Slide Gate Closing—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.

¹²When the design is finalized, one option under consideration is that an automatic system 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.

¹³When the design is finalized, one option under consideration is that an automatic system 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.

CTM Movement to the Waste Package Port—The CTM operator moves the CTM from the cask port into position over the waste package port. The CTM operator uses a visual alignment system in conjunction with a camera view to ensure alignment with the port. Once positioned, the operator lowers the skirt of the CTM.

CTM Slide Gate and Port Slide Gate Opening—The CTM operator opens the CTM slide gate and the waste package port slide gate.

Canister Lowering into a Waste Package—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 operator makes fine adjustments of the CTM position until alignment is verified. The operator lowers the canister into position in the waste package and disengages the grapple, verifies disengagement (camera and indicator), and then retracts the grapple.

CTM Slide Gate and Port Slide Gate Closing and CTM Movement away from the Port—Once the grapple is raised, the operator closes the CTM slide gate, closes the waste package port slide gate, lifts the CTM skirt, and moves the CTM away from the waste package port.

E6.4.1.5 Naval Lift Adapter and Shield Ring Removal

Waste Package Port Slide Gate Opening—The CTM operator opens the waste package port slide gate.

Naval Canister Lifting Adapter Unbolting from a Naval Canister—Crew members unbolt the naval canister lifting adapter from the naval canister using common tools.

Waste Package Port Slide Gate Closure—The CTM operator closes the waste package port slide gate.

CTM Movement to Waste Package Port, Waste Package Port Slide Gate Opening, and Naval Canister Lifting Adapter with Naval Cask Shield Ring Retrieval—The CTM operator moves the CTM into position over the waste package port. The CTM operator uses a visual alignment system in conjunction with a camera view to ensure alignment with the port. Once positioned, the operator lowers the skirt of the CTM. The CTM and port slide gates are opened, and the CTM retrieves the lift adapter and shield ring.

Waste Package Port Slide Gate Closure and Naval Cask Shield Ring Staging—With the lifting adapter and shield loaded in the CTM, the operator closes the CTM and port slide gates and moves the adapter and shield ring to their staging area for removal and storage.

E6.4.1.6 Waste Package Preparation for Loading Room Departure

Grapple Exchange—The CTM operator moves the CTM to the CTM Maintenance Area, where a crew member manually removes the canister grapple and attaches the inner lid grapple. At this point, the CTM operator sets the ASD to the proper setting for lifting the waste package inner lid (shield plug with spread ring). The operator closes the slide gate and lifts the skirt.

CTM Movement to Waste Package Inner Lid Station—Once the skirt is lifted, the operator remotely moves the empty CTM, positions it over the waste package inner lid station, then lowers the skirt and opens the CTM slide gate.

Waste Package Inner Lid Lifting into the CTM and Waste Package Inner Lid Movement to the Waste Package—Once the CTM is positioned, the operator lowers the grapple, engages the grapple, verifies grapple engagement via camera and indicator, and lifts the waste package inner lid into the CTM. The CTM operator closes the CTM slide gate and lifts the skirt. Quality control verifies this step. The operator remotely moves the CTM and positions it over the waste package. The CTM operator uses a visual alignment system in conjunction with a camera view to ensure alignment with the center of the port.

Waste Package Port Slide Gate Opening, Waste Package Inner Lid Placement in a Waste Package, and Waste Package Slide Gate Closure—The CTM operator lowers the skirt, opens the waste package port slide gate, opens the CTM slide gate, and lowers the inner lid into position. Once in position the CTM operator disengages the grapple, verifies full disengagement (via camera and indicator), retracts the grapple, and closes the waste package and CTM slide gates.

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 canister transfer with the CTM 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 the 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 Description	Applicable ESD	Preliminary Value	Justification
51A-OpCTMdrop001-HFI-COD	Operator Drops Object onto Canister during CTM Operations: The following CTM activities require heavy objects to be moved over the canister: installation of the waste package inner lids and removal of the cask lid (HLW) or the naval shielding (naval waste). It is possible that these objects can be dropped onto the canister while being lifted with the CTM.	7	2E-03	In this step, the operator can potentially drop the cask lid (HLW), the naval shield ring (naval waste), the waste package inner lid, or the waste package spread ring onto the canister. There are several ways for this failure to occur, including: <ul style="list-style-type: none"> 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 which 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 CTM significantly misaligned with the cask port. This misalignment can cause part of the lid to get 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 51A-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 lid, the cable can snap, causing the lid to drop onto the canister. There are several electromechanical safeguards to prevent this, including: load cell interlock, motor temperature interlock and the cable design. <p>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. 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. Because the operation is performed remotely, this is a somewhat complex process (x2) as opposed to an extremely complex process (which would be x3). This HFE was assessed to be less likely than a cask impact or a railcar/truck trailer collision, and, indeed, the preliminary value reflects this.</p>
51A-OpCTMdrop002-HFI-COD	Operator Drops Canister during CTM Operations: All variations of CTM activities require the canister to be lifted and transferred to a waste package. During this lift, the operator can drop the canister (i.e., by improper grapple engagement).	7	2E-03	Moving a canister with the CTM is very similar to moving an object with the CTM during cask transfer (51A-OpCTMdrop001-HFI-COD), and has the same failure modes. There are two differences between moving a canister and moving an object (specifically, the lid): the canister drop due to lifting too high (two-block) is analyzed in a separate HFE, and the naval canister has an additional failure mode (i.e., failure to remove all the bolts before removing the shield ring/lift fixture). Therefore, it was considered acceptable to assign the same preliminary value to this HFE as moving an object with the CTM during cask transfer (51A-OpCTMdrop001-HFI-COD).
51A-OpCTMdrin01-HFI-COD	Operator Lifts Object or Canister too High with CTM: It is possible that, while lifting objects such as the canister or waste package inner lid, the operator can cause a two-block failure by lifting the object too high.	7	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 (i.e., optical sensor) and other anti-two-block equipment (i.e., 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.
51A-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 cask, when the operator attempts to remove the cask lid with the CTM, the load is significantly heavier than the CTM is rated for, and could result in a drop of the cask. This failure mode is only applicable to HLW, as naval canisters have no lid.	7	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. This failure was not assigned a 1.0 like other failures which are ANDed with mechanical failures because the load cell is never bypassed. For this failure to occur, the preparation crew must fail to remove all the bolts and fail to verify on the check list 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 lid is lifted 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.
51A-OpNoUnBoltDP-HFI-NOD	Operator Fails to Remove Lid Bolts, Resulting in Impact, Drop, or Tipover [Naval Waste]	7	N/A	There is no lid on casks containing naval waste. Therefore this failure mode was omitted from the analysis.

Table E6.4-1. HFE Group #4 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-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.	7	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 object 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 is in object lift mode, it would automatically stop too soon, but the operator would have to fail to notice that the canister is not high enough when closing the port and CTM side gates on the canister. For a canister, the operator would also have to fail to rely on the optical sensor and also fail to close the slide gate to accomplish this HFE. There are interlocks, such as the load cell interlock, which prevent the CTM from exerting enough force to snap the cable and drop the canister or object. There is also an interlock which prevents horizontal motion if the slide gate is not closed, but this interlock can be bypassed during normal maintenance. Due to the complicated nature of this failure, the interlock was not separately modeled for this HFE, but, rather, was included in the preliminary value. This failure was considered highly unlikely and accordingly assigned a preliminary value of 0.001.
51A-OpCTMGate1-HFI-NOD	Operator Inappropriately Closes Slide or Port Gate during Vertical Canister Movement and Continues Lifting: If the operator signals the CTM side 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 hoist, severing the cables. The NSDB requires the gate motors 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.	7	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 involved in 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 can, if it is even possible, put the ASD in manual mode. If the operator does put the ASD in manual mode, it is unlikely that the operator can 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.
51A-OpCTMImpact2-HFI-COD	Operator Causes Canister Impact with Lid during CTM Operations (HLW): The cask lid, when removed by the CTM, is staged such that the canister must travel over it to move from one port to another. If the lid is improperly stowed, the CTM can collide with the lid. This failure mode is not applicable to naval waste because the cask lid is removed in the Cask Preparation Area.	7	N/A	The more likely case is that the operator fails to restore the ASD to canister-lift mode after moving the lid. For all waste forms except the 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 still has 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.
51A-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.	7	1.0	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 is returned from analysis because, if the lid was 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.

Table E6.4-1. HFE Group #4 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-OpDirExpose1-HF1NOD	<i>Operator Causes Direct Exposure During CTM Activities (all CTM movements):</i> If an operator inadvertently opens the shield door and enters the Unloading Room while the canister is being lifted out of the cask, there is a direct exposure. Likewise, if the operator inadvertently opens the port gate when the CTM is not over the cask/waste package with its shield skirt lowered, then an operator on the second floor (Canister Transfer Room) can get a direct exposure.	12	1.0	Direct exposure during CTM activities can happen if an operator inadvertently opens the shield door to the Unloading Room while the canister is being lifted, or, if an operator opens the port gate (with a cask under it) while the shield skirt is not lowered over the port. In order to accomplish either of these scenarios, an interlock must also fail. The shield door cannot be easily bypassed and is never bypassed during normal operations or normal maintenance. However, the port gate interlock may be bypassed as part of normal maintenance. As was previously discussed, the HRA team assigned all unsafe actions that are combined with interlocks an HEP of 1.0.
51A-OpDirExpose2-HF1NOD	<i>Operator Causes Direct Exposure During CTM Activities (movement into waste package):</i> For canister loading in a waste package, if the waste package is not pre-staged in the Cask Unloading Room, the operator can lower the canister to the floor of the Unloading Room and then place the waste package lid directly on the canister. A person present in the Waste Package Closure Room is exposed. Placing the waste package beneath the cask port is part of the staging activities before HF operations for waste package loading. Waste package 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 waste package is not staged, the CTM operator has the chance to notice when replacing the canister inside the waste package (camera view looking down on waste package). This failure received a preliminary value of 0.01 for failure to pre-stage the AO and 0.01 for failure to notice during prejob check or when loading the waste package, resulting in a total preliminary value of 0.0001. This preliminary value is consistent with the preliminary value for failure to install a waste package shield ring (HFE Group#7: Waste Package Export; 51A-OpShieldRing-HF1NOD), which has a very similar failure mode. There is an interlock which prevents this failure, but, because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in the HFE below (51A-OpFailRstInt-HF1NOM).	12	1E-04	For canister loading in a waste package, if the waste package is not pre-staged in the Cask Unloading Room, the operator can lower the canister to the floor of the Unloading Room and then place the waste package lid directly on the canister. A person present in the Waste Package Closure Room is exposed. Placing the waste package beneath the cask port is part of the staging activities before HF operations for waste package loading. Waste package 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 waste package is not staged, the CTM operator has the chance to notice when replacing the canister inside the waste package (camera view looking down on waste package). This failure received a preliminary value of 0.01 for failure to pre-stage the AO and 0.01 for failure to notice during prejob check or when loading the waste package, resulting in a total preliminary value of 0.0001. This preliminary value is consistent with the preliminary value for failure to install a waste package shield ring (HFE Group#7: Waste Package Export; 51A-OpShieldRing-HF1NOD), which has a very similar failure mode. There is an interlock which prevents this failure, but, because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in the HFE below (51A-OpFailRstInt-HF1NOM).
51A-OpFailRstInt-HF1NOM	<i>Operator Fails to Restore Interlock after Maintenance:</i> There are several interlocks that are bypassed during normal maintenance. Failure to restore the interlock which prevents the port gate from opening before a receptacle is placed underneath the port is explicitly modeled here. If the bypass is not restored, this could result in a direct exposure due to the HFE above (51A-OpDirExpose2-HF1NOD).	12	1E-02	If the maintenance bypass for the interlock which prevents the cask port gate from opening before a waste package is placed underneath the port bypass is not restored, this could result in a direct exposure due to the HFE above (51A-OpDirExpose2-HF1NOD). This interlock would be bypassed during CTM maintenance. This failure would require the crew member to fail to reset the bypass and to fail to properly perform the prejob check of the CTM equipment. These failures were 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.
51A-OpFailISG-HF1NOD	<i>Operator Fails to Close the CTM Slide Gate before Moving the CTM with the Canister Inside the Bell:</i> If the canister is inside the CTM with the shield skirt raised and slide gate open, then personnel on the 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 raise if the slide gate is open, but this interlock would most likely be bypassed during maintenance.	12	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 which prevents this failure, but, because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in the HFE above (51A-OpFailRstInt-HF1NOM). 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.
51A-OpNDiscoAir-HF1NOD	<i>Operator Causes Spurious Movement of CTT while Canister is Being Loaded:</i> 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 disconnect the air supply, the CTT can get a spurious signal during canister lifting that can cause a collision of the CTT into the canister.	7	1E-03	While in the Unloading Room, the CTT is parked with the air supply disconnected. The CTT is controlled locally (i.e., via pendant), and there are no operators in the Unloading 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 Cask 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 which prevents 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.

Table E6.4-1. HFE Group #4 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-OpWPTTSpor01-HFI-NOD	Operator Causes Spurious Movement of WPTT while Canister is Being Loaded: The WPTT is controlled remotely. If the operator sends a signal for the WPTT to move during canister lowering, the WPTT can impact the canister.	7	1E-03	While the canister is being lifted with the CTM, an operator can inadvertently signal the WPTT to move. The controls for the WPTT are on a separate control board, and the WPTT operator is not involved in the CTM operations. The WPTT operator does not begin work until after the CTM operator is done and hands off the checklist to the WPTT operator. This failure requires a significant departure from normal operations. The analysis could not identify any contexts in which the WPTT or CTM operator would believe it is appropriate to move the WPTT during this operation. In order for the WPTT to move while a canister is being loaded, an interlock must also fail. 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.
51A-OpTiltDown01-HFI-NOD	Operator Initiates Premature Tilt-down during Transfer to Closure Area: The WPTT is controlled remotely. If the operator sends a signal for the WPTT to tilt down during canister lowering, the WPTT can impact the canister.	7	1.0	The operator can cause the WPTT to prematurely tilt down. The WPTT operator is not supposed to be operating near the controls for the WPTT during CTM operations. The WPTT operator has no reason to be near the controllers, much less to begin tilt down. Tilt-down only occurs during waste package load out in the Waste Package Load Out Room, and the controller for the WPTT tilt-down is distinct from other WPTT controls. In order to accomplish this failure, several interlocks must also fail. These interlocks (i.e., an interlock taking power away from the WPTT when the port gate is open and an interlock between the tilt-down mechanism and the docking station) do not have a bypass. The HRA team has assigned all unsafe actions that are combined with interlocks an HEP of 1.0.
Spurious movement of CTT during CTM activities	Operator Causes Spurious Movement of CTT while Canister is Being Loaded	7	N/A	The CTT is locally controlled and siting in the Unloading Room deflated. There are no personnel in the Unloading Room during this operation, and there is an interlock on the shield door that prevents access to the room while the canister is being removed from the cask. This failure was omitted from analysis because it involves several mechanical and human failures, including violation of the procedural control which restricts access to the Unloading Room. Furthermore, if a person enters the Unloading Room during canister removal, they would receive a direct exposure; this failure is captured in 51A-OpDirExpose1-HFI-NOD.

NOTE: AO = aging overpack; CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HFE = human failure event; HLW = high-level radioactive waste; NSDB = nuclear safety design basis; PSF = performance-shaping factor; SSC = structure, system, or component; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

E6.4.3 Detailed Analysis for HFE Group #4

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 E6.4.3.2.

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 E6.4.3.3 and E6.4.3.4, 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 E6.4.3.4. Four quantification methods are utilized in this quantification:

- CREAM (Ref. E8.1.18)
- HEART/NARA (Ref. E8.1.28 and 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 E6.4.4.

E6.4.3.1 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 IHF PCSA model determined that there were two HFEs in this group 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 E6.4-2.

Table E6.4-2. Group #4 HFEs Requiring Detailed Analysis

HFE	Description	Preliminary Value
51A-OpCTMdrop001-HFI-COD	Operator causes drop of object onto canister during CTM operations	2E-03
51A-OpCTMdrop002-HFI-COD	Operator causes drop of canister during CTM operations (low-level drop)	2E-03

NOTE: CTM = canister transfer machine; HFE = human failure event.

Source: Original

E6.4.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the 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, event sequence analysis).

The vulnerabilities discussed in this section pertain only to those aspects of the CTM activities that relate to potential human failure scenarios relevant to the HFEs listed above. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during the CTM activities, but these have no bearing on this analysis.

E6.4.3.2.1 Operating Team Characteristics

CTM operator—The CTM operator is located in the IHF Control Room. The CTM operator receives standard training for crane operations and observes operations prior to operating 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 to prepare the CTM for canister transfer, including affixing the appropriate grapple for a particular canister. Training consists of observation and “hands-on” instruction for the CTM preparation process. The CTM is prepared by a team of two crew members.

E6.4.3.2.2 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 the grapple (e.g., it can move the hoist within the bell). A flat screen display shows the 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 semiautomated 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. 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 is located just above the CTM slide gate (~2 in.). 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 Overlimit—The load cell overlimit 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.

E6.4.3.2.3 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.

E6.4.3.2.4 Formal Rules and 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.

E6.4.3.2.5 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 be informed 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 as the dependency described above, 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.

E6.4.3.2.6 Operator Expectations

Anticipatory Actions—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 can expect that failures are mitigated by design features without serious consequences, which promotes complacency in the operations.

Consequences of Failure—The lifting process is simple, the goal is clear, and problems are not expected. There is a tendency for the CTM operator to focus on future tasks while the hoist is in motion rather than concentrate on the ongoing task.

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 does not expect a failure or expect the engagement indicator to show a failure. The operator can also not expect that the grapple is not properly attached to the hoist (i.e., the operator can expect and trust that the crew members have properly prepared the CTM).

E6.4.3.3 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) leading 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 to provide the complete context for 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 E4.2.2.

Table E6.4-3 summarizes all of the HFE scenarios developed for the HFEs in this group.

Table E6.4-3. HFE Scenarios and Expected Human Failures for Group #4

HFE	HFE Scenarios
<p>51A-OpCTMdrop001-HFI-COD</p> <p><i>Operator Causes Drop of Object onto Canister during CTM Operations</i></p>	<p>HFE Scenario 1(a): (1) Crew member improperly installs grapple; (2) Pre-operational check fails to note improper installation; (3) Primary grapple interlock gives false positive signal; (4) Operator fails to notice bad connection between hoist and grapple through camera ; (5) Grapple/lid or grapple/shield ring drops from hoist and strikes canister</p> <p>HFE Scenario 1(b): (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 or shield ring drops from grapple and strikes canister</p> <p>HFE Scenario 1(c)^a: (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 or shield ring to drop</p> <p>HFE Scenario 1(d)^a: (1) CTT is not sufficiently centered under port; (2) Operator fails to notice CTT 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 to drop</p> <p>HFE Scenario 1(e): (1) Operator activates grapple disengagement switch prematurely; (2) Load cell disengagement interlock fails; (3) Lid or shield ring drops from grapple and strikes canister</p>
<p>51A-OpCTMdrop002-HFI-COD</p> <p><i>Operator Causes Drop of Canister during CTM Operations (Low-Level Drop)</i></p>	<p>HFE Scenario 2(a): (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</p> <p>HFE Scenario 2(b): (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</p> <p>HFE Scenario 2(c)^b: (1) CTT is not sufficiently centered under port; (2) Operator fails to notice CTT not sufficiently centered; (3) Operator fails to notice canister 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 canister to drop.</p> <p>HFE Scenario 2(d): (1) Crew member fails to fully withdraw lift fixture bolts; (2) Operator fails to notice canister is rising with lift fixture and shield ring; (3) Canister drops from lift fixture.</p>

NOTE: ^aScenarios 1(c) and 1(d) are only applicable to HLW. These scenarios do not apply to placing the waste package inner lid or removing the naval shield ring, because they can only occur over the canister when lifting a transportation cask lid.

^bThis scenario only applies to naval waste because the HLW cask lid was removed in the prep area.

ASD = adjustable speed drive; CTM= canister transfer machine; CTT = cask transfer trolley;
HFE = human failure event; HLW = high-level radioactive waste.

Source: Original

Since there are two HFEs identified for detailed analysis in this group, the scenarios are organized under these two HFE categories, with the scenarios numbered for the first category as 1(a), 1(b), 1(c), 1(d), and 1 (e) and similarly for the second category.

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 E6.4-3.

The HFE scenarios summarized in Table E6.4-3 are discussed and quantified in detail in the following sections.

E6.4.3.4 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 E6.4-3.

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.

E6.4.3.4.1 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.

$$\text{ASD height control fails} = 3.4E-5$$

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 applied to the system versus its capacity to bear the load.

The first drop considered is where a canister (naval) 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 provide a significant safety margin against overload failures (Ref. E8.1.2). 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 our 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 is:

$$\text{Mechanical failure of hoist under overload causes naval canister drop} = 0.25$$

The other drops are evaluated relative to this. First considered the similar case where the lid or shield ring is jammed in the port and the hoist is straining to lift the jammed object is considered. In this case, the force generated by the hoist is the same, but the weight of the lid and shield ring 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:

$$\text{Mechanical failure of hoist under overload causes lid/shield ring drop} = 0.1$$

Next is considered the condition where the grapple is either not properly connected to the hoist or the grapple itself is only partially engaged to the canister/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:

$$\begin{aligned} \text{Grapple/canister drops from hoist} &= 0.25 \\ \text{Canister drops from grapple} &= 0.25 \end{aligned}$$

Regarding the case of a lid and shield ring, again the force is lower than the above canister case and also lower than jammed lid/shield ring 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/shield ring there is always the possibility that the drop would occur when the object was not over the canister, or would occur in a manner that the object would not impact the canister (it would only strike the structure of the transportation cask or waste package). In the absence of analysis, the HRA team has applied and 50-50 chance of this occurring, which reduces the probability by a factor of two. Therefore:

$$\begin{aligned}\text{Grapple/object drops from hoist and strikes canister} &= 0.05 \\ \text{Object drops from grapple and strikes canister} &= 0.05\end{aligned}$$

Given the information available about the design, the analyses in existence, and the knowledge of the requirements of NOG-1 (level 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.

E6.4.3.4.2 Quantification of HFE Scenarios for 51A-OpCTMdrop001-HFI-COD: Operator Causes Drop of Object onto Canister during CTM Operations

This event applies to both dropping a transportation cask lid during removal or a waste package inner lid during placement, however scenarios 1(c) and 1(d) would not apply during waste package lid placement since they can only occur during lifting a transportation cask lid or naval shield ring.

E6.4.3.4.2.1 HFE Group #4 Scenario 1(a) for 51A-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 or grapple/shield ring 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 cask lid. 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 waste package 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 generic task type (GTT) A5, and 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 $\times 11$, 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 assessed proportion of affect (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 that the environment is poor, but rather that it is simply not optimal. The full affect EPC would be $\times 8$, 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 it is somewhat physically demanding. Given the tradeoffs, the APOA is set at 0.1.
- EPC 13: Operator under-load/boredom. The full affect EPC would be $\times 3$, 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:

$$\begin{aligned} &\text{Crew member improperly installs grapple} = \\ &0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006 \quad (\text{Eq. E-1}) \end{aligned}$$

Preoperational Check Fails to Note Improper Installation—There are two crew members responsible for preparing the CTM for each operation. 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 activities to perform other than checking the first crew member’s installation, 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.

Each of the two crew members has a distinct set of assignments, although they collaborate when needed and cross check each other's work. For this action, 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, 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 (Ref. E8.1.26).

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 and is quantified in Section E6.4.3.4.1.

Primary grapple 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 lining up the secondary grapple with the lifting device. However, as the lift begins, the operator is watching through the cameras. This gives the operator the opportunity to note that the grapple is not properly connected (for example, 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 or shield ring back down to recheck the connection. However, the operator is not expecting there to be any problems in this 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 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 “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:

$$\text{Operator fails to notice a bad connection between the hoist and grapple through the camera} = 0.003 \times 4 \times 2 \times 0.8 = 0.02$$

Grapple/Lid or Grapple/Shield Ring Drops from Hoist and Strikes Canister—Just because the lift is occurring with an improper grapple installation does not mean that the lid or shield ring and grapple falls. 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 or shield ring and grapple, once dropped, would fall in an orientation that would impact the canister in the transportation cask or waste package 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 transportation cask or waste package structure).

This event is quantified in Section E6.4.3.4.1.

$$\text{Grapple/object drops from hoist} = 0.05$$

HEP Calculation for Scenario 1(a)—The events in the HEP model for Scenario 1(a) are presented in Table E6.4-4.

Table E6.4-4. HEP Model for Group #4 Scenario 1(a) for 51A-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 grapple 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/object drops from hoist and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E-5 \times 0.02 \times 0.05 = 1E-11 \quad (\text{Eq. E-2})$$

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:

$$1E-5 \times 2.7E-5 < 1E-8$$

E6.4.3.4.2.2 HFE Group #4 Scenario 1(b) for 51A-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 or shield ring 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 an 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 EPCs:

- 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 $\times 11$, 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 $\times 4$. 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 $\times 3$, 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:

$$\text{Operator fails to fully engage grapple} = 0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad (\text{Eq. E-3})$$

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 E6.4.3.4.1.

$$\text{Grapple engagement interlock gives false positive signal} = 2.7\text{E-}5$$

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 (for example, unexpected lid/shield ring 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 or shield ring back down to recheck the connection. However, the operator is not expecting any problems in this 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. Once the operator has verified that the correct action was performed initially, and this is confirmed by the false positive from the interlock, 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:

$$\text{Operator fails to notice grapple not fully engaged through camera} = 1.0$$

Lid or Shield Ring 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 both the lids and shield ring are much lighter. Additionally, even if the lid/shield ring 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 transportation cask or

waste package 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 transportation cask or waste package structure).

This event is quantified in Section E6.4.3.4.1.

$$\text{Lid drops from grapple} = 0.05$$

HEP Calculation for Scenario 1(b)—The events in the HEP model for Scenario 1(b) are presented in Table E6.4-5.

Table E6.4-5. HEP Model for Group #4 Scenario 1(b) for 51A-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	Object drops from grapple and strikes canister	0.05

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C \times D = 0.07 \times 2.7E-5 \times 1.0 \times 0.05 = 1E-7 \quad (\text{Eq. E-4})$$

E6.4.3.4.2.3 HFE Group #4 Scenario 1(c) for 51A-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 or shield ring to 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 object 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 third way this could occur is simply a mechanical failure of the height control set point of the ASD.

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 a 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 can be best represented by task execution error NARA GTT A1, and 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.
- 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 E6.4.3.4.1.

ASD height control fails = $3.4E-5$

Operator Fails to Notice Lift is Taking Too Long—Lifting an object 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 or shield ring 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 holds the lift button until the lift automatically stops. This operation has been performed many times in the past by the operator, and the operator has an instinctive feel for how long the lift takes. If an 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 IHF Control Room. The CPC for an interpretation task with advantageous working conditions is 0.8.

Applying these factors yields the following:

$$\text{Operator fails to notice lift is taking too long} = 0.01 \times 0.8 = 0.008$$

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) by trusting 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 wasn’t 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 short-cuts 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 E6.4.3.4.1.

Load cell interlock fails = $2.7E-5$

Mechanical Failure of Hoist under Overload Causes Lid or Shield Ring 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/shield ring falls (the hoist motor could overload and fail before the lid becomes detached from the hoist) or that the lid or shield ring, once dropped, falls in an orientation that would impact the canister in the transportation cask or waste package (the orientation of the falling lid may cause it to only impact the transportation cask or waste package structure).

This event is quantified in Section E6.4.3.4.1.

Mechanical failure of hoist under overload causes object drop = 0.1

HEP Calculation for Scenario 1(c)—The events in the HEP model for Scenario 1(c) are presented in Table E6.4-6.

Table E6.4-6. HEP Model for Group #4 Scenario 1(c) for 51A-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 object drop	0.1

NOTE: ASD = adjustable speed drive; HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$\{A \times (D + E1) + [(B + C) \times (D + E2)]\} \times F \times G = \{0.0007 \times (0.008 + 0.2) + [(0.005 + 3.4E-5) \times (0.008 + 0.05)]\} \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-5})$$

E6.4.3.4.2.4 HFE Group #4 Scenario 1(d) for 51A-OpCTMdrop001-HFI-COD

1. CTT is not sufficiently centered under port
2. Operator fails to notice CTT 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:

$$\begin{aligned} \text{CTT is not sufficiently centered under port} &= \\ 0.003 \times 0.5 \times 0.8 &= 0.002 \end{aligned}$$

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 that the operator has failed in an observation of the relative locations of the grapple and the lid, or that the canister is not perfectly centered, but rather that the operator’s decision is that it doesn’t matter (“it’s close enough”) is incorrect. 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 adequate 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 Lid Tilt and Continues Lift—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 lid tilting 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:

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. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable for the operator to find a creative technique to accomplish this. 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 non-bias case is applied here:

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.

Lid catches and jams in port = 0.5

Load Cell Overload Interlock Fails—This is a mechanical failure of the interlock. This event is quantified in Section E6.4.3.4.1.

Load cell interlock fails = $2.7E-5$

Mechanical Failure of Hoist under Overload Causes Lid Drop—This event is quantified in Section E6.4.3.4.1.

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 E6.4-7.

Table E6.4-7. HEP Model for Group #4 Scenario 1(d) for 51A-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:

$$A \times B \times (C + D) \times E \times F \times G = 0.002 \times 0.05 \times (0.02 + 0.05) \times 0.5 \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-6})$$

E6.4.3.4.2.5 HFE Group #4 Scenario 1(e) for 51A-OpCTMdrop001-HFI-COD

1. Operator activates grapple disengagement switch prematurely
2. Load cell disengagement interlock fails
3. Lid or shield ring drops from grapple and strikes canister.

Operator Activates Grapple Disengagement Switch Prematurely—Once engaged with the lid/shield ring, the grapple remains engaged until the object 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 (for example, when 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 (repetitions, jumps, and 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:

$$\begin{aligned} \text{Operator activates grapple disengagement switch prematurely} &= \\ 0.003 \times 0.8 \times 0.8 &= 0.002 \end{aligned}$$

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 E6.4.3.4.1.

$$\text{Load cell disengagement interlock fails} = 2.7\text{E-}5$$

Lid or Shield Ring Drops from Grapple and Strikes Canister—In order for the lid or shield ring to actually drop, the grapple disengagement mechanism would need to overcome the dead weight friction caused by the weight of the lid or shield ring. In the case of the canister, this is clearly expected to be true, but the lid and the shield ring both weigh much less than the canister; thus, it is not clear. However, there is still a chance that the grapple would not disengage or would not disengage while the lid or shield ring is over the open 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 or shield ring). Finally, the object 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.

$$\text{Object drops from grapple and strikes canister} = 0.1$$

HEP Calculation for Scenario 1(e)—The events in the HEP model for Scenario 1(e) are presented in Table E6.4-8.

Table E6.4-8. HEP Model for Group #4 Scenario 1(e) for 51A-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	Object drops from grapple and strikes canister	0.1

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.002 \times 2.7E-5 \times 0.1 < 1E-8 \quad (\text{Eq. E-7})$$

E6.4.3.4.2.6 HEP for HFE 51A-OpCTMdrop001-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for lifting a lid off an HLW cask follows:

$$\begin{aligned} &51A\text{-OpCTMdrop001-HFI-COD (lid lift)} = \\ &\text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(c)} + \text{HFE 1(d)} + \text{HFE 1(e)} = \\ &(<1E-8) + 1E-7 + (<1E-8) + (<1E-8) + (<1E-8) = 2E-7 \end{aligned} \quad (\text{Eq. E-8})$$

The Boolean expression for the overall HFE (all scenarios) for lifting a shield ring off a naval canister follows:

$$\begin{aligned} &51A\text{-OpCTMdrop001-HFI-COD (shield ring lift)} = \\ &\text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(c)} + \text{HFE 1(e)} = \\ &(<1E-8) + 1E-7 + (<1E-8) + (<1E-8) = 2E-7 \end{aligned} \quad (\text{Eq. E-9})$$

The Boolean expression for the overall HFE (all scenarios) for placing an inner lid on a waste package follows:

$$\begin{aligned} &51A\text{-OpCTMdrop001-HFI-COD (lid placement)} = \\ &\text{HFE 1(a)} + \text{HFE 1(b)} + \text{HFE 1(e)} = \\ &2E-8 + 1E-7 + (<1E-8) = 2E-7 \end{aligned} \quad (\text{Eq. E-10})$$

HLW canisters have one lid lift and one inner lid placement as part of their processing. The Boolean expression for the overall HFE for HLW (a lid removal and a lid placement) follows:

$$51A\text{-OpCTMdrop001-HFI-COD (total)} = 51A\text{-OpCTMdrop001-HFI-COD (lid lift)} + \\ 51A\text{-OpCTMdrop001-HFI-COD (lid placement)} = 2E-7 + 2E-7 = 4E-7 \quad (\text{Eq. E-11})$$

Naval canisters have one shield ring lift and one inner lid placement as part of their processing. The Boolean expression for the overall HFE for naval waste (a shield ring removal and an inner lid placement) follows:

$$51A\text{-OpCTMdrop001-HFI-COD (total)} = 51A\text{-OpCTMdrop001-HFI-COD} \\ (\text{shield ring lift}) + 51A\text{-OpCTMdrop001-HFI-COD (lid placement)} \\ = 2E-7 + 2E-7 = 4E-7 \quad (\text{Eq. E-12})$$

E6.4.3.4.3 Quantification of HFE Scenarios for 51A-OpCTMdrop002-HFI-COD: Operator Causes Drop of Canister during CTM Operations (Low-Level Drop)

E6.4.3.4.3.1 HFE Group #4 Scenario 2(a) for 51A-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 canister to be processed. While it is possible that this operation does not need to be performed (it may be the same grapple as for the cask lid), it is uncertain how often this occurs, so this analysis considers that this action needs to be performed each time. The crew member can improperly secure the grapple to the hoist. This makes the grapple appear to be secured in place when it is not.

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 $\times 11$, 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 that 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 it 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:

$$\begin{aligned} &\text{Crew member improperly installs grapple} = \\ &0.0001 \times [(11-1) \times 0.2 + 1] \times [(8-1) \times 0.1 + 1] \times [(3-1) \times 0.1 + 1] = 0.0006 \quad (\text{Eq. E-13}) \end{aligned}$$

Preoperational Check Fails to Note Improper Installation—There are two crew members responsible for preparing the CTM for each operation. 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 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.

For the action being analyzed, the second crew member has helped initially with the connection of the grapple to line it up but then moves 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 adjusted for high dependence is from THERP Table 20-21, item (4)(e)), which is 0.6.

$$\text{Preoperational check fails to note improper installation} = 0.6 \quad (\text{Eq. E-14})$$

Grapple 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 E6.4.3.4.1.

$$\text{Grapple interlock gives false positive signal} = 2.7\text{E}-5$$

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 view through the camera

shows the grapple and its connection to the hoist. The operator is not focused on that connection while lining up the 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 (for example, unexpected canister movement to one side or tilting of the grapple). This is an opportunity to question the stability of the connection and to lower the canister back down to recheck the connection. However, the operator does not expect any problems in this operation and 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.

$$\text{Operator fails to notice bad connection between hoist and grapple through} = \\ 0.003 \times 4 \times 2 \times 0.8 = 0.02$$

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 E6.4.3.4.1.

$$\text{Grapple/canister drops from hoist} = 0.25$$

HEP Calculation for Scenario 2(a)—The events in the HEP model for Scenario 2(a) are presented in Table E6.4-9.

Table E6.4-9. HEP Model for HFE Group #4 Scenario 2(a) for 51A-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 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:

$$A \times B \times C \times D \times E = 0.0006 \times 0.6 \times 2.7E-5 \times 0.02 \times 0.25 < 1E-8 \quad (\text{Eq. E-15})$$

E6.4.3.4.3.2 HFE Group #4 Scenario 2(b) for 51A-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.

CTM 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. If the operator sees that the grapple has not properly engaged, then the operator disengages and repositions the grapple and tries again to engage.

In this task, the operator aligns the grapple visually using the camera view and then 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 $\times 11$, 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 $\times 4$. 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 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 $\times 3$, 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:

$$\text{Operator fails to fully engage grapple} = 0.005 \times [(11-1) \times 0.2 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] = 0.07 \quad (\text{Eq. E-16})$$

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 E6.4.3.4.1.

$$\text{Grapple engagement interlock gives false positive signal} = 2.7\text{E-}5$$

CTM Operator Fails to Notice Grapple Not Fully Engaged through Camera—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 engaged (for example, unexpected canister movement to one side or tilting of the grapple), which allows the operator the opportunity to question the stability of the connection and to lower the canister back down to recheck the connection. However, the operator does not expect any problems in this operation and tends 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 through the camera. The CTM operator believes that the correct action was performed initially, and this was confirmed by the false positive from the interlock, so this 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 can be completed successfully even with improper installation.

This event is quantified in Section E6.4.3.4.1.

$$\text{Canister drops from grapple} = 0.25$$

HEP Calculation for Scenario 2(b)—The events in the HEP model for Scenario 2(b) are presented in Table E6.4-10.

Table E6.4-10. HEP Model for HFE Group #4 Scenario 2(b) for 51A-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:

$$A \times B \times C \times D = 0.07 \times 2.7E-5 \times 1.0 \times 0.25 = 5E-7 \quad (\text{Eq. E-17})$$

E6.4.3.4.3.3 HFE Group #4 Scenario 2(c) for 51A-OpCTMdrop002-HFI-COD

1. CTT is not sufficiently centered under port
2. Operator fails to notice CTT not sufficiently centered
3. Operator fails to notice canister 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 canister drop. (NOTE: This scenario only applies to naval canisters 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 cask is not properly centered, it is possible that the naval canister could strike the ceiling around the cask port rather than rising smoothly through the cask port. This only applies to naval canisters because their cask lids are removed in the preparation area. For HLW any misalignment would be discovered during the lid lift by the CTM. In order for the naval canister to hit the unloading room ceiling during lift, the cask would have to be off-center by more 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:

$$\text{CTT is not sufficiently centered under port (dual-purpose canister/transportation cask)} = 0.003 \times 0.5 \times 0.8 \times 0.5 = 0.001$$

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 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 that the operator has failed in an observation of the relative locations of the grapple and the lid, or that the canister is not perfectly centered, but rather that the operator's decision is that it doesn't matter (it's "close enough") is incorrect. 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 adequate 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:

$$\begin{aligned} \text{Operator fails to notice that CTT not sufficiently centered} &= \\ 0.01 \times 5 &= 0.05 \end{aligned}$$

Operator Fails to Notice Canister Contacting Ceiling and Continues Lift—The CTM operator is able to see the naval canister through the camera display. When the naval canister 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 canister 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:

$$\begin{aligned} \text{Operator fails to notice canister contacting ceiling and continues lift} &= \\ 0.003 \times 3 &= 0.01 \end{aligned}$$

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 non-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 naval canister 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 E6.4.3.4.1.

$$\text{Load cell interlock fails} = 2.7E-5$$

Mechanical Failure of Hoist under Overload Causes Canister 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 canister. However, just because the hoist keeps pulling does not mean that

the naval canister falls (the hoist motor could overload and fail before the naval canister becomes detached from the hoist).

This event is quantified in Section E6.4.3.4.1.

Mechanical failure of hoist under overload causes canister drop = 0.25

HEP Calculation for Scenario 2(c)—The events in the HEP model for Scenario 2(c) are presented in Table E6.4-11.

Table E6.4-11. HEP Model for HFE Group #4 Scenario 2(c) for 51A-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 canister 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 canister drop	0.25

NOTE: CTT = cask transfer trolley; HEP = human error probability..

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times (C + D) \times E \times F = 0.001 \times 0.05 \times (0.01 + 0.03) \times 2.7E-5 \times 0.25 < 1E-8 \quad (\text{Eq. E-18})$$

E6.4.3.4.3.4 HFE Group # 4 Scenario 2(d) for 51A-OpCTMdrop002-HFI-COD

1. Crew member fails to fully withdraw lift fixture bolts
2. Operator fails to notice canister is rising with lift fixture and shield ring
3. Canister drops from lift fixture.

Crew Member Fails to Fully Withdraw Lift Fixture Bolts—The lift fixture for the naval canister is attached to both the canister and the shield ring. The lift fixture roughly looks like two concentric circles. The center circle has three bolts which attach the fixture to the canister, and the outer circle has several bolts which attach the fixture to the shield ring. A crew member is in the Canister Transfer Room, standing over the waste package port gate using long reach tools to unbolt the fixture from the canister. The crew member loosens the bolts until there is no resistance and there is confidence that the bolt is completely loose. The crew member does not remove the bolts from the fixture. This crew member is highly trained and performs bolt removal daily.

The crew member uses a long-reach tool to loosen the bolts. Since the bolts are not actually removed and the threads cannot be seen, the bolts are loosened until each one rotates freely. This unsafe action can be represented by NARA GTT A1, adjusted by the following CPCs:

- 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 $\times 11$, 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 complete the task and get to an area of lower radiation levels and also to keep the process moving for production reasons, but these are not compelling time pressure. 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 APOA anchor for 0.5 is that the operator must work at a fast pace with reduced time for checking. In this case, it is not that the operator must work at a fast pace, but rather that the operator wants to work quickly. Overall, it is reasonable to set APOA at 0.3.
- EPC 11: Poor, ambiguous or ill-matched system feedback. While the operator can be said to have feedback (the feel of a bolt moving freely). This EPC is applied to account for the operator only having this indirect feedback. The full affect EPC would be $\times 4$. 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 presence of indirect feedback only is deemed to represent full effect. The APOA is set at 1.0.
- EPC 13: Operator under-load/boredom. The full affect EPC would be $\times 3$, 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.
- EPC 14: A conflict between immediate and long term objectives. This EPC looks further at the issue of the operator wishing to get to a lower radiation area versus the need to complete the tasks. The full affect EPC is 2.5, which applies to a conflict between two very significant and important tasks, one of which has greater time urgency. The APOA anchor for 0.1 is for an operator having an immediate personal need, but there is an obvious safety task requiring completion. This appears reasonable for this task, so the APOA is set at 0.1.
- EPC 16: No obvious way of keeping track of progress during an activity. This addresses that there are no job aids that can track the loosening of the bolts; the crew member has to remember which ones are finished. The full affect EPC is 2. The APOA anchor for 0.1 is for a task of 5 to 9 steps. This task is three steps (three bolts). It appears reasonable to set the APOA at 0.05.

Using the NARA HEP equation yields the following:

$$\begin{aligned} &\text{Crew member fails to fully withdraw lift fixture bolts} = \\ &0.005 \times [(11-1) \times 0.3 + 1] \times [(4-1) \times 1.0 + 1] \times [(3-1) \times 0.1 + 1] \times [(2.5-1) \times 0.1 + 1] \\ &\quad \times [(2-1) \times 0.05 + 1] = 0.2 \qquad \qquad \qquad \text{(Eq. E-19)} \end{aligned}$$

Operator Fails to Notice Canister is Rising with Lift Fixture and Shield Ring—When the CTM operator is in the process of lifting the shield ring, the view through the camera shows the canister and its connection to the hoist. The operator is focused on that connection, due to specific training to ensure that the canister is free from the grapple/hoist. As the lift begins, the operator watches through the cameras, this is an opportunity to note that the canister is beginning to lift. This is also an opportunity to stop and ask the other crew member to return and finish unbolting. However, the operator does not be expecting there to be any problems in this operation and tends to believe that any perceived problems are illusions caused by the distortions of viewing through a camera. In addition to a camera view, there is also a view of the loadcell meter which indicates that the load on the hoist, which is also checked when beginning a lift.

In this case, the CTM operator fails to observe the lifting of the lift device and shield ring, and does not see (through the camera) or otherwise detect (by observing the output of the load cell on the control panel) that the canister is rising. This can be represented by CREAM CFF O3, adjusted by the following CPCs with value not equal to 1.0:

- CFF O3: Observation not made. (Omission. Overlooking a signal or a measurement). The baseline HEP is 0.003.
- CPC “Adequacy of Training/Preparation”: This routine task is well trained and practiced. The CPC value for an observation task with adequate training and high experience is 0.8.

Applying these factor yields the following:

$$\begin{aligned} &\text{Operator fails to notice canister is rising with lift fixture and shield ring} \\ &= 0.003 \times 0.8 = 0.003 \end{aligned}$$

Canister Drops from Lift Fixture—Just because the lift is occurring with partial engagement of one or more bolts does not mean that the canister falls. The safety margins built into these systems mean that it is possible that the canister can lift with the fixture and shield ring and be discovered later in the operation, allowing the operator to put it back down undamaged.

This event is quantified in Section E6.4.3.4.1.

$$\text{Canister drops from lift fixture} = 0.25$$

HEP Calculation for Scenario 2(d)—The events in the HEP model for Scenario 2(d) are presented in Table E6.4-12.

Table E6.4-12. HEP Model for HFE Group #4 Scenario 2(d) for 51A-OpCTMdrop002-HFI-COD

Designator	Description	Probability
A	Crew member fails to fully withdraw lift fixture bolts	0.2
B	Operator fails to notice canister is rising with lift fixture and shield ring	0.003
C	Canister drops from lift fixture	0.25

NOTE: HEP = human error probability.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B \times C = 0.2 \times 0.003 \times 0.25 = 2E-4 \quad (\text{Eq. E-20})$$

E6.4.3.4.3.5 HEP for HFE 51A-OpCTMdrop002-HFI-COD

The Boolean expression for the overall HFE (all scenarios) for moving a naval canister follows:

$$\begin{aligned} 51A\text{-OpCTMdrop002-HFI-COD (Naval Canister)} &= \text{HFE 2(a)} + \text{HFE 2(b)} + \\ &\text{HFE 2(c)} + \text{HFE 2(d)} = (<1E-8) + 5E-7 + (<1E-8) + 2E-4 = 2E-4 \quad (\text{Eq. E-21}) \end{aligned}$$

The Boolean expression for the overall HFE (all scenarios) for moving an HLW canister follows:

$$\begin{aligned} 51A\text{-OpCTMdrop002-HFI-COD (HLW)} &= \text{HFE 2(a)} + \text{HFE 2(b)} \\ &= (<1E-8) + 5E-7 = 5E-7 \quad (\text{Eq. E-22}) \end{aligned}$$

E6.4.4 Results of Detailed HRA for HFE Group #4

The final HEPs for the HFEs that required detailed analysis in HFE Group #4 are presented in Table E6.4-13 (with the original preliminary value shown in parentheses).

Table E6.4-13. Summary of HFE Detailed Analysis for HFE Group #4

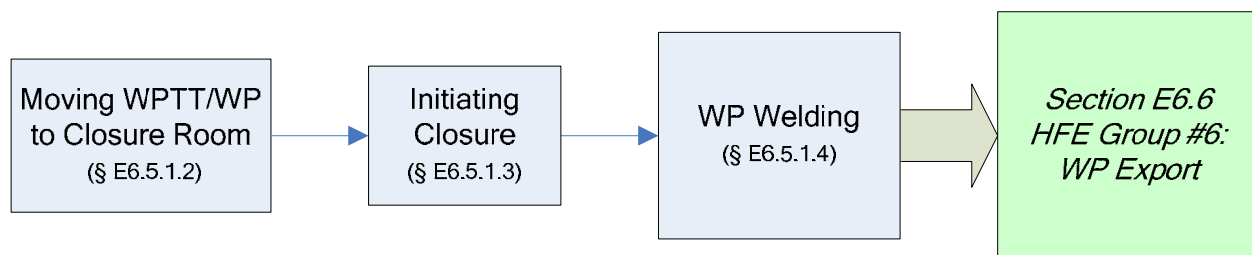
HFE	Description	Final Probability
51A-OpCTMdrop001-HFI-COD <i>Operator causes drop of object onto canister during CTM operations</i>	Operator causes drop of object onto canister during CTM operations	
	Applied to removing HLW lid and placing a waste package inner lid; does not apply to naval waste	4E-07 (2E-03)
	Applied to removing naval shield ring and placing a waste package inner lid; does not apply to HLW	4E-07 (2E-03)
51A-OpCTMdrop002-HFI-COD <i>Operator causes drop of canister during CTM operations (low-level drop)</i>	Operator causes drop of canister during CTM operations (low level drop)	
	Applied to moving an HLW canister	5E-07 (2E-03)
	Applied to moving a naval canister	2E-04 (2E-03)

NOTE: CTM = canister transfer machine; HFE = human failure event; HLW = high-level radioactive waste; WP = waste package.

Source: Original

E6.5 ANALYSIS OF HUMAN FAILURE EVENT GROUP #5: WASTE PACKAGE ASSEMBLY AND CLOSURE

HFE group #5 corresponds to the operations and initiating events associated with the ESD and HAZOP evaluation nodes listed in Table E6.0-1, covering waste package assembly and closure. The operations covered in this HFE group are shown in Figure E6.5-1. Closure activities begin with the canister in the waste package, aligned with the waste package port with the port closed. The WPTT moves the loaded waste package from the Canister Transfer Room into position underneath the Waste Package Closure Room, where the waste package is closed in preparation for export to the drifts. Closure activities include verification of the waste package/waste form, as well as welding, inerting, and polishing the package. This operation ends with the waste package being ready to be moved to the Waste Package Loadout Room, where the waste package is transferred into the TEV.



NOTE: § = Section; HFE = human failure event; WP = waste package; WPTT = waste package transfer trolley.
Source: Original

Figure E6.5-1. Activities Associated with HFE Group #5

E6.5.1 Group #5 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 waste package is secured to the WPTT and is positioned in the Waste Package Loading Room.
2. The waste package has both the inner lid and the spread ring already in place.
3. The waste package port slide gate is closed. There is an interlock between the port slide gates and the Waste Package Loading Room shield doors; the port slide gate cannot be open while the shield doors to the Waste Package Loading Room are also open.
4. All waste package assembly and closure operations are performed remotely. Operators have an adequate view of all operations via camera.

The following personnel are involved in this set of operations:

- RHS operator
- Arm operators (two)
- WPTT operator
- Quality control person
- Level 2 and 3 NDE personnel
- Supervisor.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.5.1.2 Moving the WPTT with Loaded Waste Package under Waste Package Closure Room

The WPTT operator remotely controls the WPTT with the loaded waste package and moves it underneath the Waste Package Closure Room. The WPTT rides on rails, travels at one speed, and has preprogrammed paths to follow. Only a human can start the WPTT movement or make the WPTT stop. There is a shield door between the Waste Package Loading Room and the Waste Package Positioning Room (under the Waste Package Closure Room).

E6.5.1.3 Initiating Closure Process (Loaded Waste Package with HLW or Naval Waste)

The operator uses the camera and the bumpy bar code reader to read the bar code on the waste package to ensure that it is the correct package. At this time, the operator puts the waste package serial number into the tracking chart. This step is verified by quality control.

E6.5.1.4 Waste Package Welding

E6.5.1.4.1 Expanding Spread Ring for Seal Weld

Once the spread ring position is verified, the RHS operator uses the RHS and camera to engage the spread ring expander tool. The RHS operator uses the expander tool to expand the spread ring.

E6.5.1.4.2 Sealing Weld Spread Ring to Inner Vessel and Inner Lid and Performing NDE

The welding team is composed of two arm operators, an RHS operator, a quality control person, and a level 2 and 3 NDE person(s). Each arm operator is responsible for welding half the circumference of the spread ring. The RHS operator is in charge of changing the end effectors as needed for the process (e.g., normal welding, grinding out the weld, dressing the weld). The arm operators use the robotic arm to do the actual welding, and the level 2 and 3 NDE personnel supervises, visually inspects, and verifies the weld. For this weld, there is a constant stainless steel weld wire spool feed. The level 2 and 3 NDE personnel must sign off this step.

E6.5.1.4.3 Inerting Waste Package and Performing Leak Test at Spread Ring and Purge Port Plug

All operations in this step are performed remotely. The RHS operator remotely retrieves the purge port tool and places it on top of the purge port. Once the tool is properly positioned, the operator initiates the tool and allows the helium to flow until sufficient time has passed and the pressure gage gives the proper reading. The RHS operator then sends the signals for the tool to stop helium flow, closes the cap, performs leak detection, and then checks the indicators to ensure that there are no leaks before continuing. Quality control verifies this step.

E6.5.1.4.4 Retrieval and Placement of Purge Port Cap

The RHS operator retrieves the purge port cap from its staging area, scans it with the bumpy bar code reader, documents the serial number, and places it onto the purge port. Quality control verifies this step.

E6.5.1.4.5 Welding Purge Port Cap and Performing NDE

The RHS operator installs the end effector on the robotic arm. The weld material is the same stainless steel used to weld the spread ring. The arm operator welds the cap in place, while the level 2 and 3 NDE person(s) visually inspects the process. Once welded, the RHS operator switches out the end effector for a dressing end effector, and the arm operator dresses the weld while the level 2 and 3 NDE person(s) visually inspects. A level 2 and 3 NDE must sign off this step.

E6.5.1.4.6 Retrieval and Placement of Outer Lid on the Waste Package from the Waste Package Closure Room

The RHS operator uses the camera and bumpy bar code reader to read the bar code on the waste package outer lid. At this time, the operator puts the waste package serial number into the tracking chart. This step is verified by quality control. Once the outer lid is documented, the operator retrieves the lid, engages the lid grapple, moves the lid to the proper position, and then disengages the grapple.

E6.5.1.4.7 Welding Outer Lid to Outer Barrier and Performing NDE

In preparation for this step, the RHS operator switches out the stainless steel weld feed spool for Alloy 22. This step is nearly identical to welding the inner lid (Section E6.5.1.4.2). The difference is that the end effector used has an ultrasonic testing/eddy-current testing (UT/ET) attachment that follows and tests the weld. The weld and UT/ET are verified by a level 2 and 3 NDE.

E6.5.1.4.8 Performing Stress Mitigation and NDE on Outer Lid

The RHS operator places the stress mitigation tool on the outer lid, and the operator and the level 2 and 3 NDE person(s) visually inspect the polish using a camera. Once the stress mitigation tool is done, the RHS operator removes the tool and places a UT/ET end effector on the robotic arm; the arm operator commences ultrasonic testing. The sealed waste package is verified again by a level 2 and 3 NDE.

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 waste package assembly and closure 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 Description	Applicable ESD	Preliminary Value	Justification
51A-OpWPCCollide1-HFI-NOD	<i>Operator Causes Low-Speed Collision of WPTT During Transfer to Closure Area:</i> As the WPTT is moved from the Waste Package Loading Room to the Waste Package Closure Room, the operator can cause the WPTT to collide into an SSC. The WPTT cannot physically go faster than 2.5 mph, and all collisions of the WPTT are low-speed.	8	3E-03	The WPTT is on rails, but an operator can cause a collision of the WPTT with an object in its path or into an SSC. The WPTT speed is physically limited by motor design; therefore, all collisions of the WPTT would be low-speed collisions. This failure is nearly identical to collision of the railcar while entering the facility (51A-OpRCCollide1-HFI-NOD; Section E6.1, HFE Group #1) and was assigned the same probability. This preliminary value is conservative because the path that the WPTT travels is expected to have fewer obstructions (e.g., doors, potential objects in the path) to collide with.
51A-OpTiltDown01-HFI-NOD	<i>Operator Initiates Premature Tilt-down during Transfer to Closure Area:</i> The operator can inadvertently initiate tilt-down of the waste package during transfer to the Waste Package Closure Room. If the waste package is near a facility structure, then this action could result in a collision of the waste package.	8	1.0	The operator can cause the WPTT to prematurely tilt down. The WPTT operator may be in the process of driving the WPTT to the Positioning Room. Tilt-down only occurs during waste package loadout in the Waste Package Loadout Room, and the controller for the WPTT tilt-down is distinct from other WPTT controls. In order to accomplish this failure, an interlock must also fail. This interlock, between the tilt-down mechanism and the docking station, has no bypass. As was previously discussed, the HRA team has assigned all unsafe actions that are combined with interlocks an HEP of 1.0.
WPTT derailment	<i>Operator Causes Derailment of WPTT:</i> The WPTT travels on rail from the Waste Package Loading Room to the Waste Package Positioning Room. During this transfer the operator can cause the WPTT to derail by running over a large object left on the rail or through other such mechanisms.	8	N/A ^a	In this step, the WPTT moves on rail from outside the Waste Package Loading Room to the closing position in the Waste Package Positioning Room below the Waste Package Closure Room. During this travel, there is a probability that the WPTT can derail, leading to a tipover of the WPTT. 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.
51A-OPWPInnerLid-HFI-NOD	<i>Operator Causes Direct Exposure During WP Loading:</i> If the CTM operator fails to close the port gate before lifting the shield skirt after placing a canister in a waste package, and a worker violates the procedural control by entering the Transfer Room during canister transfer activities, that worker is exposed. Also, if the CTM operators fail to install the WP inner lid and a person violates the procedural controls and enters the WP closure area when the WPTT is transferred into the room, that person gets a direct exposure. This HFE results in a potential direct exposure in the CTM transfer room and/or in the WP Closure Room. In this case, to prevent double counting, this failure event was only modeled only in ESD 12B (Direct exposure during waste package closure), not ESD 12A (Direct exposure during CTM activities) and 12B.	12	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. Similarly, installation of a WP is a very simple operation, is performed regularly, 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 inappropriately entering a radiation controlled area, by a person of a separate "team" must also occur. This HFE was considered extremely unlikely and assigned a preliminary value of 0.0001.
Improper waste package closure	<i>Operator Damages Canister during Welding:</i> The waste package inner and outer lids are welded closed as part of waste package closure activities. This task is a remote operation with a high level of automation; however, it may be possible for an operator to improperly weld the canister such that the canister becomes damaged. Note: Improper welding may also have postclosure implications. However, HFEs that have no safety consequences over the preclosure period but that may have consequences postclosure are out of the scope of this analysis and are addressed in the postclosure safety assessment.	9	N/A	The analysts could not identify any human actions that would contribute to canister damage during welding. Latent conditions due to bad welds may have postclosure consequences, but they are out of the scope of this analysis and are addressed in the postclosure safety assessment.
Drop of object	<i>Operator Drops Object on Canister with RHS:</i> The waste package inner and outer lids are welded closed as part of waste package closure activities. The RHS is used to move objects over the canister, including the outer lid, as part of this task. The operator could drop an object onto the canister during these lifts.	9	N/A ^a	In this step, the operator uses the RHS to move several objects over the waste package and canister. The outer lid is moved over the waste package. Other objects, such as spools of welding material, may also be moved over the waste package during this operation; however, the inner and outer lids are the only objects that are heavy enough to potentially damage the waste package or canister. 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.

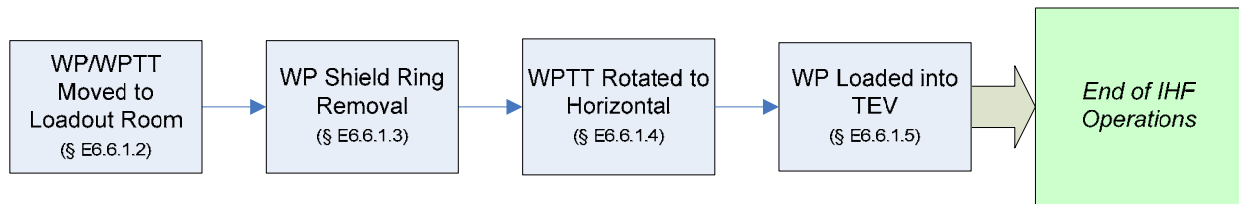
NOTE: ^a HRA preliminary value replaced by use of historic data; Attachment C provides additional information on Active Component Reliability Data
CTM = canister transfer machine; ESD = event sequence diagram; HFE = human failure event; HRA = human reliability analysis; ID = identification; IHF = Initial Handling Facility;
N/A = not applicable; RHS = remote handling system; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WPTT = waste package transfer trolley.
Source: Original

E6.5.3 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).

E6.6 ANALYSIS OF HUMAN FAILURE EVENT GROUP #6: WASTE PACKAGE EXPORT

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 waste package export. The operations covered in this HFE group are shown in Figure E6.6 1. The activities covered in HFE group #6 begin with the sealed waste package ready for emplacement, sitting vertically in the WPTT in the Waste Package Closure Room. They proceed through moving the WPTT to the Waste Package Loadout Room, removal of the waste package shield ring, translation of the WPTT enclosure to a horizontal position, and transfer of the waste package to the TEV. The operation ends when the TEV is loaded, ready for export.



NOTE: § = Section; IHF = Initial Handling Facility; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

Figure E6.6-1. Activities Associated with HFE Group #6

E6.6.1 Group #6 Base Case Scenario

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. The waste package is secured to the WPTT and positioned under the Waste Package Closure Room.
2. The waste package is sealed, inspected, and has a shield ring resting on top.
3. The TEV is staged in the loadout area, ready to be loaded—shield door open and bottom plate lowered.
4. There is an interlock between the shield door and the personnel access doors—if there is a loaded waste package in the Closure Room (load cell), the shield door does not open (and thus the WPTT cannot move into the Loadout Room) until the personnel access doors are closed and locked.

The following personnel are involved in this set of operations:

- WPTT Operator
- Crane Operator
- Signaling Crew member
- Verification Crew member
- Radiation Protection Worker
- Supervisor
- TEV Operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

E6.6.1.2 Loaded and Sealed Waste Package Movement to Waste Package Loadout Room and WPTT Docking Station Engagement

This operation is performed remotely. The WPTT operator opens the closure area shield door and moves the WPTT (on rail) to the docking station in the Waste Package Loadout Room. Once the WPTT has cleared the door, the WPTT operator closes the closure area shield door. When in the proper position by the docking station, the WPTT engages the docking station by moving an arm down. Engagement is automatic. The WPTT operator checks the indicator to ensure proper engagement before continuing.

E6.6.1.3 Waste Package Shield Ring Removal and Movement of Shield Ring to Waste Package Shield Ring Stand

At this point, the crane operator, with the aid of a signaling and a verification crew member, removes the waste package shield ring from the WPTT. It is to be determined if this operation is performed remotely or locally; this analysis describes a local operation as it is believed to be the case with greater potential for error. Here, the operator installs a lifting device (sling or hooks which connect to eye holes) on the waste package shield ring. Once the fixture is secure, the operator moves several yards away from the WPTT and signals the crane operator to lift the ring and place it on the stand. Once the shield ring is on the stand, all crew members must leave the area and close the shield door. A pre-designated person, such as the radiation protection worker, is responsible for ensuring (via a checklist) that all personnel have left the Waste Package Loadout Room and for relaying that information to the WPTT operator in the IHF Control Room.

E6.6.1.4 WPTT Horizontal Rotation

The following steps are performed remotely. The WPTT operator confirms that the Waste Package Loadout Room is empty and signals the WPTT to downend the waste package.

E6.6.1.5 Waste Package Inspection and Loading into TEV

The WPTT operator signals the transfer carriage to move the waste package under the TEV. As the waste package is moving under the TEV, the WPTT and TEV operators visually (via camera) inspect the waste package for damage; these are independent checks because the WPTT and TEV operators are in different control rooms; the WPTT operator is in the facility while the TEV operator is in the Central Control Center. Once the waste package is under the TEV, the TEV operator signals the TEV to pick up the waste package, lift the bottom shield plate, and close the shield door.

E6.6.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, 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 waste package export 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 Description	Applicable ESD	Preliminary Value	Justification
51A-OpWPCollide1-HFI-NOD	<i>Operator Causes Low-Speed Collision of WPTT During Transfer to Waste Package Loadout Room:</i> As the WPTT is moved from the Waste Package Positioning Room to the Waste Package Loadout Room, the operator can cause the WPTT to collide into an SSC. Due to the WPTT motor design all collisions of the WPTT are low-speed.	10	3E-03	The WPTT is on rails, but an operator can cause a collision of the WPTT with an object in its path or into an SSC. The WPTT speed is limited by motor design; therefore, all collisions of the WPTT would be low-speed collisions. This failure is nearly identical to collision of the railcar while entering the facility (51A-OpRCollide1-HFI-NOD; Section E6.1, HFE Group #1) and was assigned the same probability. This is a conservative preliminary value because the path the WPTT travels is expected to have fewer obstructions (e.g., doors, potential objects in the path) to collide with. This is the same failure as collision of the WPTT during transfer to the closure area (51A-OpWPCollide1-HFI-NOD; Section E6.5, HFE Group #5).
51A-OpTiltDown01-HFI-NOD	<i>Operator Initiates Premature Tilt-Down During Transfer to Waste Package Loadout Room:</i> The operator can inadvertently initiate tilt-down of the waste package during transfer to the Waste Package Loadout Room. If the waste package is near a facility structure, then this could result in a collision of the waste package.	10	1.0	The operator can cause the WPTT to prematurely tilt down. The WPTT operator is in the process of driving the WPTT to the Loadout Room. Tilt-down only occurs during waste package loadout in the Waste Package Loadout Room, and the controller for the WPTT tilt-down is distinct from other WPTT controls. In order to accomplish this failure, an interlock must also fail. This interlock, between the tilt-down mechanism and the docking station, has no bypass. As was previously discussed, the HRA Team has assigned all unsafe actions that are combined with interlocks an HEP of 1.0. This is the same failure as premature tilt-down of the WPTT during transfer to the closure area (51A-OpTiltDown01-HFI-NOD; Section E6.5, HFE Group #5).
WPTT derailment	<i>Operator Causes Derailment of WPTT:</i> The WPTT travels on rail from the Waste Package Positioning Room to the Waste Package Loadout Room. During this transfer the operator can cause the WPTT to derail by running over a large object left on the rail or through other such mechanisms.	10	N/A ^a	In this step, the WPTT moves on rail from the Waste Package Positioning Room to the Waste Package Loadout Room. During this travel, there is a probability that the WPTT can derail, leading to a tipover of the WPTT. 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.
51A-OpSDClose001-HFI-NOD	<i>Operator Closes Shield Door on Conveyance:</i> The WPTT passes through shield doors as it enters the Waste Package Loadout Room. During this transfer, the operator can close the shield door on the WPTT.	6	1.0	The WPTT passes through shield doors as it enters the Waste Package Loadout Room. During this transfer, the operator can close the shield door on the WPTT. See Section E6.0.2.3.3 for a justification of these preliminary values.
TEV_Collision	<i>Operator Drives TEV into Waste Package:</i> The TEV is pre-staged in the Waste Package Loadout Room with power off, ready to receive a waste package. Because the TEV is not moved in this operation, this failure was omitted from analysis.	11	N/A	The TEV is pre-staged in the Waste Package Loadout Room with power off, ready to receive a waste package. Because the TEV is not moved in this operation, this failure was omitted from analysis.
51A-OpTEVDClose4-HFI-NOD	<i>Operator begins Waste Package Extraction before TEV Doors Open:</i> If the operator extracts the waste package before opening the TEV shield doors, then the waste package runs into the TEV.	11	1E-03	The TEV is pre-staged, and TEV operations in this respect are very standard, so it is unlikely that the TEV operator would not open the TEV shield door/extend bed plate (0.01). The shield doors and bedplate are very visible, and there is adequate time between WPTT tilt-down and TEV loading for the operators to notice that the TEV has not been properly staged before tilt-down (fail to notice, 0.1). Therefore, the preliminary value for waste package impact due to extraction before TEV doors are open is 0.001.
51A-OpCranetilt-HFI-NOD	<i>Operator Causes Crane to Interfere with TEV or WPTT:</i> If the operator fails to properly slow the crane rigging, then the WPTT can impact the crane hook while tilting down.	11	1E-04	This operation was given the same preliminary value as "Cask Tipover during Upending and Removal" (HFE 51A-Optipover001-HFI-NOD; Section E6.2, HFE Group #2) because it is a similar operation (i.e., movement with the crane using the same type of rigging/attachments) and has similar failure modes (i.e., failure to properly slow crane rigging).
51A-OpWPTTiltUp01-HFI-NOD	<i>Operator Causes Premature Tilt-up of WPTT:</i> If the operator signals the WPTT to tilt up while the waste package is being extracted, this would result in a drop of the waste package.	11	1.0	While moving a waste package into the TEV, the operator can inadvertently cause the WPTT to tilt up, resulting in a drop of the waste package. In order to accomplish this, there are interlock(s) that must also fail. To be conservative, all unsafe actions that require an equipment failure to cause an initiating event have been assigned an HEP of 1.0.
Drop of object on WP	<i>Operator Drops Heavy Object on Waste Package:</i> During waste package export, the waste package shield ring is removed. It is possible that the shield ring can be dropped onto the waste package during this operation.	11	N/A ^a	In this step the operator moves the waste package shield ring over the waste package; the operator can potentially drop the shield ring onto the waste package. 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/rigging types. Documentation for this failure can be found in Attachment C.

Table E6.6-1. HFE Group #6 Descriptions and Preliminary Analysis (Continued)

HFE ID	HFE Description	Applicable ESD	Preliminary Value	Justification
51A-OpDirExpos3-HFI-NOD	Operator Opens Facility Door during TEV Loading: There is a gap between the tilted down WPTT and the TEV; if the operator opens the facility door while the waste package is pulled into the TEV, the operator would get a direct exposure.	12	1E-03	In the process of TEV loading, the waste package is purposefully exposed to the Waste Package Loadout Room. Because of this "shine by design" mode of TEV loading, there are many safeguards to prevent personnel from being in the Waste Package Loadout Room during TEV loading. There are two general ways for a person to be in the Waste Package Loadout Room during this operation: an operator is left in the Waste Package Loadout Room when the operation begins, or an operator enters the room after operations begin. There are procedural controls associated with the radiation protection program that limit who can be and when people can be in the Waste Package Loadout Room. There are also at least two separate checks of the room before operations begin: one locally and one from the IHF Control Room via camera. Finally, there are radiation lights and alarms (non-ITS) that activate when operations begin. If a person is left in the Waste Package Loadout Room, that person has several minutes to exit the room through clearly marked exits before they are exposed. For an operator to enter the room after operations begin, the door must be unlocked. There is an interlock that ensures that the shield doors are locked before the WPTT enters the Waste Package Loadout Room. For the shield doors to be unlocked, then, the interlock would have to fail, or a worker must ask the IHF Control Room supervisor for permission to enter. If the supervisor chooses to grant permission, the supervisor must stop operations, move the waste package to a safe and shielded state, and then unlock the shield door. If the supervisor fails to stop operations before letting the worker in, or if the operations are prematurely restarted before the worker leaves, then the worker would get a direct exposure. This failure was assessed to be highly unlikely and assigned a preliminary value of 0.001.
51A-OpShieldRing-HFI-NOD	Operator Fails to Install Waste Package Shield Ring in WPTT: If a waste package shield ring is not preinstalled in the WPTT before the canister is placed inside the waste package during CTM activities, then when operators approach the waste package to remove the shield ring in the Waste Package Loadout Room, they would get a direct exposure.	12	1E-04	The waste package shield ring is installed as part of the staging activities before IHF operations for waste package loading begin. Shield ring installation is checked off by the staging crew and is also checked off by the operations crew directly before operations begin as part of the prep job plan. If the shield ring is not installed, the CTM operator has the chance to notice when replacing the canister inside the waste package (via a camera view looking down on the missing shield ring). If the canister is empaced in the waste package, then once the CTM moves away from the port, there would be a direct exposure. This failure received a preliminary value of 0.01 for failure to install shield ring and 0.01 for failure to notice before a direct exposure occurs, resulting in a total preliminary value of 0.0001.
51A-OpFailInt-HFI-NOM	Operator Fails to Restore Interlock after Maintenance: There is an interlock that prevents the waste package port gate from opening if a waste package containing a shield ring is not below the port. This interlock may be bypassed during normal maintenance. If the bypass is not restored, this could contribute to HFE 51A-OpShieldRing-HFI-NOD.	12	1E-02	There is an interlock that prevents the port gate from opening if a waste package containing a waste package shield ring is not below the port. This interlock may be bypassed during normal maintenance. If the bypass is not restored by the maintenance worker and not discovered by the prep job check, this could contribute to HFE 51A-OpShieldRing-HFI-NOD. 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.
WPTT uncontrolled tilt-down	Operator causes uncontrolled tilt-down of WPTT	10	N/A	No human actions were identified that would contribute to an uncontrolled tilt-down.

NOTE: ^aHRA preliminary value replaced by use of historic data (Attachment C).

CTM = canister transfer machine; HEP = human error probability; HFE = human failure event; IHF = Initial Handling Facility; ITS = important to safety; N/A = not applicable; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

E6.6.3 Detailed Analysis for HFE Group #6

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 Part 63 (Ref. E8.2.1) 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 E6.6.3.2.

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:

1. ATHEANA expert judgment (Ref. E8.1.22)
2. CREAM (Ref. E8.1.18)
3. HEART/NARA (Ref. E8.1.28 and Ref. E8.1.11)
4. THERP (Ref. E8.1.26).

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 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 about 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 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 IHF PCSA model determined that there is one HFE in this group whose preliminary value was too high to demonstrate compliance with the performance objectives stated in 10 CFR 63.111(Ref. E8.2.1). This HFE is presented in Table E6.6-2.

Table E6.6-2. Group #6 HFE Requiring Detailed Analysis

HFE	Description	Preliminary Value
51A-OpDirExpose3-HFI-NOD	Operator causes direct exposure while loading TEV	1E-03

NOTE: HFE = human failure event; TEV = transport and emplacement vehicle.

Source: Original

E6.6.3.2 Assessment of Potential Vulnerabilities (Step 5)

For those HFEs requiring detailed analysis, the first step in the ATHEANA (Ref. E8.1.22) 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 that 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 waste package export that relate to potential human failure scenarios relevant to the listed HFE. Other vulnerabilities exist that would be relevant to other potential HFEs that can occur during the waste package export operation, but these have no bearing on this analysis.

E6.6.3.2.1 Operating Team Characteristics

WPTT Operator—Located in the Operations Room, the WPTT operator has received training for the WPTT and has observed operations prior to being allowed to operate the WPTT on a dry run. The WPTT operator has signed off to operate the WPTT based on an evaluation of proficiency during a dry run. The WPTT operator has been observed on initial operations before being signed off for solo operation. A single operator is assigned to the WPTT operation.

Waste Package Handling Crane Operator—Located in the Operations Room for this set of operations, the waste package handling crane operator has received training for crane operations and has observed operations prior to being allowed to operate the crane on a dry run. The waste package handling crane operator has signed off to operate the crane based on an evaluation of proficiency during a dry run. The waste package handling crane operator has been observed on initial operations before being signed off for solo operation. A single operator is assigned to the waste package handling crane operation.

Radiation Protection Worker—The radiation worker is a fully certified health physics technician, whose job is to monitor radiation during cask-related activities. The radiation worker is responsible for stopping operations if high radiation levels are detected.

Supervisor—The supervisor is in the IHF Control Room during TEV loading. The supervisor is in charge of verifying proper operations and is also the only one who can grant other personnel access to the Waste Package Loadout Room (via pass code and key) from the IHF Control Room.

E6.6.3.2.2 Operation and Design Characteristics

No humans are in the Waste Package Loadout Room during this operation; all operators are located remotely in the IHF Control Room. Crew members only enter this room for waste package preparation, which happens before the waste package is loaded. The height of the hoist yoke is displayed digitally on a control panel. A joystick is used for fine motion alignment of the grapple (which can move the hoist within the bell). Flat screen displays show the view from a camera mounted on the boom above the yoke. The control interface for adjustable speed drive (ASD) is incorporated into the panel.

All doors from the Waste Package Loadout Room can be opened from the inside in case of an emergency.

To open the facility shield door to the Waste Package Loadout Room, two people are required: one person has to unlock the shield door locally, and the other (a supervisor) has to unlock the door from the IHF Control Room.

The personnel access door can only be opened from the IHF Control Room and requires two separate actions (i.e., entering a pass code and then inserting a key). Only a supervisor is able to perform this action. However, the personnel access door is unlocked during waste package preparation and must be relocked before TEV loading begins.

Radiation control signs and flashing lights are provided outside the door during TEV loading. These are non-ITS equipment.

After personnel have removed the waste package shield ring and left the loadout area, the radiation protection worker or other pre-designated person ensures that the Waste Package Loadout Room is vacant and signals the WPTT operator that it is safe to begin tilt-down.

A public address announcement is made inside the area to alert workers to clear the area before the WPTT is tilted. Intercom communications and television monitoring between workers and the IHF Control Room ensure that the operator knows if exit is delayed.

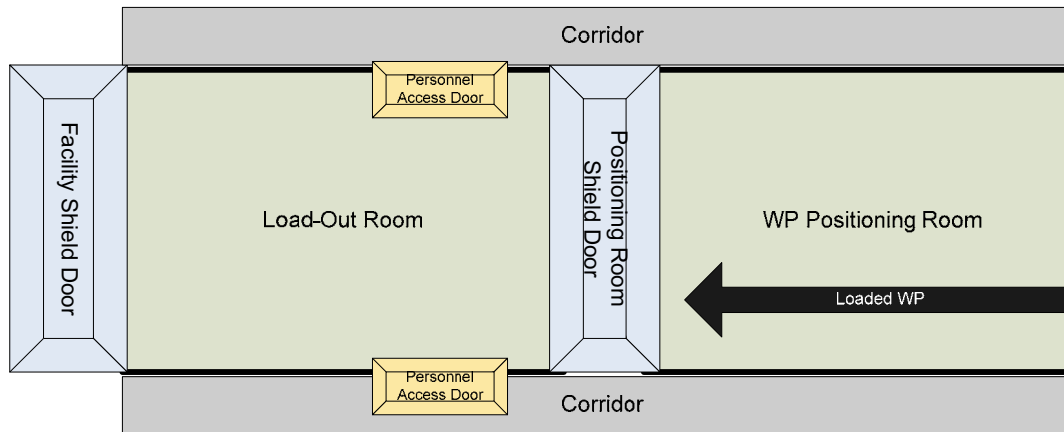
Interlocks—The Waste Package Positioning Room has a load cell that can differentiate between an empty waste package and a loaded waste package. If there is a loaded waste package in the Waste Package Positioning Room, the Waste Package Positioning Room shield door cannot open to allow the WPTT to move to the Waste Package Loadout Room for export unless the facility shield door and the personnel shield doors are locked. Figure E6.6-2 shows the location of the various shield doors; this illustration is conceptual and does not provide a precise representation of the actual configuration.

E6.6.3.2.3 Operational Conditions

There are no specific influencing operational conditions for this HFE group.

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 Waste Package Loadout Room except during scheduled times. A personnel accountability system is associated with entering and exiting the Waste Package Loadout Room. Personnel are required to check in with the supervisor and tag in and tag out before entering or after leaving the Waste Package Loadout Room.



Source: Original

Figure E6.6-2. Waste Package Positioning Room and Waste Package Loadout Room Conceptual Configuration

E6.6.3.2.5 Operator Tendencies and Informal Rules

Consequences of Failure—The operations are performed remotely. No personnel are in the vicinity of the operation, and so the threat of physical injury is absent. The WPTT operator expects that failures are mitigated by design features without serious consequences, which promotes complacency in the operations.

Anticipatory Actions—The loadout process is remote, has a high degree of automation, and problems of any kind are not expected. There is a tendency for the WPTT operator to focus on future tasks while the waste package is being loaded into the TEV.

Requests to Enter Loadout Room—The supervisor is present in the IHF Control Room and aware of the stage of TEV loading. Serious consequences are associated with personnel being present in the Waste Package Loadout Room while a TEV is being loaded. Therefore, the supervisor is very cautious not to admit anyone into the Waste Package Loadout Room during this time. If access to the room is necessary, the supervisor either stops operations and tilts up the WPTT or makes sure that the TEV is fully loaded with shield doors closed before admitting a worker into the room.

E6.6.3.2.6 Operator Expectations

Anticipatory Actions—No one attempts to enter the Waste Package Loadout Room without a compelling reason.

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 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 E6.6-3 summarizes the HFE scenarios developed for the HFE in this group.

Table E6.6-3. HFE Scenarios and Expected Human Failures for Group #6

HFE	HFE Scenarios
51A-OpDirExpose3-HFI-NOD <i>Operator causes direct exposure while loading TEV</i>	HFE Scenario 1(a): (1) A crew member remains in the Waste Package Loadout Room after an evacuation is ordered OR a WPTT operator fails to order an evacuation; (2) radiation protection worker fails to check if room is empty or radiation protection worker fails to recognize that someone is still in the room; (3) the crew member fails to notice that loadout is occurring OR the crew member fails to exit the room in time to avoid exposure. HFE Scenario 1(b) ^a : (1) A crew member requests reentry into the Waste Package Loadout Room; (2) the supervisor agrees to allow access. HFE Scenario 1(c): (1) The personnel access shield door is left open; (2) the interlock OR the load cell fails and the WPTT enters the Waste Package Loadout Room.

NOTE: ^a This failure sequence requires several additional failures to actually result in a direct exposure once the crew member is let inside the Loadout Room, such as: the supervisor fails to request stop of the loadout operation OR WPTT operator fails to stop the operation as requested OR the supervisor fails to verify that the operation has stopped before opening door OR the supervisor prematurely restarts operation. Instead of quantifying each scenario, it is conservatively considered that if the supervisor allowed access to the Loadout Room once the WPTT was there, it would result in a direct exposure.

HFE = human failure event; WPTT = waste package transfer trolley.

Source: Original

Since there is only one HFE identified for detailed analysis in this group, the scenarios are organized under this HFE category, with the scenarios numbered as 1(a), 1(b), and 1(c).

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 below.

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 then 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.

$$\text{Interlock fails to perform function} = 2.7E-05$$

Load Cell Failure—This mechanical failure was used for the load sensor used to evaluate if there is a loaded WPTT in the positioning room. The mechanical failure probability for a load cell, represented by a pressure sensor from Attachment C, Table C4-1, is approximately $4.0E-03$ /demand.

$$\text{Load cell fails} = 4.0E-03$$

E6.6.3.4.2 Quantification of HFE Scenarios for 51A-OpDirExpose3-HFI-NOD: Operator Causes Direct Exposure during TEV Loading

E6.6.3.4.2.1 HFE Group #6 Scenario 1(a) for 51A-OpDirExpose3-HFI-NOD

1. A crew member remains on the second floor of the Waste Package Loadout Room after an evacuation is ordered OR a WPTT operator fails to order an evacuation.
2. Radiation Protection Worker fails to check if the room is empty OR fails to recognize that someone is still in the room.
3. A crew member fails to notice that loadout is occurring OR a crew member fails to exit the room in time to avoid exposure.

A Crew Member Remains on the Second Floor of the Waste Package Loadout Room after an Evacuation Is Ordered—Prior to moving a loaded waste package to the Waste Package Loadout Room, there may be maintenance or (empty) waste package preparation activities going on in the Waste Package Loadout Room. Once the WPTT is ready to be moved to the Waste Package Loadout Room, the WPTT operator makes an announcement for all personnel to leave the Waste Package Loadout Room.

Even if the WPTT operator notifies workers to leave the Load out Room, it is possible that they would not do so. The action of leaving is quite simple, but the communication of the request

could be missed by virtue of the person being engrossed in a task. This can be represented by NARA GTT D1, adjusted for 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 applies to a proliferation of information, but it can be applied to masking by any distracting mechanism. The full effect is $\times 10$, which applies to significant levels of distraction. In this case, the level of distraction would be small as there would not be a significant amount of machine noise to mask the facility paging system announcement. The APOA is judged to be minimal, and thus is set to 0.1.

Using the HEP equation yields:

$$\text{Crew member remains on the second floor of the Waste Package Loadout Room after an evacuation is ordered} = 0.006 \times [(10-1) \times 0.1 + 1] = 0.01 \quad (\text{Eq. E-23})$$

WPTT Operator Fails to Order Evacuation—The WPTT operator is required to announce that all personnel are to leave the Waste Package Loadout Room prior to initiating movement of the WPTT into the room. This action is part of the process procedure. The operator is required to make the announcement whether or not it is believed that anyone is in the room, so this can be represented by CREAM (Ref. E8.1.18) execution CFF E5, adjusted for the following CPCs with value not equal to 1.0:

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03.
- CPC “Working Conditions”: The working conditions for the operator are in the IHF 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:

$$\begin{aligned} \text{WPTT operator fails to order an evacuation} = \\ 0.03 \times 0.8 \times 0.8 \times 0.5 \times 0.8 = 0.008 \end{aligned}$$

Radiation Protection Worker Fails to Check if Room Is Empty—This is an EOO by the radiation protection worker (or another pre-designated person) who fails to personally ensure that the Waste Package Loadout Room has been cleared of personnel. This is considered to be represented by CREAM (Ref. E8.1.18) execution CFF E5, adjusted for the following CPCs:

- CFF E5: Action missed, not performed (omission). The baseline HEP is 0.03.
- CPC “Working Conditions”: The working conditions are in the Waste Package Loadout Room with a less favorable environment than the IHF Control Room due to controlled access. The CPC for incompatible working conditions for an execution task is 2.0.
- 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”: It is anticipated that there is some time pressure to successfully perform this task so that loadout can proceed. The CPC for temporarily inadequate available time for an execution task is 1.0.
- 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:

$$\begin{aligned} \text{Radiation protection workers fail to check if the room is empty} = \\ 0.03 \times 2.0 \times 0.8 \times 1.0 \times 0.8 = 0.04 \end{aligned}$$

Radiation Protection Worker Fails to Recognize that Someone Is Still in the Room—This EOC is considered to occur due to a lack of attention or perhaps a distraction that causes the radiation protection worker to fail to perform the check properly. It is considered to be covered by HEART (Ref. E8.1.28) Generic Task (D), modified by the following EPC:

- GT (D): Fairly simple task performed rapidly or given scant attention with a baseline HEP of 0.09.
- EPC 17: Inadequate checking (HEART EPC 17). Little or no independent checking. The full effect is $\times 3$. In this case, since the radiation protection worker is completely unsupervised, the APOA is judged to be complete and is set at 1.0.

$$\begin{aligned} \text{Radiation protection worker fails to recognize that someone is still in the room} = \\ 0.09 \times [(3-1) \times 1.0 + 1] = 0.27 \end{aligned} \quad (\text{Eq. E-24})$$

Crew Member Fails to Notice that Loadout Is Occurring—If someone is left in the Waste Package Loadout Room once the WPTT operator begins tilt-down, the crew member in the Waste Package Loadout Room has a few minutes before actually getting a direct exposure (after the waste package has been tilted down and the transfer carriage removed). All exits from the Waste Package Loadout Room are clearly marked and unlocked from the inside. All crew

involved in TEV loading operations are trained and aware of the severe consequences associated with exposure to a bare waste package.

This error most closely corresponds to the CREAM (Ref. E8.1.18) observation error O3 (“Observation Not Made”).

- CFF O3: Observation not made (omission). The baseline HEP is 0.001.
- CPC “Working Conditions”: The working conditions are in the Waste Package Loadout Room with a less favorable environment than the IHF Control Room due to controlled access. The CPC for incompatible working conditions for an observation task is 2.0.
- CPC “Available Time”: It is anticipated that there is some time pressure to successfully perform this task so that load out can proceed. The CPC for temporarily inadequate available time for an observation task is 1.0.
- CPC “Adequacy of Training/Preparation”: This is a task that is clearly trained, and the risks of loadout are emphasized in training. Because it is performed frequently, there is a high level of experience. The CPC for adequate training and high experience for an observation task is 0.8.

Applying these factors yields the following:

$$\begin{aligned} \text{Crew member fails to notice that loadout is occurring} = \\ 0.001 \times 2.0 \times 1.0 \times 0.8 = 0.002 \end{aligned}$$

Crew Member Fails to Exit the Room in Time to Avoid Exposure—Training indicates the need for action in such a case. A few minutes are available to exit through clearly marked doors. This can be represented by NARA GTT C1, adjusted for the following EPCs:

- GTT C1: Simple response to a range of alarms/indications providing a clear indication of the situation (simple diagnosis required). Response might be a direct execution of simple actions or initiating other actions separately assessed. The baseline HEP is 0.0004.
- EPC 3: Time pressure. The full effect is $\times 11$, which corresponds to the operator having just enough time. In this case, there are some minutes left to act. The APOA anchor for 0.5 is that the operator must work at a fast pace. The situation is judged to be between these two anchors, and thus the APOA is set to 0.75.

Using the NARA HEP equation yields the following:

$$\begin{aligned} \text{Crew member fails to exit the room in time to avoid exposure} = \\ 0.0004 \times [(11-1) \times 0.75 + 1] = 0.003 \end{aligned} \quad (\text{Eq. E-25})$$

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 51A-OpDirExpose3-HFI-NOD

Designator	Description	Probability
A	A crew member remains on the second floor of the Waste Package Loadout Room after an evacuation is ordered	0.01
B	A WPTT operator fails to order an evacuation	0.008
C	Radiation Protection Worker fails to check if the room is empty	0.04
D	Radiation Protection Worker fails to recognize that someone is still in the room	0.27
E	A crew member fails to notice that loadout is occurring	0.002
F	A crew member fails to exit the room in time to avoid exposure	0.003

NOTE: WPTT = waste package transfer trolley.

Source: Original

The Boolean expression for this scenario follows:

$$(A + B) \times (C + D) \times (E + F) = (0.01 + 0.008) \times (0.04 + 0.27) \times (0.002 + 0.003) = (0.018) \times (0.31) \times (0.005) = 3E-5 \quad (\text{Eq. E-26})$$

E6.6.3.4.2.2 HFE Group #6 Scenario 1(b) for 51A-OpDirExpose3-HFI-NOD

1. A crew member requests reentry into the Waste Package Loadout Room.
2. The supervisor agrees to allow access.

Crew Member Requests Re-entry into the Waste Package Loadout Room—TEV loading is a normal part of operations that takes less than a few hours and is performed about twice a week. Workers are trained not to enter the Waste Package Loadout Room unless necessary for a prescheduled activity. There is a posted schedule that all the workers, including the supervisor, are aware of. Also, during loadout, there are indicators in the IHF Control Room and outside both the personnel access door and the shield door that turn on when TEV loading is in progress. These indicators, however, are non-ITS equipment, and no credit is given for their function.

Entry would have to be for some perceived urgent need in order to countermand training. This is believed to be best represented by NARA GTT A4, adjusted for the following EPCs:

- GTT A4: Judgment needed for appropriate procedure to be followed, based on interpretation of a situation that is covered by training at appropriate intervals. The baseline HEP is 0.006.
- EPC 14: Conflict between immediate and long-term objectives. The full effect is $\times 2.5$, which corresponds to deciding between two extremely significant problems, one of which is clearly more urgent than the other. The APOA anchor for 0.5 can be interpreted as suggesting situations of balancing an urgent plant need with an urgent personal need. The APOA anchor for 0.1 is that an individual has immediate personal needs, but there is an obvious safety task that requires completion. Other reasons for reducing from full effect include training and procedures that dictate a hierarchy of goals

(which, in this case, may or may not actually help). The situation in this case is judged to be between 0.1 and 0.5, and thus the APOA is set to 0.3.

Using the NARA HEP equation yields the following:

$$\begin{aligned} \text{Crew member requests reentry into the Waste Package Loadout Room} = \\ 0.006 \times [(2.5-1) \times 0.3 + 1] = 0.009 \end{aligned} \quad (\text{Eq. E-27})$$

It should be noted that there are other possible unsafe actions for this scenario, such as the supervisor either failing to request a stop of the loadout operation, failing to verify that the operation has stopped before opening the door, or prematurely restarting the operation while the worker is still in the Waste Package Loadout Room. In addition, it is possible that the WPTT operator could fail to stop the loadout operation as requested. However, these actions were considered much less likely than the primary unsafe actions cited above and, further, would only serve to drive down the overall scenario HEP value. Therefore, the analysts decided to conservatively constrain the analysis to the unsafe actions quantified above.

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 51A-OpDirExpose3-HFI-NOD

Designator	Description	Probability
A	Crew member requests reentry into the Waste Package Loadout Room	0.009
B	Supervisor agrees to allow access	0.0002

Source: Original

The Boolean expression for this scenario follows:

$$A \times B = 0.009 \times 0.0002 = 2E-06 \quad (\text{Eq. E-28})$$

E6.6.3.4.2.3 HFE Group #6 Scenario 1(c) for 51A-OpDirExpose3-HFI-NOD

1. Personnel access shield door is left open.
2. Interlock or load sensor fails and a WPTT enters the Waste Package Loadout Room.

Personnel Access Door Left Open—Before the WPTT is moved from the Waste Package Positioning Room to the Waste Package Loadout Room, a designated radiation protection worker checks that the area is free from personnel and ensures that all the personnel access doors are closed and locked. (Note: If the personnel access doors are left unlocked, a person could potentially enter the room and incur direct exposure, but this is bounded by the current scenario.)

In this scenario, the unsafe action that occurs is that one of the shield doors is left open (i.e., the shield is not fully in place). This scenario also includes the radiation protection worker being successful in ensuring that all personnel have left the room. (The unsafe action of failing to ensure that the room is empty is addressed in Scenario 1(a).)

The failure to recognize that an access door is left open is believed to be best represented by NARA GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

In addition, the WPTT operator would have to fail to verify by camera that the door was left open and fail to check the tag in/tag out board to address accountability for the location of personnel. This error is presumed to have medium dependency. Based on Table 20-21 of THERP (Ref. E8.1.26), for a baseline HEP of <0.01 and medium dependence, the appropriate dependence value would be Item (3)(a) or 0.15.

$$\begin{aligned} \text{Personnel access shield door left open} &= \\ &0.0007 \times 0.15 = 0.0001 \end{aligned}$$

Interlock or Load Cell Fails and WPTT Enters the Waste Package Loadout Room—There is an interlock between the personnel access shield doors and the Waste Package Positioning Room shield door. If there is a loaded WPTT in the Waste Package Positioning Room (load sensor), in order for the Waste Package Positioning Room shield door to open (to allow the WPTT to move into the Waste Package Loadout Room), the personnel access doors must be closed and locked. A direct exposure would occur if the interlock were to fail since nothing would stop the WPTT operator from moving the WPTT into the Waste Package Loadout Room, and nothing would prevent radiation from escaping the room.

The mechanical failure probability for an interlock, from Attachment C, Table C4-1, is approximately 2.7E-5/demand.

$$\text{Interlock fails} = 2.7E-5$$

The mechanical failure probability for a load cell, represented by a pressure sensor from Attachment C, Table C4-1, is approximately 4.0E-03/demand.

$$\text{Load cell fails} = 4.0E-03$$

$$\text{Interlock or load cell fails} = 2.7E-05 + 4.0E-03 = 0.004$$

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 51A-OpDirExpose3-HFI-NOD

Designator	Description	Probability
A	Personnel access shield door is left open	0.0001
B	Interlock or load cell fails, and a WPTT enters the Waste Package Loadout Room	4E-03

NOTE: WPTT = waste package transfer trolley.

Source: Original

The Boolean expression for this scenario follows:

$$A \times B = 0.0001 \times 4E-03 = 4E-07 \quad (\text{Eq. E-29})$$

HEP for HFE 51A-OpDirExpose3-HFI-NOD—The Boolean expression for the overall HFE (all scenarios) follows:

$$51A-OPDIREXPOSE3-HFI-NOD = \text{HEP 1(a)} + \text{HEP 1(b)} + \text{HEP 1(c)} = \\ 3E-05 + 2E-06 + 4E-07 = 3E-05 \quad (\text{Eq. E-30})$$

E6.6.4 Results of Detailed HRA for HFE Group #6

The final HEPs for the HFE that required detailed analysis in HFE Group #6 is presented in Table E6.6-7 (with the original preliminary value shown in parentheses).

Table E6.6-7. Summary of HFE Detailed Analysis for HFE Group #6

HFE	Description	Final Probability
51A-OpDirExpose3-HFI-NOD	Operator causes direct exposure while loading TEV	3E-05 (1E-3)

NOTE: TEV = transport and emplacement vehicle.

Source: Original

E7 RESULTS: HUMAN RELIABILITY ANALYSIS DATABASE

Table E7-1 presents a summary of all of the human failures identified in this analysis, and 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
51A-Liddisplace1-HFI-NOD	Operator inadvertently displaces cask lid during preparation activities	12	3	N/A ^b	N/A	Omitted from Analysis
51A-OpCaskDrop01-HFI-NOD	Operator drops cask during cask preparation activities	N/A	3	N/A ^b	N/A	Omitted from Analysis
51A-OpCICTMGate1-HFI-NOD	Operator inappropriately closes slide or port gate during vertical canister movement and continues lifting	7	4	1.00E-03	5	Preliminary
51A-OpCollide001-HFI-NOD	Operator causes low-speed collision of auxiliary vehicle with RC, TT, or CTT	1, 2, 3, 4	2, 3	3.00E-03	5	Preliminary
51A-OpCranelntfr-HFI-NOD	Operator causes WP handling crane to interfere with TEV or WPTT	11	6	1.00E-04	10	Preliminary
51A-OpCTCollide2-HFI-NOD	Operator causes low-speed collision of CTT during transfer from preparation station to Unloading Room	5	3	1.00E-03	5	Preliminary
51A-OpCTMDrint01-HFI-COD	Operator lifts object or canister too high with CTM (two-block)	7	4	1.0	N/A	Preliminary
51A-OpCTMdrop001-HFI-COD	Operator drops object onto canister during CTM operations	7	4	4.00E-07	10	Detailed
51A-OpCTMdrop002-HFI-COD	Operator drops canister during CTM operations	7	4	2.00E-04	10	Detailed
51A-OpCTMImpact1-HFI-COD	Operator moves the CTM while canister or object is below or between levels	7	4	1.00E-03	5	Preliminary
51A-OpCTMImpact2-HFI-COD	Operator causes canister impact with lid during CTM operations (HLW)	7	4	N/A ^b	N/A	Omitted from Analysis
51A-OpCTMImpact5-HFI-COD	Operator causes canister Impact with SSC during CTM operations (all)	7	4	1.0	N/A	Preliminary
51A-OpCTTImpact1-HFI-NOD	Operator causes an impact between cask and SSC due to crane operations	1,2, 3, 4	2, 3	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
51A-OpDirExpose1-HFI-NOD	Operator causes direct exposure during CTM activities (all waste forms)	12	4	1.0	N/A	Preliminary
51A-OpDirExpose2-HFI-NOD	Operator causes direct exposure during CTM activities (transfer into a WP)	12	4	1.00E-04	10	Preliminary
51A-OpDirExpose3-HFI-NOD	Operator causes direct exposure during TEV loading	12	6	3.00E-05	10	Detailed
51A-OpFailRstInt-HFI-NOM	Operator fails to restore interlock after maintenance	12	4, 6	1.00E-02	3	Preliminary
51A-OpFailSG-HFI-NOD	Operator fails to close the CTM slide gate before lifting shield skirt (while the canister is inside the bell; direct exposure)	12	4	1.00E-3	5	Preliminary
51A-OpFLCollide1-HFI-NOD	Operator causes high-speed collision of auxiliary vehicle with RC, TT, or CTT	1, 2, 3, 4	2, 3	1.0	N/A	Preliminary
51A-OpImpact0000-HFI-NOD	Operator causes impact of cask during transfer from preparation station to Unloading room	5	3	N/A ^b	N/A	Omitted from Analysis
51A-OpNoDiscoAir-HFI-NOD	Operator fails to disconnect air supply from CTT in the Unloading Room	7	4	1.00E-03	5	Preliminary
51A-OpNoUnBolt00-HFI-NOD	Operator fails to fully unbolt the cask lid before moving CTT into the Unloading Room (HLW)	7	4	1.00E-03	5	Preliminary
51A-OpNoUnBoltDP-HFI-NOD	Operator fails to fully unbolt the cask lid before moving CTT into the Unloading Room (Naval Cask)	7	4	N/A ^b	N/A	Omitted from Analysis
51A-OpNVYShield1-HFI-COW	Operator inappropriately removes naval shield ring (direct exposure)	12	3	3.00E-04	5	Preliminary
51A-OpRCCollide1-HFI-NOD	Operator causes low-speed collision between RC and facility SSCs	1	1	3.00E-03	5	Preliminary
51A-OpRCIntCol01-HFI-NOD	Operator causes high-speed collision between RC and facility SSCs	1	1	1.0	N/A	Preliminary
51A-OpRCIntCol2-HFI-NOD	Operator causes MAP to collide into RC	1	1	1.0	N/A	Preliminary
51A-OpSDClose001-HFI-NOD	Operator closes shield door on waste form in conveyance	6	OA (1,3,6)	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
51A-OpShieldRing-HFI-NOD	Operator fails to install WP shield ring in WPTT (direct exposure)	12	6	1.00E-04	10	Preliminary
51A-OpSpurMove01-HFI-NOD	Operator causes spurious movement of CTT in the Preparation Area	1, 2, 3, 4	2, 3	1.00E-04	10	Preliminary
51A-OpTEVDrClosd-HFI-NOD	Operator begins WP extraction before TEV doors open	11	6	1.00E-03	5	Preliminary
51A-OpTiltDown01-HFI-NOD	Operator prematurely tilts down the WPTT	7, 8, 10	4, 5, 6	1.0	N/A	Preliminary
51A-OpTipover001-HFI-NOD	Operator causes cask to tip over during cask upending and removal	1, 2	2	1.00E-04	10	Preliminary
51A-OpTipover002-HFI-NOD	Operator causes cask to tip over during cask preparation activities	3, 4	3	1.00E-04	10	Preliminary
51A-OpTTCollide1-HFI-NOD	Operator causes low-speed collision between TT and facility SSCs	1	1	3.00E-03	5	Preliminary
51A-OpTTIntCol01-HFI-NOD	Operator causes high-speed collision between TT and facility SSCs	1	1	1.0	N/A	Preliminary
51A-OpTTIntCol2-HFI-NOD	Operator causes MAP to collide into TT	1	1	1.0	N/A	Preliminary
51A-OpTTRollover-HFI-NOD	Operator causes rollover of TT	1	1	N/A ^b	N/A	Omitted from Analysis
51A-OpWPCollide1-HFI-NOD	Operator causes low-speed collision of WPTT into SSC	8, 10	5, 6	3.00E-03	5	Preliminary
51A-OpWPInnerLid-HFI-NOD	Operator causes direct exposure during WP loading	12	5	1.00E-04	10	Preliminary
51A-OpWPTiltUp01-HFI-NOD	Operator prematurely tilts up the WPTT	11	6	1.0	N/A	Preliminary
51A-OpWPTTSpur01-HFI-NOD	Operator causes spurious movement of WPTT during canister loading	7	4	1.00E-03	5	Preliminary
Crane Drops	Operator drops cask or drops object onto cask during crane operations	1, 2, 3, 4, 9, 11	2, 3, 5, 6	N/A ^a	N/A	Historic Data
Improper WP Closure	Operator damages canister or fails to properly weld the WP	9	5	N/A ^b	N/A	Omitted from Analysis

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	HFE Group	Basic Event Mean Probability	Error Factor	Type of Analysis
Load too Heavy	Operator causes drop of cask by attempting to lift a load that is too heavy for the crane	N/A	OA	N/A ^b	N/A	Omitted from Analysis
Moderator Introduced into Moderator-Controlled Area	Operator introduces moderator into a moderator-controlled area of the IHF	N/A	OA	N/A ^b	N/A	Omitted from Analysis
RC Derailment	Operator causes the RC to derail	1	1	N/A ^a	N/A	Historic Data
Spurious Movement of CTT during CTM Activities	Operator causes spurious movement of the CTT during CTM activities	7	4	N/A ^b	N/A	Omitted from Analysis
TEV Collision	Operator causes TEV to collide with WP or WPTT	11	6	N/A ^b	N/A	Omitted from Analysis
WPTT Derailment	Operator causes WPTT to derail	8, 10	5, 6	N/A ^a	N/A	Historic Data
WPTT Uncontrolled Tilt-down	Operator causes an uncontrolled tilt down of the WPTT	10	6	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.

CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HFE = human failure event; HLW = high-level radioactive waste; IHF = Initial Handling Facility; MAP = mobile access platform; N/A = not applicable; OA = over arching (applies to multiple HFE groups, Section E6.0.2); RC = railcar; SSC = structure, system, or component; SSCs = structures, systems, and components; ST = site transporter; TEV = transport and emplacement vehicle; TT = truck trailer; WP = waste package; WPTT = waste package transfer trolley.

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. *Initial Handling Facility Event Sequence Development Analysis*. 51A-PSA-IH00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080207.0005.
- 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)*. 800-30R-SS00-00400-000. 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.: National Aeronautics and Space Administration. 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.

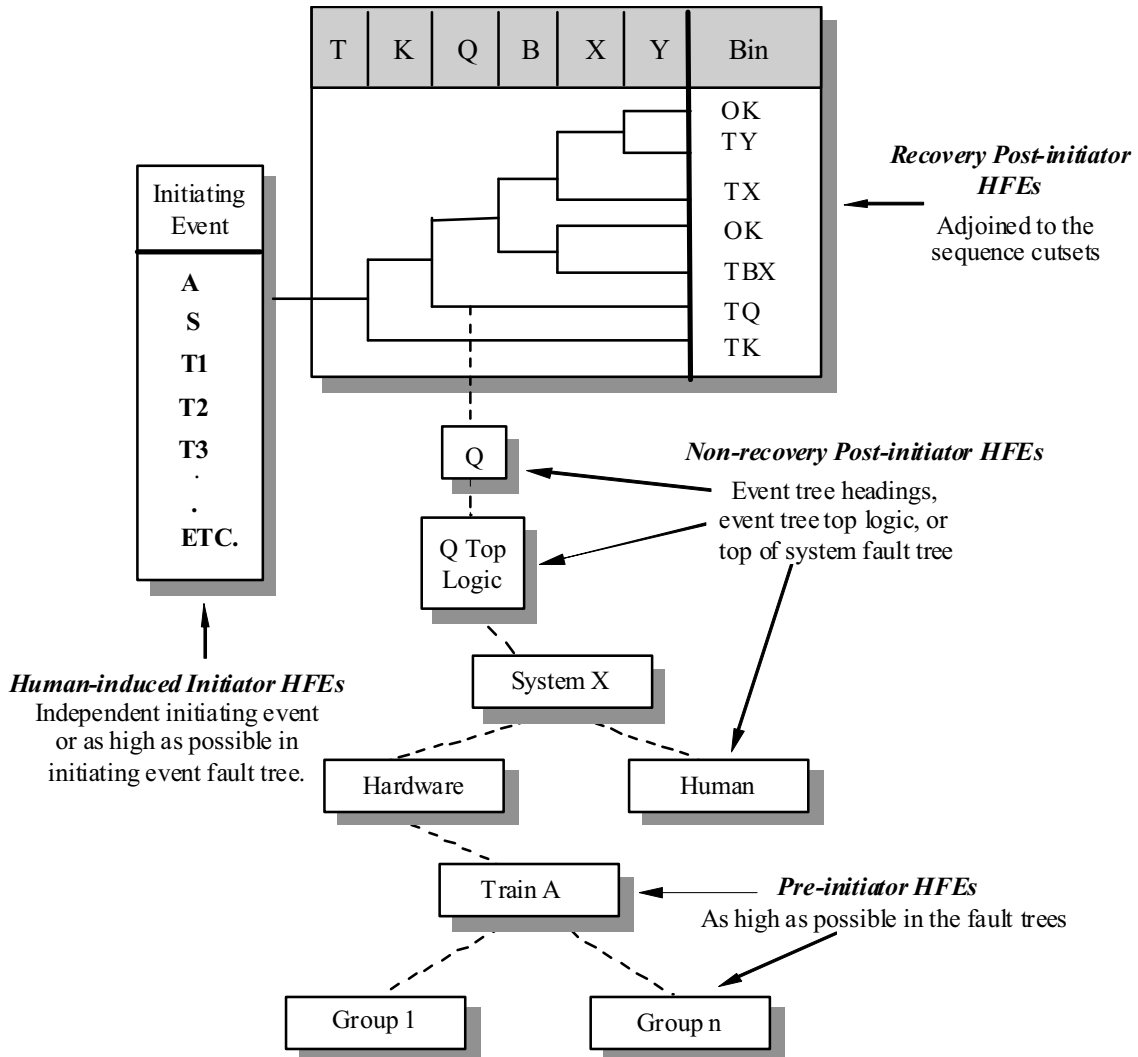
- E8.1.21 NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.
- E8.1.22 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique 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 Guttman, 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.

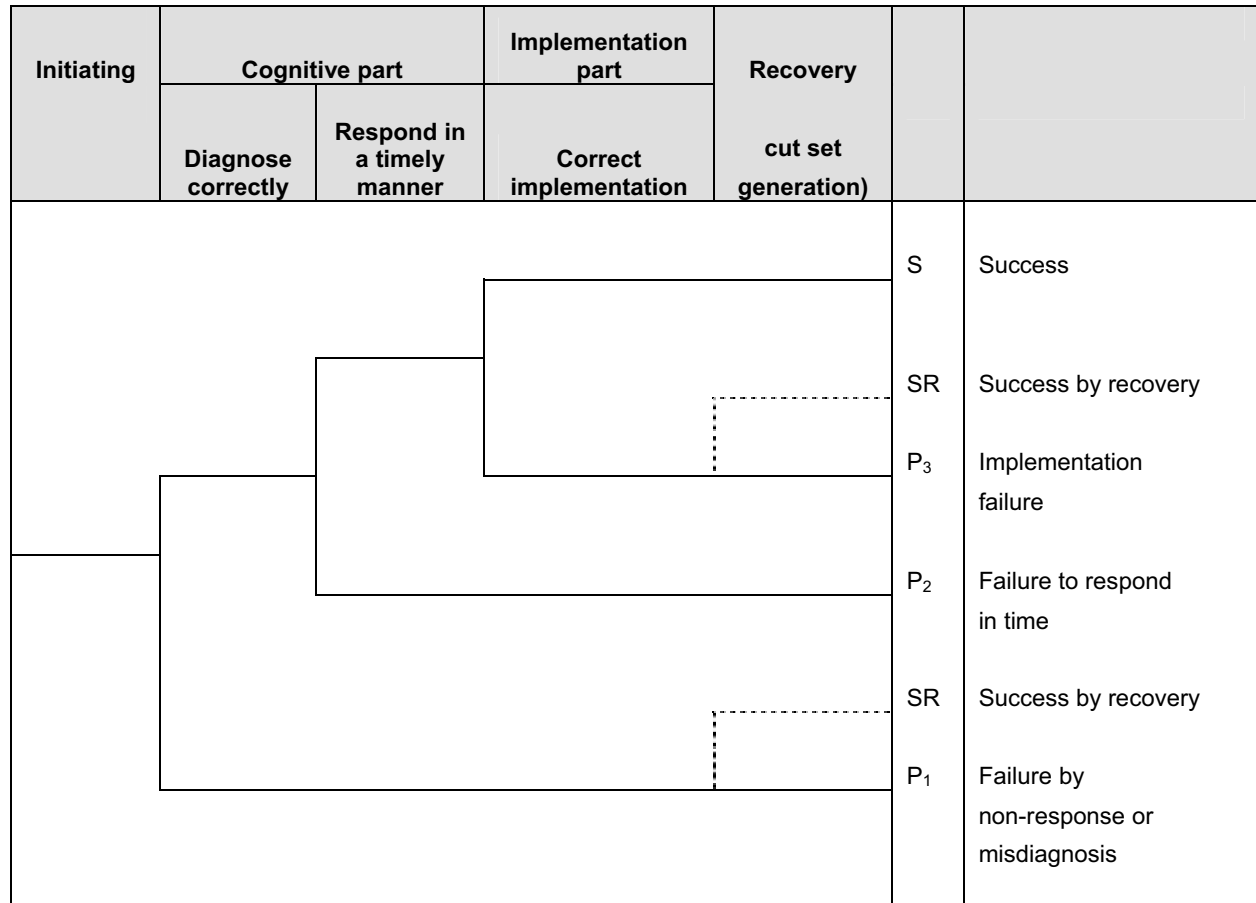


NOTE: HFE = human failure event.

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.

P₁ 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 P₂) or making an error in implementation (represented by P₃).

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 serve 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) ¹⁴	~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^{15,16}. Examples of such adjustments are also provided below; however

¹⁴ The default value is 0.1. This value is used if no preliminary assessment is performed.

¹⁵ 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.

¹⁶ 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.

these values are not taken to be firm in any sense of the word, but rather simply as examples of 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 key 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

Table E.IV-1. Comparison between NPP and YMP Operations (Continued)

NPP	YMP
	failures.
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, TEV 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 and 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.

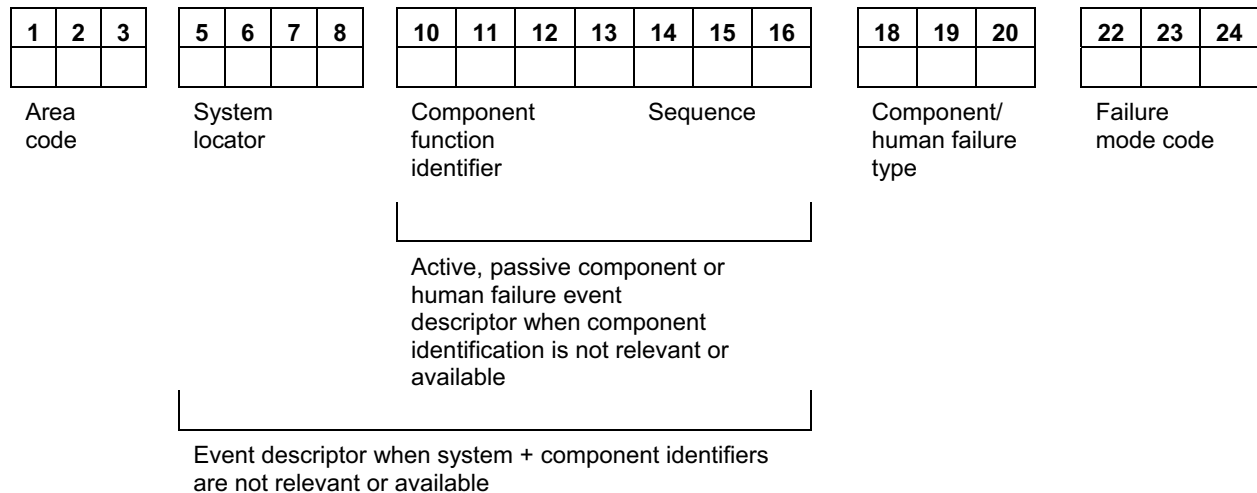
4. Simplified methods:

- 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 Wet Handling Facility is 050, the Receipt Facility is 200, the IHF 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 BSC 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

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes (Continued)

PRE-INITIATOR HFES; TYP=HFP		FMC=
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
ACRONYMS AND ABBREVIATIONS	F-7
F1 INTRODUCTION	F-8
F2 REFERENCES: DESIGN INPUTS.....	F-8
F3 BOUNDARY CONDITIONS	F-12
F3.1 INTRODUCTION	F-12
F3.2 PLANT OPERATIONAL STATE	F-12
F3.3 CREDIT FOR AUTOMATIC FIRE SUPPRESSION SYSTEMS	F-12
F3.4 NUMBER OF FIRE EVENTS TO OCCUR	F-12
F3.5 IGNITION SOURCE COUNTING.....	F-12
F3.6 FIRE CABLE AND CIRCUIT FAILURE ANALYSIS	F-12
F3.7 HEATING, VENTILATION, AND AIR CONDITIONING FIRE ANALYSIS.....	F-13
F3.8 NO OTHER SIMULTANEOUS INITIATING EVENTS	F-13
F3.9 DATA COLLECTION SCOPE.....	F-13
F3.10 COMPONENT FAILURE MODES.....	F-13
F3.11 COMPONENT FAILURE PROBABILITY	F-13
F3.12 INTERNAL EVENTS PRECLOSURE SAFETY ANALYSIS MODEL	F-13
F4 ANALYSIS METHOD.....	F-14
F4.1 INTRODUCTION	F-14
F4.2 IDENTIFICATION OF INITIATING EVENTS	F-14
F4.2.1 Identify Fire-Rated Barriers and Designate Fire Zones.....	F-14
F4.2.2 Identify the Rooms Where Waste Can Be Present	F-15
F4.2.3 Define Local Initiating Events.....	F-15
F4.2.4 Define Large Fire Initiating Events	F-15
F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY	F-16
F4.3.1 Determine the Overall Facility Fire Frequency	F-16
F4.3.2 Determine the Fire Ignition Frequency in Each Room.....	F-17
F4.4 DETERMINE INITIATING EVENT FREQUENCY.....	F-18
F4.4.1 Probability of Presence of a Target.....	F-19
F4.4.2 Probability of Propagation to a Target.....	F-19
F4.4.3 Initiating Event Frequency.....	F-22
F5 ANALYSIS.....	F-22
F5.1 INTRODUCTION	F-22
F5.2 INITIATING EVENT FREQUENCIES.....	F-23
F5.2.1 Room Area	F-23
F5.2.2 Building Ignition Frequency	F-25
F5.3 IGNITION SOURCE FREQUENCY	F-25
F5.4 IGNITION SOURCE DISTRIBUTION (EQUIPMENT LIST).....	F-27
F5.4.1 Electrical Equipment.....	F-34
F5.4.2 HVAC Equipment.....	F-35
F5.4.3 Mechanical Process Equipment	F-36

CONTENTS (Continued)

	Page
F5.4.4 Heat-Generating Process Equipment	F-37
F5.4.5 Torches, Welders, and Burners	F-37
F5.4.6 Internal Combustion Engines.....	F-38
F5.4.7 Office and Kitchen Equipment	F-38
F5.4.8 Portable and Special Equipment	F-39
F5.5 ROOM IGNITION FREQUENCY.....	F-39
F5.6 PROPAGATION PROBABILITIES.....	F-41
F5.7 INITIATING EVENT FREQUENCIES.....	F-43
F5.7.1 Residence Fractions	F-43
F5.7.2 Localized Fires.....	F-43
F5.7.3 Large Fires	F-58
F5.7.4 Contribution to Initiating Event Frequency	F-58
F5.8 MONTE CARLO SIMULATION/UNCERTAINTY DISTRIBUTIONS	F-58
F5.8.1 Uncertainty Distributions.....	F-58
F5.8.2 Monte Carlo Simulation.....	F-60
F5.9 RESULTS	F-60
APPENDIX F.I DEFINITION OF IGNITION SOURCE CATEGORY.....	F-64
APPENDIX F.II DERIVATION OF IGNITION SOURCE DISTRIBUTION AND FIRE PROPAGATION PROBABILITIES.....	F-65
APPENDIX F.III DERIVATION OF IGNITION FREQUENCY DISTRIBUTION.....	F-73
APPENDIX F.IV PROOF OF LOGNORMAL DISTRIBUTION.....	F-79
APPENDIX F.V DERIVATION OF ERROR FACTORS	F-81
APPENDIX F.VI RESULTS FROM MONTE CARLO SIMULATION	F-82

FIGURES

	Page
F5.7-1. Example of Crystal Ball Output for a Fire Initiating Event.....	F-61
F.III-1. Ignition Frequency Observations.....	F-73
F.III-2. Data Point Determination	F-74
F.III-3. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area).....	F-75
F.III-4. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area) Divided into Two Floor Area Ranges.....	F-76
F.III-5. Plot of the Ignition Frequency Data, the Predicted Ignition Frequency, and Confidence Limits for the Predicted Value	F-77

TABLES

	Page
F5.2-1. Room Areas and Total Ignition Frequency.....	F-24
F5.3-1. Ignition Frequency by Ignition Source	F-26
F5.4-1. Ignition Source Population by Room.....	F-28
F5.5-1. Fire Ignition Frequencies by Room	F-40
F5.6-1. Fire Propagation Probabilities.....	F-42
F5.7-1. NSNF Residence Fractions	F-44
F5.7-2. HLW Residence Fractions	F-47
F5.7-3. Localized Fire Initiating Event Frequencies	F-51
F5.7-4. Localized Fire Initiating Events with Multiple Rooms of Origin.....	F-56
F5.7-5. Large Fire Initiating Event Frequencies	F-59
F5.7-6. Fire Initiating Events Results Summary	F-62
F.I-1. Definition of Ignition Source Category	F-64
F.II-1. Fires in Radioactive Material Working Facilities by Originating Equipment.....	F-65
F.II-2. Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate.....	F-66
F.II-3. Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly	F-66
F.II-4. t-Distribution Value	F-67
F.II-5. Margin of Error Results at 95% Confidence Interval for Fires in Radioactive Material Working Facilities by Originating Equipment	F-68
F.II-6. Margin of Error Results at 99% Confidence Interval for Fires in Radioactive Material Working Facilities by Originating Equipment	F-68
F.II-7. Margin of Error Results at 95% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate	F-69
F.II-8. Margin of Error Results at 99% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate	F-70

TABLES (Continued)

	Page
F.II-9. Margin of Error Results at 95% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly.....	F-71
F.II-10. Margin of Error Results at 99% Confidence Interval for Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction in Which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly.....	F-72
F.III-1. Ignition Frequency Data from Figure FIII-1 and Equation FIII-1	F-75
F.III-2. Calculated Mean and Confidence Limits for the YMP Facility Ignition Frequency.....	F-78
F.IV-1. Comparison Between Crystal Ball and Excel Percentile Intervals.....	F-79
F.VI-1. Results of the Monte Carlo Simulation 97.5% Query	F-82

ACRONYMS AND ABBREVIATIONS

Acronyms

CTT	cask transfer trolley
HEPA	high-efficiency particulate air
HLW	high-level radioactive waste
HVAC	heating, ventilation, and air conditioning
IHF	Initial Handling Facility
MCC	motor control center
NFPA	National Fire Protection Association
NSNF	naval spent nuclear fuel
PCSA	preclosure safety analysis
WPTT	waste package transfer trolley
YMP	Yucca Mountain Project

F1 INTRODUCTION

This document describes the work scope, definitions and terms, method, and results for the fire analysis performed as part of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA). Fire analysis is divided into four major areas:

1. Initiating event identification
2. Initiating event quantification (including both ignition frequency and propagation probability)
3. Fragility analysis (including convolution of fragility and hazard curves)
4. 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 *IHF Fire Frequency - no suppression.xls* and *IHF 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 ANSI/ANS-58.23-2007. 2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.
- F2.2 ASME (American Society of Mechanical Engineers) 2002. 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.
- F2.3 BSC (Bechtel SAIC Company) 2007. *Equipment Motor Horsepower and Electrical Requirements Analysis*. 000-M0A-H000-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070816.0001.
- F2.4* BSC 2007. *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00001 Single Line Diagram*. 51A-E10-EEN0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0011.

- F2.5* BSC 2007. *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00002 Single Line Diagram.* 51A-E10-EEN0-00501-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0015.
- F2.6* BSC 2007. *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00003 Single Line Diagram.* 51A-E10-EEN0-00901-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0019.
- F2.7* BSC 2007. *Initial Handling Facility 480V MCC 51A-EEN0-MCC-00001 Single Line Diagram.* 51A-E10-EEN0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0012.
- F2.8* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00002 Single Line Diagram.* 51A-E10-EEN0-00301-000. REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0013.
- F2.9* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00003 Single Line Diagram.* 51A-E10-EEN0-00401-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0014.
- F2.10* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00004 Single Line Diagram.* 51A-E10-EEN0-00601-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0016.
- F2.11* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00005 Single Line Diagram.* 51A-E10-EEN0-00701-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0017.
- F2.12* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00006 Single Line Diagram.* 51A-E10-EEN0-00801-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0018.
- F2.13* BSC 2007. *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00007 Single Line Diagram.* 51A-E10-EEN0-01001-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0020.
- F2.14* BSC 2007. *Initial Handling Facility Cask Cavity Gas Sampling System Piping & Instrument Diagram.* 51A-M60-MRE0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070328.0010.
- F2.15* BSC 2007. *Initial Handling Facility Chilled Water System P&ID.* 51A-M60-PSC0-00101-000 REV A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071119.0017.
- F2.16* BSC 2007. *Initial Handling Facility Composite Vent Flow Diagram Non-Confinement HVAC Systems.* 51A-M50-VNI0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0003.

- F2.17* BSC 2007. *Initial Handling Facility Composite Vent Flow Diagram Tertiary Confinement HVAC Miscellaneous Areas.* 51A-M50-VCT0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0002.
- F2.18* BSC 2007. *Initial Handling Facility Composite Vent Flow Diagram Tertiary Confinement HVAC Supply & Exhaust Systems.* 51A-M50-VCT0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0001.
- F2.19* BSC 2007. *Initial Handling Facility Confinement Areas HEPA Exhaust System Ventilation & Instrumentation Diagram.* 51A-M80-VCT0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0005.
- F2.20* BSC 2007. *Initial Handling Facility Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram.* 51A-M80-VCT0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0004.
- F2.21* BSC 2007. *Initial Handling Facility Confinement Battery Room HEPA Exhaust System Ventilation & Instrumentation Diagram.* 51A-M80-VCT0-00202-000 REV 00B. Las Vegas, Nevada, Bechtel SAIC Company. ACC: ENG.20080102.0009.
- F2.22* BSC 2007. *Initial Handling Facility Confinement Cask Prep Area and WP Loadout Rm HVAC System Ventilation & Instrumentation Diagram.* 51A-M80-VCT0-00203-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0010.
- F2.23* BSC 2007. *Initial Handling Facility Confinement Electrical and Battery Room HVAC System Ventilation & Instrumentation Diagram.* 51A-M80-VCT0-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0008.
- F2.24* BSC 2007. *Initial Handling Facility Electrical Room Equipment Layout.* 51A-E40-EEN0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070521.0003.
- F2.25 BSC 2007. *Initial Handling Facility General Arrangement Ground Floor Plan.* 51A-P10-IH00-00102-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0017.
- F2.26 BSC 2007. *Initial Handling Facility General Arrangement Plan at Elevation +73'-0".* 51A-P10-IH00-00104-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0019.
- F2.27 BSC 2007. *Initial Handling Facility General Arrangement Second Floor Plan.* 51A-P10-IH00-00103-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071226.0018.
- F2.28* BSC 2007. *Initial Handling Facility Hot Water System P&ID.* 51A-M60-PSH0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071119.0019.

- F2.29* BSC 2007. *Initial Handling Facility Non-Confinement Areas Air Distribution System (North) Ventilation & Instrumentation Diagram*. 51A-M80-VNI0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0012.
- F2.30* BSC 2007. *Initial Handling Facility Non-Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram*. 51A-M80-VNI0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0011.
- F2.31* BSC 2007. *Initial Handling Facility Non-Confinement Operations Area HVAC System Ventilation & Instrumentation Diagram*. 51A-M80-VNI0-00104-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080102.0014.
- F2.32* BSC 2007. *Initial Handling Facility UPS 51A-EEP0-UJX-00002 Single Line Diagram*. 51A-E10-EEP0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0022.
- F2.33* BSC 2007. *Initial Handling Facility UPS 51A-EEP0-UJX-00001 Single Line Diagram*. 51A-E10-EEP0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0021.
- F2.34* 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.
- F2.35* EPRI (Electric Power Research Institute) and NRC (U.S. 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.
- F2.36* 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.
- F2.37 NFPA (National Fire Protection Association) 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.
- F2.38 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.
- F2.39* 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.

F2.40* Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. PhD Dissertation. Espoo, Finland: VTT Technical Research Centre of Finland. TIC: 259928. ISBN: 951-38-6392-1.

F2.41* 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: 0-03-014011-0.

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

The initial state of the facility is normal, with each system operating within its limiting condition of operation.

F3.3 CREDIT FOR AUTOMATIC FIRE SUPPRESSION SYSTEMS

The automatic fire suppression systems, although designed to meet all requirements and standards for fire suppression systems in nuclear facilities, are considered not important to safety, and therefore no credit is taken for their operation.

F3.4 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 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 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.35)) and *Summary & Overview*, Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36).

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 upon a 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 (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 would cease operations of the Initial Handling Facility (IHF), which further reduces the conditional probability of the occurrence of a second initiating event, given that 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 would 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 PRECLOSURE SAFETY ANALYSIS MODEL

To implement the systems analysis guidance contained herein, the fire preclosure safety analysis (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 ASME PRA *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. F2.2).

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 IHF or other facilities in the geologic repository operations area. The general methodological basis of this analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.39), which applies to facilities that are similar to the geologic repository operations area in that they are handling and disposal facilities for highly hazardous materials. This approach is data based, in that it uses actual fire ignition and fire propagation experience to determine fire initiating event frequencies. That approach has been adapted to use data applicable to the YMP waste handling facilities. To the extent applicable to a nonreactor facility, NUREG/CR-6850, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volumes 1 and 2* (Ref. F2.36 and Ref. F2.35) are also considered in the development of this analysis method. The method complies with the applicable requirements of the *ANS Fire PRA Methodology* (Ref. F2.1) that are relevant to a nonreactor 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 the 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 fire is of concern, at the YMP fire 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 action would occur due to fire that would not be much more likely to occur by other means. Of much greater concern at the 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, focuses 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; 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 waste is located. The steps of this process are provided in the following sections.

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. It should be noted 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 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 are 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 diagram.

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 would 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, as recognized in the latest fire risk guidance from *Detailed Methodology Volume 2 of EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* ((Refs. F2.35) and *Summary & Overview* (Ref. F2.36) Volume 1, Section 11.5.4, for example). There, potential large fire initiating events are identified. The general approach follows.

Except during the short time that waste forms are being lifted by a canister transfer machine, in the YMP facilities, waste forms are located 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.

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, and 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 (e.g., 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:

- *Detailed Methodology*, Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.35)
- *Summary & Overview*, Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36)
- *Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Facilities: 1988 - 1997 Unallocated Annual Averages and Narratives* (Ref. F2.37)
- *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction, 1980-1998* (Ref. F2.38)
- *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.39)
- *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. F2.40).

F4.3.1 Determine the Overall Facility Fire Frequency

There is insufficient data available regarding the total frequency of fires in facilities comparable to the YMP. NUREG/CR-6850 (Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.35) and Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36)) provides an overall frequency for a typical nuclear power plant, but these plants are much larger and more complex than the YMP facilities. Therefore, it has been decided that a more generic fire ignition frequency approach be used that relates building size to total fire frequency for various broad categories of facilities (*Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. F2.40)). 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:

$$f_m(A) = c_1A^r + c_2A^s \quad (\text{Eq. F-1})$$

where f_m is the fire ignition frequency per square meter per year, A is the floor area (in square meters) and 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:

$$c_1 = 3 \times 10^{-4}; c_2 = 5 \times 10^{-6}; r = -0.61; \text{ and } s = -0.05 \quad (\text{Eq. F-2})$$

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:

$$f_{fire} = f_m(A) * A \quad (\text{Eq. F-3})$$

F4.3.2 Determine the Fire Ignition Frequency in Each Room

The approach to allocating the fire ignition frequency is based on the approach used in *Detailed Methodology*, Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.35), and *Summary & Overview*, Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36), and *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.39). 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

Detailed Methodology, Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Refs.F2.35) and *Summary & Overview*, Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36) have data for these fractions for nuclear power plants, and *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.39) has data for these frequencies for chemical process plants. Neither of these data sets is the best for the facilities at the YMP. Therefore, the National Fire Protection Association (NFPA) was requested to provide an analysis, *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction, 1980-1998* (Ref. F2.38) of the data in their proprietary database on the distribution of fires by equipment type in all nuclear facilities of noncombustible 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 follows:

$$f_{elec-all} = f_{fire} * 0.086 \quad (\text{Eq. F-4})$$

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 *Detailed Methodology*, Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.35) and *Summary & Overview*, Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.36), and *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.39), the frequency contribution for each equipment type is divided by the total number of pieces of equipment in the facility. For example, in 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 follows:

$$f_{elec-each} = f_{elec-all} / 50 \quad (\text{Eq. F-5})$$

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 step is accomplished 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 follows:

$$f_{elec-1} = f_{elec-each} * 6 \quad (\text{Eq. F-6})$$

Determining this frequency 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, as follows:

$$f_1 = f_{elec-1} + f_{nvac-1} + f_{\dots-1} \quad (\text{Eq. F-7})$$

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_{wzi}	=	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 handled at the YMP). For example, if each waste form that passes through the IHF spends 60 minutes in the Cask Preparation Area, the probability that it is present when a fire occurs is $60 \text{ min} / (50 \text{ yrs} \times 8,760 \text{ hrs/yr} \times 60 \text{ min/hr})$. This probability 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 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 defines 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 follow:

- 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.¹
- 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:

$$f_{ier-i} = P_{wri} [f_i (FR_a + (FR_n \times (P_{pc} + P_{rc})) + (FR_f \times P_{rc}))] \quad (\text{Eq.F-8})$$

where

f_i	=	frequency of ignition, <i>i</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

¹In 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.

The values for P in the previous equation were developed from the analysis performed by NFPA (*Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction, 1980-1998* (Ref. F2.38)). 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:

- *Initial Handling Facility Electrical Room Equipment Layout* (Ref. F2.24)
- *Initial Handling Facility General Arrangement Ground Floor Plan* (Ref. F2.25).

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 is referred to as “ex-room propagation.”

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 follow:

- 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 an 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 follows:

$$f_{ief-fj-ri} = f_i \times P_{fc} \quad (\text{Eq. F-9})$$

where

- $f_{ief-fj-ri}$ = 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 follows:

$$f_{ief+-ri} = f_i \times (P_{fc} + P_{bc} + P_{b+c}) \quad (\text{Eq. F-10})$$

where

$f_{ief+r-i}$	=	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 ² .

The total fire frequency of the defined severity is the sum across all rooms relevant to the initiating event, as discussed previously.

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) time 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 IHF. This section details the analysis performed to determine these frequencies, using the methodology documented in Section F4. The following discussion of the analysis presupposes that the reader has developed a thorough understanding of the details of that methodology, as those details are not repeated in this section. 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

²Note 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.

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 IHF 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 IHF general layout drawings:

- *Initial Handling Facility General Arrangement Ground Floor Plan* (Ref. F2.25)
- *Initial Handling Facility General Arrangement Second Floor Plan* (Ref. F2.27)
- *Initial Handling Facility General Arrangement Plan at Elevation +73'-0"* (Ref. F2.26).

In some cases, the dimension intervals shown on the general arrangement drawings matched the boundaries of the rooms. Where this condition 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 were used 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 1015/31/30/2009/15, 1016/2016, 1017/2017, 1018/2018 and 1022/24/2024 occupy two floors of building space. The area obtained for these rooms was doubled to account for this fact. Rooms 1014, 2001/2010, and 2007 are not of a standard rectangular shape whose area can be calculated by multiplying a single length and width. Thus, these rooms were divided into two or three rectangles, each with a determined length and width. Addition of the area of these rectangles provides the total room area. All areas calculated in square feet were multiplied by 0.093 to obtain the area in square meters, since Equation F-1 is based in square meters.

Table F5.2-1. Room Areas and Total Ignition Frequency

Room	L1(ft)	L2(ft)	A(sq ft)	A(m ²)	L3 (ft)	L4(ft)		
1001	37	46	1702	158				
1002	127	46	5402	502	10	44		
1003	10	44	440	41				
1200 - 1225	83	90	7470	694				
1005	136	37	5032	467				
1006	39	37	1443	134				
1007	50	37	1850	172				
1008	25	37	925	86				
1009	50	37	1850	172				
1012/1011	164	88	14000	1301	24	18		
1013	6	12	72	7				
1014	4	22	192	18	8	13		
1015/31/30/2009/15	17	22	748	69	area doubled for two floors			
1016/2016	8	22	352	33	area doubled for two floors			
1017/2017	33	10	660	61	area doubled for two floors			
1018/2018	25	12	600	56	area doubled for two floors			
1019	8	22	176	16				
1020	9	10	90	8				
1021	9	12	108	10				
1022/24/2024	15	11	330	31	area doubled for two floors			
1023	62	32	1984	184				
1026	24	18	432	40				
1027	34	35	1190	111				
2001/2010	64	32	2348	218	25	12		
2002	17	37	629	58				
2003	44	75	3300	307				
2004	32	50	1600	149				
2005	42	78	3276	304				
2006	32	74	2368	220				
2007	7	25	247	23	6	12		
2008	6	12	72	7				
Total Area (m ²)				5657		50% Value		97.5% Value
Ignition Frequency (per m ² /yr)				4.79E-06	4.79E-06	4.79E-06		1.14E-05
Ignition Frequency (per yr)				2.71E-02				
Ignition Frequency (50 years - preclosure period)				1.35E+00				

NOTE: Red numbers are calculated values; green shaded cells are parameters that are assigned distributions for Crystal Ball input.

ft = foot; m² = square meter; sq ft = square foot; yr = year.

Source: Original

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 calculation 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-3. 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 somewhat in excess of one.

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 in the table. Appendix F.III contains 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 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
- 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-4 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 number is 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-5 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.

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	1.16E-01	137	8.46E-04	0.086	0.086	1.26E-01	4.05E-02
HVAC	0.080	1.09E-01	23	4.72E-03	0.080	0.080	1.20E-01	3.93E-02
Mechanical equipment	0.139	1.88E-01	64	2.94E-03	0.139	0.139	1.89E-01	5.01E-02
Heat-generating equipment	0.155	2.10E-01	0	0.00E+00	0.155	0.155	2.07E-01	5.24E-02
Torches, welders, burners	0.219	2.97E-01	542	5.47E-04	0.219	0.219	2.79E-01	5.99E-02
Internal combustion engines	0.021	2.84E-02	100	2.84E-04	0.021	0.021	4.23E-02	2.09E-02
Office/kitchen equipment	0.064	8.67E-02	10	8.67E-03	0.064	0.064	9.97E-02	3.55E-02
Portable equipment	0.102	1.38E-01	20	6.91E-03	0.102	0.102	1.45E-01	4.37E-02
No equipment involved	0.134	1.81E-01	5657	3.21E-05	0.134	0.134	1.83E-01	4.93E-02
	1.000				1.000			

NOTE: Red numbers are calculated values; green shaded cells are parameters that are assigned distributions for Crystal Ball inp ut.

HVAC = heating, ventilation, and air conditioning.

Source: Original

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 “97.5th 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 sources of ignition.

F5.4 IGNITION SOURCE DISTRIBUTION (EQUIPMENT LIST)

Compiling an initiating event frequency for the IHF is dependent on identifying many characteristics of the building, including 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 eight 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 that 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 IHF. 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 do not count as ignition sources per the counting rules are shown as *[italicized in square brackets]*. The following sections describe how the equipment was identified, categorized, and counted for the building.

Table F5.4-1. Ignition Source Population by Room

Ignition Source Room Number	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
1001 (HVAC Room)		Tertiary confinement HEPA filter units - 3 (VCTO-FLT-00001, 2, 3) HP n/a Tertiary confinement exhaust fans - 3 (VCTO-EXH-00001, 2, 3) 50 HP						Estimated 5% of all such equipment - 1
1002 (Electrical Equipment Area)	480V Load Centers - 6 cabs (EEN0-LC-00001, 2) 480V MCCs - 65 cabs (EEN0-MCC-00001-6) 75 kVA 480-208/120 Dist Xfmr 20A, B, C, D - 4 (EEN0-XFMR-00003, 4, 5, 6) 208/120V Dist Prs - 4 (EEN0-PL-00003, 4, 5, 6) 480/277V Ling Prl - 4 (EULO-PL-00001, 2, 3, 4) Uninterruptible Power System 20A, B - 2 (EEO- LUX-00001, 2) 480/277V UPS Dist Prl 20A, B, C, D, E - 5 (EEO- PL-00003, 4, 5, 6, 7) 40 kVA Maintenance Bypass Xfmr 20A - 1 (EEO-XFMR-00001) 160 kVA Maintenance Bypass Xfmr 20B - 1 (EEO-XFMR-00002) 2 DC/MIS Cabinets 1 PLC Cabinet	Electrical MCC fan coil units - 2 (VCTO-FCU-00005, 6) 25 HP [Battery Room exhaust fans - 2 (VCTO-EXH-00004, 5) 3 HP] Battery Room HEPA filter units - 2 (VCTO-FLT-00004, 5)						Estimated 10% of all such equipment - 2
1003 (Battery Room)	123VDC battery 20A - 1 (EEO-BTRY-00001) 250VDC battery 20B - 1 (EEO-BTRY-00002)							
1200-1225 (Support Area)		Support area toilet exhaust fans - 2 (VNI0-EXH-00001, 2) 5 HP					Estimated 90% of all such equipment - 9	

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source Room Number	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
1005 (WP Loadout Room)	WP handling crane panel – 1	WP Loadout Room fan coil units – 2 (VCTO-FCU-00007, 8) 15 HP	WP handling crane – 4 motors, including 2 on WP pallet yoke (HMP-C-CRN-00001, BEAM-00001) 100 kVA total; 60HP, 45HP, 7.5HP, 20HP; [2@1HP] WP Loadout Room shield door – 2 motors (IH00-DR-00004) 2@5HP 76% WP transfer trolley – 4 motors x RWF 3.04 (HL00-TRLY-00001) 150kVA total; 2@75HP, 2@30HP WP loadout platforms – 2 motors (HL00-PLAT-00001, 2) 2@5HP WP transfer carriage docking station – 1 motor (HL00-75-00001) 30 HP		Portable welding receptacle – WWWF=5 point (EEN0-RCP-00003)			Estimated 10% of all such equipment – 2
1006 (WP Positioning Room)			WP Positioning Room shield doors 1 & 2 – 4 motors (IH00-DR-00002, 3) 4@7.5HP 22% WP transfer trolley – 4 motors x RWF 0.88 (HL00-TRLY-00001) 150kVA total; 2@75HP, 2@30HP				Estimated 5% of all such equipment – 1	
1007 (WP Loading Room)			2% WP transfer trolley – 4 motors x RWF 0.08 (HL00-TRLY-00001) 150kVA total; 2@75HP, 2@30HP				Estimated 5% of all such equipment – 1	
1008 (Cask Unloading Room)			Cask Unloading Room shield door – 1 motors (IH00-DR-00001) 20 HP 3% Cask transfer trolley – 1 power drive x RWF 0.03 (HM00-TRLY-00001) 5 HP				Estimated 5% of all such equipment – 1	
1009 (CTM Maintenance Area)					Portable welding receptacle – WWWF=5 point (EEN0-RCP-00002)		Estimated 10% of all such equipment – 2	

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source Room Number	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
1012 (Cask Preparation Area) incl. 1011 (Cask Sampling Equipment Area)	Cask handling crane pml - 1	Tertiary confinement fan coil units - 4 (VCTO-FCU-00001, 2, 3, 4) 25 HP	Mobile access platform - 7 motors (HMCO-PLAT-00001) 40 KVA total; 1@15 HP, 2@10 HP, 4@5 HP [2@0.5 HP] 97% cask transfer trolley - 1 power drive x RWF 0.97 (HM00-TRLY-00001) 5 HP Cask handling crane - 3 motors including 2 cask yoke motors (HM00-CRN-00001, BEAM-00001) 180 KVA total; 120HP, 12.5HP, 40HP, [2@1HP] Cask preparation crane - 3 motors (HM00-CRN-00002) 90KVA total; 60HP, 25HP, 10HP, [4HP] Cask preparation platform - 7 motors (HMHO-PLAT-00001) 4@5HP Cask receipt area overhead rollup doors 1 & 2 - 2 motors, 5KVA MP cask cooling - 1 motor, 5 HP [Cask cavity gas sampling vacuum pump - 1 motor, 1 HP] [WP inerting vacuum pump - 1 motor, 2 HP] [Cask cavity gas sampling cooling unit, 1 motor, <5hp]		3 portable welding receptacles - WWF=15 points (EEN0-RCP-00004, 5, 6)	Site prime mover 100 points		Estimated 20% of all such equipment - 4
1013 (Corridor)								
1014 (Corridor)								
1015/1031/10302009/2015 (Stair/Elevator)			Passenger elevator 1 - 1 motor, 50 KVA					
1016/2016 (Stair)								
1017/2017 (Stair)								
1018/2018 (Stair)								
1019 (Fire Water Valve Riser Room)								
1020 (Fire Water Valve Riser Room)								

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source Room Number	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
1021 (Fire Water Valve Riser Room)								
1022/1024/2024 (Elevator)			Passenger elevator 2 – 1 motor, 50 KVA					
1023 (Utility Room)	480V Load Center – 5 cabs (EEN0-LC-00003) 480V MCC – 10 cabs (EEN0-MCC-00007)		HVAC chilled water pumps – 2 motors (PSCO-P-00001-A, B) 2@50 HP Hot water pumps – 2 motors (PSHO-P-00001-A, B) 2@15 HP		Primary welding station – 400 points			
1026 (Dry LLW Storage Room)								
1027 (LLW Sump Room)		Liquid LLW sampling pump – 1 motor (MLW0-P-00001) 0.5HP [Liquid LLW sump pump – 1 motor (MLW0-P-00002) 2HP]						
2001/2010 (Operations Room)	Control consoles – 6	Operations Room fan coil units – 2 (VN10-FCU-00001, 2) 15 HP					Estimated 10% of all such equipment – 1	Estimated 5% of all such equipment – 1
2002 (WP Closure Equipment Room)	Control system and electrical cabinets – 13							Estimated 5% of all such equipment – 1
2003 (HVAC Equipment Area)		Tertiary confinement air handling units – 3 (VCTO-AHU-00001, 2, 3) 100 HP						Estimated 5% of all such equipment – 1

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source Room Number	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
2004 (Waste Package Closure Room)			Waste Package Closure Room crane - 2 motors (HW00-CRN-00001) 52.5kVA total; 35HP, 7.5HP, [2HP] [Burnishing tool (HWS0-TOOL-00001), low HP motors] Weld dressing end effectors - 2 (HWW0-TOOL-0003, 4) machining/sparking, [2 motors @4.5 HP] [Remote handling system (HWH0-HEQ-00003) - various small motors] [Waste package closure system robot arms - 2 (HWH0-HEQ-00001, 2) - various small motors] Waste package closure system vacuum pump - 1 motor, 1@10HP [Waste package closure system chiller - 3 motors, 3@1HP] Waste package closure system hydraulic pump - 1		Weld end effectors - WWF=117 points (HWW0-TOOL-00001, 2)			Estimated 10% of all such equipment - 2
2005 (Canister Transfer Area)	CTM panel - 1		CTM maintenance crane - 2 motors (HTCO-CRN-0001) 62.5 kVA total, 35HP, 7.5HP, 2HP [Cask and WP port slide gates - 4 motors (HTCO-HTCH-00001, 2) 1 kVA, 4@0.5HP] Canister transfer machine - 5 motors (HTCO-FHM-00001) 133 kVA total, 2@7.5HP, 45HP, 60HP, 5HP, [3HP]					Estimated 5% of all such equipment - 1
2006 (Waste Package Closure Support Room)								Estimated 5% of all such equipment - 1

Table F5.4-1. Ignition Source Population by Room (Continued)

Ignition Source Room Number	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
2007 (Corridor)								
2008 (Corridor)								

NOTE: Red numbers indicate the actual count used. Equipment displayed in italicized text do not count as ignition sources per the counting rules. RWF is room weighting factor for equipment that can be in multiple rooms. The factor represents the percentage of exposure (i.e., waste residence) time that the piece of equipment spends in the particular room. For the office and kitchen equipment and for the portable/process equipment, these percentages 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. WWF is the welding weighting factor, which 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 hr/wk in the primary maintenance welding location and 5 hr/yr in each satellite welding location (for repairs that must be performed locally). Waste package closure room welding is estimated based on 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 13 hours per waste package; (3) the IHF will process 450 waste packages. Also, 450 x 13/50 is 117 hours per year (a score of 117). Power ratings are for each motor unless otherwise noted. Pieces of equipment that are in the room in question but do not count as ignition sources per the counting rules are shown as *italicized in square brackets*. CTM = canister transfer machine; HEPA = high-efficiency particulate air; HP = horsepower; HVAC = heating, ventilation, and air conditioning; IHF = Initial Handling Facility; kVA = kilovolts-ampere; LW = low-level radioactive waste; MCC = motor control center; MP = mechanical process; n/a = not applicable; pnl = panel; RWF = room weighting factor; V = volt; VDC = volt direct current; WP = waste package; WWF = welding weighting factor; Xlrmr = transformer.

Source: Original

F5.4.1 Electrical Equipment

Information regarding electrical equipment was gathered solely from the following single line diagrams and electrical room layout drawings:

- *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00001 Single Line Diagram* (Ref. F2.4)
- *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00002 Single Line Diagram.* (Ref. F2.5)
- *Initial Handling Facility 480 V Load Center 51A-EEN0-LC-00003 Single Line Diagram.* (Ref F2.6)
- *Initial Handling Facility 480V MCC 51A-EEN0-MCC-00001 Single Line Diagram.* (Ref. F2.7)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00002 Single Line Diagram.* (Ref. F2.8)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00003 Single Line Diagram.* (Ref. F2.9)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00004 Single Line Diagram.* (Ref. F2.10)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00005 Single Line Diagram.* (Ref. F2.11)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00006 Single Line Diagram.* (Ref. F2.12)
- *Initial Handling Facility 480 V MCC 51A-EEN0-MCC-00007 Single Line Diagram.* (Ref. F2.13)
- *Initial Handling Facility UPS 51A-EEP0-UJX-00001 Single Line Diagram.* (Ref. F2.33)
- *Initial Handling Facility UPS 51A-EEP0-UJX-00002 Single Line Diagram* (Ref. F2.32)
- *Initial Handling Facility General Arrangement Ground Floor Plan* (Ref. F2.25)

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 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:

- *Initial Handling Facility Composite Vent Flow Diagram Tertiary Confinement HVAC Supply & Exhaust Systems* (Ref. F2.18)
- *Initial Handling Facility Composite Vent Flow Diagram Tertiary Confinement HVAC Miscellaneous Areas* (Ref. F2.17)
- *Initial Handling Facility Composite Vent Flow Diagram Non-Confinement HVAC Systems* (Ref. F2.16)
- *Initial Handling Facility Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram* (Ref. F2.20)
- *Initial Handling Facility Confinement Areas HEPA Exhaust System Ventilation & Instrumentation Diagram* (Ref. F2.19)
- *Initial Handling Facility Confinement Electrical and Battery Room HVAC System Ventilation & Instrumentation Diagram* (Ref. F2.23)
- *Initial Handling Facility Confinement Battery Room HEPA Exhaust System Ventilation & Instrumentation Diagram* (Ref. F2.21)
- *Initial Handling Facility Confinement Cask Prep Area and WP Loadout Rm HVAC System Ventilation & Instrumentation Diagram* (Ref. F2.22)
- *Initial Handling Facility Non-Confinement Areas HVAC Supply System Ventilation & Instrumentation Diagram* (Ref. F2.30)
- *Initial Handling Facility Non-Confinement Areas Air Distribution System (North) Ventilation & Instrumentation Diagram* (Ref. F2.29)
- *Initial Handling Facility Non-Confinement Operations Area HVAC System Ventilation & Instrumentation Diagram* (Ref. F2.31).

HVAC equipment consists of HEPA filters, exhaust fans, air handling units, fan coil units, and sump pumps. Because any motor with a horse power of five or more is considered to be an initiator. The number of motors and the horsepower of each motor are determined for all applicable HVAC equipment identified. A piece of equipment containing a motor 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 process and instrumentation drawings:

- *Initial Handling Facility General Arrangement Ground Floor Plan* (Ref. F2.25)
- *Initial Handling Facility General Arrangement Second Floor Plan* (Ref. F2.27)
- *Initial Handling Facility General Arrangement Plan At Elevation +73'-0"* (Ref. F2.26)
- *Equipment Motor Horsepower and Electrical Requirements Analysis* (Ref. F2.3)
- *Initial Handling Facility Cask Cavity Gas Sampling System Piping & Instrument Diagram* (Ref. F2.14)
- *Initial Handling Facility Chilled Water System P&ID* (Ref. F2.15)
- *Initial Handling Facility Hot Water System P&ID* (Ref. F2.28).

Mechanical process equipment includes most of the motorized equipment, including 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 five 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 that 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 *Preliminary Throughput Study for the Initial Handling Facility* (Ref. F2.34). The waste package transfer trolley (WPTT) and cask transport trolley (CTT) were identified as the only two pieces of mobile equipment that occupy more than one room.

The total time the CTT spends in the Cask Unloading Room (1008) is calculated from the following procedures (in parenthesis) identified in the process throughput:

- Move loaded transportation cask on CTT to Cask Unloading Room—52 minutes (1.2.13)
- Remove naval spent fuel canister from naval transportation cask—56 minutes (2.2)
- Place canister in waste package—151 minutes (2.3)
- Move empty transportation cask to Cask Preparation Area—47 minutes (1.4.1).

The total time the CTT spends in the Cask Preparation Area (1012) is calculated by subtracting the total amount of time the CTT is in either room from the total time of the procedure (11,679 minutes).

Movement of the WPTT in the IHF includes rooms 1005, 1006, and 1007. The total time the WPTT spends in the Waste Package Positioning Room (1006) is calculated from the following procedures (in parenthesis) identified in the process throughput:

- Move WPTT in vertical position through Waste Package Positioning Room into Waste Package Loading Room—40 minutes (4.1.13)
- Close waste package—2,510 minutes (3.1)
- Move loaded, sealed waste package to Waste Package Loadout Room—20 minutes (4.2.1).

The total time the WPTT spends in the Waste Package Loading Room (1007) is calculated from the following procedures (in parenthesis) identified in the process throughput:

- Move WPTT in vertical position through Waste Package Positioning Room into Waste Package Loading Room—40 minutes (4.1.13)
- Place canister in waste package—151 minutes (2.3)
- Receive loaded waste package in Waste Package Positioning Cell—20 minutes (3.1.1).

The total time the WPTT spends in the Waste Package Loadout Room (1005) is calculated by subtracting the total amount of time the WPTT is in either room 1006 or 1007 from the total time of the process (11,679 minutes).

The time a mobile equipment item spends in each room is used 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 count is represented on the equipment list as the residence weighting factor.

F5.4.4 Heat-Generating Process Equipment

This equipment includes such things as furnaces, dryers, and other such equipment, except for that equipment associated with the HVAC, which is counted separately as discussed previously. 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 5 hours of use per year, and so each is assigned a score of 5 points. 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 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 IHF also has the waste package closure system, which has weld-end effectors. The number of hours of operation per year for the weld-end effectors on the waste package closure system is estimated based on the throughput time-and-motion study and the number of waste packages expected to be handled, as follows:

- The preclosure period is 50 years.
- The welding machine actually operates for 13 hours per waste package.
- The IHF processes 450 waste packages; $450 \times 13/50$ is 117 hours per year (a score of 117).

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 is one transporter in the IHF that uses internal combustion engines, which provides the entire contribution of fire ignition from the internal combustion engines category. The site prime mover/tractor is assigned a total of 100 points. While the prime mover is mobile, it moves only within the combined open rooms 1012 and 1011. Because these rooms are open to each other and treated as a single room, it was not necessary to account for movement of the site prime mover; the 100 points are assigned to room 1012/1011.

Locations of the internal combustion engines were determined solely from the general layout drawings.

F5.4.7 Office and 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 one to four 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.

Table F5.5-1. Fire Ignition Frequencies by Room

Room	Ignition Source Category and Room-by-Room Population											Room Ignition Frequency		
	Electrical	HVAC	Mechanical Equipment	Heat-Generating Equipment	Torches, Welders, Burners	Internal Combustion Engines	Office/Kitchen Equipment	Portable Equipment	No Equipment Involved					
1001		6										1	158	4.03E-02
1002	95	4										2	502	1.29E-01
1003	2												41	3.00E-03
1200-1225		2									9		694	1.10E-01
1005	1	2	12.04		5							2	467	7.73E-02
1006			4.88									1	134	2.56E-02
1007			0.08									1	172	1.27E-02
1008			1.03									1	86	1.27E-02
1009					5							2	172	2.21E-02
1012/1011	1	4	23.97		15	100						4	1301	1.96E-01
1013	1												7	1.06E-03
1014													18	5.72E-04
1015/31/30/2009/15			1										69	5.17E-03
1016/2016													33	1.05E-03
1017/2017													61	1.97E-03
1018/2018													56	1.79E-03
1019			1										16	3.47E-03
1020			1										8	3.21E-03
1021			1										10	3.26E-03
1022/24/2024			1										31	3.93E-03
1023	15	2	4		400								184	2.49E-01
1026													40	1.29E-03
1027													111	3.55E-03
2001	6	2									1		218	3.02E-02
2002	13											1	58	1.98E-02
2003		3										1	307	3.09E-02
2004			6									2	149	1.00E-01
2005	1		7		117							1	304	3.81E-02
2006	1											1	220	1.48E-02
2007	1												23	1.58E-03
2008													7	2.15E-04
TOTAL	137	23	64	0	542	100	10	20						1.14E+00

NOTE: Red numbers are calculated values.
HVAC = heating, ventilation, and air conditioning.

Source: Original

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 “category population” column for all categories except “no equipment involved,” as explained in Section F5.3.

The “no equipment involved” column of Table F5.5-1 is equal to the area of the room, because each unit in this category is a single square meter.³ These values are taken from Table F5.2-1, in the “A” column (square meters).

The final column on Table F5.5-1, the “room ignition frequency” column, implements the generic forms of Equations F-6 and F-7. 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 “frequency per unit” column. Per Equation F-6, the number of units in each category (green text) is multiplied by the corresponding frequency per unit for that category. Per Equation F-7, 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. It should be noted 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, presupposes that the ignition sources in the building cover each of the ignition source categories used in the analysis. However, the IHF does not have any equipment that fits the definition of heat-generating process equipment (welders have their own category), so this contribution does not apply to IHF.

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.

³ As discussed in the methodology section, in the case where no equipment is involved the size of the room represents the relative contribution to the overall frequency.

Table F5.6-1. Fire Propagation Probabilities

Automatic Suppression Functional	Alternative definition	Conditional Probability	Sampled Value	Mean Fraction	97.5% Value	97.5th Percentile Add
Automatic Suppression Functional						
Extent of propagation	Alternative definition					
Confined to object of origin	No propagation	0.551	0.551	0.551	0.667	0.117
Confined to part of room of origin	Spreads through part of room of origin	0.317	0.317	0.317	0.426	0.109
Confined to room of origin	Spreads throughout room of origin	0.028	0.028	0.028	0.066	0.038
Confined to fire-rated area of origin	Spreads throughout fire-rated area of origin	0.005	0.005	0.005	0.020	0.016
Confined to floor of origin	Spreads throughout floor of origin	0.069	0.069	0.069	0.128	0.059
Confined to structure of origin	Spreads throughout building	0.028	0.028	0.028	0.055	0.028
Extended beyond structure of origin	Breaches building boundary	0.005	0.005	0.005	0.020	0.016
		1.000	1.000			
Automatic Suppression Fails						
Extent of propagation	Alternative definition					
Confined to object of origin	No propagation	0.621	0.621	0.621	0.725	0.104
Confined to part of room of origin	Spreads through part of room of origin	0.149	0.149	0.149	0.226	0.076
Confined to room of origin	Spreads throughout room of origin	0.004	0.004	0.004	0.017	0.013
Confined to fire-rated area of origin	Spreads throughout fire-rated area of origin	0.057	0.057	0.057	0.107	0.050
Confined to floor of origin	Spreads throughout floor of origin	0.004	0.004	0.004	0.017	0.013
Confined to structure of origin	Spreads throughout building	0.161	0.161	0.161	0.240	0.079
Extended beyond structure of origin	Breaches building boundary	0.004	0.004	0.004	0.017	0.013
		1.000	1.000			

NOTE: Red numbers are calculated values; green shaded cells are parameters that are assigned distributions for Crystal Ball input.

Source: Original

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 describe the culmination of these data, concluding 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 is vulnerable in a particular area of the building and in a particular configuration. The source for all of the times related to naval spent nuclear fuel (NSNF) and high-level radioactive waste (HLW) is the *Preliminary Throughput Study for the Initial Handling Facility* (Ref. F2.34). Table F5.7-1 shows the vulnerabilities for NSNF and the times that contribute to the overall time of vulnerability. The column labeled “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 surface preclosure operations. Similar to the NSNF residence fractions, the process throughputs have been used to determine residence fractions for HLW (Table F5.7-2).

F5.7.2 Localized Fires

Initiating event frequencies have been divided into two types of calculations: localized and large fires. Table F5.7-3 contains all of the calculations contributing to the localized fire initiating event frequencies.

F5.7.2.1 Room Groupings

The first column of Table F5.7-3 identifies the room(s) of origin. If the vulnerability is expected to occur in a single room that has 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, where the room where the vulnerability occurs has open doors or gates to other rooms, or where the room shares a qualified fire area with other rooms. Table F5.7-4 lists all of the vulnerabilities that have more than one room of origin, as well as 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 nonqualified 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.”

For rooms of origin, the “frequency per unit” column is populated by the results in Section F5.3. Frequency per unit 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 F5.5 (Room Ignition Frequency).

Table F5.7-1. NSNF Residence Fractions

IHF Residence Times and Fractions			
Section I - Localized Fires			
BFD Task	Steps (if needed)	Time (min)	Fraction
TC/NSNF on Railcar in Vestibule/Prep Area w/SPM (Diesel Present)			
1.1.4	Steps 1-4	46	
Total		46	1.8E-06
TC/NSNF on Railcar in Prep Area w/o SPM (No Diesel Present)			
1.1.4	Step 5	70	
1.3.1		136	
1.3.2		120	
1.3.3		30	
1.3.4		138	
1.3.5		17	
1.3.6		20	
Total		531	2.0E-05
TC/NSNF on CTT in Prep Area			
1.3.7		25	
1.3.8		78	
Not in BFD	Cavity gas sampling	45	
1.3.9		95	
1.3.10		32	
1.3.11		241	
1.3.12		65	
1.3.13	Steps 1-5	30	
Total		611	2.3E-05
TC/NSNF on CTT in Unloading Room			
1.3.13	Steps 5-9	32	
2.2.1		35	
2.2.2		2	
2.2.3		15	
Total		84	3.2E-06
NSNF in CTM in Transfer Room			
2.2.3	Step 2 (again)	10	
2.2.4		2	
2.3.1		6	
2.3.2		2	
2.3.3	Step 1	15	
Total		35	1.3E-06

Table F5.7-1. NSNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (min)	Fraction
NSNF in WP in Loading Room			
2.3.3	again	20	
2.3.14		7	
2.3.15		1	
2.3.16		15	
2.3.17		1	
2.3.18		18	
2.3.19		2	
2.3.20		18	
2.3.21		2	
2.3.5		30	
2.3.6		11	
2.3.7		2	
2.3.8		15	
2.3.9		2	
3.1.1	Step 1	20	
Total		164	6.2E-06
NSNF in WP in Positioning/Closure Room			
3.1		7005	
4.2.1	Steps 1-2	15	
Total		7020	2.7E-04
NSNF in WP in Loadout Room			
4.2.1	Steps 2-4	20	
Not in BFD	TEV into facility	32	
4.2.2		25	
4.2.3		60	
4.2.4	Steps 1-3	15	
Total		152	5.8E-06
NSNF/WP in TEV in Loadout Room			
4.2.4	Steps 3-7	27	
Total		27	1.0E-06
Section II - Large Fire			
TC/NSNF w/SPM Present (Diesel)			
1.1.4	Steps 1-4	46	
Total		46	1.8E-06

Table F5.7-1. NSNF Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (min)	Fraction
TC/NSNF w/o SPM Present (No Diesel)			
1.1.4	Step 5	70	
1.3.1		136	
1.3.2		120	
1.3.3		30	
1.3.4		138	
1.3.5		17	
1.3.6		20	
1.3.7		25	
1.3.8		78	
Not in BFD	Cavity gas sampling	45	
1.3.9		95	
1.3.10		32	
1.3.11		241	
1.3.12		65	
1.3.13		47	
2.2.1		35	
2.2.2		2	
Total		1196	4.6E-05
NSNF in CTM			
2.2.3		15	
2.2.4		2	
2.3.1		6	
2.3.2		2	
Total		25	9.5E-07
NSNF in WP			
2.3.3		20	
2.3.14		7	
2.3.15		1	
2.3.16		15	
2.3.17		1	
2.3.18		18	
2.3.19		2	
2.3.20		18	
2.3.21		2	
2.3.5		30	
2.3.6		11	
2.3.7		2	
2.3.8		15	
2.3.9		2	
3.1		7005	
4.2.1		20	
Not in BFD	TEV into facility	32	
4.2.2		25	
4.2.3		60	
4.2.4		42	
Total		7328	2.8E-04

NOTE: BFD = block flow diagram; CTT = cask transfer trolley; IHF = Initial Handling Facility; min = minute;
NSNF = naval spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transport and
emplacement vehicle; w/o = without; WP = waste package.

Source: Original

Table F5.7-2. HLW Residence Fractions

IHF Residence Times and Fractions		
Section I - Localized Fires		
BFD Task	Steps (if needed)	Fraction
TC/HLW on Railcar in Vestibule/Prep Area w/SPM (Diesel Present)		
1.1.4		31
Total		31
TC/HLW on Railcar in Prep Area w/o SPM (No Diesel Present)		
1.2.2		161
1.2.3		20
1.2.4		40
1.2.5		15
1.2.6	Steps 1-2	10
Total		246
TC/HLW on CTT in Prep Area		
1.2.6	Steps 2-5	20
1.2.7		35
Not in BFD	Cavity gas sampling	45
1.2.8		46
Not in BFD	Prep cask crane	15
1.2.9		55
1.2.10	Steps 1-6	35
Total		251

pia:
IMPORTANT: Analysis boundary condition, in conformance with the throughput analysis, is that all HLW arrives in truck casks (one HLW canister to a cask). All frequency values up through the CTM are **per canister**. All frequency values for the WP are **per waste package**. Since five canisters are placed in a waste package, the waste form count for fire effects on WP is one-fifth of the waste form count for canisters. This boundary condition is bounding since it maximizes the residence time of HLW in the facility (i.e., it takes much more time to process five truck casks than a single rail cask containing five canisters).

Table F5.7-2. HLW Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (m)	Fraction
TC/HLW on CTT in Unloading Room			
1.2.10	Steps 6-10	32	
2.1.1		35	
2.1.25		2	
2.1.3		17	
2.1.4		15	
Not in BFD		34	
2.1.5		7	
2.1.6		15	
Total		157	6.0E-06

pja:
The process of moving five canisters means that at least one canister will be in the WP from the time the first one enters until the last one enters. The rate limiting step once the first canister enters is the amount of time it takes to export the empty TC after the canister is removed by the CTM. This process takes 572 minutes per cask (BFD 1.4). Once the first canister enters the WP, 572 minutes later the next TC can enter the facility. The sum total of this critical path "delay" is four times this amount (while the second through fifth casks are processed).

pja:
Similarly, each of the subsequent casks needs to have its canister removed and played in the WP and the TC lid played back on the TC prior to sending the empty TC from the facility, which delays processing of the subsequent TC. Again, this applies only to the second through fifth canisters, except for BFD 2.3, which includes putting the TC lid back on. This delay applies to all 5 canisters because it also delays closure of the WP after the last canister is loaded.

HLW in CTM in Transfer Room			
2.1.6	Step 2 (again)	10	
2.1.7		2	
2.3.1		6	
2.3.2		2	
2.3.3	Step 1	10	
Total		30	1.1E-06

HLW in WP in Loading Room			
1.4	x4 (casks 2-5)	2288	
1.1.4	x4 (canisters 2-5)	124	
1.2	x4 (canisters 2-5)	1956	
2.1	x4 (canisters 2-5)	508	
2.3	x4 (canisters 1-5)	470	
3.1.1	Step 1	20	
Total		5366	2.0E-04

HLW in WP in Positioning/Closure Room			
3.1		7116	
4.2.1	Steps 1-2	15	
Total		7131	2.7E-04

Table F5.7-2. HLW Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (min)	Fraction
HLW in WP in Loadout Room			
4.2.1	Steps 2-4	20	
Not in BFD	TEV into facility	32	
4.2.2		25	
4.2.3		60	
4.2.4	Steps 1-3	15	
Total		152	5.8E-06
HLW/WP in TEV in Loadout Room			
4.2.4	Steps 3-7	27	
Total		27	1.0E-06
Section II - Large Fire			
TC/HLW w/SPM Present (Diesel)			
1.1.4		31	
Total		31	1.2E-06
TC/HLW w/o SPM Present (No Diesel)			
1.2.2		161	
1.2.3		20	
1.2.4		40	
1.2.5		15	
1.2.6		25	
1.2.7		35	
Not in BFD	Cavity gas sampling	45	
1.2.8		46	
Not in BFD	Prep cask crane	15	
1.2.9		55	
1.2.10		47	
2.1.1		35	
2.1.2		2	
2.1.3		17	
2.1.4		15	
Not in BFD		34	
2.1.5		7	
2.1.6		15	
Total		629	2.4E-05

Table F5.7-2. HLW Residence Fractions (Continued)

BFD Task	Steps (if needed)	Time (min)	Fraction
HLW in CTM in Transfer Room			
2.1.34		20	
2.1.35		2	
2.1.36		5	
2.1.37		2	
2.1.38	Step 1	10	
four more		156	
Total		195	7.4E-06
HLW in WP			
1.4	x4 (casks 2-5)	2288	
1.1.4	x4 (canisters 2-5)	124	
1.2	x4 (canisters 2-5)	1956	
2.1	x4 (canisters 2-5)	508	
2.3	x5 (canisters 1-5)	470	
3.1		7116	
4.2		159	
Total		12621	4.8E-04

NOTE: BFD = block flow diagram; CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high-level radioactive waste; IHF = Initial Handling Facility; m = minute; NSNF = naval spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Table F5.7-3. 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)	TC/HLW
1008	Entry represents a vulnerability due to the cask transfer trolley												
	Electrical	0	8.46E-04			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	HVAC	0	4.72E-03			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	Mechanical equipment	1.03	2.94E-03		1.03	0.061		0.211	3.2E-06	2.0E-09	6.0E-06	3.8E-09	3.8E-09
	Heat-generating equipment	0	0.00E+00			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	Torches, welders, burners	0	5.47E-04			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	Internal combustion engines	0	2.84E-04			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	Office/kitchen equipment	0	8.67E-03			0.061		0.211	3.2E-06	0.0E+00	6.0E-06	0.0E+00	0.0E+00
	Portable equipment	1	6.91E-03		1	0.061		0.211	3.2E-06	4.7E-09	6.0E-06	8.7E-09	8.7E-09
	No equipment involved	86	3.21E-05		30	0.061		0.211	3.2E-06	4.3E-09	6.0E-06	8.0E-09	8.0E-09
	Localized Fire Threatens Waste Form in Unloading Room												
	Localized Fire Threatens TC/NSNF in Unloading Room									1.1E-08		2.1E-08	
	Localized Fire Threatens TC/HLW in Unloading Room												
Entry represents a vulnerability due to the WP transfer trolley													
FA-00-05	Electrical	0	8.46E-04			0.061		0.211	2.7E-04	0.0E+00	2.7E-04	0.0E+00	0.0E+00
	HVAC	0	4.72E-03			0.061		0.211	2.7E-04	0.0E+00	2.7E-04	0.0E+00	0.0E+00
	Mechanical equipment	10.88	2.94E-03		10.88	0.061		0.211	2.7E-04	8.6E-06	2.7E-04	8.7E-06	8.7E-06
	Heat-generating equipment	0	0.00E+00			0.061		0.211	2.7E-04	0.0E+00	2.7E-04	0.0E+00	0.0E+00
	Torches, welders, burners	117	5.47E-04		117	0.061		0.211	2.7E-04	1.7E-05	2.7E-04	1.7E-05	1.7E-05
	Internal combustion engines	0	2.84E-04			0.061		0.211	2.7E-04	0.0E+00	2.7E-04	0.0E+00	0.0E+00
	Office/kitchen equipment	0	8.67E-03			0.061		0.211	2.7E-04	0.0E+00	2.7E-04	0.0E+00	0.0E+00
	Portable equipment	3	6.91E-03			0.061		0.211	2.7E-04	3.4E-07	2.7E-04	3.4E-07	3.4E-07
	No equipment involved	283	3.21E-05		134	0.061		0.211	2.7E-04	1.4E-06	2.7E-04	1.4E-06	1.4E-06
Propagation from rooms in FA-00-02													
1002			1.29E-01					0.057	2.7E-04	2.0E-06	2.7E-04	2.0E-06	2.0E-06
1003			3.00E-03					0.057	2.7E-04	4.6E-08	2.7E-04	4.7E-08	4.7E-08
1009			2.21E-02					0.057	2.7E-04	3.4E-07	2.7E-04	3.4E-07	3.4E-07
1012			1.96E-01					0.057	2.7E-04	3.0E-06	2.7E-04	3.1E-06	3.1E-06
1026			1.29E-03					0.057	2.7E-04	2.0E-08	2.7E-04	2.0E-08	2.0E-08
1027			3.55E-03					0.057	2.7E-04	5.4E-08	2.7E-04	5.5E-08	5.5E-08
2003			3.09E-02					0.057	2.7E-04	4.7E-07	2.7E-04	4.8E-07	4.8E-07
2005			3.81E-02					0.057	2.7E-04	5.9E-07	2.7E-04	5.9E-07	5.9E-07
2006			1.48E-02					0.057	2.7E-04	2.3E-07	2.7E-04	2.3E-07	2.3E-07
	Localized Fire Threatens Waste Form in Positioning Room												
	Localized Fire Threatens WP/NSNF in Positioning Room									3.4E-05		3.5E-05	
	Localized Fire Threatens WP/HLW in Positioning Room												

Table F5.7-3. Localized Fire Initiating Event Frequencies (Continued)

Room of Origin (includes comments field as needed)	Ignition Source (if Applicable)	Number in Room (diesel present)	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)
FA-00-02	Electrical	97	8.48E-04						TC/NSNF		TC/HLW	
	HVAC	11	4.72E-03	4		0.061	97	0.211	1.8E-06	8.8E-09	1.2E-06	5.9E-09
	Mechanical equipment	30.97	2.94E-03	10.97	3	0.061	7	0.211	1.8E-06	3.7E-08	1.2E-06	2.5E-08
	Heat-generating equipment	0	0.00E+00			0.061	17	0.211	1.8E-06	6.5E-08	1.2E-06	4.4E-08
	Torches, welders, burners	20	5.47E-04			0.061	20	0.211	1.8E-06	1.2E-09	1.2E-06	0.0E+00
	Internal combustion engines	100	2.84E-04	100		0.061	20	0.211	1.8E-06	5.0E-08	1.2E-06	7.9E-10
	Office/kitchen equipment	0	8.67E-03			0.061		0.211	1.8E-06	0.0E+00	1.2E-06	3.4E-08
	Portable equipment	10	6.91E-03		1	0.061	9	0.211	1.8E-06	9.2E-09	1.2E-06	6.2E-09
	No equipment involved	2585	3.21E-05	274	120	0.061	2191	0.211	1.8E-06	2.4E-08	1.2E-06	1.6E-08
Propagation from rooms in FA-00-02												
1003			3.00E-03			0.057		0.057	1.8E-06	3.0E-10	1.2E-06	2.0E-10
1026			1.29E-03			0.057		0.057	1.8E-06	1.3E-10	1.2E-06	8.7E-11
1027			3.55E-03			0.057		0.057	1.8E-06	3.6E-10	1.2E-06	2.4E-10
2006			1.48E-02			0.057		0.057	1.8E-06	1.5E-09	1.2E-06	1.0E-09
2004			1.00E-01			0.057		0.057	1.8E-06	1.0E-08	1.2E-06	6.8E-09
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/SPM (Diesel Present)												
Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/SPM (Diesel Present)										2.1E-07		1.4E-07
Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/SPM (Diesel Present)												
Entry represents a vulnerability due to the railcar (no diesel present)									TC/NSNF		TC/HLW	
FA-00-02	Electrical	97	8.48E-04						TC/NSNF		TC/HLW	
	HVAC	11	4.72E-03	4		0.061	97	0.211	2.0E-05	1.0E-07	9.4E-06	4.7E-08
	Mechanical equipment	30.97	2.94E-03	10.97	3	0.061	7	0.211	2.0E-05	4.2E-07	9.4E-06	2.0E-07
	Heat-generating equipment	0	0.00E+00			0.061	17	0.211	2.0E-05	7.5E-07	9.4E-06	3.5E-07
	Torches, welders, burners	20	5.47E-04			0.061	20	0.211	2.0E-05	0.0E+00	9.4E-06	0.0E+00
	Internal combustion engines	0	2.84E-04			0.061	20	0.211	2.0E-05	1.4E-08	9.4E-06	6.3E-09
	Office/kitchen equipment	0	8.67E-03			0.061		0.211	2.0E-05	0.0E+00	9.4E-06	0.0E+00
	Portable equipment	10	6.91E-03		1	0.061	9	0.211	2.0E-05	0.0E+00	9.4E-06	0.0E+00
	No equipment involved	2585	3.21E-05	274	120	0.061	2191	0.211	2.0E-05	1.1E-07	9.4E-06	4.9E-08
Propagation from rooms in FA-00-02												
1003			3.00E-03			0.057		0.057	2.0E-05	2.8E-07	9.4E-06	1.3E-07
1026			1.29E-03			0.057		0.057	2.0E-05	3.5E-09	9.4E-06	1.6E-09
1027			3.55E-03			0.057		0.057	2.0E-05	1.5E-09	9.4E-06	6.9E-10
2006			1.48E-02			0.057		0.057	2.0E-05	4.1E-09	9.4E-06	1.9E-09
2004			1.00E-01			0.057		0.057	2.0E-05	1.7E-08	9.4E-06	8.0E-09
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/SPM (No Diesel Present)												
Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/SPM (No Diesel Present)										1.8E-06		8.4E-07
Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/SPM (No Diesel Present)												

Table F5.7-3. 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)
Entry represents a vulnerability due to the canister transfer machine												
FA-00-02	Electrical	97	8.46E-04	1		0.061	96	0.211	1.3E-06	7.8E-09	1.1E-06	6.6E-09
	HVAC	11	4.72E-03			0.061	11	0.211	1.3E-06	4.2E-09	1.1E-06	3.6E-09
	Mechanical equipment	30.97	2.94E-03	7	0	0.061	23.97	0.211	1.3E-06	3.3E-08	1.1E-06	2.8E-08
	Heat-generating equipment	0	0.00E+00			0.061		0.211	1.3E-06	0.0E+00	1.1E-06	0.0E+00
	Torches, welders, burners	20	5.47E-04			0.061	20	0.211	1.3E-06	8.9E-10	1.1E-06	7.7E-10
	Internal combustion engines	100	2.84E-04			0.061	100	0.211	1.3E-06	2.3E-09	1.1E-06	2.0E-09
	Office/kitchen equipment	0	8.67E-03			0.061		0.211	1.3E-06	0.0E+00	1.1E-06	0.0E+00
	Portable equipment	10	6.91E-03			0.061	10	0.211	1.3E-06	5.6E-09	1.1E-06	4.8E-09
	No equipment involved	2585	3.21E-05	30	120	0.061	2435	0.211	1.3E-06	8.7E-09	1.1E-06	7.5E-09
Propagation from rooms in FA-00-02												
1003			3.00E-03					0.057	1.3E-06	2.3E-10	1.1E-06	2.0E-10
1026			1.29E-03					0.057	1.3E-06	9.9E-11	1.1E-06	8.4E-11
1027			3.55E-03					0.057	1.3E-06	2.7E-10	1.1E-06	2.3E-10
2006			1.48E-02					0.057	1.3E-06	1.1E-09	1.1E-06	9.7E-10
2004			1.00E-01					0.057	1.3E-06	7.7E-09	1.1E-06	6.6E-09
Localized Fire Threatens Waste Form in CTM in Transfer Room												
Localized Fire Threatens NSNF in CTM in Transfer Room										7.2E-08		6.2E-08
Localized Fire Threatens HLW in CTM in Transfer Room												

NOTE: Red numbers are calculated values; blue shaded cells are the resultant median initiating event frequencies.

CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high-level radioactive waste; IE = initiating event; NSNF = naval spent nuclear fuel; SPM = site prime mover;

TC = transportation cask; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

Table F5.7-4. Localized Fire Initiating Events with Multiple Rooms of Origin

Rooms	Vulnerability	Justification
1006 2004	WP transfer trolley	Room 1006 is open to 2004 during the welding procedures
1007 2005	WP transfer trolley	Room 1007 is open to 2005 for operation of the canister transfer machine
1002 1009 1012 2003 2005	Cask transfer trolley Railcar (diesel present) Railcar (no diesel present) Canister transfer machine	These rooms are open to each other at all times due to the open construction of the IHF

NOTE: IHF = Initial Handling Facility; WP = waste package.

Source: Original

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 are assigned a location at the target, near the target, or away from the target. These locations are shown in their respective columns in Table F5.7-3 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 approximately 3 m (at target), between approximately 3 m and 7 m (near target), or further than 7 m away from the 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 m² is considered at the target, and the next 120 m² is considered near the target). The remaining square meters are entered as away from target. For vulnerable waste forms in motion, the “at target” value is the total square meters 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. Remaining square meters are 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, Section F4.4.2.1). The frequency per (ignition source) unit is taken from the “frequency per unit” column of Table F5.3-1. 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 or Table F5.7-2, as appropriate. The “contribution to IE frequency” column implements Equation F-8 to provide the total initiating event frequency contribution from a fire that starts in the room where the waste form resides.

There is also a section of Table F5.7-3 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, Section F4.4.2.2). For these rooms, the “contribution to IE frequency” column implements the generic form of Equation F-9, 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 F5.7-5 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-10. The target exposure time (fraction) is once again taken from Table F5.7-1 and Table F5.7-2. 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, Section F5.7.1) contribute to the final calculation of the contribution to initiating event frequency (cells highlighted in blue in Table F5.7-3 and Table F5.7-5). 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 from 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 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.

Table F5.7-5. Large Fire Initiating Event Frequencies

Large Fire Threatens Waste Form	Large fires are those that spread beyond the boundaries of a fire area, up through those that breach the building boundary.	Propagation Probability beyond Fire-rated Area	Total Ignition Frequency	Target Exposure Time (Fraction)	Contribution to IE Frequency
Large Fire Threatens TC/NSNF w/SPM Present (Diesel)		0.169	1.14E+00	1.8E-06	3.4E-07
Large Fire Threatens TC/NSNF w/o SPM Present (No Diesel)		0.169	1.14E+00	4.6E-05	8.8E-06
Large Fire Threatens NSNF in CTM		0.169	1.14E+00	9.5E-07	1.8E-07
Large Fire Threatens NSNF in WP		0.169	1.14E+00	2.8E-04	5.4E-05
Large Fire Threatens TC/HLW w/SPM Present (Diesel)		0.169	1.14E+00	1.2E-06	2.3E-07
Large Fire Threatens TC/HLW w/o SPM Present (No Diesel)		0.169	1.14E+00	2.4E-05	4.6E-06
Large Fire Threatens HLW in CTM		0.169	1.14E+00	7.4E-06	1.4E-06
Large Fire Threatens HLW in WP		0.169	1.14E+00	4.8E-04	9.3E-05

NOTE: Blue shaded cells are the resultant median initiating event frequencies.

CTM = canister transfer machine; HLW = high-level radioactive waste; IE = initiating event; NSNF = naval spent nuclear fuel; SPM = site prime mover;
TC = transportation cask; w/ = with; w/o = without; WP = waste package.

Source: Original

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 for which the simulation produces results (IE 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. This task is set within the software to be done 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 would 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 HLW in the canister transfer machine in the Canister Transfer Area.

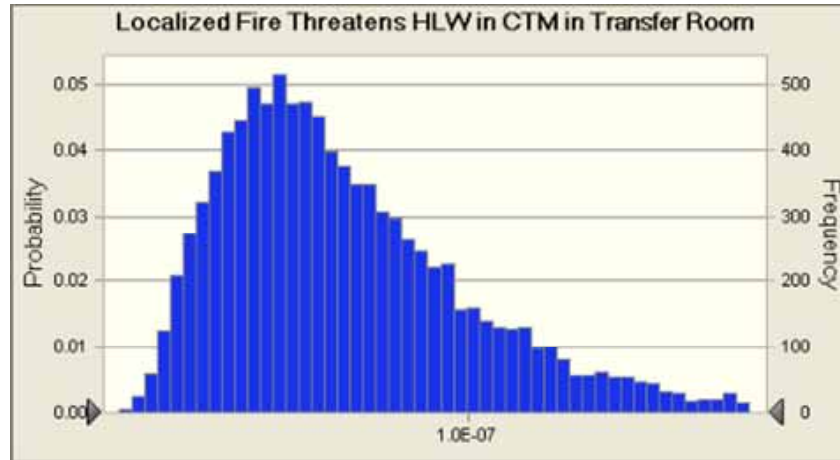
These results provide a statistical reference for the variance of each initiating event frequency. As seen in Section F5.7.2, Table F5.7-3, the baseline initiating event frequency for this case is 6.2×10^{-8} . The Crystal Ball results give insight into this frequency, showing that given the variability of the inputs, the true result could lie anywhere between 7.1×10^{-9} and 4.0×10^{-7} , with a mean of 6.9×10^{-8} , a standard deviation of 3.8×10^{-8} , and a lognormal shape. Crystal Ball was run for all of the initiating events, and a summary of the results, giving the distribution parameters of each distribution, is shown in Table F5.7-6. The 97.5th percentile values in Table F5.7-6 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 is the error factors, these figures 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 97.5th 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.

Forecast: Localized Fire Threatens HLW in CTM in Transfer Room

Cell: M174

Summary:

Entire range is from 7.1E-09 to 4.0E-07
Base case is 6.2E-08
After 10,000 trials, the std. error of the mean is 3.8E-10



Statistics:

	Forecast values
Trials	10,000
Mean	6.9E-08
Median	6.1E-08
Mode	8.3E-08
Standard Deviation	3.8E-08
Variance	1.4E-15
Skewness	1.71
Kurtosis	8.43
Coeff. of Variability	0.5447
Minimum	7.1E-09
Maximum	4.0E-07
Range Width	3.9E-07
Mean Std. Error	3.8E-10

Forecast: Localized Fire Threatens HLW in CTM in Transfer Room (cont'd)

Cell: M174

Percentiles:

	Forecast values
0%	7.1E-09
10%	3.1E-08
20%	3.9E-08
30%	4.7E-08
40%	5.4E-08
50%	6.1E-08
60%	7.0E-08
70%	8.0E-08
80%	9.4E-08
90%	1.2E-07
100%	4.0E-07

Figure F5.7-1. Example of Crystal Ball Output for a Fire Initiating Event

Table F5.7-6. Fire Initiating Events Results Summary

Initiating Event	Equipment	Mean	Median	97.5% Value	EF	Type
Localized Fire Threatens Waste Form in WPTT in WP Loadout Room	WP transfer trolley					
Localized fire threatens WP/NSNF in WPTT in WP Loadout Room		4.9E-07	4.5E-07	1.1E-06	2.1E+00	Lognormal
Localized fire threatens WP/HLW in WPTT in WP Loadout Room		4.9E-07	4.5E-07	1.1E-06	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in WP in TEV WP Loadout Room	Transportation emplacement vehicle					
Localized fire threatens WP/NSNF in TEV in WP Loadout Room		8.8E-08	7.9E-08	1.9E-07	2.1E+00	Lognormal
Localized fire threatens WP/HLW in TEV in WP Loadout Room		8.8E-08	7.9E-08	1.9E-07	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in Cask Unloading room	Cask transfer trolley					
Localized fire threatens TC/NSNF in Cask Unloading room		1.2E-08	1.1E-08	2.7E-08	2.2E+00	Lognormal
Localized fire threatens TC/HLW in Cask Unloading room		2.2E-08	2.0E-08	5.1E-08	2.2E+00	Lognormal
Localized Fire Threatens Waste Form in WP Positioning Room	WP transfer trolley					
Localized fire threatens WP/NSNF in WP Positioning Room		3.8E-05	3.4E-05	8.3E-05	2.1E+00	Lognormal
Localized fire threatens WP/HLW in WP Positioning Room		3.8E-05	3.4E-05	8.4E-05	2.1E+00	Lognormal
Localized Fire Threatens Waste Form in WP Loading Room	WP transfer trolley					
Localized fire threatens WP/NSNF in WP Loading Room		3.5E-07	3.1E-07	8.5E-07	2.3E+00	Lognormal
Localized fire threatens WP/HLW in WP Loading Room		1.2E-05	1.0E-05	2.8E-05	2.3E+00	Lognormal

Table F5.7-6. Fire Initiating Events Results Summary (Continued)

Initiating Event	Equipment	Mean	Median	97.5% Value	EF	Type
Localized Fire Threatens Waste Form in CTT in Cask Preparation Area	Cask transfer trolley					
Localized fire threatens TC/NSNF in CTT in Cask Preparation Area		1.3E-06	1.1E-06	3.1E-06	2.3E+00	Lognormal
Localized fire threatens TC/HLW in CTT in Cask Preparation Area		5.3E-07	4.6E-07	1.3E-06	2.3E+00	Lognormal
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/SPM (Diesel Present)	Railcar					
Localized fire threatens TC/NSNF on railcar in the Cask Preparation Area w / SPM (diesel present)		2.3E-07	2.1E-07	5.1E-07	2.1E+00	Lognormal
Localized fire threatens TC/HLW on railcar in the Cask Preparation Area w / SPM (diesel present)		1.5E-07	1.4E-07	3.5E-07	2.1E+00	Lognormal
Localized Fire Threatens Waste Form on Railcar in the Cask Preparation Area w/oSPM (No Diesel Present)	Railcar					
Localized fire threatens TC/NSNF on railcar in the Cask Preparation Area w/o SPM (no diesel present)		2.0E-06	1.8E-06	4.5E-06	2.2E+00	Lognormal
Localized fire threatens TC/HLW on railcar in the Cask Preparation Area w/o SPM (no diesel present)		9.3E-07	8.3E-07	2.1E-06	2.2E+00	Lognormal
Localized Fire Threatens Waste Form in CTM in Transfer Room	Canister transfer machine					
Localized fire threatens NSNF in CTM in Transfer Room		8.1E-08	7.1E-08	1.9E-07	2.3E+00	Lognormal
Localized fire threatens HLW in CTM in Transfer Room		6.9E-08	6.1E-08	1.7E-07	2.3E+00	Lognormal
Large Fire Threatens TC/NSNF (Diesel)	-	3.7E-07	3.3E-07	8.7E-07	2.2E+00	Lognormal
Large Fire Threatens TC/NSNF (No Diesel)	-	9.7E-06	8.6E-06	2.3E-05	2.2E+00	Lognormal
Large Fire Threatens NSNF in CTM	-	2.0E-07	1.8E-07	4.7E-07	2.2E+00	Lognormal
Large Fire Threatens NSNF in WP	-	5.9E-05	5.3E-05	1.4E-04	2.2E+00	Lognormal
Large Fire Threatens TC/HLW (Diesel)	-	2.5E-07	2.2E-07	5.8E-07	2.2E+00	Lognormal
Large Fire Threatens TC/HLW (No Diesel)	-	5.1E-06	4.5E-06	1.2E-05	2.2E+00	Lognormal
Large Fire Threatens HLW in CTM	-	1.6E-06	1.4E-06	3.7E-06	2.2E+00	Lognormal
Large Fire Threatens HLW in WP	-	1.0E-04	9.1E-05	2.4E-04	2.2E+00	Lognormal

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high-level radioactive waste; NSNF = naval spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

**APPENDIX F.I
DEFINITION OF IGNITION SOURCE CATEGORY**

Table F.I-1. Definition of Ignition Source Category

Ignition Source Category	NFPA Equipment Categories Included
Electrical equipment	Fixed wiring; transformer, associated over current or disconnect equipment; meter, meter box; power switchgear, 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
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; unclassified air conditioning, refrigeration systems
Mechanical process 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, unknown mechanical equipment
Heat-generating process equipment	Casting, molding, or forging equipment; heat-treating equipment; dryers; furnaces; incinerators
Torches, welders, and burners	Torches, welders, burners
Internal combustion engines	Internal combustion engines
Office and kitchen equipment	Television, radio, stereo; fixed food-warming appliance; fixed or stationary oven; 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.

HVAC = heating, ventilation, and air conditioning; NFPA = National Fire Protection Association.

Source: Ref. F2.38

**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 noncombustible construction as defined by the NFPA. The NFPA data is taken from *Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Non-Combustible Construction* (Ref. F2.38).

The first data set provides a distribution of fire ignition as a function of the ignition source category, as defined in Appendix F.I. 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 equipment	16	9%
HVAC equipment	15	8%
Mechanical process equipment	26	14%
Heat-generating process equipment	29	16%
Torches, welders, and burners	41	22%
Internal combustion engines	4	2%
Offices and kitchen equipment	12	6%
Portable and special equipment	19	10%
No equipment involved	25	13%
Total	187	100%

NOTE: HVAC = heating, ventilation, and air conditioning.

Source: Ref. F2.38.

Table F.II-2. Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction 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
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. F2.38.

Table F.II-3. Structure Fires in Radioactive Material Working Facilities and Nuclear Energy Plants of Noncombustible Construction 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
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. F2.38.

The method chosen for calculating the confidence interval of the data is the following margin of error calculation:

$$ME = \sqrt{\frac{p(1-p)}{n}} \times t \tag{Eq. F.II-1}$$

where

- ME = margin of error
- p = event probability
- n = number of samples
- t = t -distribution value (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 Value

t-distribution			
		α	
		0.025	0.005
ν	60	2.000	2.660
	120	1.980	2.617

Source: Ref. F2.41.

where

α = one minus the confidence interval divided by two (e.g., a 95% confidence interval corresponds to an α of 0.025)

ν = degrees of freedom (number of samples minus one)

For the data sets analyzed, CIs of 95% and 99% were analyzed 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. 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 F.II-1, obtaining t from Table F.II-4. For this example, t is 1.98 because the degrees of freedom ($\nu = n-1 = 186$) is greater than 120, and the CI is 95%, making $\alpha = 0.025$. 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 interval.

Table F.II-5. Margin of Error Results at 95% Confidence Interval for Fires in Radioactive Material Working Facilities by Originating Equipment

Equipment Type	Occurrences	Probability	Margin of Error (95% confidence)	Probability range based on Margin of Error (%)	Occurrences range based on Margin of
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			

NOTE: HVAC = heating, ventilation, and air conditioning.

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	Occurrences	Probability	Margin of Error (99% confidence)	Probability range based on Margin of Error (%)	Occurrences range based on Margin of
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			

NOTE: HVAC = heating, ventilation, and air conditioning.

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 Noncombustible Construction in Which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate

Extent of Flame Damage	Occurrences	Probability	Margin of Error (95% confidence)	Probability range based on Margin of Error (%)		Occurrences range based on Margin of Error	
				≤ p ≤	≤ p ≤	≤ 0 ≤	≤ 0 ≤
Confined to object of origin	54	6.21E-01	± 1.04E-01	51.67	72.48	44.78	62.81
Confined to part of room/area of origin	13	1.49E-01	± 7.65E-02	7.3	22.59	6.33	19.58
Confined to room of origin	0.33	3.79E-03	± 1.32E-02	0	1.7	0	1.47
Confined to fire-rated compartment of origin	5	5.75E-02	± 4.99E-02	0.76	10.74	0.66	9.31
Confined to floor of origin	0.33	3.79E-03	± 1.32E-02	0	1.7	0	1.47
Confined to structure of origin	14	1.61E-01	± 7.88E-02	8.21	23.97	7.11	20.77
Extended beyond structure of origin	0.33	3.79E-03	± 1.32E-02	0	1.7	0	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 Noncombustible Construction in Which No Automatic Suppression System Was Present or the Automatic Suppression System Failed to Operate

Extent of Flame Damage	Occurrences	Probability	Margin of Error (99% confidence)	Probability range based on Margin of Error (%)		Occurrences range based on Margin of Error	
				48.24 ≤ p ≤	75.91	41.8 ≤ O ≤	65.78
Confined to object of origin	54	6.21E-01	± 1.38E-01	4.78 ≤ p ≤	25.11	4.14 ≤ O ≤	21.76
Confined to part of room/area of origin	13	1.49E-01	± 1.02E-01	0 ≤ p ≤	2.13	0 ≤ O ≤	1.85
Confined to room of origin	0.33	3.79E-03	± 1.75E-02	0 ≤ p ≤	12.39	0 ≤ O ≤	10.74
Confined to fire-rated compartment of origin	5	5.75E-02	± 6.64E-02	0 ≤ p ≤	2.13	0 ≤ O ≤	1.85
Confined to floor of origin	0.33	3.79E-03	± 1.75E-02	5.61 ≤ p ≤	26.57	4.86 ≤ O ≤	23.03
Confined to structure of origin	14	1.61E-01	± 1.05E-01	0 ≤ p ≤	2.13	0 ≤ O ≤	1.85
Extended beyond structure of origin	0.33	3.79E-03	± 1.75E-02				
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 Noncombustible Construction in Which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly

Extent of Flame Damage	Occurrences	Probability	Margin of Error (95% confidence)	Probability range based on Margin of Error (%)			Occurrences range based on Margin of Error		
				43.38	≤ p ≤	66.72	31.52	≤ O ≤	48.48
Confined to object of origin	40	5.51E-01	± 1.17E-01	20.74	≤ p ≤	42.57	15.07	≤ O ≤	30.93
Confined to part of room/area of origin	23	3.17E-01	± 1.09E-01	0	≤ p ≤	6.59	0	≤ O ≤	4.79
Confined to room of origin	2	2.75E-02	± 3.84E-02	0	≤ p ≤	2.03	0	≤ O ≤	1.47
Confined to fire-rated compartment of origin	0.33	4.54E-03	± 1.58E-02	0.94	≤ p ≤	12.82	0.68	≤ O ≤	9.32
Confined to floor of origin	5	6.88E-02	± 5.94E-02	0	≤ p ≤	6.59	0	≤ O ≤	4.79
Confined to structure of origin	2	2.75E-02	± 3.84E-02	0	≤ p ≤	2.03	0	≤ O ≤	1.47
Extended beyond structure of origin	0.33	4.54E-03	± 1.58E-02						
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 Noncombustible Construction in Which the Fire Was Too Small to Activate the Automatic Suppression System or the Automatic System Operated Properly

Extent of Flame Damage	Occurrences	Probability	Margin of Error (99% confidence)	Probability range based on Margin of Error (%)		Occurrences range based on Margin of Error	
				Margin of Error (%)	≤ p ≤	Occurrences	≤ O ≤
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

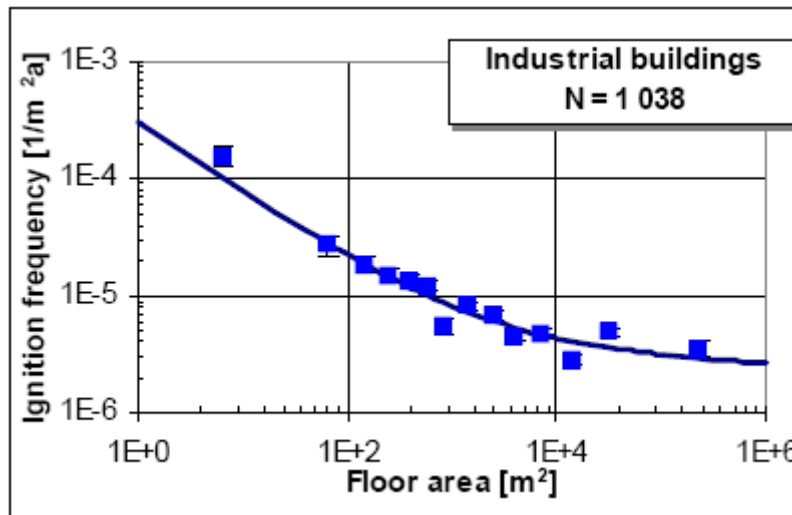
For proper consideration of the fire frequency analysis of the Canister Receipt and Closure Facility, Wet Handling Facility, IHF, and Receipt Facility, it was necessary to develop an uncertainty distribution for the industrial building fire frequency. The *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. F2.40) used to develop these frequencies presents an equation with floor area as an input to determine frequency. The following equation is developed based on sample data collected:

$$f_m''(A) = c_1 A^r + c_2 A^s \tag{Eq. F.III-1}$$

where

- f_m'' = the annual fire frequency per square meter of floor area
- A = the floor area
- $c_1, c_2, r,$ = constants determined by the line of best fit derived from the data and s

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.



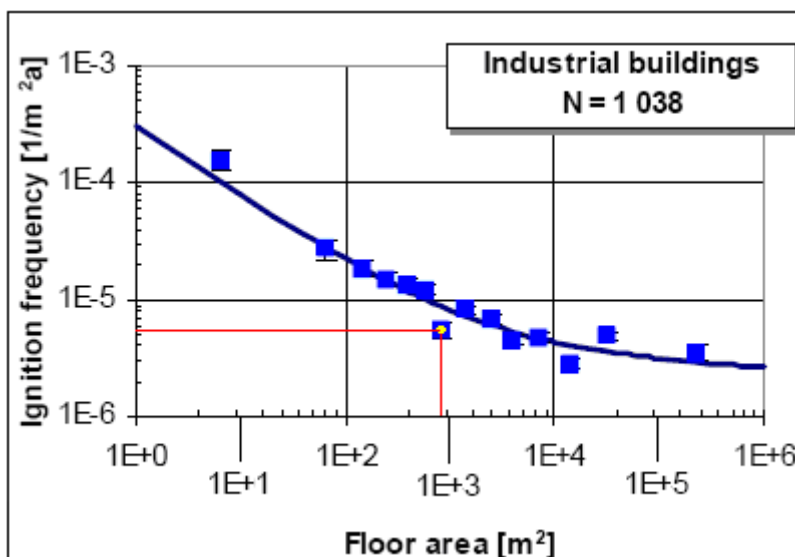
NOTE: m = meter.

Source: (Ref F2.40)

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 label to the 1E+3 label. 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.



NOTE: m = meter.

Source: (Ref F2.40)

Figure F.III-2. Data Point Determination

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 task is accomplished using the following methodology.

Statistics: Probability, Inference, and Decision (Ref. F2.41) outline 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, as illustrated in Figure F.III-3.

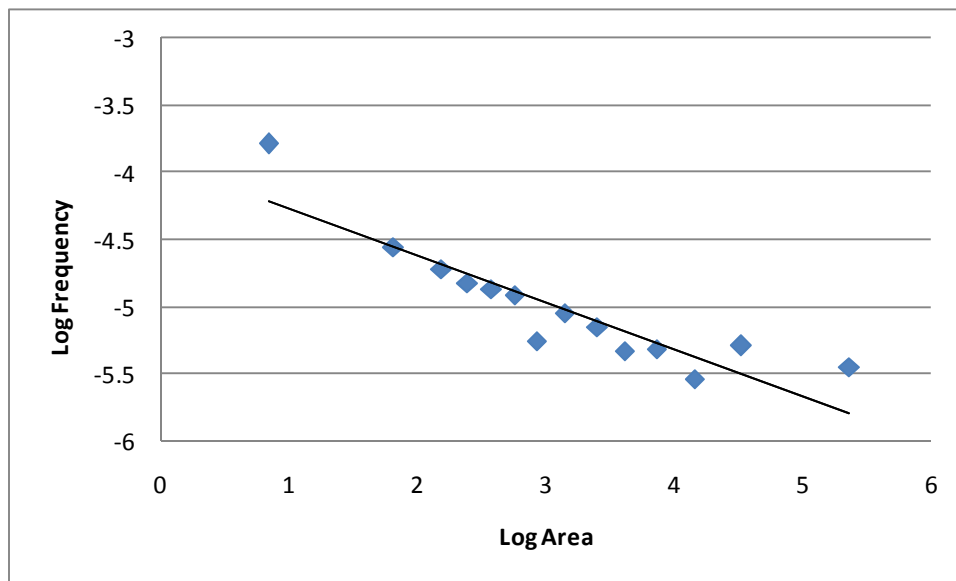
As shown in Figures F.III-1 and F.III-3, the portion of the curve for buildings less than 1,000 m² has a steeper slope than the portion of the curve for buildings larger than 1,000 m². For that reason, the data were divided into two ranges as shown in Figure F.III-4. Because all of the YMP facilities have floor areas larger than 1,000 m², the remaining analysis focused on the upper end of the floor area range.

Table F.III-1. Ignition Frequency Data from Figure FIII-1 and Equation FIII-1

Graphically Determined Data Points		From Equation 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}

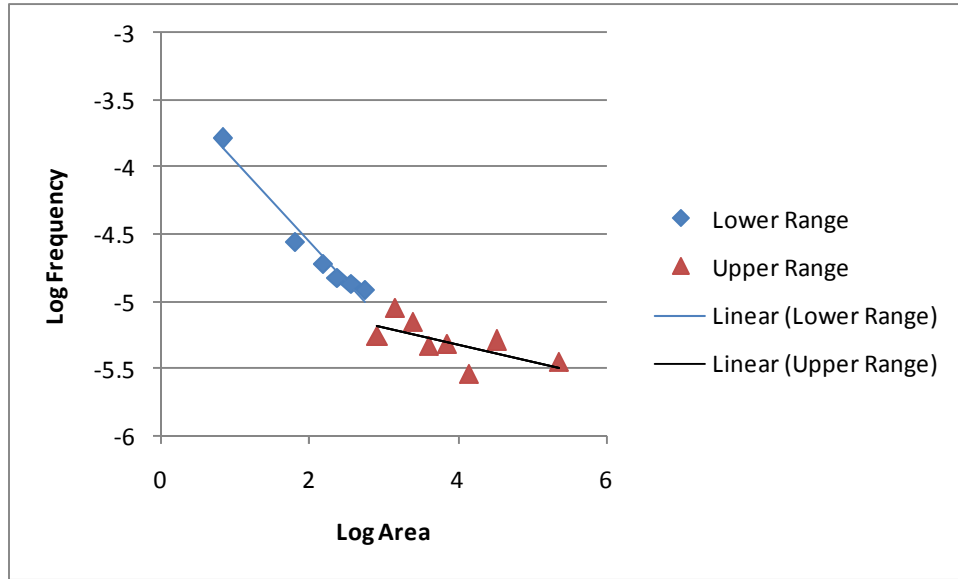
NOTE: m = meter; yr = year.

Source: Original



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:

$$\hat{y} \pm a \frac{s_{xy}}{\sqrt{n-2}} \sqrt{n+1 + \frac{(x-m_x)^2}{s_x^2}} \quad (\text{Eq. F.III-2})$$

$$s_{xy} = \sqrt{s_y^2(1-r_{xy}^2)} \quad (\text{Eq. F.III-3})$$

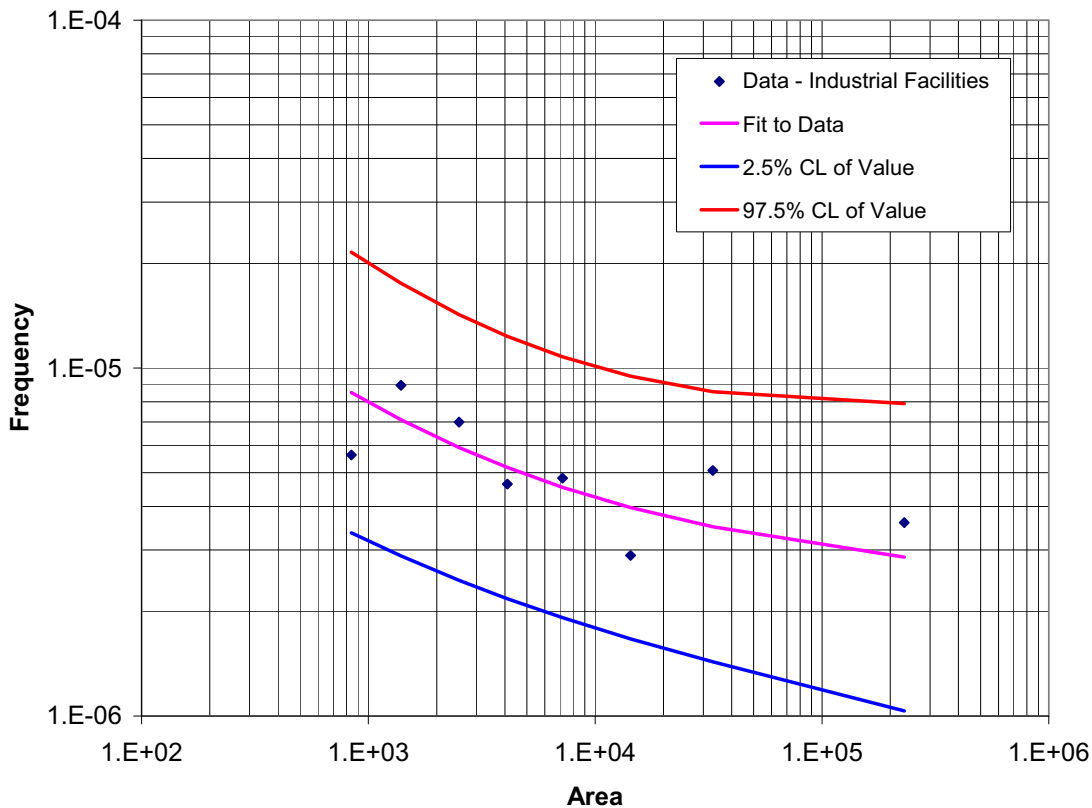
$$r_{xy} = \frac{\sum_{i=0}^{i=n} (x_i - m_x)(y - m_y)}{n s_x s_y} \quad (\text{Eq. F.III-4})$$

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 = the number of data points used in the linear regression analysis (eight for the upper floor area range)
- a = the $1-(\alpha/2)$ 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 antilog 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 m ² /yr)		
	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: CRCF = Canister Receipt and Closure Facility; IHF = Initial Handling Facility; LCL = lower confidence limit; RF = Receipt Facility; UCL = upper confidence limit; WHF = Wet Handling Facility.

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 F.VI) shows the calculated distributions at ten percentile intervals. Crystal Ball also provides the mean and the median of the distributions.

The Microsoft Excel function, LOGNORMDIST, can be utilized to calculate the corresponding 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.

$$\mu = \ln(\text{median}) \tag{Eq. F.IV-1}$$

$$\sigma = \sqrt{2 \ln\left(\frac{\text{mean}}{\text{median}}\right)} \tag{Eq. F.IV-2}$$

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 1.5%. 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
1.3E-06	0.0	0	0.0
5.1E-06	8.7	10	1.3
6.5E-06	19.2	20	0.8
7.7E-06	29.8	30	0.2
8.9E-06	40.2	40	0.2
1.0E-05	50.0	50	0.0
1.2E-05	60.6	60	0.6
1.3E-05	70.7	70	0.7

Table F.IV-1. Comparison Between Crystal Ball and Excel Percentile Intervals (Continued)

Forecast Values	Excel Calculated Percentiles	Crystal Ball Percentiles	Difference
1.6E-05	80.3	80	0.3
2.0E-05	90.1	90	0.1
6.8E-05	100.0	100	0.0
Mu	-11.5	Mean	1.2E-05
Sigma	0.5	Median	1.0E-05

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.

$$\sigma = \sqrt{2 \ln \left(\frac{\text{mean}}{\text{median}} \right)} \quad (\text{Eq. F.V-1})$$

$$\text{EF} = e^{\sigma \times 1.645} \quad (\text{Eq. F.V-2})$$

The resultant error factors for each initiating event frequency are displayed in Table F5.7-6, 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 F5.7-6) 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
RESULTS FROM MONTE CARLO SIMULATION**

Table F.VI-1. Results of the Monte Carlo Simulation 97.5% Query

Initiating Event	97.5% Percentile	Mean
Large fire threatens HLW in CTM	3.7E-06	1.6E-06
Large fire threatens HLW in WP	2.4E-04	1.0E-04
Large fire threatens NSNF in CTM	4.7E-07	2.0E-07
Large fire threatens NSNF in WP	1.4E-04	5.9E-05
Large fire threatens TC/HLW w/o SPM present (no diesel)	1.2E-05	5.1E-06
Large fire threatens TC/HLW w/ SPM present (diesel)	5.8E-07	2.5E-07
Large fire threatens TC/NSNF w/o SPM present (no diesel)	2.3E-05	9.7E-06
Large fire threatens TC/NSNF w/ SPM present (diesel)	8.7E-07	3.7E-07
Localized fire threatens HLW in CTM in Canister Transfer Room	1.7E-07	6.9E-08
Localized fire threatens NSNF in CTM in Canister Transfer Room	1.9E-07	8.1E-08
Localized fire threatens TC/HLW in CTT in Cask Preparation Area	1.3E-06	5.3E-07
Localized fire threatens TC/HLW in Cask Unloading Room	5.1E-08	2.2E-08
Localized fire threatens TC/HLW on railcar in Cask Preparation Area w/SPM (no diesel present)	2.1E-06	9.3E-07
Localized fire threatens TC/HLW on railcar in Cask Preparation Area w/SPM (diesel present)	3.5E-07	1.5E-07
Localized fire threatens TC/NSNF in CTT in Cask Preparation Area	3.1E-06	1.3E-06
Localized fire threatens TC/NSNF in Cask Unloading Room	2.7E-08	1.2E-08
Localized fire threatens TC/NSNF on railcar in Cask Preparation Area w/oSPM (no diesel present)	4.5E-06	2.0E-06
Localized fire threatens TC/NSNF on railcar in Cask Preparation Area w/SPM (diesel present)	5.1E-07	2.3E-07
Localized fire threatens WP/HLW in WP Loading Room	2.8E-05	1.2E-05
Localized fire threatens WP/HLW in WP Positioning Room	8.4E-05	3.8E-05
Localized fire threatens WP/HLW in TEV in WP Loadout room	1.9E-07	8.8E-08
Localized fire threatens WP/HLW in WPTT in WP Loadout room	1.1E-06	4.9E-07
Localized fire threatens WP/NSNF in WP Loading Room	8.5E-07	3.5E-07
Localized fire threatens WP/NSNF in WP Positioning Room	8.3E-05	3.8E-05
Localized fire threatens WP/NSNF in TEV in WP Loadout room	1.9E-07	8.8E-08
Localized fire threatens WP/NSNF in WPTT in WP Loadout room	1.1E-06	4.9E-07

NOTE: CTM = canister transfer machine; CTT = cask transfer trolley; HLW = high-level radioactive waste;
NSNF = naval spent nuclear fuel; SPM = site prime mover; TC = transportation cask; TEV = transport and
emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Crystal Ball 'extract data' output.

The Crystal Ball report, 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 1/30/2008 at 9:48:01

Simulation stopped on 1/30/2008 at 9:49:00

Run preferences:

Number of trials run	10,000
Monte Carlo	
Random seed	

Run statistics:

Total running time (sec)	59.45
Trials/second (average)	168
Random numbers per sec	2,860

Crystal Ball data:

Assumptions	17
Correlations	0
Correlated groups	0
Decision variables	0
Forecasts	26

Forecasts

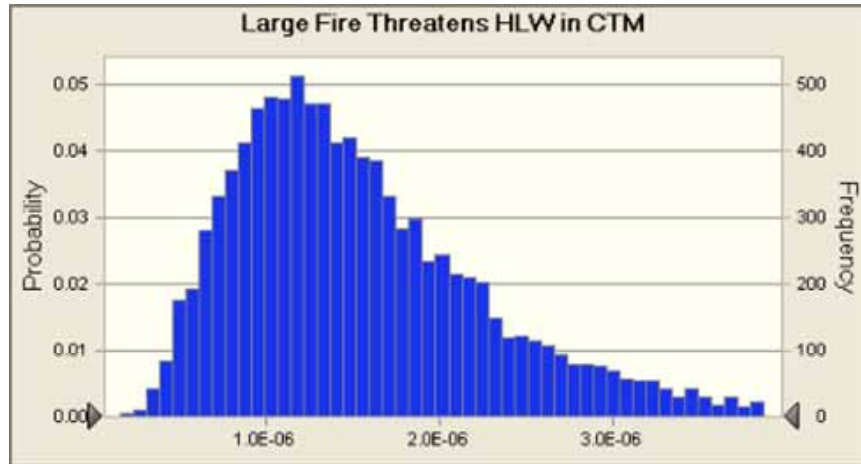
Worksheet: [IHF Fire Frequency - no suppression.xls]Initiating Event Frequency

Forecast: Large Fire Threatens HLW in CTM

Cell: K187

Summary:

Entire range is from 1.6E-07 to 9.6E-06
Base case is 1.4E-06
After 10,000 trials, the std. error of the mean is 8.2E-09



Statistics:

	Forecast values
Trials	10,000
Mean	1.6E-06
Median	1.4E-06
Mode	1.8E-06
Standard Deviation	8.2E-07
Variance	6.7E-13
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	1.6E-07
Maximum	9.6E-06
Range Width	9.4E-06
Mean Std. Error	8.2E-09

Forecast: Large Fire Threatens HLW in CTM (cont'd)

Cell: K187

Percentiles:

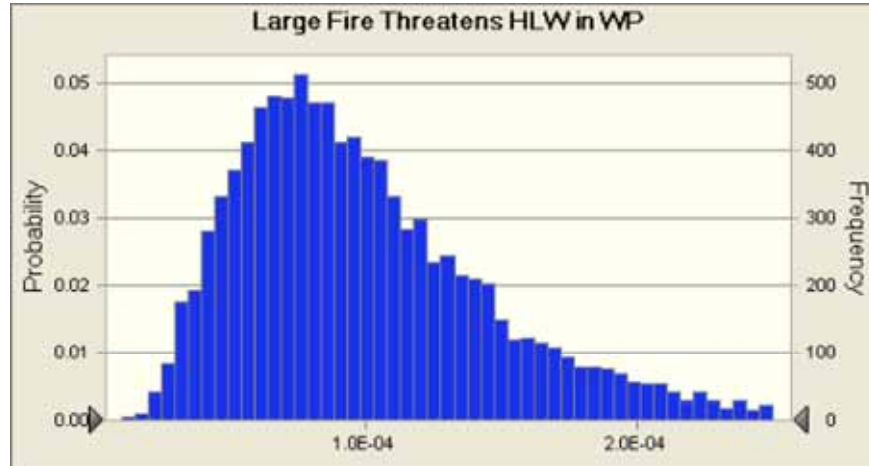
	Forecast values
0%	1.6E-07
10%	7.4E-07
20%	9.3E-07
30%	1.1E-06
40%	1.2E-06
50%	1.4E-06
60%	1.6E-06
70%	1.8E-06
80%	2.1E-06
90%	2.6E-06
100%	9.6E-06

Forecast: Large Fire Threatens HLW in WP

Cell: K188

Summary:

Entire range is from 1.0E-05 to 6.2E-04
Base case is 9.3E-05
After 10,000 trials, the std. error of the mean is 5.3E-07



Statistics:

	Forecast values
Trials	10,000
Mean	1.0E-04
Median	9.1E-05
Mode	1.1E-04
Standard Deviation	5.3E-05
Variance	2.8E-09
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	1.0E-05
Maximum	6.2E-04
Range Width	6.1E-04
Mean Std. Error	5.3E-07

Forecast: Large Fire Threatens HLW in WP (cont'd)

Cell: K188

Percentiles:

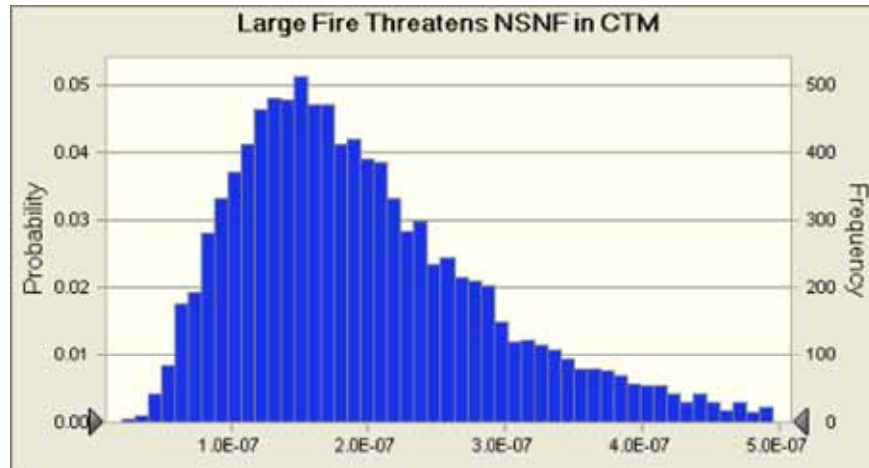
	Forecast values
0%	1.0E-05
10%	4.8E-05
20%	6.0E-05
30%	7.1E-05
40%	8.1E-05
50%	9.1E-05
60%	1.0E-04
70%	1.2E-04
80%	1.4E-04
90%	1.7E-04
100%	6.2E-04

Forecast: Large Fire Threatens NSNF in CTM

Cell: K183

Summary:

Entire range is from 2.0E-08 to 1.2E-06
Base case is 1.8E-07
After 10,000 trials, the std. error of the mean is 1.0E-09



Statistics:

Forecast values

Trials	10,000
Mean	2.0E-07
Median	1.8E-07
Mode	2.3E-07
Standard Deviation	1.0E-07
Variance	1.1E-14
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	2.0E-08
Maximum	1.2E-06
Range Width	1.2E-06
Mean Std. Error	1.0E-09

Forecast: Large Fire Threatens NSNF in CTM (cont'd)

Cell: K183

Percentiles:

Forecast values

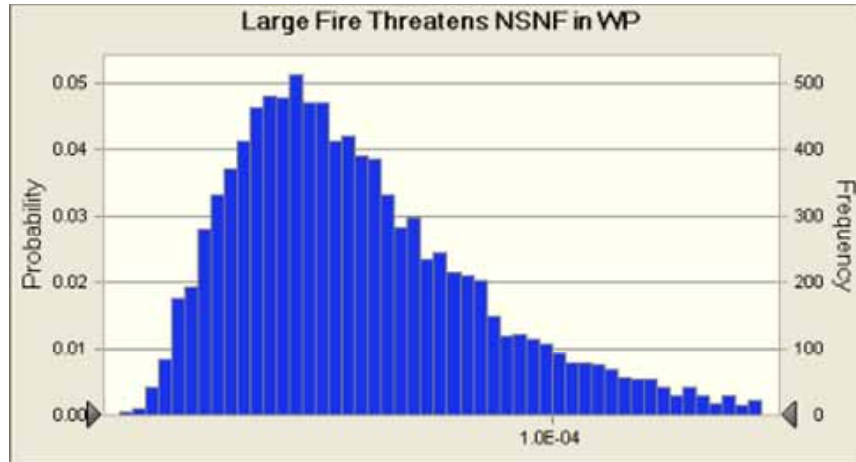
0%	2.0E-08
10%	9.5E-08
20%	1.2E-07
30%	1.4E-07
40%	1.6E-07
50%	1.8E-07
60%	2.0E-07
70%	2.3E-07
80%	2.7E-07
90%	3.4E-07
100%	1.2E-06

Forecast: Large Fire Threatens NSNF in WP

Cell: K184

Summary:

Entire range is from 6.0E-06 to 3.6E-04
Base case is 5.4E-05
After 10,000 trials, the std. error of the mean is 3.1E-07



Statistics:

	Forecast values
Trials	10,000
Mean	5.9E-05
Median	5.3E-05
Mode	6.7E-05
Standard Deviation	3.1E-05
Variance	9.4E-10
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	6.0E-06
Maximum	3.6E-04
Range Width	3.5E-04
Mean Std. Error	3.1E-07

Forecast: Large Fire Threatens NSNF in WP (cont'd)

Cell: K184

Percentiles:

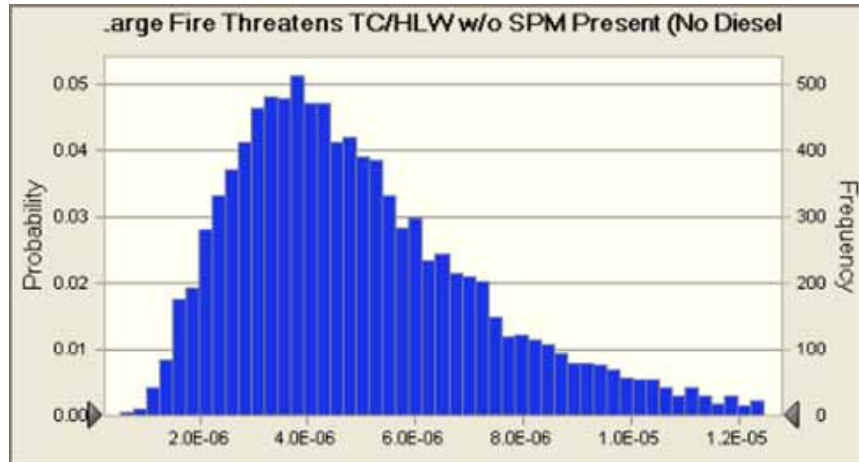
	Forecast values
0%	6.0E-06
10%	2.8E-05
20%	3.5E-05
30%	4.1E-05
40%	4.7E-05
50%	5.3E-05
60%	6.0E-05
70%	6.8E-05
80%	8.0E-05
90%	9.9E-05
100%	3.6E-04

Forecast: Large Fire Threatens TC/HLW w/o SPM Present (No Diesel)

Cell: K186

Summary:

Entire range is from 5.1E-07 to 3.1E-05
Base case is 4.6E-06
After 10,000 trials, the std. error of the mean is 2.6E-08



Statistics:

	Forecast values
Trials	10,000
Mean	5.1E-06
Median	4.5E-06
Mode	5.7E-06
Standard Deviation	2.6E-06
Variance	6.9E-12
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	5.1E-07
Maximum	3.1E-05
Range Width	3.0E-05
Mean Std. Error	2.6E-08

Forecast: Large Fire Threatens TC/HLW w/o SPM Present (No Diesel) (cont'd)

Cell: K186

Percentiles:

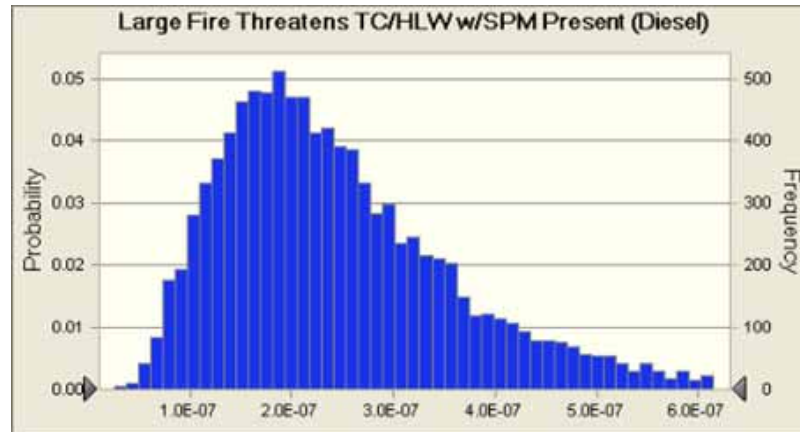
Percentiles:	Forecast values
0%	5.1E-07
10%	2.4E-06
20%	3.0E-06
30%	3.5E-06
40%	4.0E-06
50%	4.5E-06
60%	5.1E-06
70%	5.9E-06
80%	6.9E-06
90%	8.5E-06
100%	3.1E-05

Forecast: Large Fire Threatens TC/HLW w/SPM Present (Diesel)

Cell: K185

Summary:

Entire range is from 2.5E-08 to 1.5E-06
Base case is 2.3E-07
After 10,000 trials, the std. error of the mean is 1.3E-09



Statistics:

Forecast values

Trials	10,000
Mean	2.5E-07
Median	2.2E-07
Mode	2.8E-07
Standard Deviation	1.3E-07
Variance	1.7E-14
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	2.5E-08
Maximum	1.5E-06
Range Width	1.5E-06
Mean Std. Error	1.3E-09

Forecast: Large Fire Threatens TC/HLW w/SPM Present (Diesel) (cont'd)

Cell: K185

Percentiles:

Forecast values

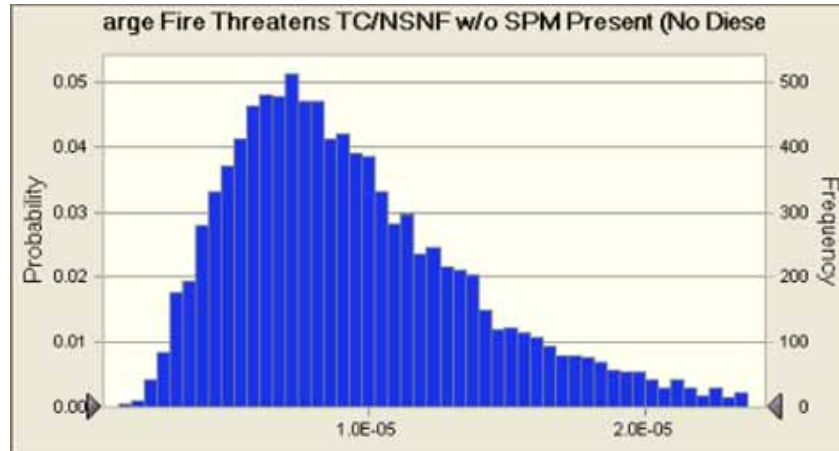
0%	2.5E-08
10%	1.2E-07
20%	1.5E-07
30%	1.7E-07
40%	2.0E-07
50%	2.2E-07
60%	2.5E-07
70%	2.9E-07
80%	3.4E-07
90%	4.2E-07
100%	1.5E-06

Forecast: Large Fire Threatens TC/NSNF w/o SPM Present (No Diesel)

Cell: K182

Summary:

Entire range is from 9.8E-07 to 5.9E-05
 Base case is 8.8E-06
 After 10,000 trials, the std. error of the mean is 5.0E-08



Statistics:

Forecast values

Trials	10,000
Mean	9.7E-06
Median	8.6E-06
Mode	1.1E-05
Standard Deviation	5.0E-06
Variance	2.5E-11
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	9.8E-07
Maximum	5.9E-05
Range Width	5.8E-05
Mean Std. Error	5.0E-08

Forecast: Large Fire Threatens TC/NSNF w/o SPM Present (No Diesel) (cont'd)

Cell: K182

Percentiles:

Forecast values

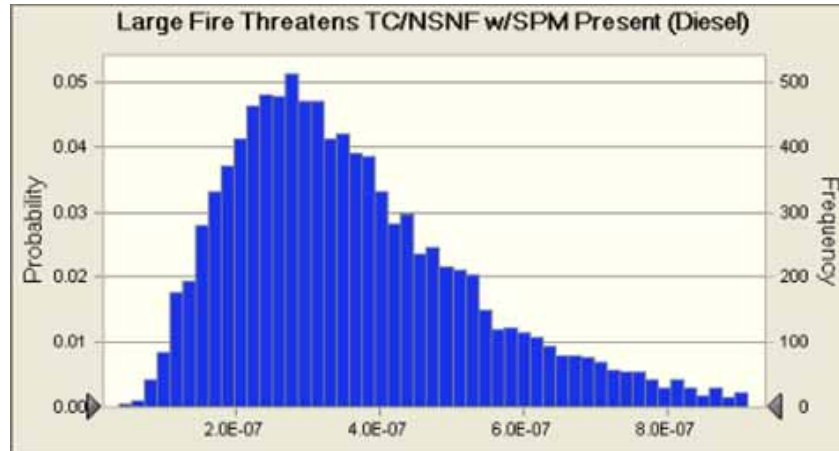
0%	9.8E-07
10%	4.5E-06
20%	5.7E-06
30%	6.7E-06
40%	7.6E-06
50%	8.6E-06
60%	9.8E-06
70%	1.1E-05
80%	1.3E-05
90%	1.6E-05
100%	5.9E-05

Forecast: Large Fire Threatens TC/NSNF w/SPM Present (Diesel)

Cell: K181

Summary:

Entire range is from 3.8E-08 to 2.3E-06
 Base case is 3.4E-07
 After 10,000 trials, the std. error of the mean is 1.9E-09



Statistics:

Forecast values

Trials	10,000
Mean	3.7E-07
Median	3.3E-07
Mode	4.2E-07
Standard Deviation	1.9E-07
Variance	3.7E-14
Skewness	1.55
Kurtosis	7.42
Coeff. of Variability	0.5162
Minimum	3.8E-08
Maximum	2.3E-06
Range Width	2.2E-06
Mean Std. Error	1.9E-09

Forecast: Large Fire Threatens TC/NSNF w/SPM Present (Diesel) (cont'd)

Cell: K181

Percentiles:

Forecast values

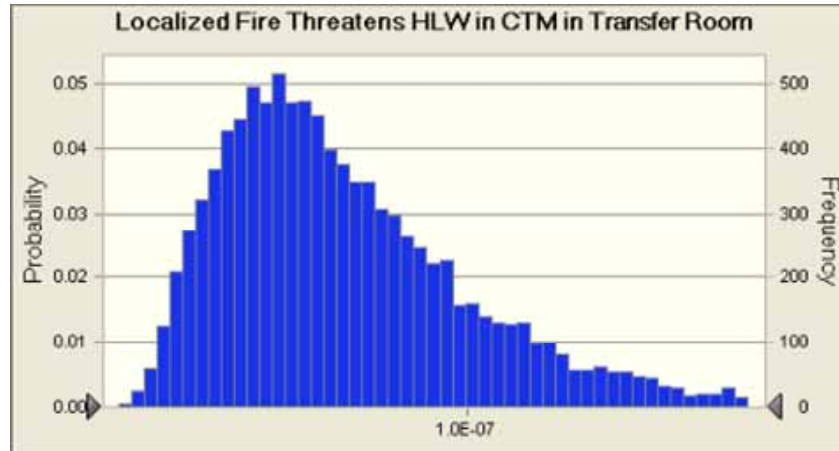
0%	3.8E-08
10%	1.7E-07
20%	2.2E-07
30%	2.6E-07
40%	2.9E-07
50%	3.3E-07
60%	3.8E-07
70%	4.3E-07
80%	5.0E-07
90%	6.2E-07
100%	2.3E-06

Forecast: Localized Fire Threatens HLW in CTM in Transfer Room

Cell: M174

Summary:

Entire range is from 7.1E-09 to 4.0E-07
Base case is 6.2E-08
After 10,000 trials, the std. error of the mean is 3.8E-10



Statistics:

	Forecast values
Trials	10,000
Mean	6.9E-08
Median	6.1E-08
Mode	8.3E-08
Standard Deviation	3.8E-08
Variance	1.4E-15
Skewness	1.71
Kurtosis	8.43
Coeff. of Variability	0.5447
Minimum	7.1E-09
Maximum	4.0E-07
Range Width	3.9E-07
Mean Std. Error	3.8E-10

Forecast: Localized Fire Threatens HLW in CTM in Transfer Room (cont'd)

Cell: M174

Percentiles:

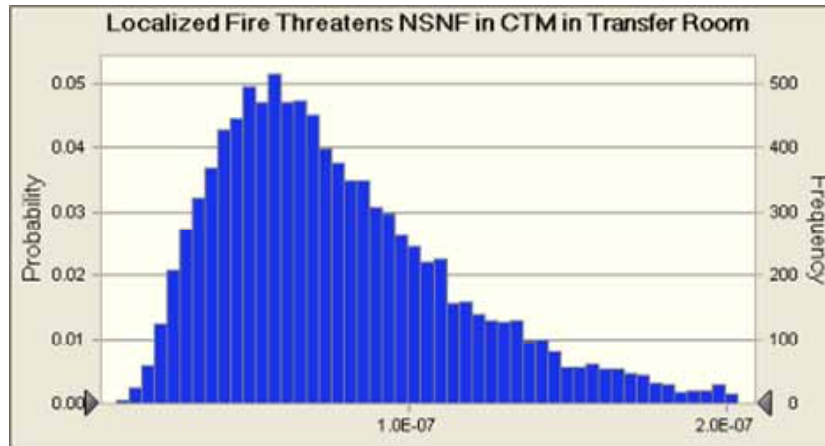
	Forecast values
0%	7.1E-09
10%	3.1E-08
20%	3.9E-08
30%	4.7E-08
40%	5.4E-08
50%	6.1E-08
60%	7.0E-08
70%	8.0E-08
80%	9.4E-08
90%	1.2E-07
100%	4.0E-07

Forecast: Localized Fire Threatens NSNF in CTM in Transfer Room

Cell: K173

Summary:

Entire range is from 8.3E-09 to 4.6E-07
Base case is 7.3E-08
After 10,000 trials, the std. error of the mean is 4.4E-10



Statistics:

Forecast values

Trials	10,000
Mean	8.1E-08
Median	7.1E-08
Mode	9.7E-08
Standard Deviation	4.4E-08
Variance	1.9E-15
Skewness	1.71
Kurtosis	8.43
Coeff. of Variability	0.5447
Minimum	8.3E-09
Maximum	4.6E-07
Range Width	4.5E-07
Mean Std. Error	4.4E-10

Forecast: Localized Fire Threatens NSNF in CTM in Transfer Room (cont'd)

Cell: K173

Percentiles:

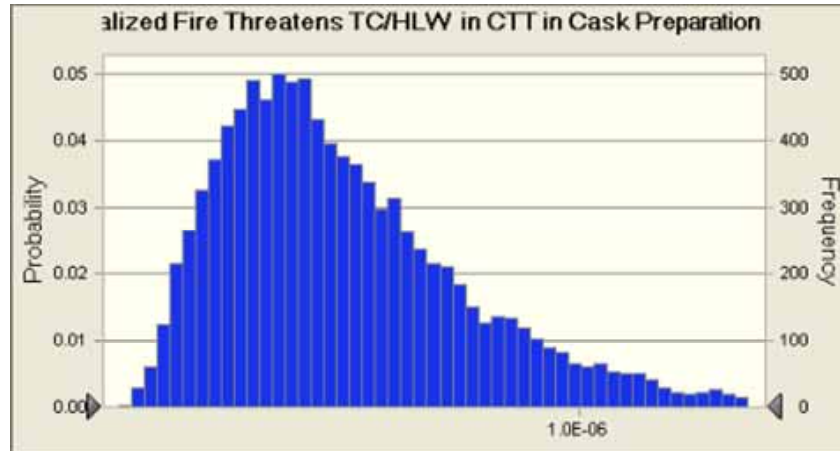
Forecast values

0%	8.3E-09
10%	3.6E-08
20%	4.6E-08
30%	5.4E-08
40%	6.2E-08
50%	7.1E-08
60%	8.1E-08
70%	9.3E-08
80%	1.1E-07
90%	1.4E-07
100%	4.6E-07

Forecast: Localized Fire Threatens TC/HLW in CTT in Cask Preparation Area Cell: M114

Summary:

Entire range is from 4.4E-08 to 3.1E-06
 Base case is 4.7E-07
 After 10,000 trials, the std. error of the mean is 2.9E-09



Statistics:

	Forecast values
Trials	10,000
Mean	5.3E-07
Median	4.6E-07
Mode	6.5E-07
Standard Deviation	2.9E-07
Variance	8.6E-14
Skewness	1.74
Kurtosis	8.64
Coeff. of Variability	0.5586
Minimum	4.4E-08
Maximum	3.1E-06
Range Width	3.1E-06
Mean Std. Error	2.9E-09

Forecast: Localized Fire Threatens TC/HLW in CTT in Cask Preparation Area Cell: M114 (cont'd)

Percentiles:

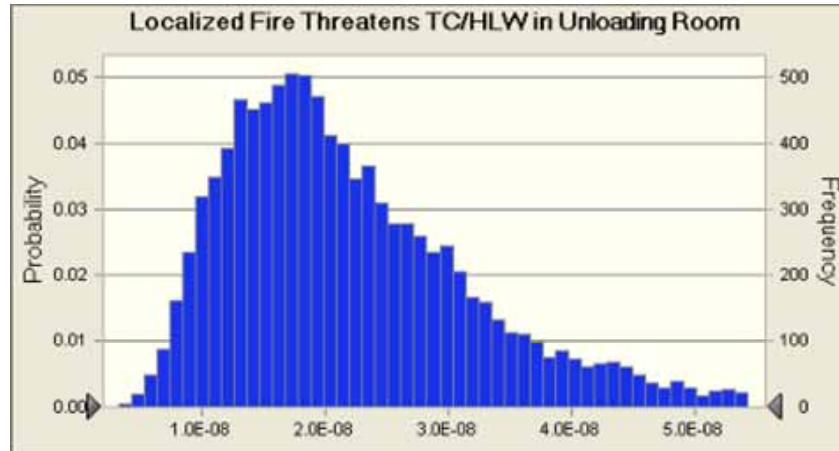
	Forecast values
0%	4.4E-08
10%	2.3E-07
20%	2.9E-07
30%	3.5E-07
40%	4.0E-07
50%	4.6E-07
60%	5.3E-07
70%	6.1E-07
80%	7.1E-07
90%	8.9E-07
100%	3.1E-06

Forecast: Localized Fire Threatens TC/HLW in Unloading Room

Cell: M46

Summary:

Entire range is from 3.2E-09 to 1.2E-07
Base case is 2.1E-08
After 10,000 trials, the std. error of the mean is 1.1E-10



Statistics:

	Forecast values
Trials	10,000
Mean	2.2E-08
Median	2.0E-08
Mode	2.0E-08
Standard Deviation	1.1E-08
Variance	1.3E-16
Skewness	1.65
Kurtosis	8.00
Coeff. of Variability	0.5047
Minimum	3.2E-09
Maximum	1.2E-07
Range Width	1.1E-07
Mean Std. Error	1.1E-10

Forecast: Localized Fire Threatens TC/HLW in Unloading Room (cont'd)

Cell: M46

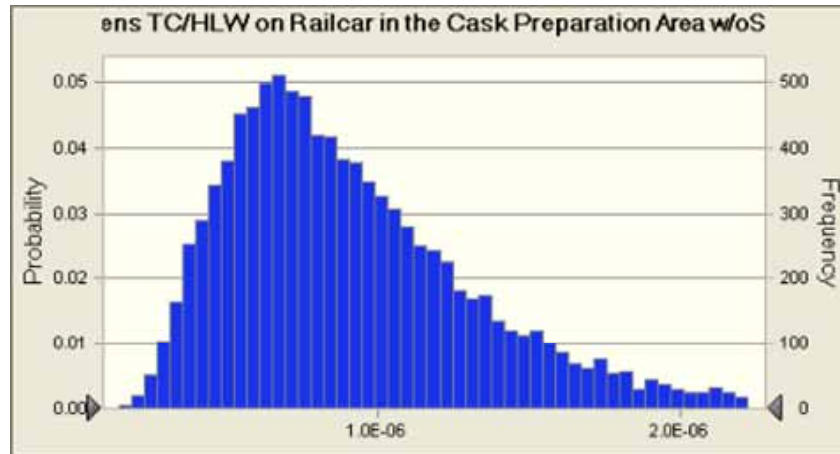
Percentiles:

	Forecast values
0%	3.2E-09
10%	1.1E-08
20%	1.3E-08
30%	1.6E-08
40%	1.8E-08
50%	2.0E-08
60%	2.3E-08
70%	2.6E-08
80%	3.0E-08
90%	3.7E-08
100%	1.2E-07

Forecast: Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/oSPM (No Diesel Present) Cell: M154

Summary:

Entire range is from 1.4E-07 to 4.9E-06
 Base case is 8.4E-07
 After 10,000 trials, the std. error of the mean is 4.6E-09



Statistics:

Statistics:	Forecast values
Trials	10,000
Mean	9.3E-07
Median	8.3E-07
Mode	9.9E-07
Standard Deviation	4.6E-07
Variance	2.1E-13
Skewness	1.62
Kurtosis	7.86
Coeff. of Variability	0.4970
Minimum	1.4E-07
Maximum	4.9E-06
Range Width	4.7E-06
Mean Std. Error	4.6E-09

Forecast: Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/oSPM (No Diesel Present) (cont'd) Cell: M154

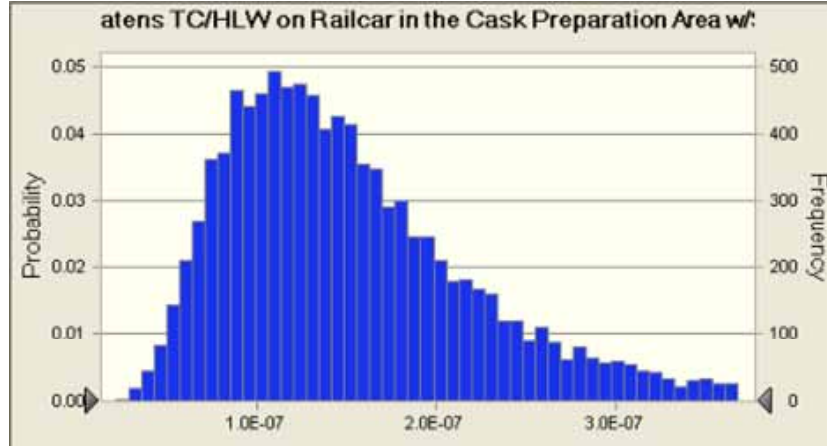
Percentiles:

Percentiles:	Forecast values
0%	1.4E-07
10%	4.6E-07
20%	5.6E-07
30%	6.5E-07
40%	7.3E-07
50%	8.3E-07
60%	9.4E-07
70%	1.1E-06
80%	1.2E-06
90%	1.5E-06
100%	4.9E-06

Forecast: Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/SPM (Diesel Present) Cell: M134

Summary:

Entire range is from 2.2E-08 to 7.8E-07
 Base case is 1.4E-07
 After 10,000 trials, the std. error of the mean is 7.6E-10



Statistics:	Forecast values
Trials	10,000
Mean	1.5E-07
Median	1.4E-07
Mode	1.7E-07
Standard Deviation	7.6E-08
Variance	5.8E-15
Skewness	1.56
Kurtosis	7.42
Coeff. of Variability	0.4932
Minimum	2.2E-08
Maximum	7.8E-07
Range Width	7.6E-07
Mean Std. Error	7.6E-10

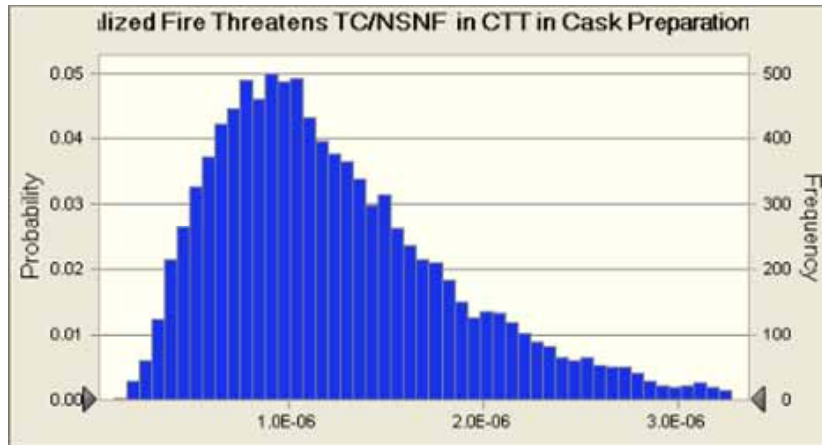
Forecast: Localized Fire Threatens TC/HLW on Railcar in the Cask Preparation Area w/SPM (Diesel Present) (cont'd) Cell: M134

Percentiles:	Forecast values
0%	2.2E-08
10%	7.6E-08
20%	9.3E-08
30%	1.1E-07
40%	1.2E-07
50%	1.4E-07
60%	1.6E-07
70%	1.8E-07
80%	2.1E-07
90%	2.5E-07
100%	7.8E-07

Forecast: Localized Fire Threatens TC/NSNF in CTT in Cask Preparation Area Cell: K113

Summary:

Entire range is from 1.1E-07 to 7.6E-06
 Base case is 1.2E-06
 After 10,000 trials, the std. error of the mean is 7.1E-09



Statistics:	Forecast values
Trials	10,000
Mean	1.3E-06
Median	1.1E-06
Mode	1.6E-06
Standard Deviation	7.1E-07
Variance	5.1E-13
Skewness	1.74
Kurtosis	8.64
Coeff. of Variability	0.5586
Minimum	1.1E-07
Maximum	7.6E-06
Range Width	7.5E-06
Mean Std. Error	7.1E-09

Forecast: Localized Fire Threatens TC/NSNF in CTT in Cask Preparation Area Cell: K113 (cont'd)

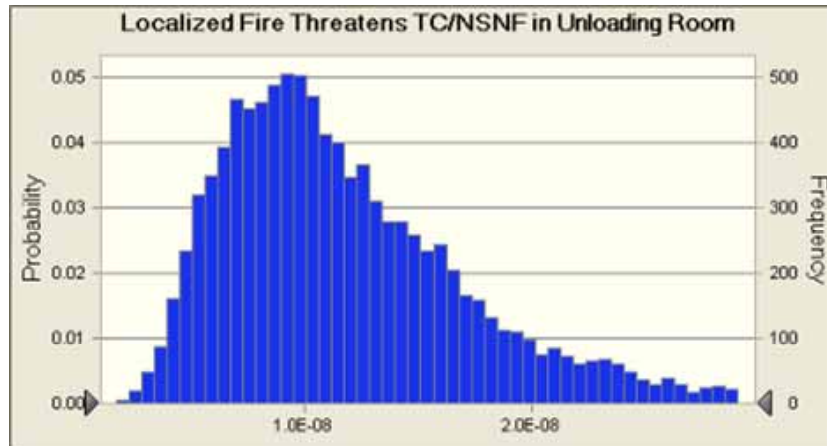
Percentiles:	Forecast values
0%	1.1E-07
10%	5.5E-07
20%	7.1E-07
30%	8.5E-07
40%	9.8E-07
50%	1.1E-06
60%	1.3E-06
70%	1.5E-06
80%	1.7E-06
90%	2.2E-06
100%	7.6E-06

Forecast: Localized Fire Threatens TC/NSNF in Unloading Room

Cell: K45

Summary:

Entire range is from 1.7E-09 to 6.3E-08
Base case is 1.1E-08
After 10,000 trials, the std. error of the mean is 6.1E-11



Statistics:

Forecast values

Trials	10,000
Mean	1.2E-08
Median	1.1E-08
Mode	1.1E-08
Standard Deviation	6.1E-09
Variance	3.7E-17
Skewness	1.65
Kurtosis	8.00
Coeff. of Variability	0.5047
Minimum	1.7E-09
Maximum	6.3E-08
Range Width	6.1E-08
Mean Std. Error	6.1E-11

Forecast: Localized Fire Threatens TC/NSNF in Unloading Room (cont'd)

Cell: K45

Percentiles:

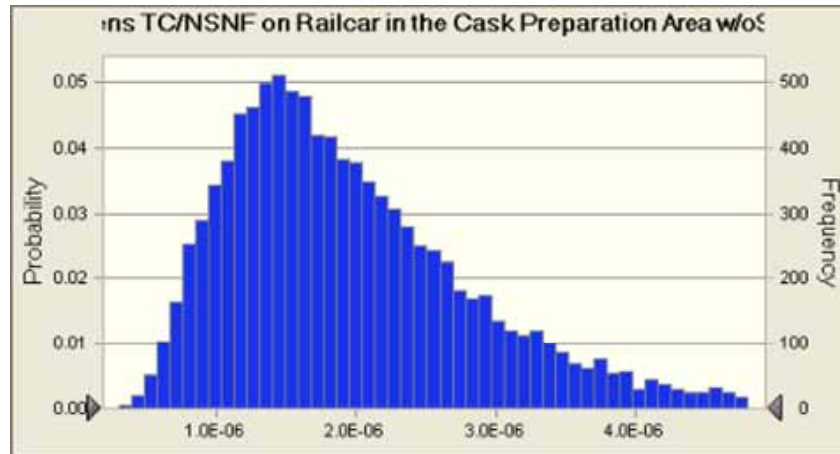
Forecast values

0%	1.7E-09
10%	5.8E-09
20%	7.2E-09
30%	8.4E-09
40%	9.5E-09
50%	1.1E-08
60%	1.2E-08
70%	1.4E-08
80%	1.6E-08
90%	2.0E-08
100%	6.3E-08

Forecast: Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/oSPM (No Diesel Present) Cell: K153

Summary:

Entire range is from 3.1E-07 to 1.1E-05
 Base case is 1.8E-06
 After 10,000 trials, the std. error of the mean is 1.0E-08



Statistics:

	Forecast values
Trials	10,000
Mean	2.0E-06
Median	1.8E-06
Mode	2.1E-06
Standard Deviation	1.0E-06
Variance	9.9E-13
Skewness	1.62
Kurtosis	7.86
Coeff. of Variability	0.4970
Minimum	3.1E-07
Maximum	1.1E-05
Range Width	1.0E-05
Mean Std. Error	1.0E-08

Forecast: Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/oSPM (No Diesel Present) (cont'd) Cell: K153

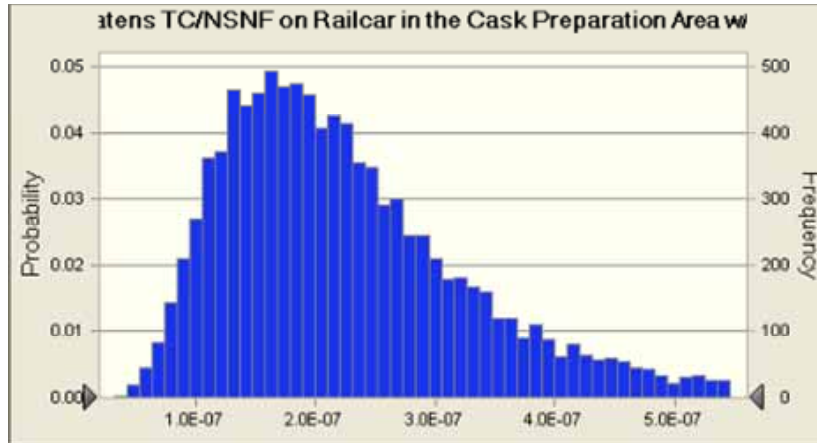
Percentiles:

	Forecast values
0%	3.1E-07
10%	9.8E-07
20%	1.2E-06
30%	1.4E-06
40%	1.6E-06
50%	1.8E-06
60%	2.0E-06
70%	2.3E-06
80%	2.7E-06
90%	3.3E-06
100%	1.1E-05

Forecast: Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/SPM (Diesel Present) Cell: K133

Summary:

Entire range is from 3.2E-08 to 1.2E-06
 Base case is 2.1E-07
 After 10,000 trials, the std. error of the mean is 1.1E-09



Statistics:	Forecast values
Trials	10,000
Mean	2.3E-07
Median	2.1E-07
Mode	2.5E-07
Standard Deviation	1.1E-07
Variance	1.3E-14
Skewness	1.56
Kurtosis	7.42
Coeff. of Variability	0.4932
Minimum	3.2E-08
Maximum	1.2E-06
Range Width	1.1E-06
Mean Std. Error	1.1E-09

Forecast: Localized Fire Threatens TC/NSNF on Railcar in the Cask Preparation Area w/SPM (Diesel Present) (cont'd) Cell: K133

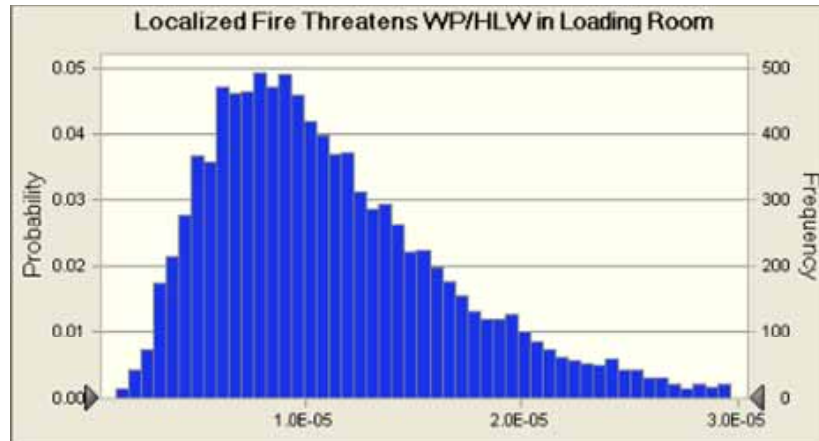
Percentiles:	Forecast values
0%	3.2E-08
10%	1.1E-07
20%	1.4E-07
30%	1.6E-07
40%	1.8E-07
50%	2.1E-07
60%	2.3E-07
70%	2.6E-07
80%	3.1E-07
90%	3.8E-07
100%	1.2E-06

Forecast: Localized Fire Threatens WP/HLW in Loading Room

Cell: M94

Summary:

Entire range is from 1.3E-06 to 6.8E-05
Base case is 1.1E-05
After 10,000 trials, the std. error of the mean is 6.4E-08



Statistics:	Forecast values
Trials	10,000
Mean	1.2E-05
Median	1.0E-05
Mode	1.5E-05
Standard Deviation	6.4E-06
Variance	4.2E-11
Skewness	1.77
Kurtosis	8.92
Coeff. of Variability	0.5566
Minimum	1.3E-06
Maximum	6.8E-05
Range Width	6.6E-05
Mean Std. Error	6.4E-08

Forecast: Localized Fire Threatens WP/HLW in Loading Room (cont'd)

Cell: M94

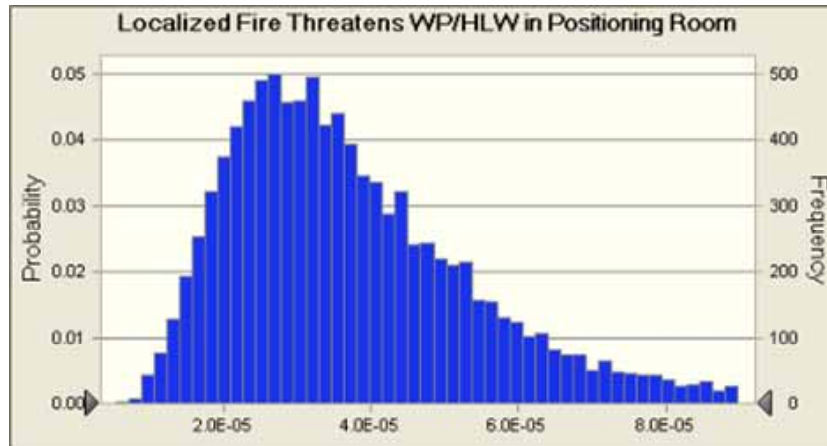
Percentiles:	Forecast values
0%	1.3E-06
10%	5.0E-06
20%	6.5E-06
30%	7.7E-06
40%	8.9E-06
50%	1.0E-05
60%	1.2E-05
70%	1.3E-05
80%	1.6E-05
90%	2.0E-05
100%	6.8E-05

Forecast: Localized Fire Threatens WP/HLW in Positioning Room

Cell: M70

Summary:

Entire range is from 5.5E-06 to 1.9E-04
Base case is 3.5E-05
After 10,000 trials, the std. error of the mean is 1.8E-07



Statistics:

Forecast values

Trials	10,000
Mean	3.8E-05
Median	3.4E-05
Mode	4.4E-05
Standard Deviation	1.8E-05
Variance	3.4E-10
Skewness	1.57
Kurtosis	7.55
Coeff. of Variability	0.4832
Minimum	5.5E-06
Maximum	1.9E-04
Range Width	1.8E-04
Mean Std. Error	1.8E-07

Forecast: Localized Fire Threatens WP/HLW in Positioning Room (cont'd)

Cell: M70

Percentiles:

Forecast values

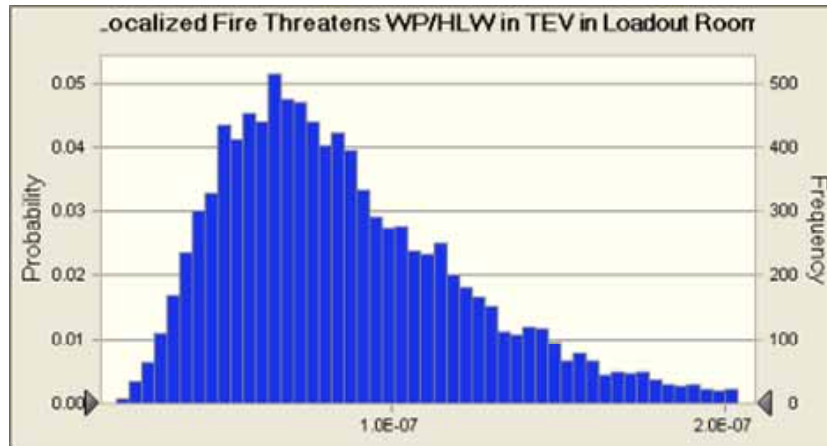
0%	5.5E-06
10%	1.9E-05
20%	2.3E-05
30%	2.7E-05
40%	3.1E-05
50%	3.4E-05
60%	3.8E-05
70%	4.4E-05
80%	5.1E-05
90%	6.2E-05
100%	1.9E-04

Forecast: Localized Fire Threatens WP/HLW in TEV in Loadout Room

Cell: M32

Summary:

Entire range is from 1.7E-08 to 4.0E-07
 Base case is 8.0E-08
 After 10,000 trials, the std. error of the mean is 4.1E-10



Statistics:

Forecast values

Trials	10,000
Mean	8.8E-08
Median	7.9E-08
Mode	8.0E-08
Standard Deviation	4.1E-08
Variance	1.7E-15
Skewness	1.48
Kurtosis	6.89
Coeff. of Variability	0.4723
Minimum	1.7E-08
Maximum	4.0E-07
Range Width	3.8E-07
Mean Std. Error	4.1E-10

Forecast: Localized Fire Threatens WP/HLW in TEV in Loadout Room (cont'd)

Cell: M32

Percentiles:

Forecast values

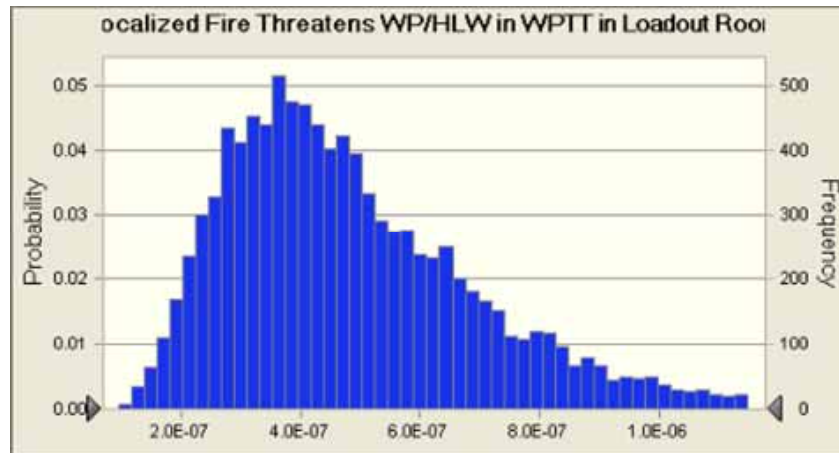
0%	1.7E-08
10%	4.5E-08
20%	5.4E-08
30%	6.3E-08
40%	7.1E-08
50%	7.9E-08
60%	8.9E-08
70%	1.0E-07
80%	1.2E-07
90%	1.4E-07
100%	4.0E-07

Forecast: Localized Fire Threatens WP/HLW in WPTT in Loadout Room

Cell: M18

Summary:

Entire range is from 9.5E-08 to 2.2E-06
Base case is 4.5E-07
After 10,000 trials, the std. error of the mean is 2.3E-09



Statistics:

Forecast values

Trials	10,000
Mean	4.9E-07
Median	4.5E-07
Mode	4.5E-07
Standard Deviation	2.3E-07
Variance	5.5E-14
Skewness	1.48
Kurtosis	6.89
Coeff. of Variability	0.4723
Minimum	9.5E-08
Maximum	2.2E-06
Range Width	2.1E-06
Mean Std. Error	2.3E-09

Forecast: Localized Fire Threatens WP/HLW in WPTT in Loadout Room (cont'd)

Cell: M18

Percentiles:

Forecast values

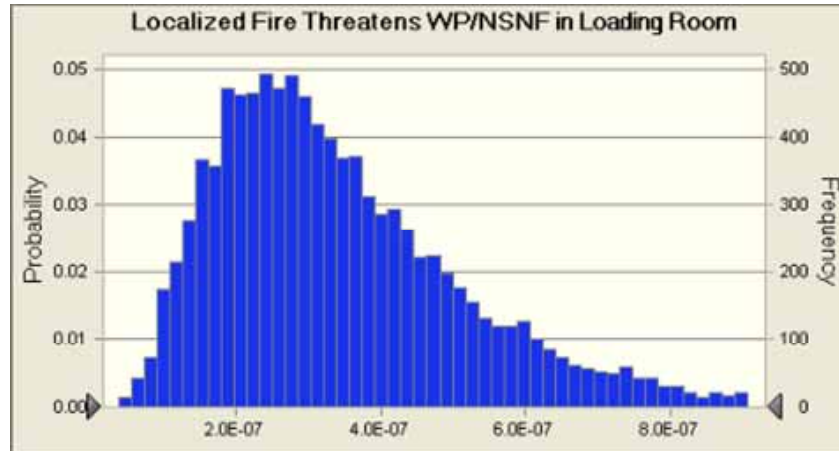
0%	9.5E-08
10%	2.5E-07
20%	3.1E-07
30%	3.5E-07
40%	4.0E-07
50%	4.5E-07
60%	5.0E-07
70%	5.7E-07
80%	6.6E-07
90%	8.0E-07
100%	2.2E-06

Forecast: Localized Fire Threatens WP/NSNF in Loading Room

Cell: K93

Summary:

Entire range is from 3.9E-08 to 2.1E-06
Base case is 3.2E-07
After 10,000 trials, the std. error of the mean is 2.0E-09



Statistics:

Forecast values

Trials	10,000
Mean	3.5E-07
Median	3.1E-07
Mode	4.5E-07
Standard Deviation	2.0E-07
Variance	3.9E-14
Skewness	1.77
Kurtosis	8.92
Coeff. of Variability	0.5566
Minimum	3.9E-08
Maximum	2.1E-06
Range Width	2.0E-06
Mean Std. Error	2.0E-09

Forecast: Localized Fire Threatens WP/NSNF in Loading Room (cont'd)

Cell: K93

Percentiles:

Forecast values

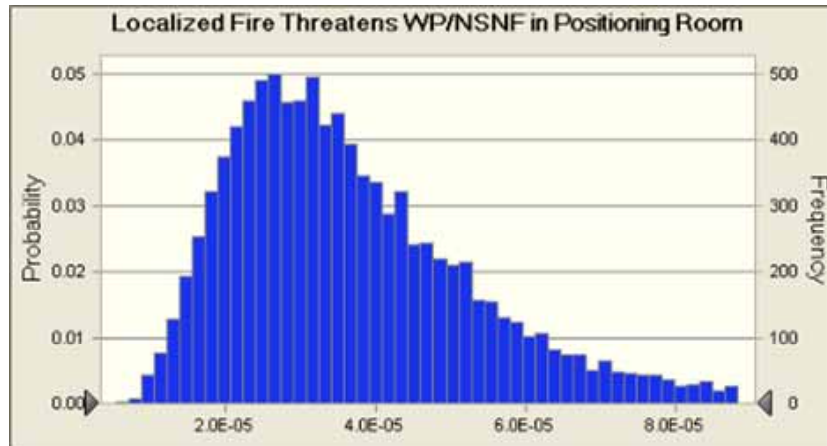
0%	3.9E-08
10%	1.5E-07
20%	2.0E-07
30%	2.4E-07
40%	2.7E-07
50%	3.1E-07
60%	3.6E-07
70%	4.1E-07
80%	4.8E-07
90%	6.0E-07
100%	2.1E-06

Forecast: Localized Fire Threatens WP/NSNF in Positioning Room

Cell: K69

Summary:

Entire range is from 5.4E-06 to 1.9E-04
Base case is 3.4E-05
After 10,000 trials, the std. error of the mean is 1.8E-07



Statistics:

Forecast values

Trials	10,000
Mean	3.8E-05
Median	3.4E-05
Mode	4.4E-05
Standard Deviation	1.8E-05
Variance	3.3E-10
Skewness	1.57
Kurtosis	7.55
Coeff. of Variability	0.4832
Minimum	5.4E-06
Maximum	1.9E-04
Range Width	1.8E-04
Mean Std. Error	1.8E-07

Forecast: Localized Fire Threatens WP/NSNF in Positioning Room (cont'd)

Cell: K69

Percentiles:

Forecast values

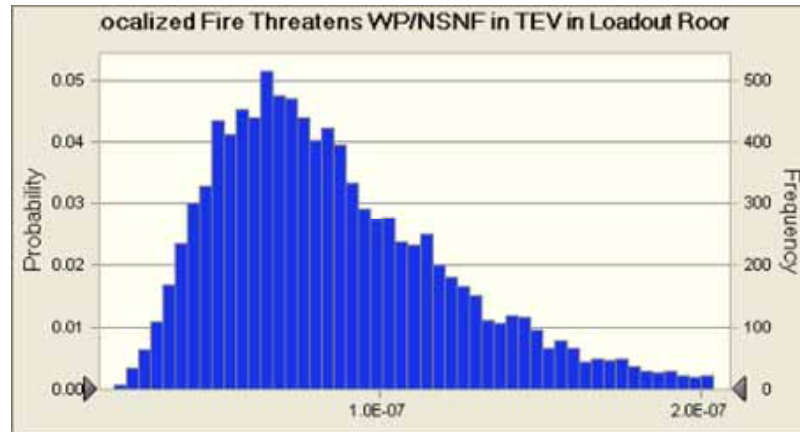
0%	5.4E-06
10%	1.9E-05
20%	2.3E-05
30%	2.6E-05
40%	3.0E-05
50%	3.4E-05
60%	3.8E-05
70%	4.3E-05
80%	5.0E-05
90%	6.1E-05
100%	1.9E-04

Forecast: Localized Fire Threatens WP/NSNF in TEV in Loadout Room

Cell: K31

Summary:

Entire range is from 1.7E-08 to 4.0E-07
Base case is 8.0E-08
After 10,000 trials, the std. error of the mean is 4.1E-10



Statistics:

	Forecast values
Trials	10,000
Mean	8.8E-08
Median	7.9E-08
Mode	8.0E-08
Standard Deviation	4.1E-08
Variance	1.7E-15
Skewness	1.48
Kurtosis	6.89
Coeff. of Variability	0.4723
Minimum	1.7E-08
Maximum	4.0E-07
Range Width	3.8E-07
Mean Std. Error	4.1E-10

Forecast: Localized Fire Threatens WP/NSNF in TEV in Loadout Room (cont'd)

Cell: K31

Percentiles:

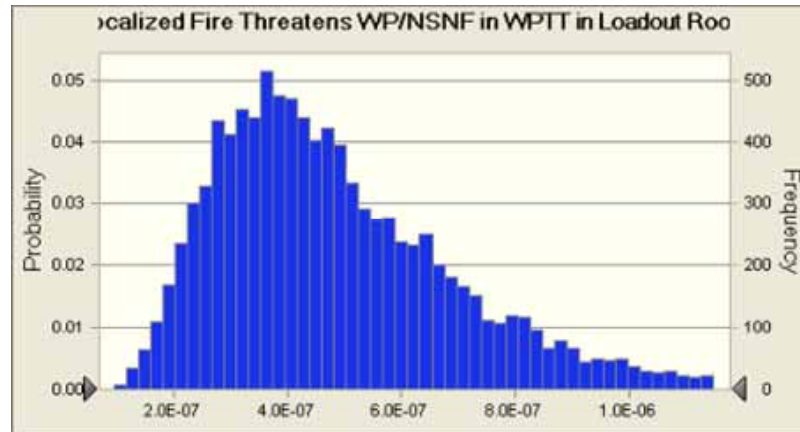
	Forecast values
0%	1.7E-08
10%	4.5E-08
20%	5.4E-08
30%	6.3E-08
40%	7.1E-08
50%	7.9E-08
60%	8.9E-08
70%	1.0E-07
80%	1.2E-07
90%	1.4E-07
100%	4.0E-07

Forecast: Localized Fire Threatens WP/NSNF in WPTT in Loadout Room

Cell: K17

Summary:

Entire range is from 9.5E-08 to 2.2E-06
Base case is 4.5E-07
After 10,000 trials, the std. error of the mean is 2.3E-09



Statistics:

Forecast values

Trials	10,000
Mean	4.9E-07
Median	4.5E-07
Mode	4.5E-07
Standard Deviation	2.3E-07
Variance	5.5E-14
Skewness	1.48
Kurtosis	6.89
Coeff. of Variability	0.4723
Minimum	9.5E-08
Maximum	2.2E-06
Range Width	2.1E-06
Mean Std. Error	2.3E-09

Forecast: Localized Fire Threatens WP/NSNF in WPTT in Loadout Room (cont'd)

Cell: K17

Percentiles:

Forecast values

0%	9.5E-08
10%	2.5E-07
20%	3.1E-07
30%	3.5E-07
40%	4.0E-07
50%	4.5E-07
60%	5.0E-07
70%	5.7E-07
80%	6.6E-07
90%	8.0E-07
100%	2.2E-06

Assumptions

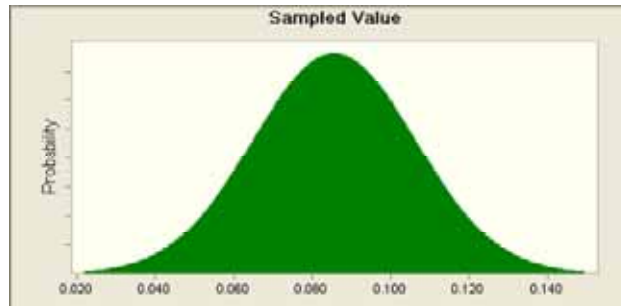
Worksheet: [IHF Fire Frequency - no suppression.xls]Ignition Source Frequency

Assumption: Sampled Value

Cell: H2

Normal distribution with parameters:

Mean	0.086	(=I2)
97.5%	0.126	(=J2)

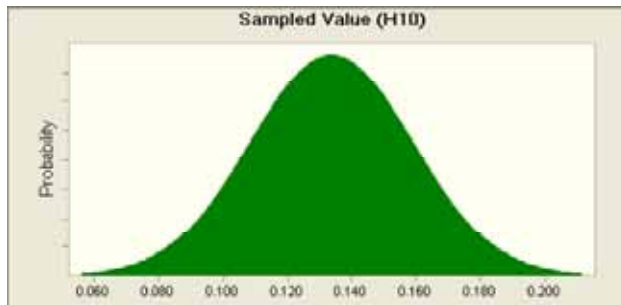


Assumption: Sampled Value (H10)

Cell: H10

Normal distribution with parameters:

Mean	0.134	(=I10)
97.5%	0.183	(=J10)

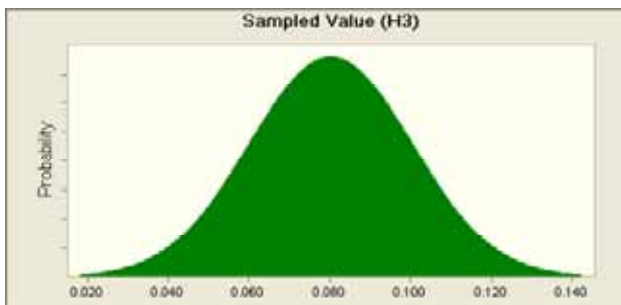


Assumption: Sampled Value (H3)

Cell: H3

Normal distribution with parameters:

Mean	0.080	(=I3)
97.5%	0.120	(=J3)

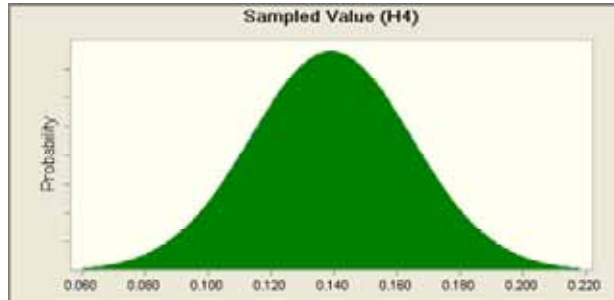


Assumption: Sampled Value (H4)

Cell: H4

Normal distribution with parameters:

Mean	0.139	(=I4)
97.5%	0.189	(=J4)

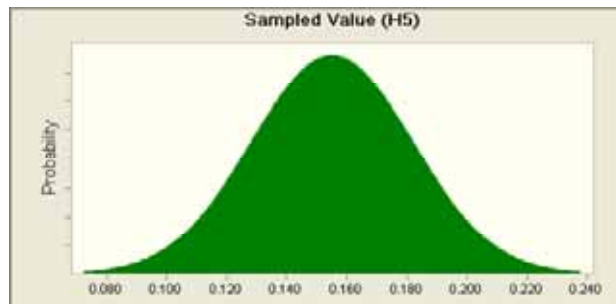


Assumption: Sampled Value (H5)

Cell: H5

Normal distribution with parameters:

Mean	0.155	(=I5)
97.5%	0.207	(=J5)

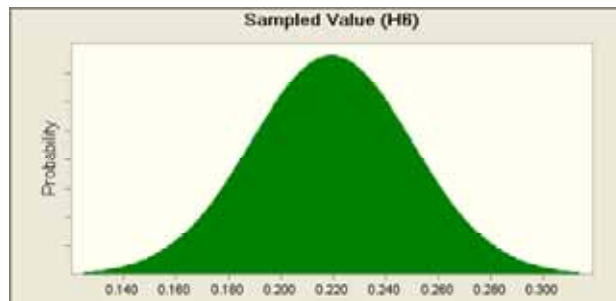


Assumption: Sampled Value (H6)

Cell: H6

Normal distribution with parameters:

Mean	0.219	(=I6)
97.5%	0.279	(=J6)

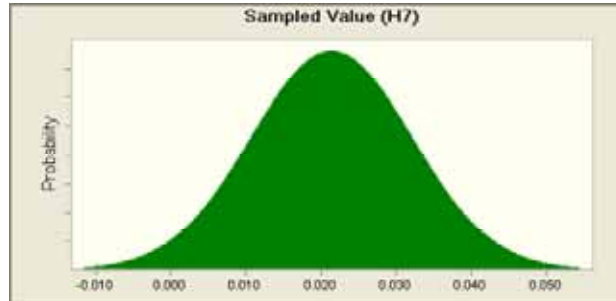


Assumption: Sampled Value (H7)

Cell: H7

Normal distribution with parameters:

Mean	0.021	(=I7)
97.5%	0.042	(=J7)

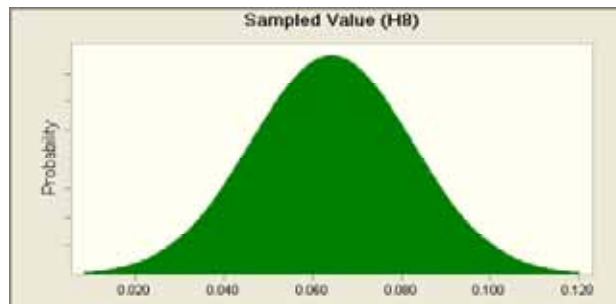


Assumption: Sampled Value (H8)

Cell: H8

Normal distribution with parameters:

Mean	0.064	(=I8)
97.5%	0.100	(=J8)

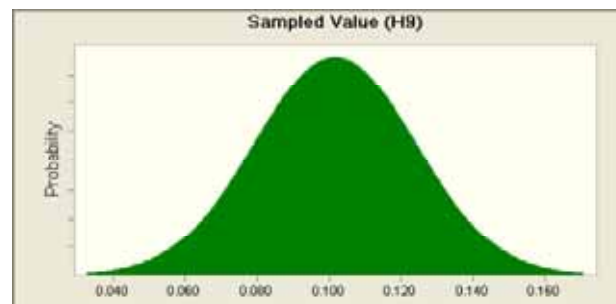


Assumption: Sampled Value (H9)

Cell: H9

Normal distribution with parameters:

Mean	0.102	(=I9)
97.5%	0.145	(=J9)



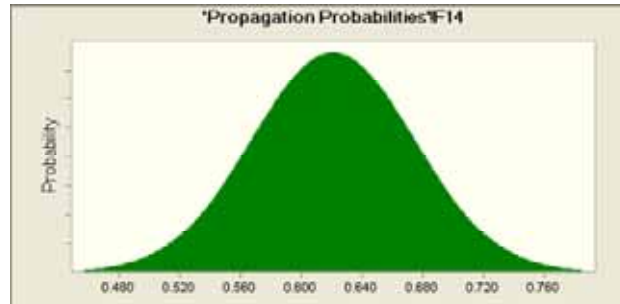
Worksheet: [IHF Fire Frequency - no suppression.xls]Propagation Probabilities

Assumption: F14

Cell: F14

Normal distribution with parameters:

Mean	0.621	(=G14)
97.5%	0.725	(=H14)

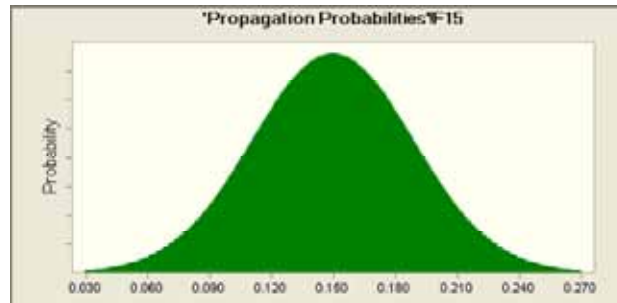


Assumption: F15

Cell: F15

Normal distribution with parameters:

Mean	0.149	(=G15)
97.5%	0.226	(=H15)

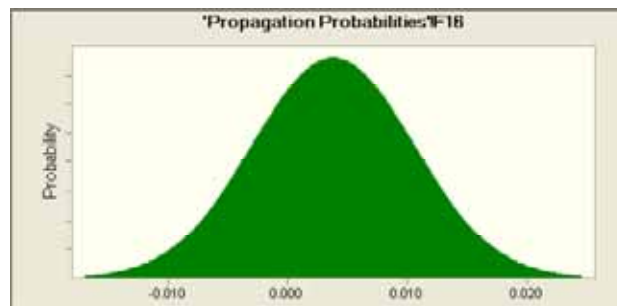


Assumption: F16

Cell: F16

Normal distribution with parameters:

Mean	0.004	(=G16)
97.5%	0.017	(=H16)

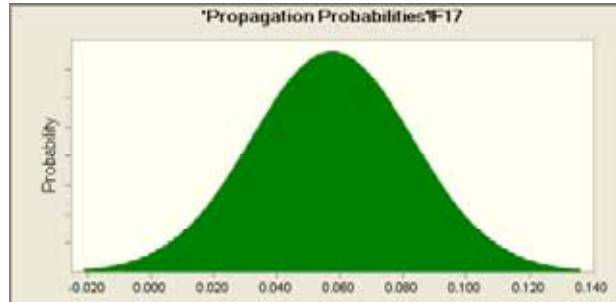


Assumption: F17

Cell: F17

Normal distribution with parameters:

Mean	0.057	(=G17)
97.5%	0.107	(=H17)

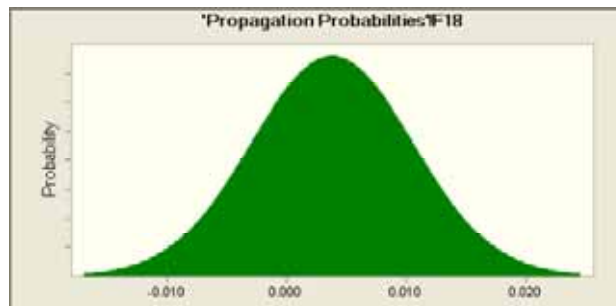


Assumption: F18

Cell: F18

Normal distribution with parameters:

Mean	0.004	(=G18)
97.5%	0.017	(=H18)

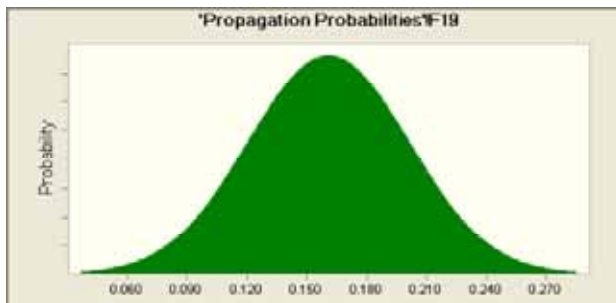


Assumption: F19

Cell: F19

Normal distribution with parameters:

Mean	0.161	(=G19)
97.5%	0.240	(=H19)

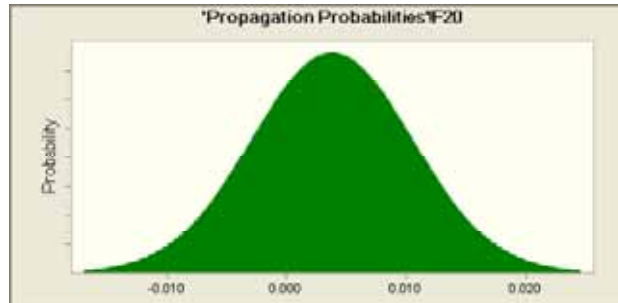


Assumption: F20

Cell: F20

Normal distribution with parameters:

Mean	0.004	(=G20)
97.5%	0.017	(=H20)



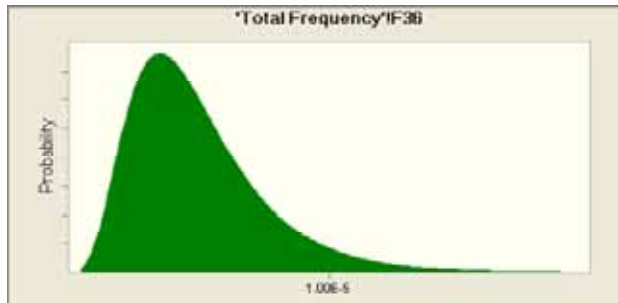
Worksheet: [IHF Fire Frequency - no suppression.xls]Total Frequency

Assumption: F36

Cell: F36

Lognormal distribution with parameters:

50%	4.79E-6	(=G36)
97.5%	1.14E-5	(=I36)



End of Assumptions

ATTACHMENT G
EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES

ATTACHMENT G

EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES

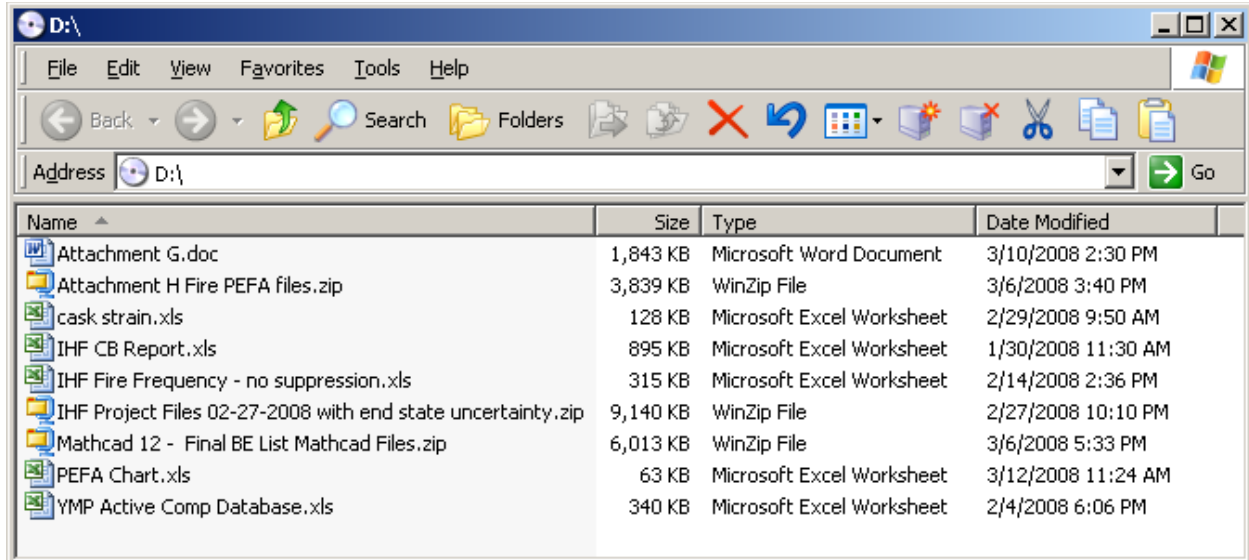
Attachment G contains the event sequence quantification summary table (Table G-1) referenced by Section 6.7. It also contains Table G-2, *Event Sequence Grouping and Categorization*; Table G-3, *Beyond Category 2 Final Event Sequences Summary*; and Table G-4, *Important to Criticality Final Event Sequences 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.

ATTACHMENT H
SAPPHIRE 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.



Name	Size	Type	Date Modified
Attachment G.doc	1,843 KB	Microsoft Word Document	3/10/2008 2:30 PM
Attachment H Fire PEFA files.zip	3,839 KB	WinZip File	3/6/2008 3:40 PM
cask strain.xls	128 KB	Microsoft Excel Worksheet	2/29/2008 9:50 AM
IHF CB Report.xls	895 KB	Microsoft Excel Worksheet	1/30/2008 11:30 AM
IHF Fire Frequency - no suppression.xls	315 KB	Microsoft Excel Worksheet	2/14/2008 2:36 PM
IHF Project Files 02-27-2008 with end state uncertainty.zip	9,140 KB	WinZip File	2/27/2008 10:10 PM
Mathcad 12 - Final BE List Mathcad Files.zip	6,013 KB	WinZip File	3/6/2008 5:33 PM
PEFA Chart.xls	63 KB	Microsoft Excel Worksheet	3/12/2008 11:24 AM
YMP Active Comp Database.xls	340 KB	Microsoft Excel Worksheet	2/4/2008 6:06 PM