NUREG/CP-0303 EPRI 3002005205
Volume 1 of 5

Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES)-2012

Volume 1
Module 1: Probabilistic Risk Analysis (PRA)

Based on the Joint
NRC-RES/EPRI Training Workshops
Conducted in 2012

Weeks of July 16 and September 24, 2012

Bethesda, MD

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

Electric Power Research Institute
3420 Hillview Avenue
Palo Alto, CA 94304

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop IDCC
   Washington, DC 20402-0001
   Internet: bookstore.gpo.gov
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Rd., Alexandria, VA 22312-0002
   www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES)-2012

NRC-RES/EPRI Fire PRA Workshop
Volume 1: Module 1: PRA

NUREG/CP-0303
Volume 1 of 5

EPRI 3002005205

Manuscript Completed: July 2015
Date Published: April 2016

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research (RES)
Washington, DC 20555-0001

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304

U.S. NRC-RES Project Manager
M. H. Salley

EPRI Project Manager
A. Lindeman

ORGANIZATION THAT PREPARED THIS DOCUMENT:

U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or
e-mail askepri@epri.com.

COURSE TRAINING INSTRUCTORS AND PROJECT MANAGERS

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

Susan Cooper – Module 4 HRA

Gabriel Taylor – Module 2 Electrical Analysis

Sandia National Laboratories
1515 Eubank SE
Albuquerque, NM 87185

Steven Nowlen – Module 3 Fire Analysis

Jeff LaChance – Module 1 PRA

National Institute of Standards and Technology
100 Bureau Dr.
Gaithersburg, MD 20899

Kevin McGrattan – Module 5 Adv. Fire Modeling

Electric Power Research Institute
3420 Hillview Avenue
Palo Alto, CA 94303

Stuart Lewis – Module 4 HRA

Science Applications International Corp.
1671 Dell Ave, Suite 100
Campbell, CA 95008

Bijan Najafi

Francisco Joglar-Biloch – Module 3 Fire Analysis

Dan Funk (EDAN Engineering) – Module 2 Electrical

Richard Anoba (Anoba Consulting Services)–Module 1 PRA

Erin Collins –Module 4 HRA

Fred Mowrer (California Polytechnic State University) – Module 5 Adv. Fire Modeling

Kendra Wright /Nicholas Melly
U.S. NRC-RES Project Managers

Ashley Lindeman
EPRI Project Manager

CITATIONS

This report was prepared by:

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

Principal Investigators:

F. Gonzalez
K. Hamburger
T. Rivera
P. Smith
D. Stroup
K. Wright

This report describes research sponsored jointly by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research and EPRI.

The report is a corporate document that should be cited in the literature in the following manner:

Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES)-2012, NRC-RES/EPRI Fire PRA Workshop, Volume 1: Overall Course and Module 1: PRA, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC 20555-0001, and Electric Power Research Institute, Palo Alto, CA, NUREG/CP-0303 and EPRI 3002005205.

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) and the Electric Power Research Institute (EPRI) working under a memorandum of understanding (MOU) jointly conducted two sessions of the NRC– RES/EPRI Fire Probabilistic Risk Assessment (PRA) Workshop on July 16–20, 2012, and September 24–28, 2012, at the Bethesda Marriott in Bethesda, MD. The purpose of the workshop was to provide detailed, hands-on training on the fire PRA methodology described in the technical document, NUREG/CR-6850 (EPRI 1011989) entitled "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities." This fire PRA methodology document supports implementation of the risk-informed, performance-based rule in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.48(c) endorsing National Fire Protection Association (NFPA) Standard 805, as well as other applications such as exemptions or deviations to the agency's current regulations and fire protection significance determination process (SDP) phase 3 applications.

RES and EPRI provided training in five subject areas related to fire PRA, namely: fire PRA, electrical analysis, fire analysis, fire human reliability analysis (HRA), and advanced fire modeling. Participants selected one of these subject areas and spent the duration of the course in that module. The HRA module reviewed guidance provided in NUREG-1921 (EPRI 1023001), "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines," while the fire modeling module reviewed the fire modeling guidance provided in NUREG-1934 (EPRI 1019195), "Nuclear Power Plant Fire Modeling Application Guide." For each technical area, the workshop also included a 1-day module introducing the fundamentals of the subject. The purpose of the fundamentals modules was to assist students without an extensive background in the technical area in understanding the in-depth training modules that followed. Attendance in the fundamentals modules was optional. The workshop's format allowed for in-depth presentations and practical examples directed toward the participant's area of interest.

This NUREG/CP documents both of the two sessions of the NRC-RES/EPRI Fire PRA Workshop delivered in 2012 and includes the slides and handout materials delivered in each module of the course as well as video recordings of the training that was delivered. This NUREG/CP can be used as an alternative training method for those who were unable to physically attend the training sessions. This report can also serve as a refresher for those who attended one or more training sessions and could also be useful preparatory material for those planning to attend future sessions.

<u>NRC Disclaimer:</u>

This document's text and video content are intended solely for use as training tools. No portions of their content are intended to represent NRC's conclusions or regulatory positions, and they should not be interpreted as such.

CONTENTS

FIGURES

ACKNOWLEDGMENTS

The authors of this report greatly appreciate the contributions made by instructors and students at the 2012 NRC-RES/EPRI Fire PRA Workshop.

In addition, we want to extend our gratitude to Tojuana Fortune-Grasty (NRC's publications analyst) and the NRC's printing specialist's team whose invaluable support and expertise were critical to ensuring the published report's quality. We also extend a special thanks and appreciation to Anita Aikins-Afful (RES/DRA administrative assistant) for providing the technical edit of this report.

ACRONYMS

ACB	Air-cooled Circuit Breaker
ACRS	Advisory Committee on Reactor Safeguards
AEP	Abnormal Event Procedure
AFW	Auxiliary Feedwater
AGS	Assistant General Supervisor
AOP	Abnormal Operating Procedure
AOV	Air Operated Valve
ASEP	Accident Sequence Evaluation Program
ATHEANA	A Technique for Human Event Analysis
ATS	Automatic Transfer Switch
ATWS	Anticipated Transient Without Scram
BAT	Boric Acid Tank
BNL	Brookhaven National Laboratory
BWR	Boiling-Water Reactor
CBDT	Cause-Based Decision Tree
CCDP	Conditional Core Damage Probability
CF	Cable (Configuration) Factors
CCPS	Center for Chemical Process Safety
CCW	Component Cooling Water
CDF	Core Damage Frequency
CFD	Computational Fluid Dynamics
CFR	Code of Federal Regulations
CLERP	Conditional Large Early Release Probability
CM	Corrective Maintenance
CR	Control Room
CRS	Cable and Raceway (Database) System
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
CWP	Circulating Water Pump
DC	Direct Current
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EDS	Electrical Distribution System
EF	Error Factor
EI	Erroneous Status Indicator
EOP	Emergency Operating Procedure
EPR	Ethylene-Propylene Rubber
EPRI	Electric Power Research Institute
ET	Event Tree
FEDB	Fire Events Database
FEP	Fire Emergency Procedure

FHA	Fire Hazards Analysis
FIVE	Fire-Induced Vulnerability Evaluation (EPRI TR 100370)
FMRC	Factory Mutual Research Corporation
FPRAIG	Fire PRA Implementation Guide (EPRI TR 105928)
FRSS	Fire Risk Scoping Study (NUREG/CR-5088)
FSAR	Final Safety Analysis Report
HCR	Human Cognitive Reliability
HEAF	High Energy Arcing Fault
HEP	Human Error Probability
HFE	Human Failure Event
HPI	High-Pressure Injection
HPCI	High-Pressure Coolant Injection
HRA	Human Reliability Analysis
HRR	Heat Release Rate
HTGR	High-Temperature Gas-cooled Reactor
HVAC	Heating, Ventilation, and Air Conditioning
ICDP	Incremental Core Damage Probability
ILERP	Incremental Large Early Release Probability
INPO	Institute for Nuclear Power Operations
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination of External Events
IS	Ignition Source
ISLOCA	Interfacing Systems Loss of Coolant Accident
KS	Key Switch
LCO	Limiting Condition of Operation
LERF	Large Early Release Frequency
LFL	Lower Flammability Limit
LOC	Loss of Control
LOCA	Loss-of-Coolant Accident
LPG	Liquefied Petroleum Gas
LP/SD	Low Power and Shutdown
LWGR	Light-Water-cooled Graphite Reactors (Russian design)
MCB	Main Control Board
MCC	Motor Control Center
MCR	Main Control Room
MG	Motor-Generator
MFW	Main Feedwater
MOV	Motor-Operated Valve
MQH	McCaffrey, Quintiere, and Harkleroad's Method
MS	Main Steam
MSIV	Main Steam Isolation Valve
NC	No Consequence
NEI	Nuclear Energy Institute
NEIL	Nuclear Electric Insurance Limited
NFPA	National Fire Protection Association

NPP	Nuclear Power Plant
NPSH	Net Positive Suction Head
NQ cable	Non-Qualified (IEEE-383) cable
NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
P&ID	Piping and Instrumentation Diagram
PE	Polyethylene
PM	Preventive Maintenance
PMMA	Polymethyl Methacrylate
PORV	Power-Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factor
PTS	Pressurized Thermal Shock
PVC	Polyvinyl Chloride
PWR	Pressurized Water Reactor
Q cable	Qualified (IEEE-383) cable
RBMK	Reactor Bolshoy Moshchnosty Kanalny (high-power channel reactor)
RCIC	Reactor Core Isolation Cooling
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RDAT	Computer program for Bayesian analysis
RES	Office of Nuclear Regulatory Research (at NRC)
RHR	Residual Heat Removal
RI/PB	Risk-Informed / Performance-Based
RPS	Reactor Protection System
RWST	Refueling Water Storage Tank
SCBA	Self-Contained Breathing Apparatus
SDP	Significance Determination Process
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SMA	Seismic Margin Assessment
SNPP	Simplified Nuclear Power Plant
SO	Spurious Operation
SOV	Solenoid Operated Valve
SPAR-H	Standardized Plant Analysis Risk HRA
SRV	Safety Relief Valve
SSD	Safe Shutdown
SSEL	Safe Shutdown Equipment List
SST	Station Service Transformer
SUT	Start-up Transformer
SW	Service Water
SWGR	Switchgear
T/G	Turbine/Generator
T-H	Thermal Hydraulic
THERP	Technique for Human Error Rate Prediction

TGB	Turbine-Generator Building
TSP	Transfer Switch Panel
UAT	Unit Auxiliary Transformer
VCT	Volume Control Tank
VTT	Valtion Teknillinen Tutkimuskeskus (Technical Research Centre of Finland)
VVER	The Soviet (now Russian Federation) designation for light-water pressurized reactor
XLPE	Cross-Linked Polyethylene
ZOI	Zone of Influence

1

INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) approved the risk-informed and performance-based alternative regulation in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.48(c) in July 2004, which allows licensees the option of using fire protection requirements contained in the National Fire Protection Association (NFPA) Standard 805, “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants, 2001 Edition,” with certain exceptions. To support licensees’ use of that option, the NRC’s Office of Nuclear Regulatory Research (RES) and the Electric Power Research Institute (EPRI) jointly issued NUREG/CR-6850 (EPRI 1011989), “Fire PRA Methodology for Nuclear Power Facilities,” in September 2005. That report documents state-of-the art methods, tools, and data for conducting a fire probabilistic risk assessment (PRA) in a commercial nuclear power plant (NPP) application. This report is intended to serve the needs of a fire risk analysis team by providing a general framework for conducting the overall analysis, as well as specific recommended practices to address each key aspect of the analysis. Participants from the U.S. nuclear power industry supported demonstration analyses and provided peer review of the program. Methodological issues raised in past fire risk analyses, including the Individual Plant Examination of External Events (IPEEE), are addressed to the extent allowed by the current state-of-the-art and the overall project scope. Although the primary objective of the report is to consolidate existing state-of-the-art methods, in many areas, the newly documented methods represent a significant advance over previous methods.

NUREG/CR-6850 does not constitute regulatory requirements, and the NRC’s participation in the study neither constitutes nor implies regulatory approval of applications based on the analysis contained in that document. The analyses and methods documented in that report represent the combined efforts of individuals from RES and EPRI. Both organizations provided specialists in the use of fire PRA to support this work. However, the results from that combined effort do not constitute either a regulatory position or regulatory guidance.

In addition, NUREG/CR-6850 can be used for risk-informed, performance-based approaches and insights to support fire protection regulatory decision making in general.

However, it is not sufficient to merely develop a potentially useful method, such as NUREG/CR- 6850, and announce its availability. It is also necessary to teach potential users how to properly use the method. To meet this need RES and EPRI have collaboratively conducted the NRC-RES/EPRI Fire PRA Workshops to train interested parties in the application of this methodology since 2005. The course is provided in five parallel modules covering tasks from NUREG/CR-6850 “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities” Reference [1].

These five training modules are:

- Module 1: PRA/Systems Analysis – This module covers the technical tasks for development of the system response to a fire including human failure events. Specifically, this module covers Tasks/Sections 2, 4, 5, 7, 14, and 15 of Reference [1].

- Module 2: Electrical Analysis – This module covers the technical tasks for analysis of electrical failures as the result of a fire. Specifically, this module covers Tasks/Sections 3, 9, and 10 of Reference [1].

- Module 3: Fire Analysis – This module covers technical tasks involved in development of fire scenarios from initiation to target (e.g., cable) impact. Specifically, this module covers Tasks/Sections 1, 6, 8, 11, and 13 of Reference [1].

- Module 4: Fire Human Reliability Analysis – This module covers the technical tasks associated with identifying and analyzing operator actions and performance during a postulated fire scenario. Specifically, this module covers Task 12 as outlined in Reference [1] based on the application of the approaches documented in Reference [2].

- Module 5: Advanced Fire Modeling – This module was added to the training in 2011. It covers the fundamentals of fire science and provides practical implementation guidance for the application of fire modeling in support of a fire PRA. Module 5 covers fire modeling applications for Tasks 8 and 11 as outlined in Reference [1] based on the material presented in Reference [3].

The first three modules are based directly on the "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," EPRI 1011989, and NUREG/CR-6850 [1]. However, that document did not cover fire human reliability analysis (HRA) methods in detail. In 2010, the training materials were enhanced to include a fourth module based on a more recent EPRI/RES collaboration and the then draft guidance document, EPRI 1019196, NUREG-1921 [2] published in late 2009. The training materials are based on this draft document including the consideration of public comments received on the draft report and the team's responses to those comments. In 2011 a fifth training module on Advanced Fire Modeling techniques and concepts was added to the course. This module is based on another joint RES/EPRI collaboration and a draft guidance published in January 2010, NUREG-1934 EPRI 1019195 [3].

In 2012 an additional first day of training was included in the NRC-RES/EPRI Fire PRA Workshop to cover principal elements of each technical area covered in the Fire PRA course, i.e., PRA, HRA, Electrical Analysis, and Fire Analysis. This introductory module was intended to assist in preparing the students to understand the in-depth fire PRA training modules that followed. The introductory modules were not intended to be a substitute for education and/or training in the subject matter. The intent was that they would serve as a primer for those individuals who lacked such training or those who were cross-training in an area other than their primary area of expertise.

The four introductory modules listed below (referred to as Module 0) were offered in parallel on the first day of the workshop.

Module 0a: Principles of PRA
Module 0b: Principles of Electrical Analysis
Module 0c: Principles of Fire Science and Modeling
Module 0d: Principles of HRA

These sub-modules are included in the text and on the accompanying DVDs as a part of their related module.

1.1 About this Text

"Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES) – 2012", is a collection of the materials that were presented at the two sessions of the NRC-RES/EPRI Fire PRA conducted July 16–20, 2012, and September 24-28, 2012.

The 2012 workshop was video recorded and adapted as an alternative training method for those who were unable to physically attend the training sessions. This NUREG/CP is comprised of the materials supporting those videos and includes the five volumes below (the videos are enclosed on DVD in the published paper copies of this NUREG/CP). This material can also serve as a refresher for those who attended one or more of the training sessions, and would be useful preparatory material for those planning to attend a session.

MARIAFIRES is comprised of 5 volumes.

Volume 1 – Module 0a Principles of PRA and Module 1: PRA/Systems Analysis
Volume 2 – Module 0b Principles of Electrical Analysis and Module 2: Electrical Analysis
Volume 3 – Module 0c Principles of Fire Science and Modeling and Module 3: Fire Analysis
Volume 4 – Module 0d Principles of HRA and Module 4: Fire Human Reliability Analysis
Volume 5 – Module 5: Advanced Fire Modeling

Integral to Modules 1, 2 and 3 is a set of hands-on problems based on a conceptual generic nuclear power plant (NPP) developed for training purposes. This generic plant is referred to in this text and in classroom examples as SNPP (Simplified Nuclear Power Plant). The same generic NPP is used in all three modules. Chapter 2 of this document provides the background information for the problem sets of each module, including a general description of the sample power plant and the internal events PRA needed as input to the fire PRA. The generic NPP defined for this training is an extremely simplified one that in many cases does not meet any regulatory requirements or good engineering practices. For training purposes, the design features presented highlight the various aspects of the fire PRA methodology.

For Module 4 and 5, independent sets of examples are used to illustrate key points of the analysis procedures. The examples for these two modules are not tied to the simplified plant. Module 4 uses examples that were derived largely from pilot applications of the proposed fire HRA methods and on independent work of the EPRI and RES HRA teams. The examples for Module 5 were taken directly from Reference [3] and represent a range of typical NPP fire scenarios across a range of complexity and that highlight some of the computation challenges associated with the NPP fire PRA fire modeling applications.

A short description of the Fire PRA technical tasks is provided below. For further details, refer to the individual task descriptions in EPRI 1011989, NUREG/CR-6850, Volume 2. The figure presented at the end of this chapter provides a simplified flow chart for the analysis process and indicates which training module covers each of the analysis tasks.

Plant Boundary Definition and Partitioning (Task 1). The first step in applying the fire PRA methodology is to define the physical boundary of the analysis and to divide the area within that boundary into analysis compartments.

Fire PRA Component Selection (Task 2). The selection of components that are to be credited for plant shutdown following a fire is a critical step in any fire PRA. Components selected would generally include many, but not necessarily all, components credited in the 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating prior to January 1, 1979," post-fire safe shutdown (SSD) analysis. Additional components will likely be selected, potentially including most, but not all, components credited in the plant's internal events PRA. Also, the proposed methodology would likely introduce components beyond either the 10 CFR 50 Appendix R list or the internal events PRA model. Such components are often of interest because of concern for multiple spurious actuations that may threaten the credited functions and components, as well as from concerns about fire effects on instrumentation used by the plant crew to respond to the event.

Fire PRA Cable Selection (Task 3). This task provides instructions and technical considerations associated with identifying cables supporting those components selected in Task 2 above. In previous fire PRA methods (such as EPRI Fire-Induced Vulnerability Evaluation (FIVE) and Fire PRA Implementation Guide), this task was relegated to the SSD analysis and its associated databases. NUREG/CR-6850 (EPRI 1011989) offers a more structured set of rules for selection of cables.

Qualitative Screening (Task 4). This task identifies fire analysis compartments that can be shown, without quantitative analysis, to have little or no risk significance. Fire compartments may be screened out if they contain no components or cables identified in Tasks 2 and 3 and if they cannot lead to a plant trip because of either plant procedures, an automatic trip signal, or technical specification requirements.

Plant Fire-Induced Risk Model (Task 5). This task discusses steps for the development of a logic model that reflects plant response following a fire. Specific instructions have been provided for treatment of fire-specific procedures or plans. These procedures may impact availability of functions and components or include fire-specific operator actions (e.g., self- induced station blackout).

Fire Ignition Frequency (Task 6). This task describes the approach to develop frequency estimates for fire compartments and scenarios. Significant changes from the EPRI FIVE method have been made in this task. The changes generally relate to the use of challenging events, considerations associated with data quality, and increased use of a fully component-based ignition frequency model (as opposed to the location/component-based model used, for example, in FIVE).

Quantitative Screening (Task 7). A fire PRA allows the screening of fire compartments and scenarios based on their contribution to fire risk. This approach considers the cumulative risk associated with the screened compartments (i.e., the ones not retained for detailed analysis) to ensure that a true estimate of fire risk profile (as opposed to vulnerability) is obtained.

Scoping Fire Modeling (Task 8). This step provides simple rules to define and screen fire ignition sources (and therefore fire scenarios) in an unscreened fire compartment.

Detailed Circuit Failure Analysis (Task 9). This task provides an approach and technical considerations for identifying how the failure of specific cables will impact the components included in the fire PRA SSD plant response model.

Circuit Failure Mode Likelihood Analysis (Task 10). This task considers the relative likelihood of various circuit failure modes. This added level of resolution may be a desired option for those fire scenarios that are significant contributors to the risk. The methodology provided in NUREG/CR-6850 (EPRI 1011989) benefits from the knowledge gained from the tests performed in response to the circuit failure issue.

Detailed Fire Modeling (Task 11). This task describes the method to examine the consequences of a fire. This includes consideration of scenarios involving single compartments, multiple fire compartments, and the main control room. Factors considered include initial fire characteristics; fire growth in a fire compartment or across fire compartments; detection and suppression; electrical raceway fire barrier systems, and damage from heat and smoke. Special consideration is given to turbine generator (T/G) fires, hydrogen fires, high-energy arcing faults (HEAF), cable fires, and main control board (MCB) fires. Considerable improvements can be found in the method for this task over the EPRI FIVE and Fire PRA Implementation Guide in nearly all technical areas.

Post-Fire Human Reliability Analysis (Task 12). This task considers operator actions for manipulation of plant components. The analysis task procedure provides structured instructions for identification and inclusion of these actions in the fire PRA. The procedure also provides instructions for estimating screening human error probabilities (HEPs) before detailed fire modeling results (e.g., fire growth and damage behaviors) have necessarily been developed or detailed circuit analyses (e.g., can the circuit spuriously actuate as opposed to simply assuming it can actuate) have been completed. In a fire PRA, the estimation of HEP values with high confidence is critical to the effectiveness of screening. This report does not develop a detailed fire HRA methodology. A number of HRA methods can be adopted for fire with appropriate additional instructions that superimpose fire effects on any of the existing HRA methods such as the Technique for Human Error Rate Prediction (THERP), Causal Based Decision Tree (CBDT), A Technique for Human Event Analysis (ATHEANA), etc. This would improve consistency across analyses (i.e., fire and internal events PRA).

Seismic Fire Interactions (Task 13). This task is a qualitative approach to help identify the risk from any potential interactions between an earthquake and a fire.

Fire Risk Quantification (Task 14). The task summarizes what is to be done for quantification of the fire risk results.

Uncertainty and Sensitivity Analyses (Task 15). This task describes the approach to follow for identifying and treating uncertainties throughout the fire PRA process. The treatment may vary from quantitative estimation and propagation of uncertainties where possible (e.g., in fire frequency and non-suppression probability) to identification of sources without quantitative estimation. The treatment may also include one-at-a-time variation of individual parameter values or modeling approaches to determine the effect on the overall fire risk (i.e., sensitivity analysis).

Fire PRA Documentation (Task 16). This task describes the approach to follow for documenting the Fire PRA process and its results. Figure 1 shows the relationship between the above 16 technical tasks from EPRI 1011989, NUREG/CR-6850, Volume 2.

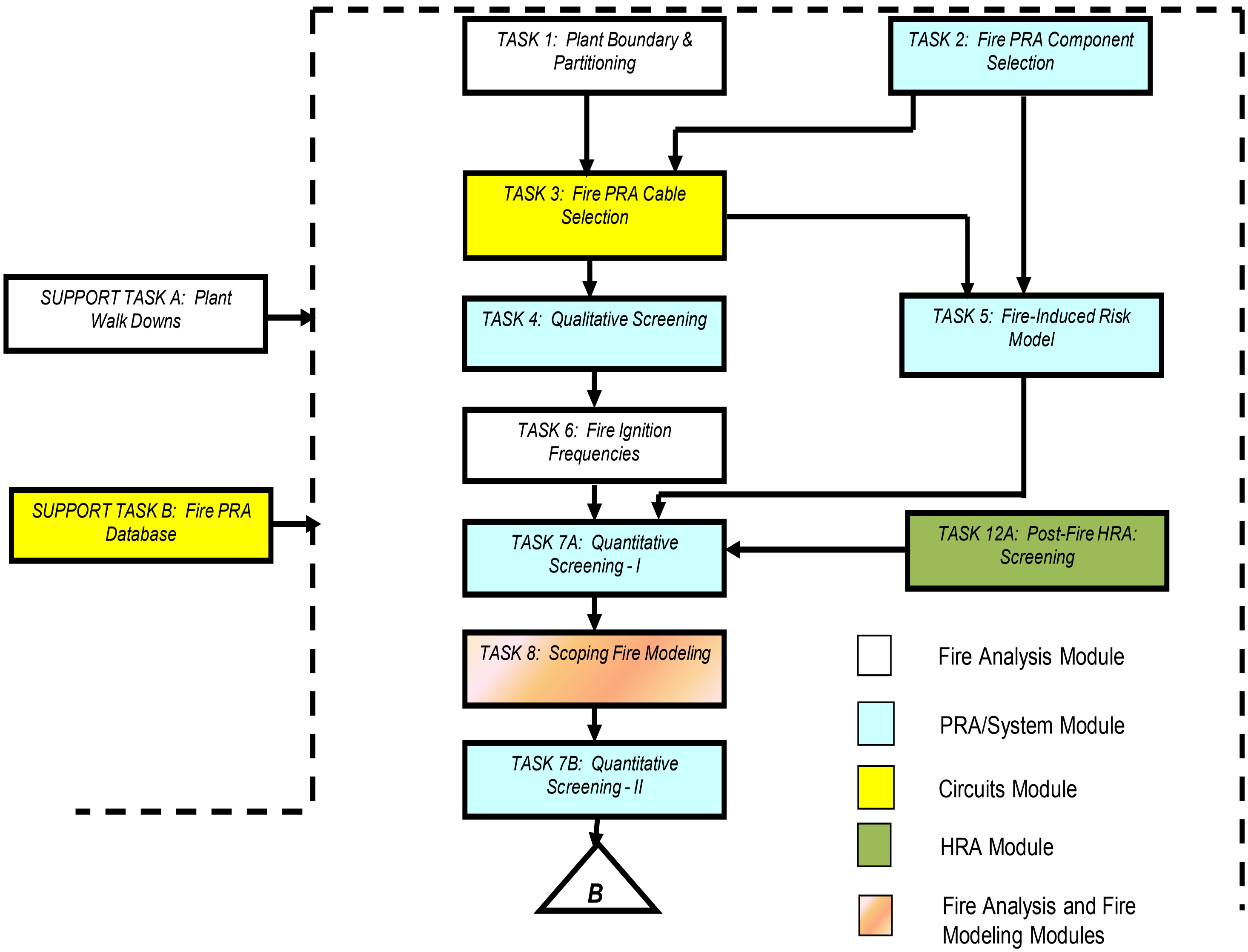


Figure 0-1 Relationship of Technical Tasks in NUREG/CR 6850 Volume 2

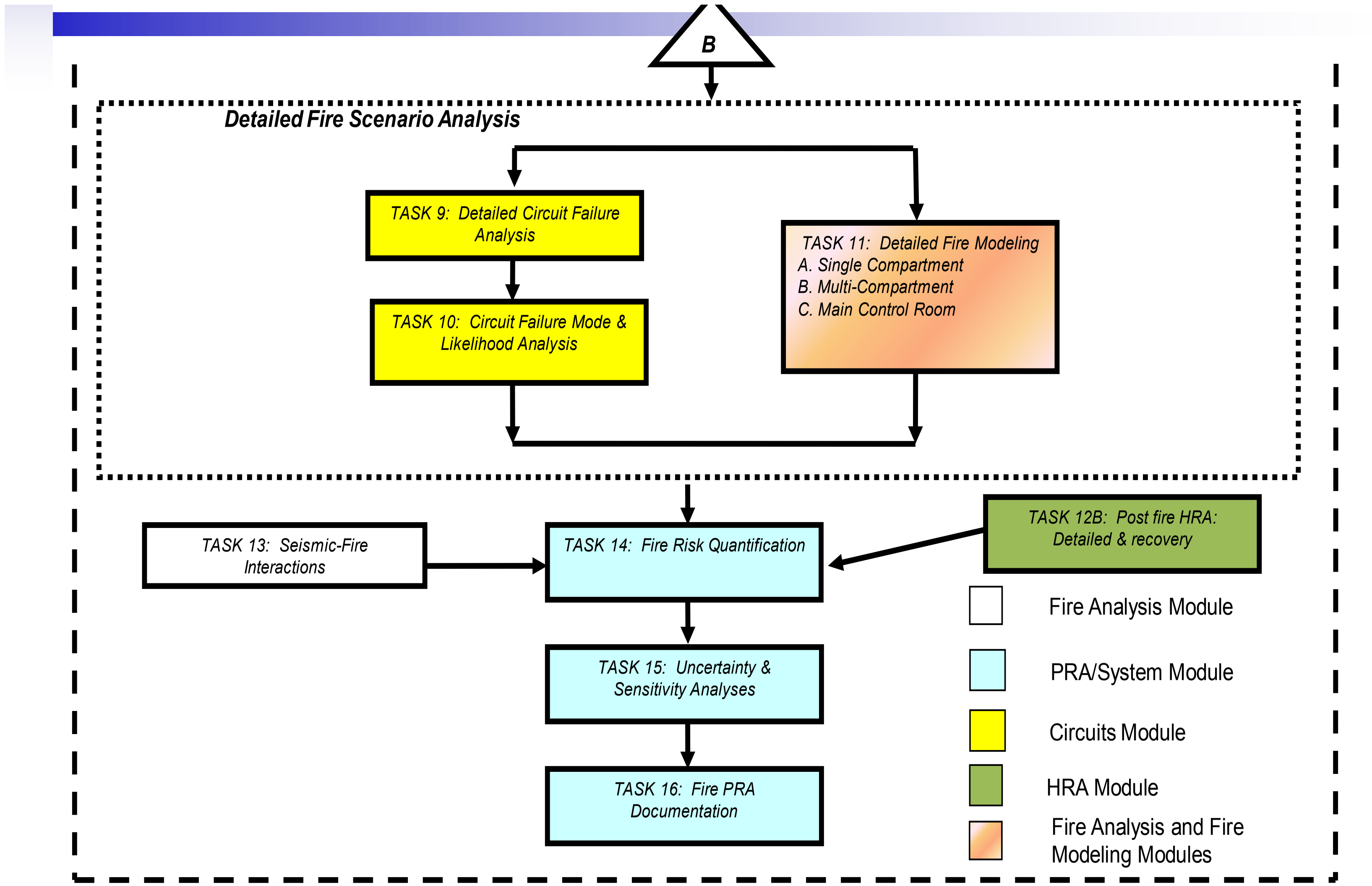


Figure 0-2 Note: "B" is from Task 7B (Previous Page)

References

1. NUREG/CR-6850, EPRI 1011989, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, September 2005.

2. NUREG-1921, EPRI 1023001, *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines*, May 2012.

3. NUREG-1934, EPRI 1023259, *Nuclear Power Plant Fire Modeling Application Guide,* November 2012[1].

[1] At the time of the 2012 NRC-RES/EPRI Fire PRA Workshop, this final report had not yet been published. A draft for public comment was used to conduct the training.

2

EXAMPLE CASE PLANT-GENERAL INFORMATION

2.1 Overall Plant Description

This chapter provides background information about the generic plant used in the hands-on problem sets of Modules 1, 2 and 3. Note that the examples used in Module 4 (HRA) are not based on the example case plant. The following notes generally describe the example case plant, including its layout:

1. The plant is a pressurized water reactor (PWR) consisting of one primary coolant loop, which consists of one steam generator, one reactor coolant pump and the pressurizer. A chemical volume control system and multiple train High Pressure Injection system, as well as a single train residual heat removal system interface with the primary system

2. The secondary side of the plant contains a main steam and feedwater loop associated with the single steam generator, and a multiple train auxiliary feedwater system to provide decay heat removal.

3. The operating conditions and parameters of this plant are similar to that of a typical PWR. For example, the primary side runs at about 2,200 psi pressure. The steam generator can reject the decay heat after a reactor trip. There is a possibility for feed and bleed.

4. It is assumed that the reactor is initially at 100% power.

5. The plant is laid out in accordance with Figures 1 through 9. The plant consists of a containment building, auxiliary building, turbine building, diesel generator building and the yard. All other buildings and plant areas are shown but no details are provided.

2.2 Systems Description

This section provides a more detailed description of the various systems within the plant and addressed in the case studies. Each system is described separately.

2.2.1 Primary Coolant System

The following notes and Figure 10 define the primary coolant system:

1. The primary coolant loop consists of the reactor vessel, one reactor coolant pump, and one steam generator and the pressurizer, along with associated piping.

2. The pressurizer is equipped with a normally closed power operated relief valve (PORV), which is an air operated valve (AOV-1) with its pilot solenoid operated valve (SOV-1). There is also a normally open motor operated block valve (MOV-13) upstream of the PORV.

3. The pressure transmitter (PT-1) on the pressurizer provides the pressure indication for the primary coolant system and is used to signal a switch from chemical volume control system (CVCS) to high pressure injection (HPI) configuration. That is, PT-1 provides the automatic signal for high pressure injection on low RCS pressure. It also provides the automatic signal to open the PORV on high RCS pressure.

4. A nitrogen bottle provides the necessary pressurized gas to operate the PORV in case of loss of plant air but does not have sufficient capacity to support long-term operation.

2.2.2 Chemical Volume Control and High Pressure Injection Systems

The following notes and Figure 10 define the shared CVCS and HPI System:

1. The CVCS normally operates during power generation.

2. Valve type and position information include:

Table 2-1 Chemical volume control and high pressure injection systems valve type and position information

Valve	Type	Status on Loss of Power (Or Air as applicable)	Position During Normal Operation	Motor Power (hp)
AOV-2	Air Operated Valve	Fail Closed	Open	N/A
AOV-3	Air Operated Valve	Fail Open	Open	N/A
MOV-1	Motor Operated Valve	Fail As Is	Closed	>5
MOV-2	Motor Operated Valve	Fail As Is	Open	<5
MOV-3	Motor Operated Valve	Fail As Is	Closed	<5
MOV-4	Motor Operated Valve	Fail As Is	Closed	<5
MOV-5	Motor Operated Valve	Fail As Is	Closed	<5
MOV-6	Motor Operated Valve	Fail As Is	Closed	>5
MOV-9	Motor Operated Valve	Fail As Is	Closed	>5

3. One of the two HPI pumps runs when the CVCS is operating.

4. One of the two HPI pumps is sufficient to provide all injection needs after a reactor trip and all postulated accident conditions.

5. HPI and CVCS use the same set of pumps.
6. On a need for safety injection, the following lineup takes place automatically:

    - AOV-3 closes.

- MOV-5 and MOV-6 open.

- MOV-2 closes.

- Both HPI pumps receive start signal, the stand-by pump starts and the operating pump continues operating.

- MOV-1 and MOV-9 open.

7. HPI supports feed and bleed cooling when all secondary heat removal is unavailable. When there is a low level indication on the steam generator, the operator will initiate feed and bleed cooling by starting the HPI pumps and opening the PORV.

8. HPI is used for re-circulating sump water after successful injection in response to a loss-of-coolant accident (LOCA) or successful initiation of feed and bleed cooling. For recirculation, upon proper indication of low refueling water storage tank (RWST) level and sufficient sump level, the operator manually opens MOV-3 and MOV-4, closes MOV-5 and MOV-6, starts the RHR pump, and aligns component cooling water (CCW) to the RHR heat exchanger.

9. RWST provides the necessary cooling water for the HPI pumps during injection. During the recirculation mode, HPI pump cooling is provided by the recirculation water.

10. There are level indications of the RWST and containment sump levels that are used by the operator to know when to switch from high pressure injection to recirculation cooling mode.

11. The air compressor provides the motive power for the air-operated valves but the detailed connections to the various valves are not shown.

2.2.3 Residual Heat Removal System

The following notes and Figure 10 define the residual heat removal (RHR) system:

1. The design pressure of the RHR system downstream of MOV-8 is low.

2. Valve type and position information include the following:

Table 2-2 Residual Heat Removal System Valve Type and Position Information

Valve	Type	Status on Loss of Power	Position During Normal Operation	Motor Power (hp)
MOV-7	Motor Operated Valve	Fail As Is	Closed (breaker racked out)	>5
MOV-8	Motor Operated Valve	Fail As Is	Closed	>5
MOV-20	Motor Operated Valve	Fail As Is	Closed	>5

3. Operators have to align the system for shutdown cooling, after reactor vessel depressurization from the control room by opening MOV-7 and MOV-8, turn the RHR pump on and establish cooling in the RHR heat exchanger.

2.2.4 Auxiliary Feedwater System

The following notes and Figure 11 define the Auxiliary Feedwater (AFW) System:

1. One of three pumps of the AFW system can provide the necessary secondary side cooling for reactor heat removal after a reactor trip.

2. Pump AFW-A is motor-driven, AFW-B is steam turbine-driven, and AFW-C is diesel-driven.

3. Valve type and position information include the following:

Table 2-3 Auxiliary Feedwater System Valve Type and Position Information

Valve	Type	Status on Loss of Power	Position During Normal Operation	Motor Power (hp)
MOV-10	Motor Operated Valve	Fail As Is	Closed	>5
MOV-11	Motor Operated Valve	Fail As Is	Closed	>5
MOV-14	Motor Operated Valve	Fail As Is	Closed	<5
MOV-15	Motor Operated Valve	Fail As Is	Closed	<5
MOV-16	Motor Operated Valve	Fail As Is	Closed	<5
MOV-17	Motor Operated Valve	Fail As Is	Closed	<5
MOV-18	Motor Operated Valve	Fail As Is	Closed	>5
MOV-19	Motor Operated Valve	Fail As Is	Closed	<5

4. Upon a plant trip, main feedwater isolates and AFW automatically initiates by starting AFW-A and AFW-C pumps, opening the steam valves MOV-14 and MOV-15 to operate the AFW-B steam-driven pump, and opening valves MOV-10, MOV-11, and MOV-18.

5. The condensate storage tank (CST) has sufficient capacity to provide core cooling until cold shutdown is achieved.

6. The test return paths through MOVs-16, 17, and 19 are low-flow lines and do not represent significant diversions of AFW flow even if the valves are open.

7. There is a high motor-temperature alarm on AFW pump A. Upon indication in the control room, the operator is to stop the pump immediately and have the condition subsequently checked by dispatching a local operator.

8. The atmospheric relief valve opens, as needed, automatically to remove decay heat if the main condenser path should be unavailable.

9. The connections to the main turbine and main feedwater are shown in terms of one main steam isolation valve (MSIV) and a check valve. Portions of the plant beyond these interfacing components will not be addressed in the course.

10. Atmospheric dump valve AOV-4 is used to depressurize the steam generator in case of a tube rupture.

2.2.5 Electrical System

Figure 12 is a one-line diagram of the Electrical Distribution System (EDS). Safety-related buses are identified by the use of alphabetic letters (e.g., SWGR-A, MCC-B1, etc.) while the non-safety buses use numbers as part of their designations (e.g., SWGR-1 and MCC-2).

The safety-related portions of the EDS include 4,160-volt (V) switchgear buses SWGR-A and SWGR-B, which are normally powered from the startup transformer SUT-1. In the event that offsite power is lost, these switchgear buses receive power from emergency diesel generators EDG-A and EDG-B. The 480-V safety-related load centers (LC-A and LC-B) receive power from the switchgear buses via station service transformers SST-A and SST-B. The motor control centers (MCC-A1 and MCC-B1) are powered directly from the load centers. The MCCs provide motive power to several safety-related motor-operated valves (MOVs) and to dc buses DC BUS-A and DC BUS-B via battery chargers BC-A and BC-B. The two 125-V dc batteries, BAT-A and BAT-B, supply power to the dc buses in the event that all ac power is lost. DC control power for the 4,160-V, safety-related switchgear is provided through distribution panels PNL-A and PNLB. The 120 V ac vital loads are powered from buses VITAL-A and VITAL-B, which in turn receive their power from the dc buses through inverters INV-A and INV-B.

The non-safety portions of the EDS reflect a similar hierarchy of power flow. There are important differences, however. For example, 4,160-V SWGR-1 and SWGR-2 are normally energized from the unit auxiliary transformer (UAT-1) with backup power available from SUT-1. A cross-tie breaker allows one non-safety switchgear bus to provide power to the other. Non-safety load centers LC-1 and LC-2 are powered at 480 V from the 4,160-V switchgear via SST-1 and SST-2. These load centers provide power directly to the non-safety MCCs. The non-vital dc bus (DC BUS-1) can be powered from either MCC via an automatic transfer switch (ATS-1) and battery charger BC-1 or directly from the 125-V dc battery, BAT-1.

2.2.6 Other Systems

The following systems and equipment are mentioned in the plant description but not explicitly included in the fire PRA:

- Component Cooling Water (CCW) – provides cooling to letdown heat exchanger and the RHR heat exchanger– assumed to be available at all times.
- It is assumed that the control rods can successfully insert and shutdown the reactor under all conditions.

- It is assumed that the emergency core cooling system (ECCS) and other AFW related instrumentation and control circuits (other than those specifically noted in the diagrams) exist and are perfect such that in all cases, they would sense the presence of a LOCA or other need to trip the plant and provide safety injection and auxiliary feedwater by sending the proper signals to the affected components (i.e., close valves and start pumps, insert control rods, etc.).

- Instrument air is required for operation of AOV-1, AOV-2, AOV-3, and AOV-4.

2.3 Plant Layout

The following notes augment the information provided in Figures 1 through 9 (Drawings A-01 through A09):

- The main structures of the plant are as follows:
  - containment
  - auxiliary building
  - turbine building
  - diesel generator building
  - intake structure
  - security building

- In Figure 1 (Drawing A-01), the dashed lines represent the fence that separates two major parts: the yard and switchyard.

- Switchyard is located outside the yard with a separate security access.

- CST, RWST, UAT, main transformer and SUT are located in the open in the yard.

- All walls shown in Figures 1 through 8 (Drawings A-01 through A-08) should be assumed to be fire rated.

- All doors shown in Figures 1 through 8 (Drawings A-01 through A-08) should be assumed as fire rated and normally closed.

- Battery rooms A and B are located inside the respective switchgear rooms with 1-hour rated walls, ceilings and doors.

- All cable trays are open type. Vertical cable trays are designated as VCBT and horizontal cable trays as HCBT. For horizontal cable trays, the number following the letters indicates the elevation of the cable tray. For example, HCBT+35A denotes a horizontal cable tray at elevation +35 ft (11 meters).

- The stairwell in the auxiliary building provides access to all the floors of the building. The doors and walls are fire rated and doors are normally closed.

2.4 SNPP Drawings

The following 12 pages provide schematic drawings of the generic NPP, SNPP. Drawings A-01 through A-09 are general physical layout drawings providing plan and elevation views of the plant. These drawings also identify the location of important plant equipment. Drawing A-10 provides a piping and instrumentation diagram (P&ID) for the primary coolant system, and drawing A-11 provides a P&ID for the secondary systems. Drawing A-12 is a simplified one-line diagram of the plant power distribution system.

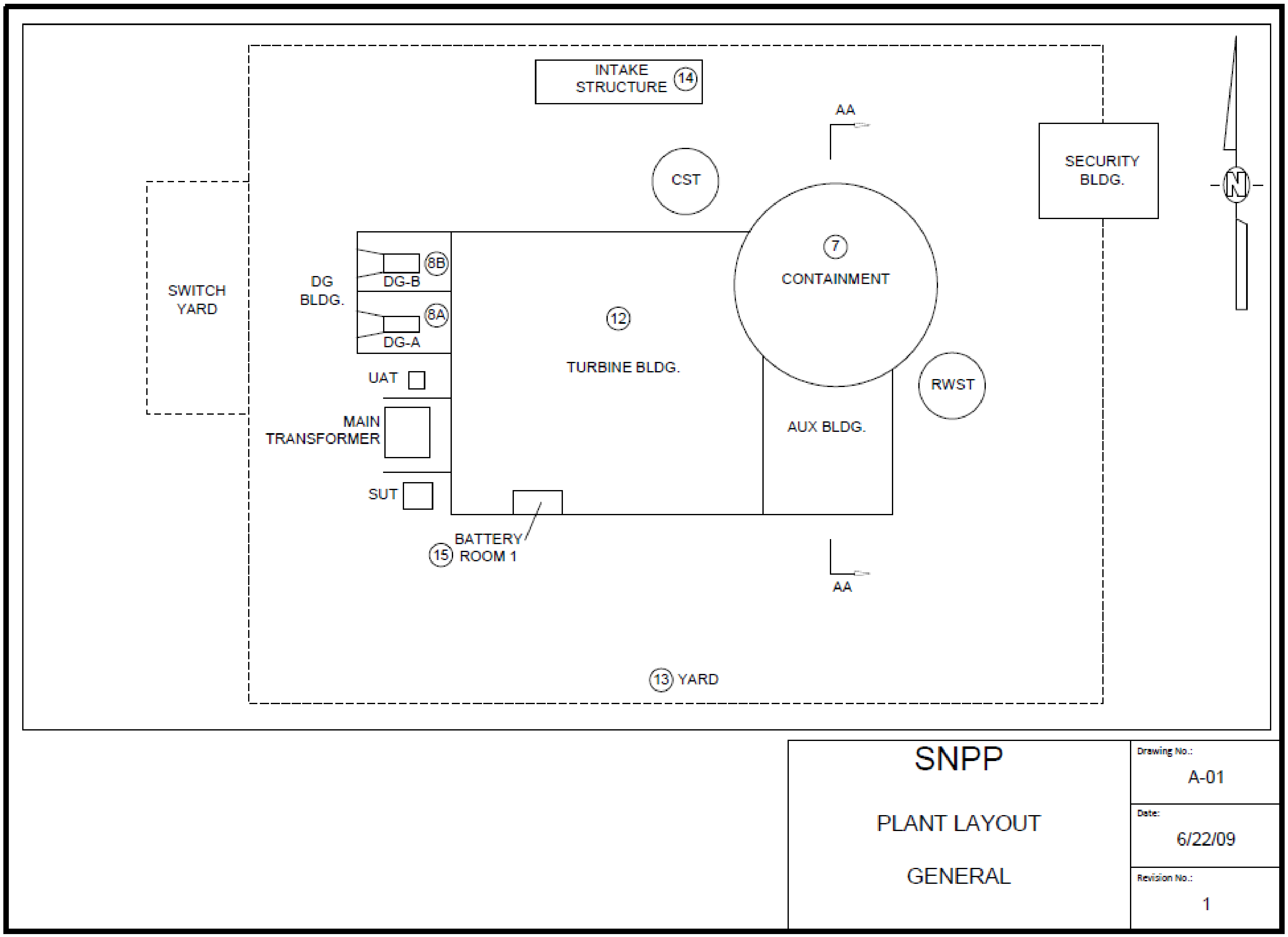


Figure 2-1 General Plant Layout

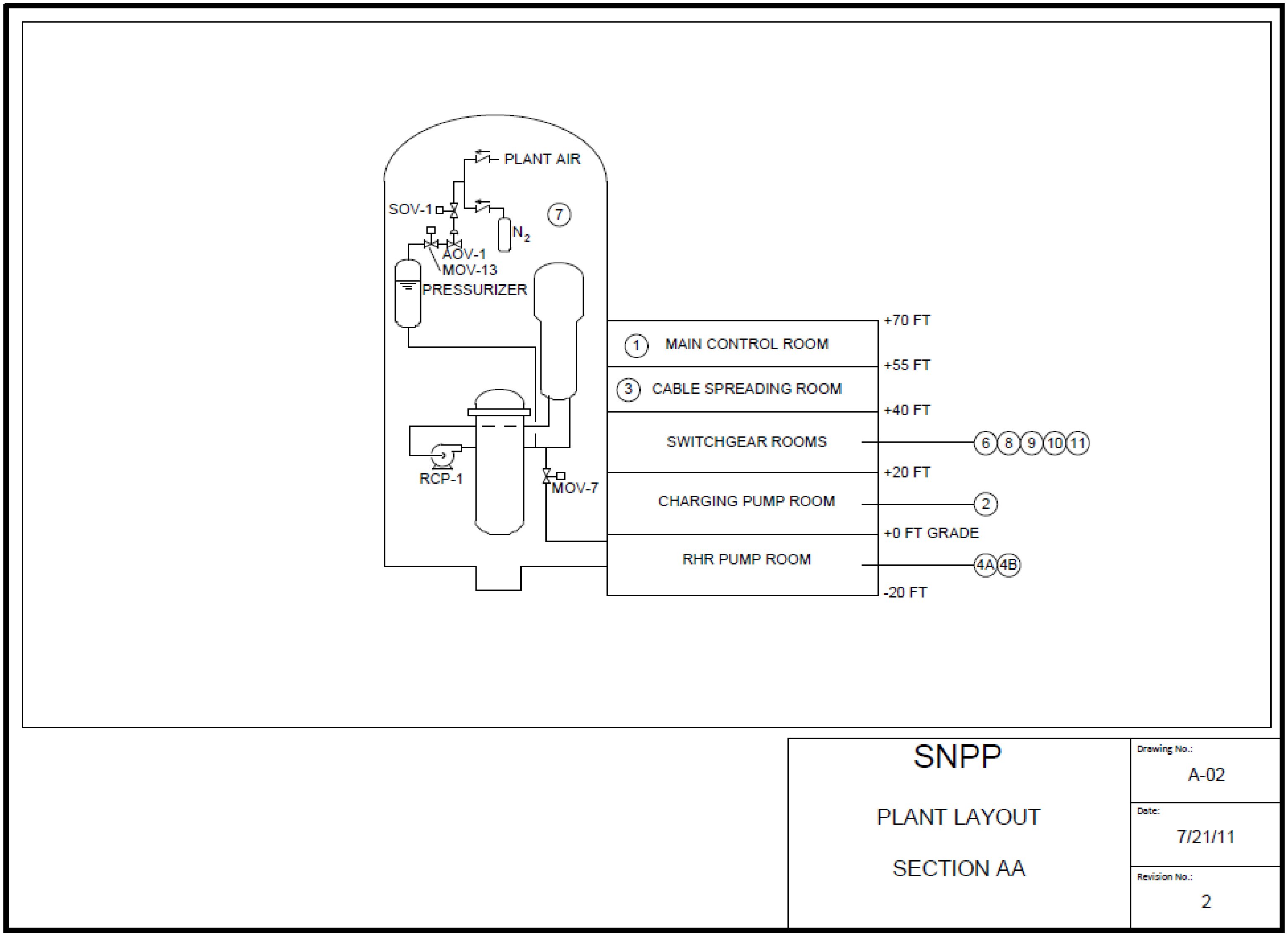


Figure 2-2 Plant Layout Section AA

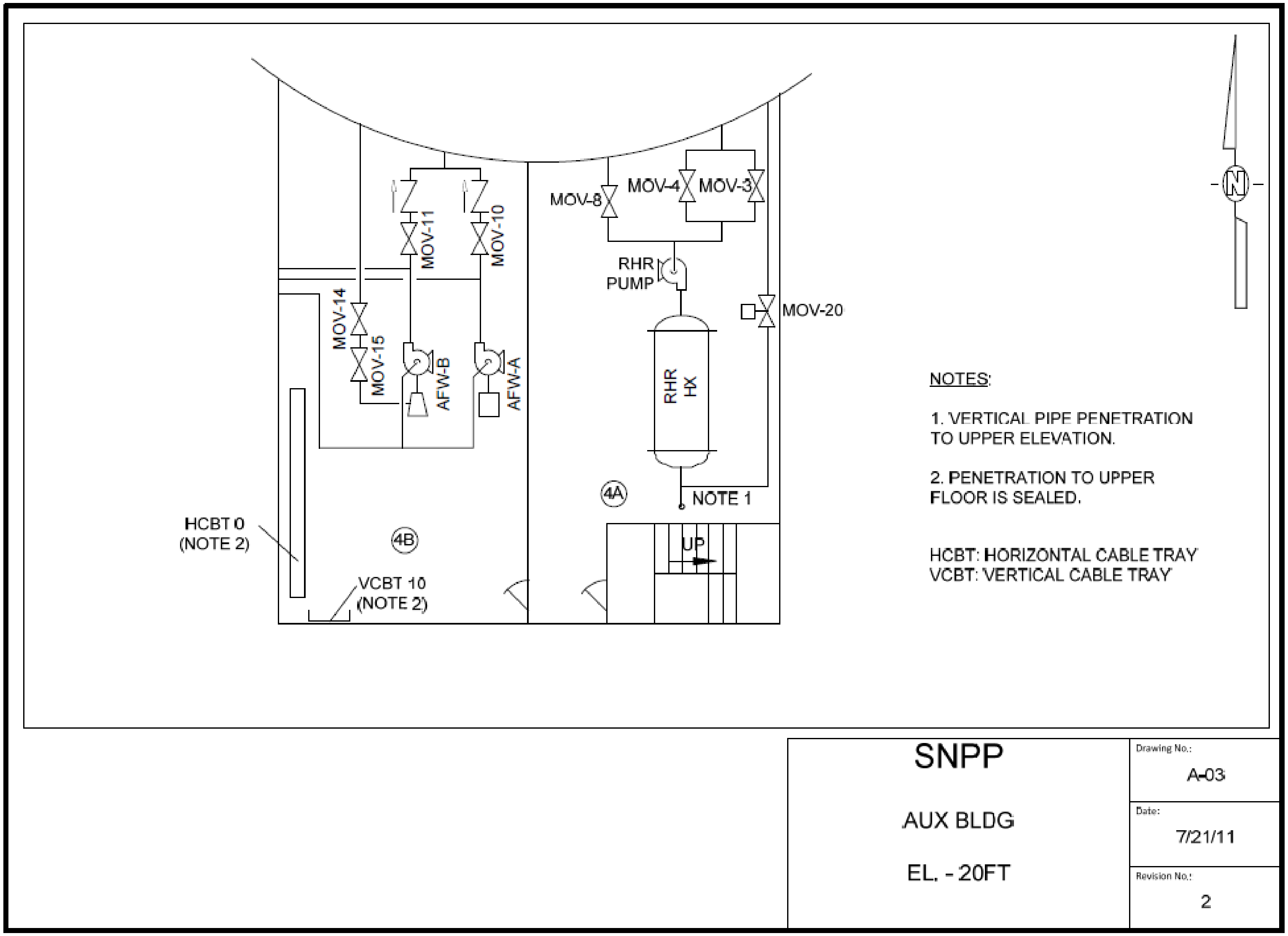


Figure 2-3 Auxiliary Building - Elevation 20 Ft.

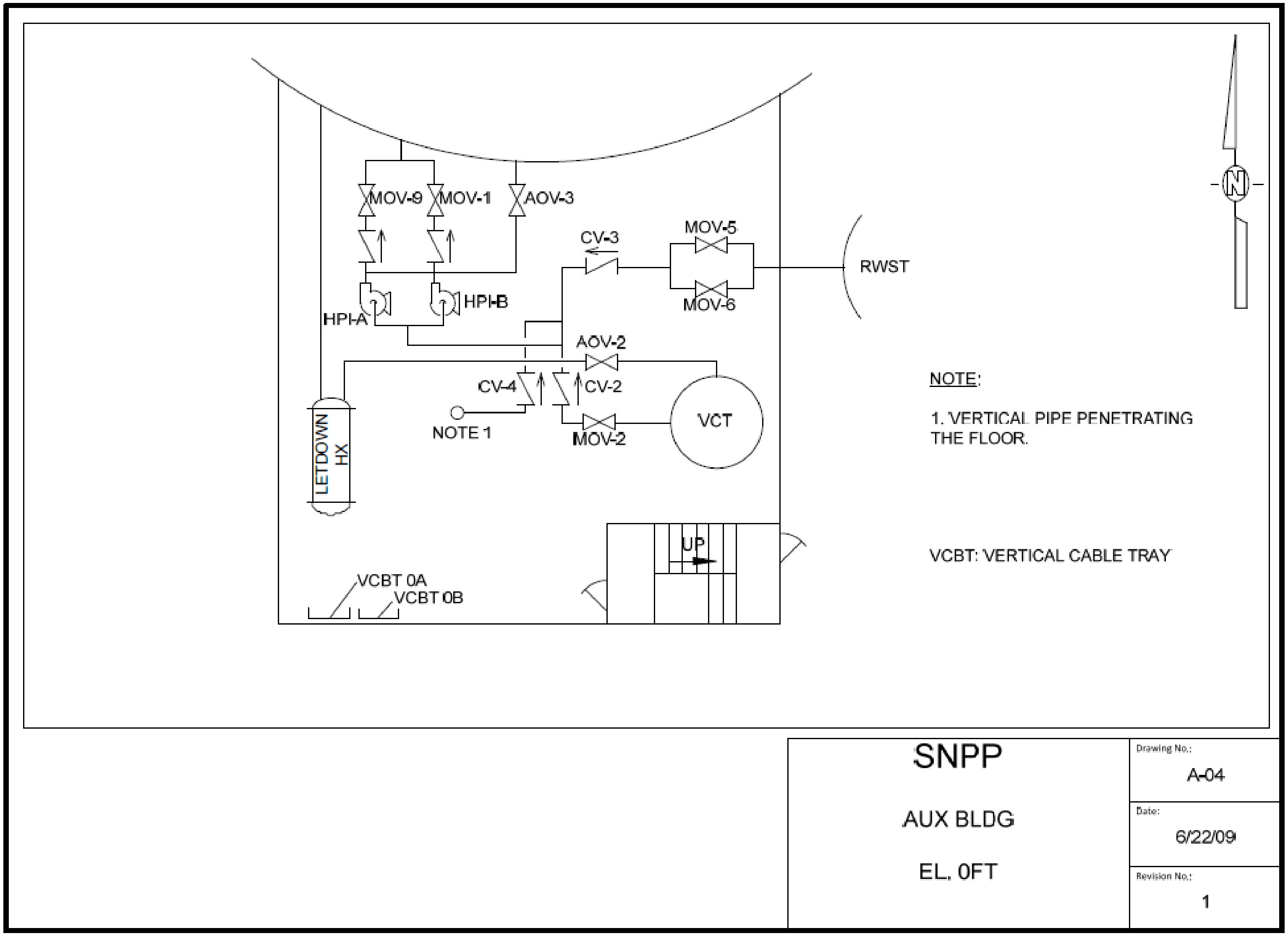


Figure 2-4 Auxiliary Building – Elevation 0 Ft

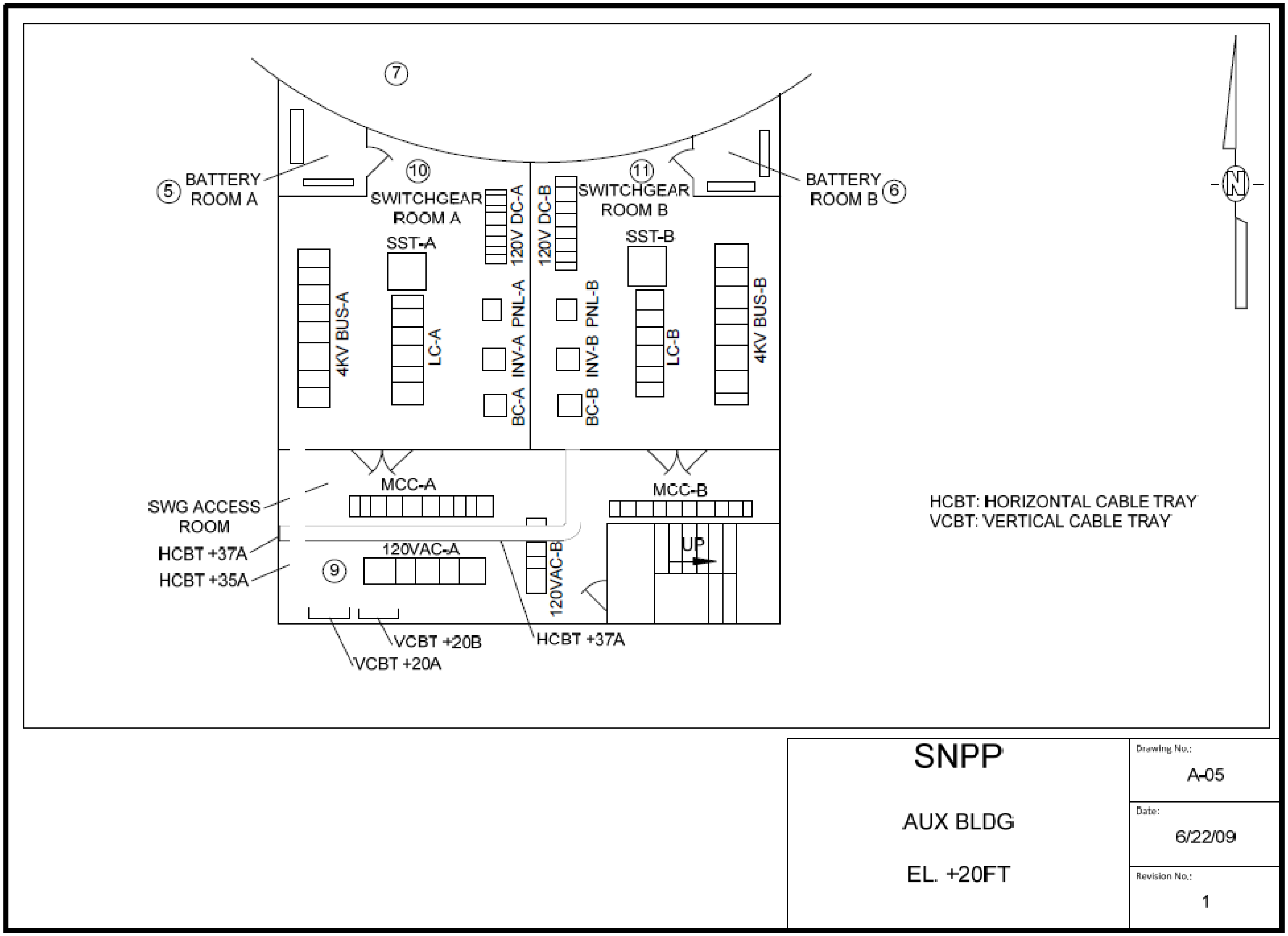


Figure 2-5 Auxiliary Building – Elevation +20 Ft.

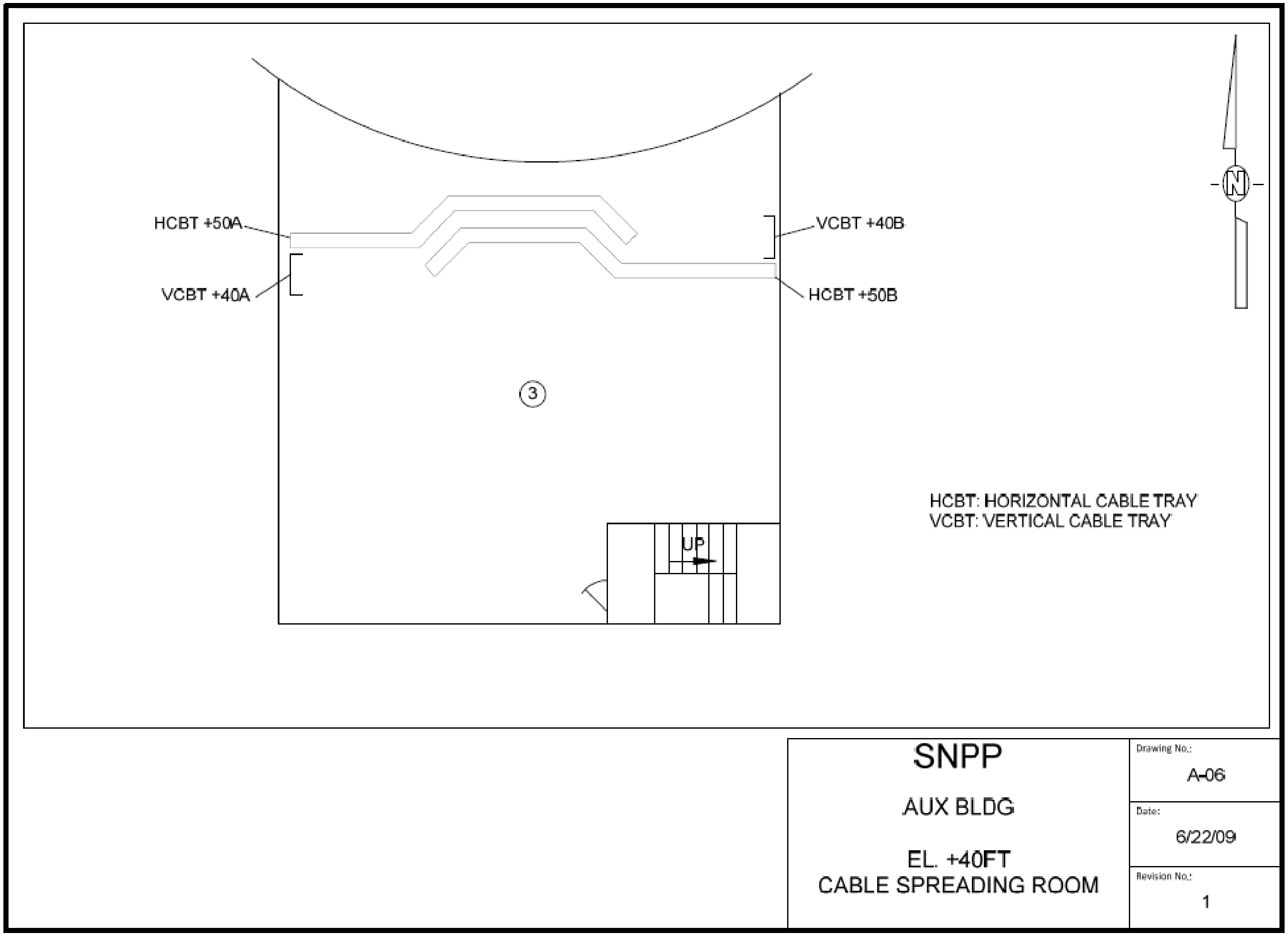


Figure 2-6 Auxiliary Building – Elevation +40 Ft.

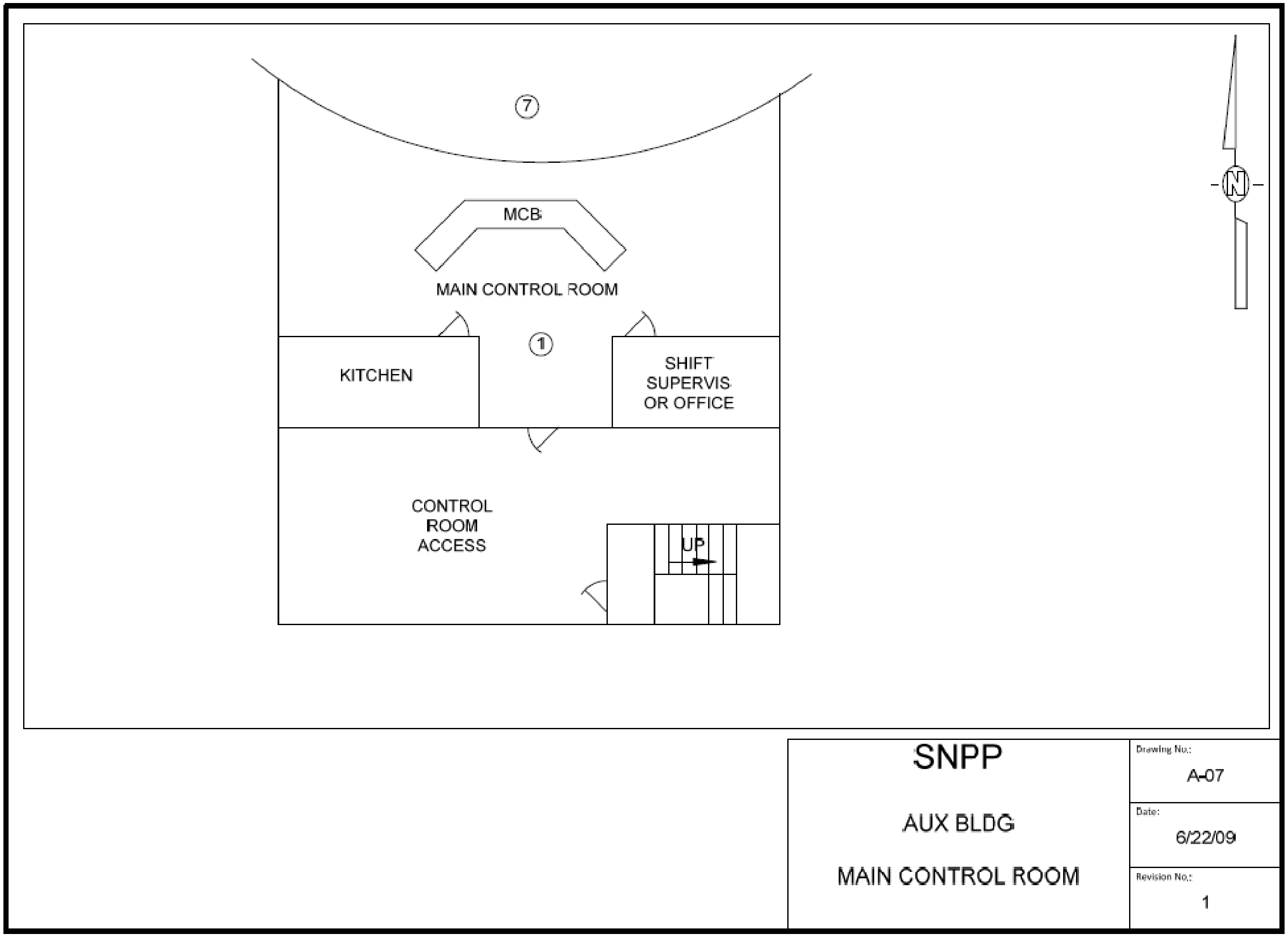


Figure 2-7 Auxiliary Building Main Control Room

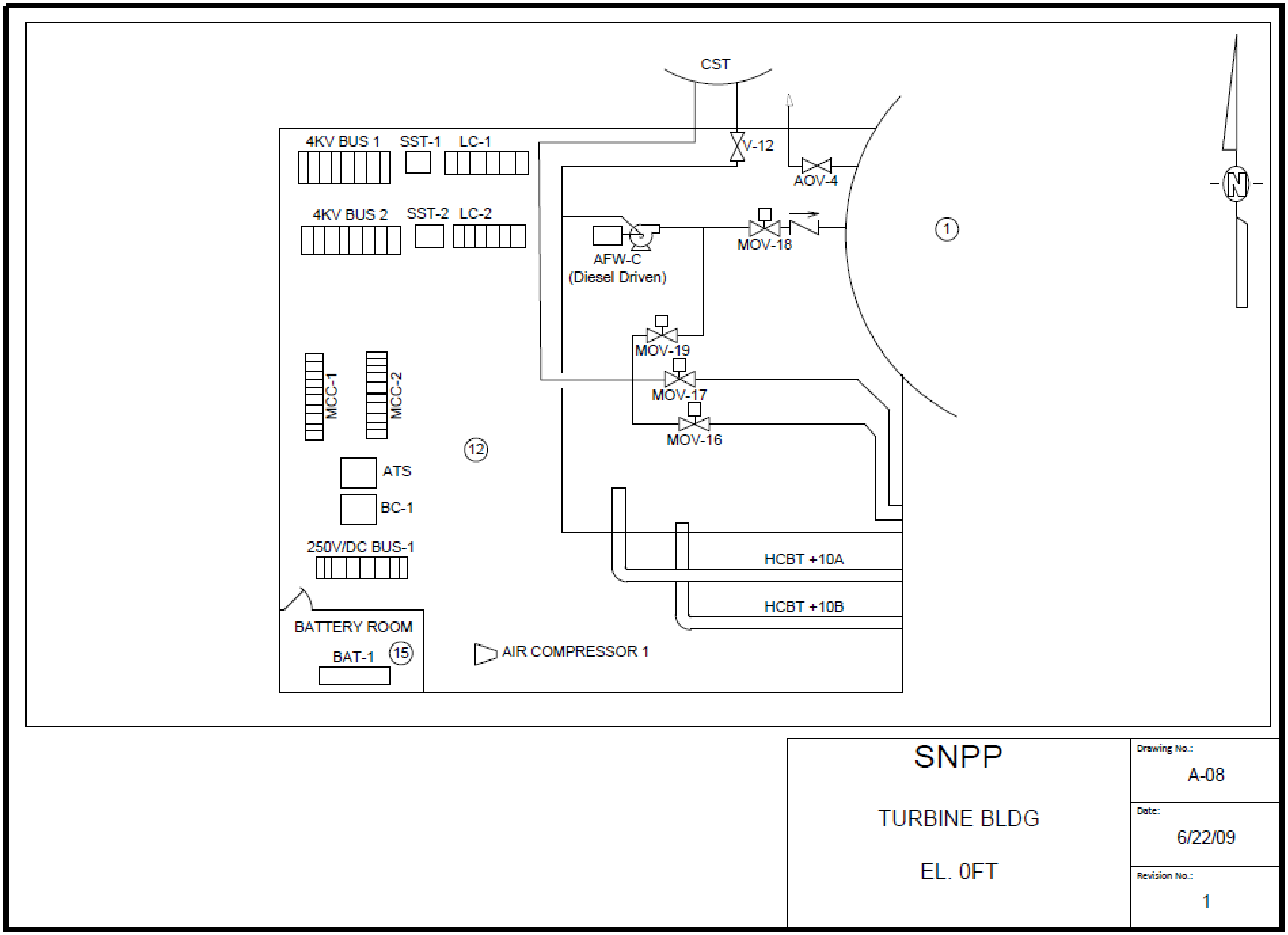


Figure 2-8 Turbine Building – Elevation 0 Ft.

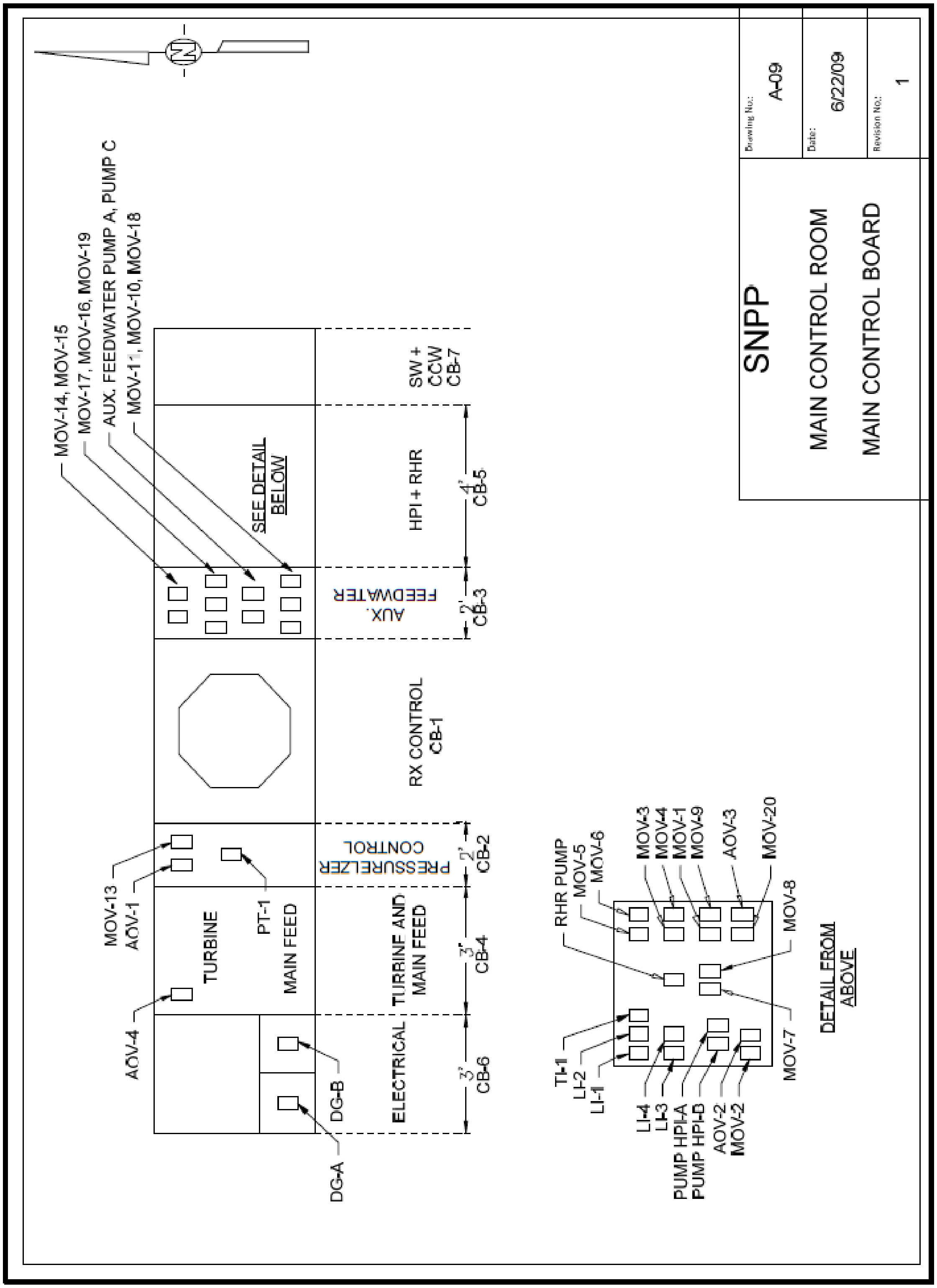


Figure 2-9 Main Control Board

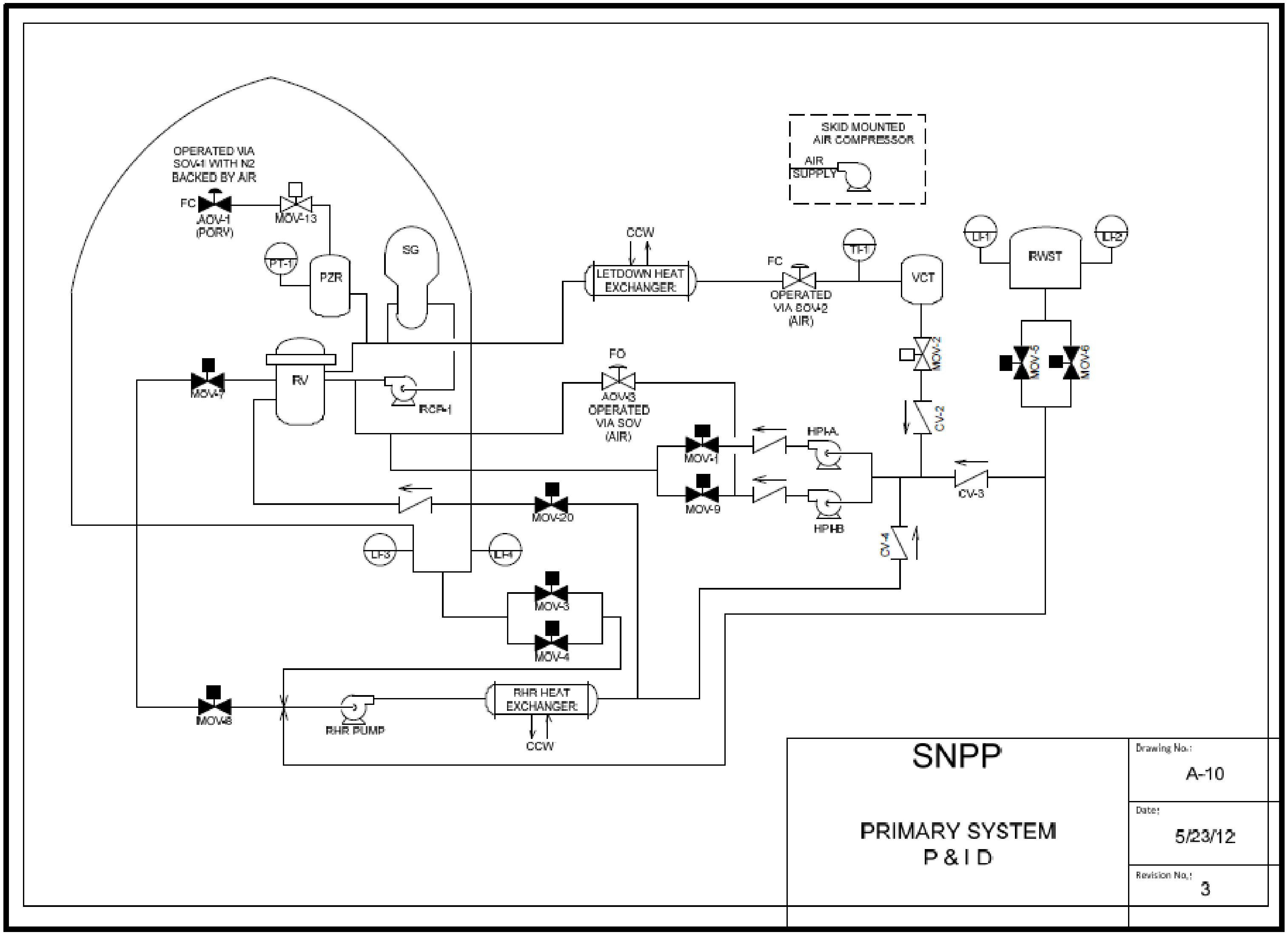


Figure 2-10 Primary System P&ID

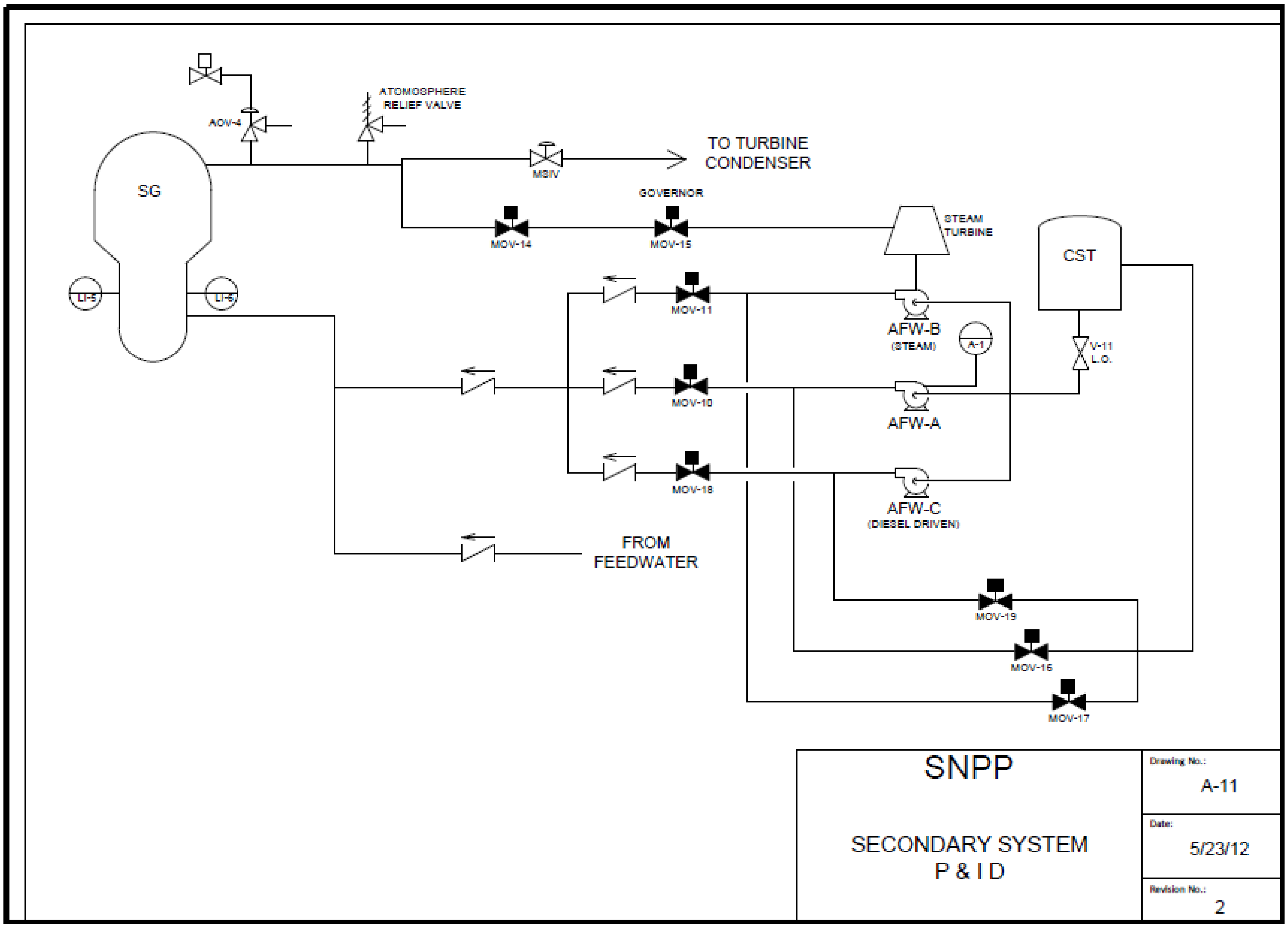


Figure 2-11 Secondary System P&ID

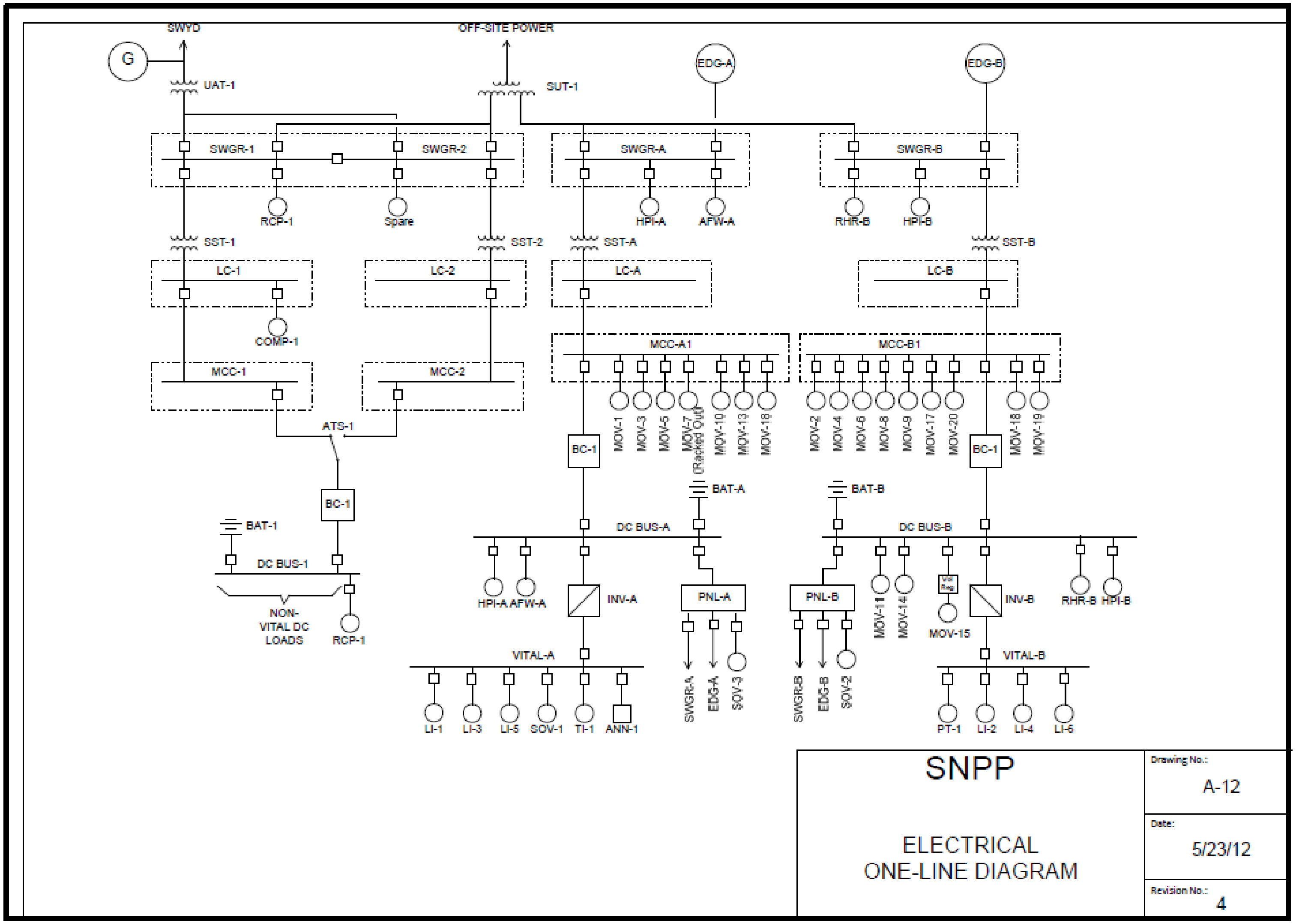


Figure 2-12 Electrical One-Line Diagram

3

PRINCIPLES OF PRA

The slides that follow were presented on the first day of the NRC-RES/EPRI Fire PRA Workshop during the extra day of training dedicated to presenting the fundamentals of the various subject areas to be covered during the remainder of the week.

Basics of Nuclear Power Plant Probabilistic Risk Assessment

Basics of Nuclear Power Plant Probabilistic Risk Assessment

Joint RES/EPRI Fire PRA Workshop
July and September, 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Course Objectives

- Introduce PRA modeling and analysis methods applied to nuclear power plants
  - Initiating event identification
  - Event tree and fault tree model development
  - Human reliability analysis
  - Data analysis
  - Accident sequence quantification
  - LERF analysis

Course Outline

1. Overview of PRA
2. Initiating Event Analysis
3. Event Tree Analysis
4. Fault tree Analysis
5. Human Reliability Analysis
6. Data Analysis
7. Accident Sequence Quantification
8. LERF Analysis

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 3

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

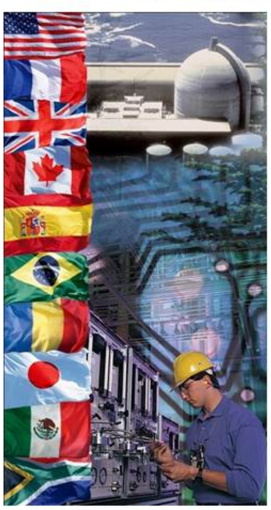
Overview of PRA

ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

CURTISS WRIGHT Flow Control Company SCIENTECH

SAIC Science Applications International Corporation
From Science to Solutions



Overview of PRA

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

What is Risk?

- Arises from a “Danger” or “Hazard”
- Always associated with undesired event
- Involves both:
  - likelihood of undesired event
  - severity (magnitude) of the consequences

Risk Definition

- Risk - the frequency with which a given consequence occurs

$$\text{Risk}\left[\frac{\text{Consequence Magnitude}}{\text{Unit of Time}}\right] =$$

$$\text{Frequency}\left[\frac{\text{Events}}{\text{Unit of Time}}\right] \times \text{Consequences}\left[\frac{\text{Magnitude}}{\text{Event}}\right]$$

Risk Example: Death Due to Accidents

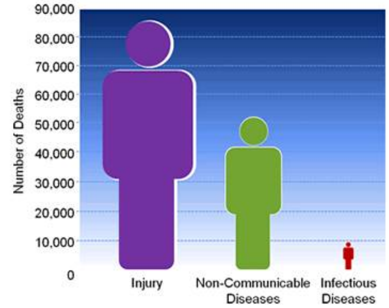
- Societal Risk = 93,000 accidental-deaths/year in 1991

  (based on Center for Disease Control actuarial data)
- Average Individual Risk

  = (93,000 Deaths/Year)/250,000,000 Total U.S. Pop.

  = 3.7E-04 Deaths/Person-Year

  ≈ 1/2700 Deaths/Person-Year
- In any given year, approximately 1 out of every 2,700 people in the entire U.S. population will suffer an accidental death



More people ages 1–44 die from injuries than from any other cause, including cancer, HIV, or the flu.

Note: www.cdc.gov latest data (2009) 38.4 unintentional deaths per 100,000, thus average individual risk ≈ 3.8E-04 Deaths/Person-Year

Risk Example: Death Due to Cancer

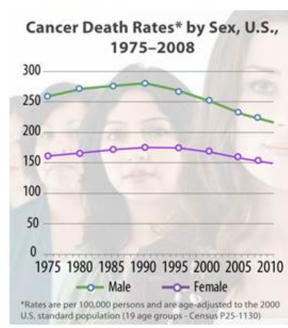
- Societal Risk = 538,000 cancer-deaths/year in 1991

  (based on Center for Disease Control actuarial data)
- Average Individual Risk

  = (538,000 Cancer-Deaths/Year)/250,000,000 Total U.S. Pop.

  = 2.2E-03 Cancer-Deaths/Person-Year

  ≈ 1/460 Cancer-Deaths/Person-Year
- In any given year, approximately 1 person out of every 460 people in the entire U.S. population will die from cancer



Note: www.cdc.gov latest data (2007) 217.8 cancer deaths per 100,000, thus average individual risk ≈ 2.2E-03 Deaths/Person-Year

NRC Quantitative Health Objectives (QHOs)

- Originally known as the Probabilistic Safety Goals
  - NRC adopted two probabilistic safety goals on August 21, 1986
- High-level goal: incremental risk from nuclear power plant operation < 0.1% of all risks
  - Average individual (within 1 mile of plant) early fatality (accident) risk
    < 5E-7/year
  - Average individual (within 10 miles of plant) latent fatality (cancer) risk
    < 2E- 6/year
- Lower level subsidiary goals were derived from the high-level QHOs
  - Frequency of significant core damage (CDF) < 1E-4/year
  - Frequency of large early release of fission products from containment (LERF) < 1E-5/year

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview
Slide 9
A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

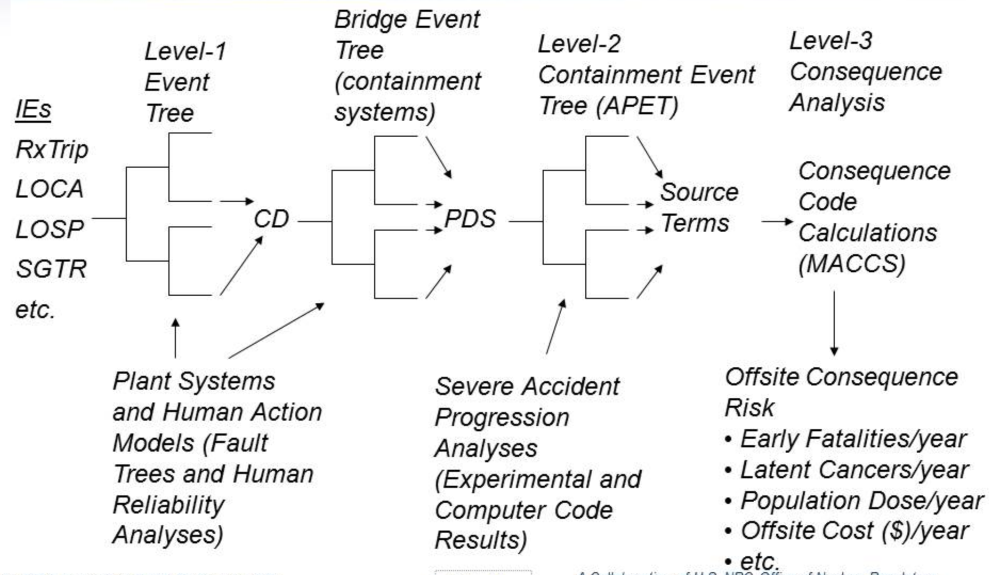
Overview of PRA Process

- PRAs are performed to find severe accident weaknesses and provide quantitative results to support decision-making. Three levels of PRA have evolved:

Level	An Assessment of:	Result
1	Plant accident initiators and systems'/operators' response	Core damage frequency & contributors
2	Frequency and modes of containment failure	Categorization & frequencies of containment releases
3	Public health consequences	Estimation of public & economic risks

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview
Slide 10
A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Overview of Level-1/2/3 PRA

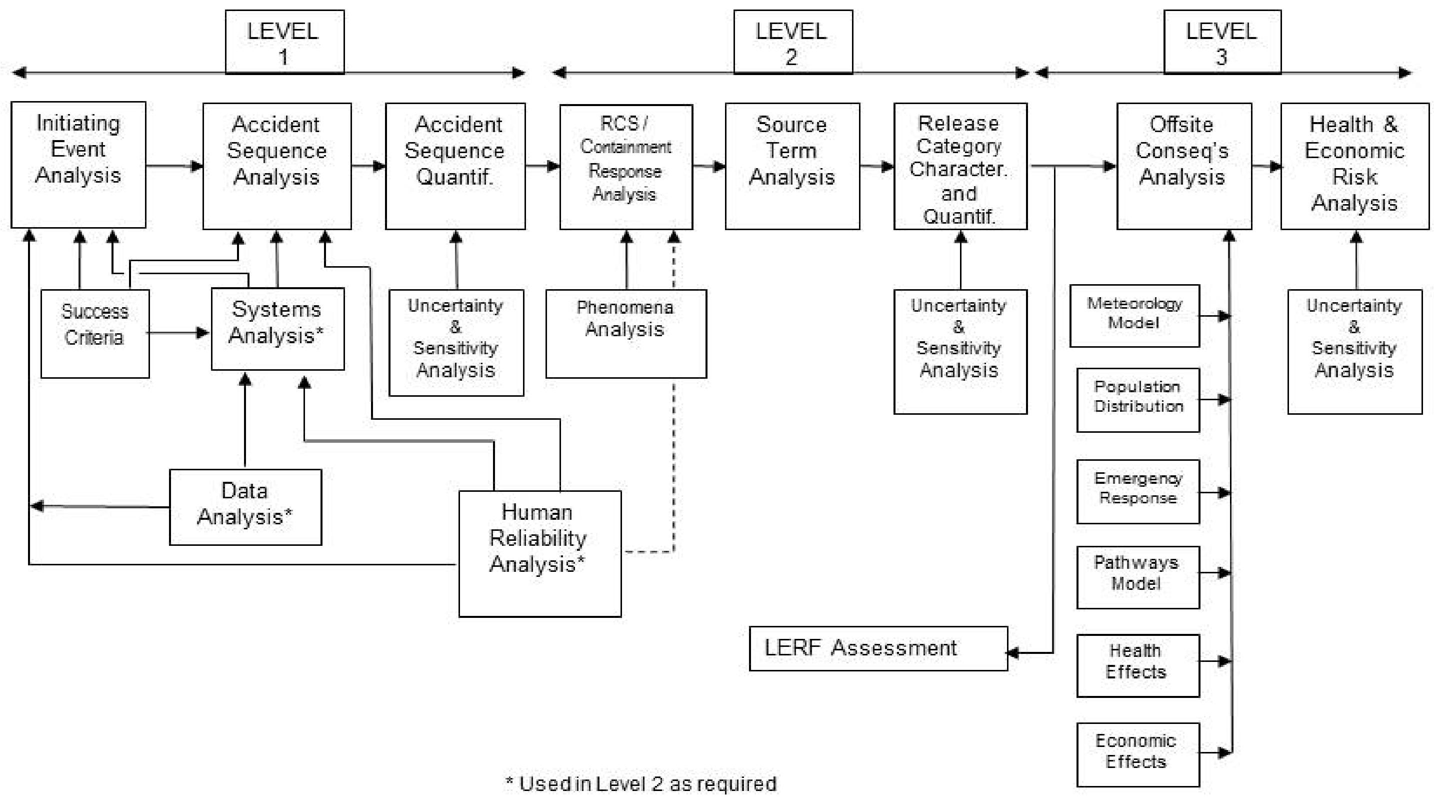


Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 11

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

PRA Classification

- Internal Hazards – risk from accidents initiated internal to the plant
  - Includes internal events, internal flooding and internal fire events
- External Hazards – risk from external events
  - Includes seismic, external flooding, high winds and tornadoes, airplane crashes, lightning, hurricanes, etc.
- At-Power – accidents initiated while plant is critical and producing power (operating at >X%* power)
- Low Power and Shutdown (LP/SD) – accidents initiated while plant is <X%* power or shutdown
  - Shutdown includes hot and cold shutdown, mid-loop operations, refueling

**X is usually plant-specific. The separation between full and low power is determined by evolutions during increases and decreases in power*

Focus of Course is on At-Power PRA

- In early risk studies, risk from at-power operation was assumed to be dominant because during shutdown:
  - Reactor is subcritical
  - Longer time is available to respond to accidents (lower decay heat)
- However, limited risk studies of low-power and shutdown operations have suggested that shutdown risk may be significant because
  - Systems may not be available as Tech. Specs. allow more equipment to be inoperable than at power
  - Initiating events can impact operable trains of systems providing critical plant safety functions (e.g., loss of RHR)
  - Human errors are more prevalent because operators may find themselves in unfamiliar conditions not covered by training and procedures
  - Plant instruments and indications may not be available or accurate

Specific Strengths of PRA

- Rigorous, systematic analysis tool
- Information integration (multidisciplinary)
- Allows consideration of complex interactions
- Develops qualitative design insights
- Develops quantitative measures for decision making
- Provides a structure for sensitivity studies
- Explicitly highlights and treats principal sources of uncertainty

Principal Limitations of PRA

- Inadequacy of available data
- Lack of understanding of physical processes
- High sensitivity of results to assumptions
- Constraints on modeling effort (limited resources)
  - simplifying assumptions
  - truncation of results during quantification
- PRA is typically a snapshot in time
  - this limitation may be addressed by having a "living" PRA
    - plant changes (e.g., hardware, procedures and operating practices) reflected in PRA model
    - temporary system configuration changes (e.g., out of service for maintenance) reflected in PRA model
- Lack of completeness (e.g., human errors of commission typically not considered)

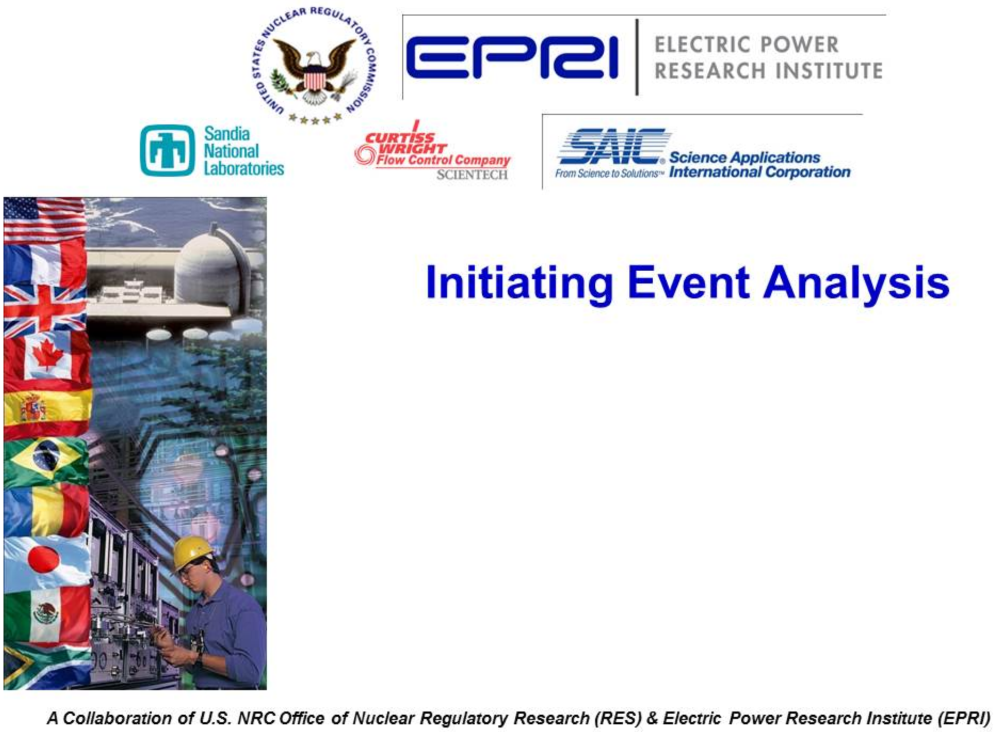
Evolution of PRA Use

- First PRA study (WASH-1400, 1975)
  - provided a better understanding of how nuclear plant accidents might occur and what the potential consequences might be
- Three Mile Island accident in 1979
  - validated the importance of PRA
  - led to efforts to improve state-of-the-art of PRA, in research into severe accident phenomena, and performance of PRAs on more reactors
- NRC Safety Goals (1986)
  - Risk to the public from nuclear power plant operation should be less than 0.1% of the total risk from other man-made causes

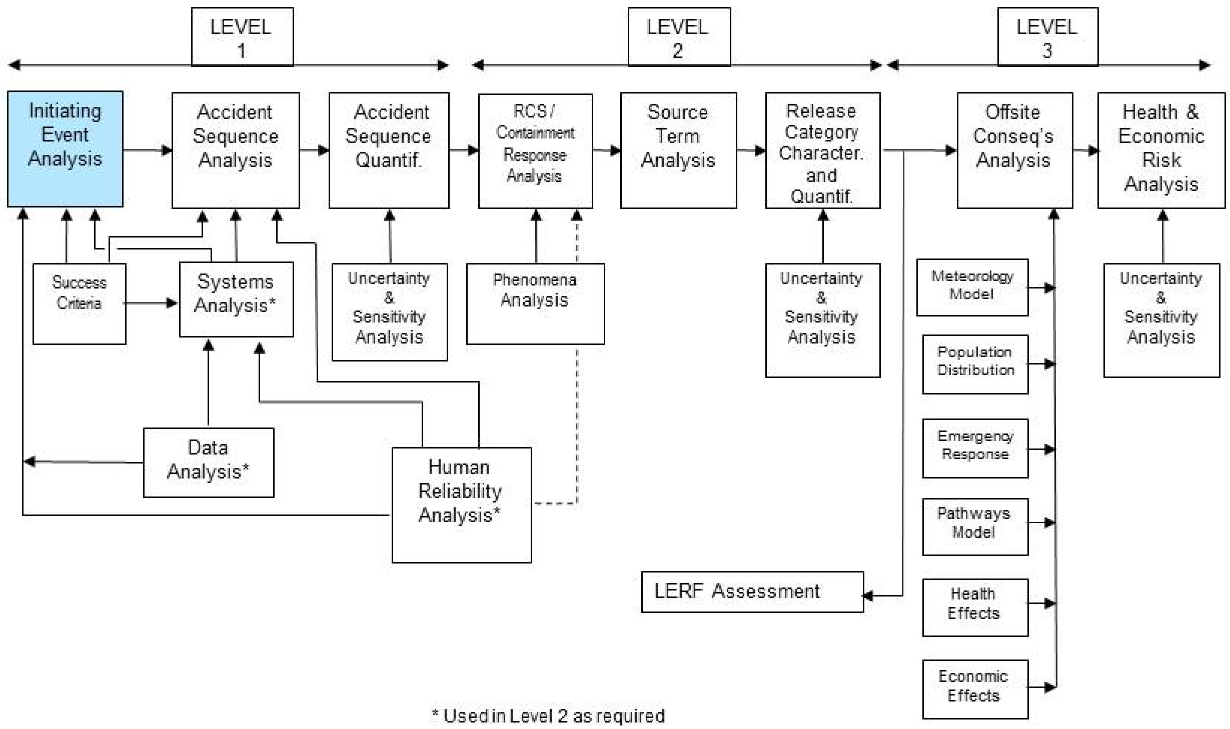
Evolution of PRA Use (cont.)

- Generic Letter 88-20 (1988)
  - requested all nuclear power plant licensees to conduct an Individual Plant Examination (IPE) to investigate plant-specific risk and identify any vulnerabilities. All plants performed a PRA. Plants later identified risk from external events in IPEEE (Individual Plant Examination of External Events)
- NRC Policy Statement on the use of PRA in regulatory matters (1995)
  - " the use of PRA technology should be increased to the extent supported by the state of the art in PRA methods and data and in a matter that complements the NRC's deterministic approach"
  - Risk-Informed Regulation Implementation Plan generated to define and organize PRA-related activities

Initiating Event Analysis



Principal Steps in PRA



* Used in Level 2 as required

Initiating Event Analysis

- Purpose: Students will learn what is an initiating event (IE), how to identify them, and group them into categories for further analysis.

Objectives:
  - Understand the relationship between initiating event identification and other PRA elements
  - Identify the types of initiating events typically considered in a PRA
  - Become familiar with various ways to identify initiating events
  - Become familiar with criteria for eliminating initiating events
  - Understand how initiating events are grouped
- References:
  - NUREG/CR-2300, NUREG/CR-5750, NUREG/CR-3862, NUREG/CR-4550, Volume 1, NUREG/CR-6928

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 21

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Initiating Events

- Definition – Any potential occurrence that could disrupt plant operations to a degree that a reactor trip or plant shutdown is required. Initiating events are quantified in terms of their frequency of occurrence (i.e., number of events per calendar year of operation)
- Can occur while reactor is at full power, low power, or shutdown
  - Focus of this session is on IEs during full power operation
- Can be internal to the plant or caused by external events
  - Focus of this session is on internal IEs
- Basic categories of internal IEs:
  - transients (initiated by failures in the balance of plant or nuclear steam supply)
  - loss-of-coolant accidents (LOCAs) in reactor coolant system
  - interfacing system LOCAs
  - LOCA outside of containment
  - special transients (generally support system initiators)

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 22

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Initiating Event Analysis

- Collect information on actual plant trips
- Identify other abnormal occurrences that could cause a plant trip or require a shutdown
- Identify the plant response to these initiators including the functions and associated systems that can be used to mitigate these events
- Grouping IEs into categories based on their impact on mitigating systems
- Quantify the frequency of each IE category (Included later in Data Analysis session)

Role of Initiating Events in PRA

- Identifying initiating events is the first step in the development of accident sequences
- Accident sequences can be conceptually thought of as a combination of:
  - an initiating event, which triggers a series of plant and/or operator responses, and
  - A combination of success and/or failure of the plant system and/or operator response that result in a core damage state
- Initiating event identification is an iterative process that requires feedback from other PRA elements
  - system analysis
  - review of plant experience and data

Methods for Identification and Grouping IEs

- Comprehensive Engineering Evaluation (commonly used)
  - Analysis of historical events
  - Comparison with other studies
  - Plant-specific design data
- Deductive methods (master logic diagram)
  - Good process when there is no history of accident initiators (e.g., an advanced reactor)
- Failure Modes and Effects Analysis (FMEA)
  - Formalized tabular process used to identify potential failures, determine the effect on the plant operation, and identify mitigating actions
  - Primarily used to examine support system failures

Comprehensive Engineering Evaluation

- Review historical events (reactor trips, shutdowns, system failures)
- Discrete spectrum of LOCA sizes considered based on location of breaks (e.g., in vs. out of containment, steam vs. liquid), components (e.g., pipe vs. SORV), and available mitigation systems
- Review comprehensive list of possible transient initiators based on existing lists (see for example NUREG/CR-3862) and from Safety Analysis Report
- Review list of initiating event groups modeled in other PRAs and adapt based on plant-specific information – typical approach for existing LWRs
- Feedback provided from other PRA taks

Sources of Data for Identifying IEs

- Plant-specific sources:
  - Licensee Event Reports
  - Scram reports
  - Abnormal, System Operation, and Emergency Procedures
  - Plant Logs
  - Safety Analysis Report (SAR)
  - System descriptions
- Generic sources:
  - NUREG/CR-3862
  - NUREG/CR-4550, Volume 1
  - NUREG/CR-5750
  - Other PRAs

Criteria for Eliminating IEs

- Some IEs may not have to modeled because:
  - Frequency is very low (e.g., <1E-7/ry)
    - ASME PRA Standard exclude ISLOCAs , containment bypass, vessel rupture from this criteria
  - Frequency is low (<1E-6/ry) and at least two trains of mitigating systems are not affected by the IE
  - Effect is slow, easily identified, and recoverable before plant operation is adversely affected (e.g., loss of control room HVAC)
  - Effect does not cause an automatic scram or an administrative demand for shutdown (e.g., waste treatment failure)

Initiating Event Grouping

- For each identified initiating event:
  - Identify the safety functions required to prevent core damage and containment failure
  - Identify the plant systems that can provide the required safety functions
- Group initiating events into categories that require the same or similar plant response
- This is an iterative process, closely associated with event tree construction. It ensures the following:
  - All functionally distinct accident sequences will be included
  - Overlapping of similar accident sequences will be prevented
  - A single event tree can be used for all IEs in a category

Example Initiating Events (PWR) from NUREG/CR-6928

Category	Initiating Event	Mean Frequency (per critical year)
B	Loss of offsite power	4.0E-2
L	Loss of condenser	0.2
P	Loss of feedwater	0.1
Q	General transient	0.8
F	Steam generator tube rupture	4.0E-3
	ATWS	8.4E-6*
G7	Large LOCA (BWR, PWR)	7.0E-6, 1.2E-6
G6	Medium LOCA (BWR, PWR)	1.0E-4, 5.0E-4
G3	Small LOCA (BWR, PWR)	5.0E-4, 6.0E-4

*From NUREG/CR-5750

Example Initiating Events (PWR) from NUREG/CR-6928 (cont.)

Category	Initiating Event	Mean Frequency (per critical year)
G2	Stuck-open relief valve (BWR, PWR)	2.0E-2, 3.0E-3
K1	High energy line break outside containment	1.0E-2*
C1+C2	Loss of vital medium or low voltage ac bus	9.0E-3
C3	Loss of vital dc bus	1.2E-3
D	Loss of instrument or control air	1.0E-2
E1	Total loss of service water, total loss of component cooling water	4.0E-4

*From NUREG/CR-5750

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 31

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

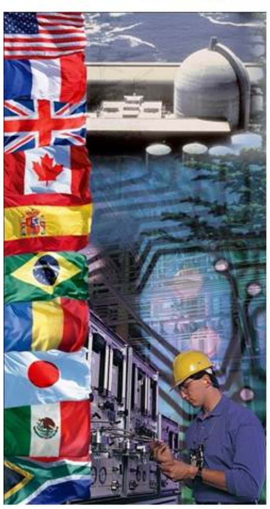
Accident Sequence Analysis

ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

Curtiss Wright Flow Control Company SCIENTECH

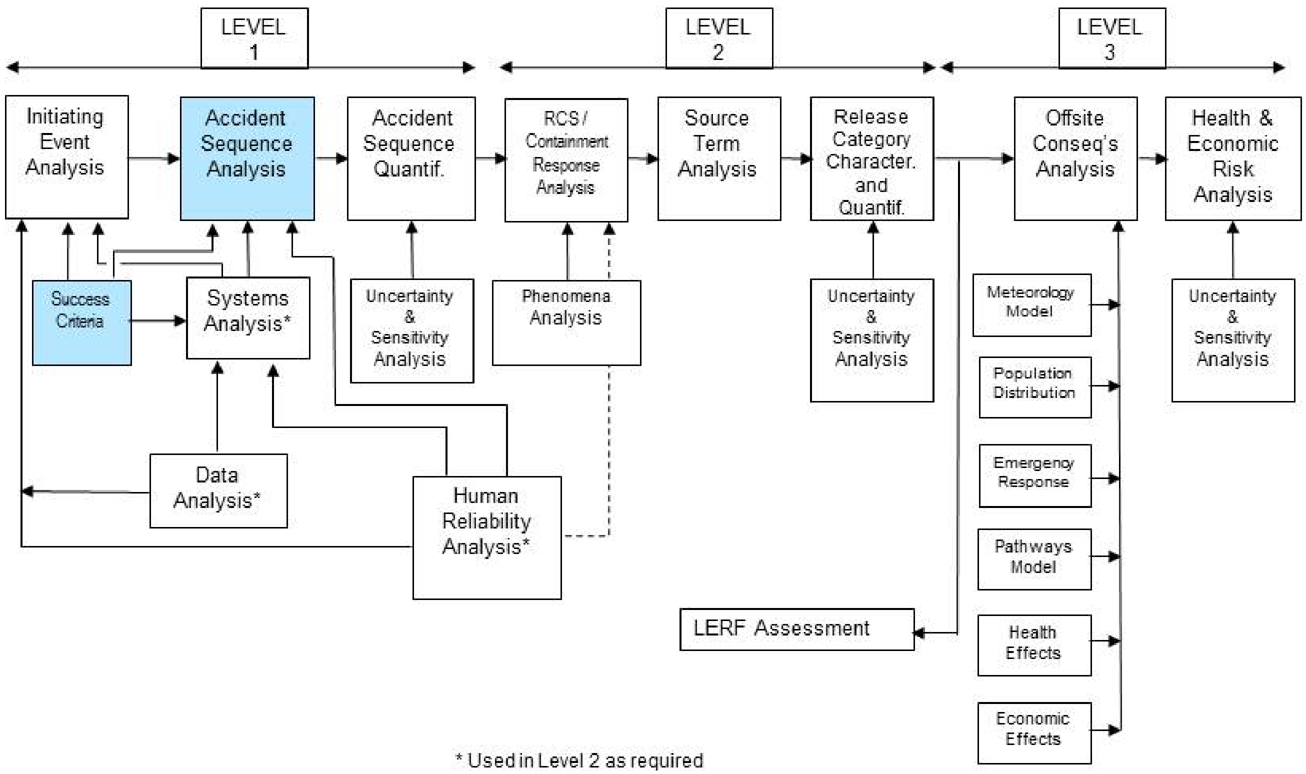
SAIC Science Applications International Corporation



Accident Sequence Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

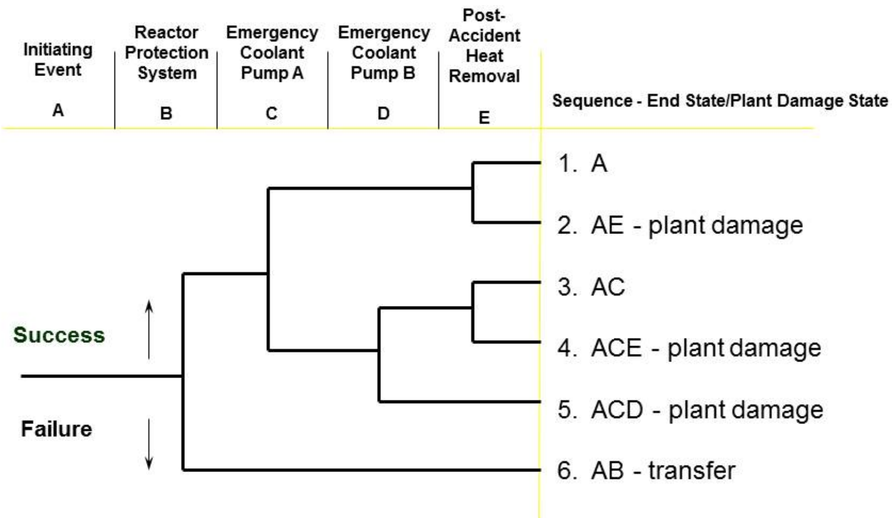
Accident Sequence Analysis

- Purpose: Students will learn purposes & techniques of accident sequence (event) analysis. Students will be exposed to the concept of accident sequences and learn how event tree analysis is related to the identification and quantification of dominant accident sequences.
- Objectives:
  - Understand purposes of event tree analysis
  - Understand currently accepted techniques and notation for event tree construction
  - Understand purposes and techniques of accident sequence identification
  - Understand how to simplify event trees
  - Understand how event tree logic is used to quantify PRAs
- References: NUREG/CR-2300, NUREG/CR-2728

Event Trees

- Typically used to model the response to an initiating event
- Features:
  - Generally, one system-level event tree for each initiating event group is developed
  - Identifies systems/functions required for mitigation
  - Identifies operator actions required for mitigation
  - Identifies event sequence progression
  - End-to-end traceability of accident sequences leading to bad outcome
- Primary use
  - Identification of accident sequences which result in some outcome of interest (usually core damage and/or containment failure)
  - Basis for accident sequence quantification

Simple Event Tree



Required Information

- Knowledge of accident initiators
- Thermal-hydraulic response during accidents
- Knowledge of mitigating systems (frontline and support) operation
- Know the dependencies between systems
- Identify any limitations on component operations
- Knowledge of procedures (system, abnormal, and emergency)

Principal Steps in Event Tree Development

- Determine boundaries of analysis
- Define critical plant safety functions available to mitigate each initiating event
- Generate functional event tree (optional)
  - Event tree heading - order & development
  - Sequence delineation
- Determine systems available to perform each critical plant safety function
- Determine success criteria for each system for performing each critical plant safety function
- Generate system-level event tree
  - Event tree heading - order & development
  - Sequence delineation

Determining Boundaries

- Mission time
  - Sufficient to reach stable state (generally 24 hours)
- Dependencies among safety functions and systems
  - Includes shared components, support systems, operator actions, and physical processes
- End States (describe the condition of both the core and containment)
  - Core OK
  - Core vulnerable
  - Core damage
  - Containment OK
  - Containment failed
  - Containment vented
- Extent of operator recovery

Critical Safety Functions

Example safety functions for core & containment

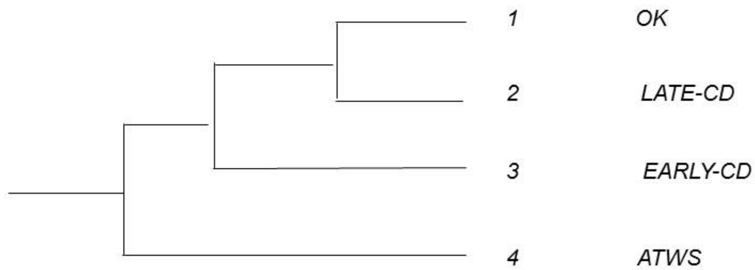
- Reactor subcriticality
- Reactor coolant system overpressure protection
- Early core heat removal
- Late core heat removal
- Containment pressure suppression
- Containment heat removal
- Containment integrity

Functional Event Tree

- High-level representation of vital safety functions required to mitigate abnormal event
  - Generic response of the plant to achieve safe and stable condition
- One functional event tree for transients and one for LOCAs
- Guides the development of more detailed system-level event tree model
- Generation of functional event trees not necessary; system-level event trees are the critical models
  - Could be useful for advanced reactor PRAs

Functional Event Tree

Initiating Event	Reactor Trip	Short term core cooling	Long term core cooling	SEQ #	STATE
IE	RX-TR	ST-CC	LT-CC		



BWR Mitigating Systems

Function	Systems
Reactivity Control	Reactor Protection System, Standby Liquid Control, Alternate Rod Insertion
RCS Overpressure Protection	Safety/Relief Valves
Coolant Injection	High Pressure Coolant Injection, High Pressure Core Spray, Reactor Core Isolation Cooling, Low Pressure Core Spray, Low Pressure Coolant Injection (RHR) Alternate Systems- Control Rod Drive Hydraulic System, Condensate, Service Water, Firewater
Decay Heat Removal	Power Conversion System, Residual Heat Removal (RHR) modes (Shutdown Cooling, Containment Spray, Suppression Pool Cooling)

System Success Criteria

- Identify systems which can perform each function
- Often includes if the system is automatically or manually actuated.
- Identify minimum complement of equipment necessary to perform function (often based on thermal/hydraulic calculations, source of uncertainty)
  - Calculations often realistic, rather than conservative
- May credit non-safety-related equipment where feasible

PWR Mitigating Systems

Function	Systems
Reactivity Control	Reactor Protection System
RCS Overpressure Protection	Safety valves, Pressurizer power-operated relief valves (PORV)
Coolant Injection	Accumulators, High Pressure Safety Injection, Chemical Volume and Control System, Low Pressure Safety Injection (LPSI), High Pressure Recirculation (may require LPSI)
Decay Heat Removal	Power Conversion System (main feedwater), Auxiliary Feedwater, Residual Heat Removal (RHR), Feed and Bleed (PORV + HPSI)

Example Success Criteria

IE	Reactor Trip	Short Term Core Cooling	Long Term Core Cooling
Transient	Auto Rx Trip or Man. Rx Trip	PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECI	PCS or 1 of 3 AFW or 1 of 2 PORVs & 1 of 2 ECR
Medium or Large LOCA	Auto Rx Trip or Man. Rx Trip	1 of 2 ECI	1 of 2 ECR

Two Basic Approaches for Event Tree Models

- Two methods are generally used to develop detailed event trees
- Event trees with boundary conditions (many event trees constructed, each with a unique set of support system BC)
  - Involves analyst quantification and identification of intersystem dependencies
  - Sometimes called Large-ET/Small-FT or PL&G approach
- Linked fault trees (event trees are the mechanism for linking the fault trees)
  - Employs Boolean logic and fault tree models to pick up intersystem dependencies
  - Sometimes called Small-ET/Large-FT approach, used by most of the PRA community

Event Tree with Boundary Conditions

- Modeling Approach
  - Objective: Explicitly separate-out dependencies to facilitate quantification of sequences
  - Focuses attention on context (i.e., the boundary conditions) for performance
  - Requires intermediate numerical results (conditional split fractions)
  - Often implemented using multiple, linked event trees
  - Sometimes referred to as Large-ET approach

Linked Fault Tree Approach

- Automatic treatment of shared event/system dependencies
  - Support system fault trees are linked into front-line and other support system fault trees
- One-step quantification
- Often use large, general-purpose fault trees
- Used by SPAR models and majority of utility PRAs
- Used in NUREG-1150 studies

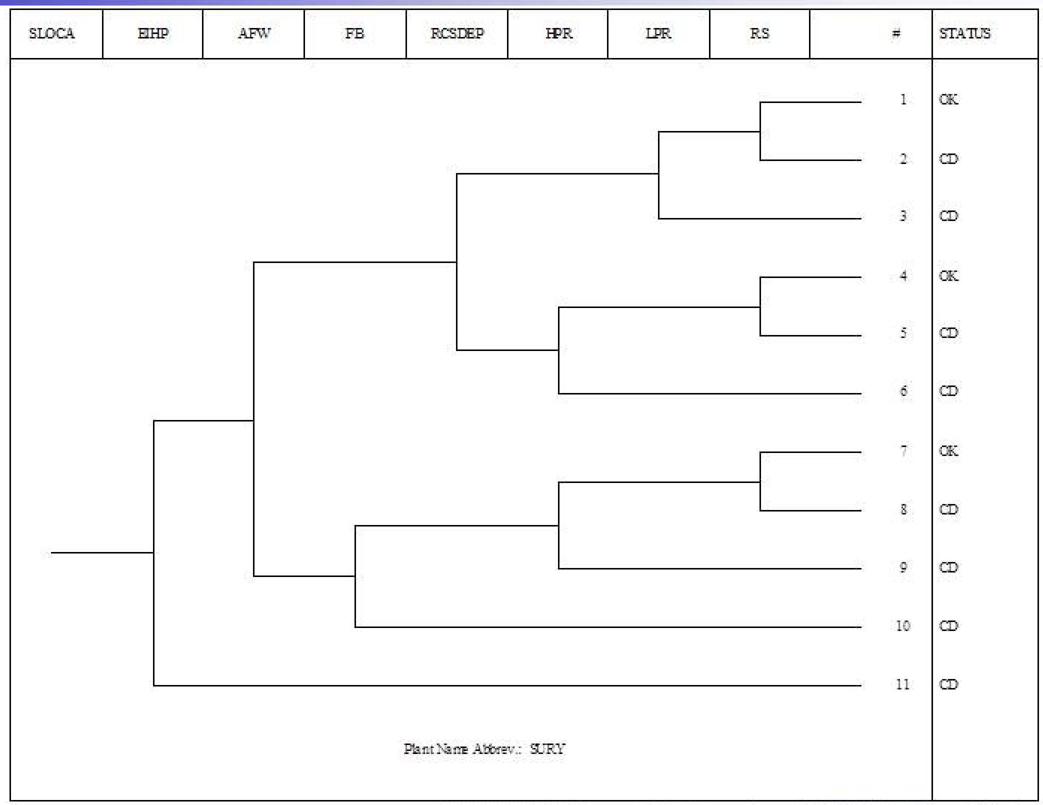
System-Level Event Tree Development

- A system-level event tree consists of an initiating event (one per tree), followed by a number of headings (top events), and a sequence of events representing the success or failure of the top events
- Top events represent the systems, components, and/or human actions required to mitigate the initiating event
- To the extent possible, top events are ordered in the time-related sequence in which they would occur
  - Selection of top events and ordering reflect emergency procedures
- Each node (or branch point) below a top event represents the success or failure of the respective top event
  - Logic is typically binary
    - Downward branch – failure of top event
    - Upward branch – success of top event
  - Logic can have more than two branches, with each branch representing a specific status of the top event

System-Level Event Tree Development (Continued)

- Dependencies among systems(needed to prevent core damage) are identified
  - Support systems can be included as top events to account for significant dependencies (e.g., diesel generator failure in station blackout event tree)
- Timing of important events (e.g., physical conditions leading to system failure) determined from thermal-hydraulic calculations
- Branches can be pruned logically (i.e., branch points for specific nodes removed) to remove unnecessary combinations of system success criteria requirements
  - This minimizes the total number of sequences that will be generated and eliminates illogical sequences
- Branches can transfer to other event tress for development
- Each path of an event tree represents a potential scenario
- Each potential scenario results in either prevention of core damage or onset of core damage (or a particular end state of interest)

Small LOCA Event Tree from Surry SDP Notebook

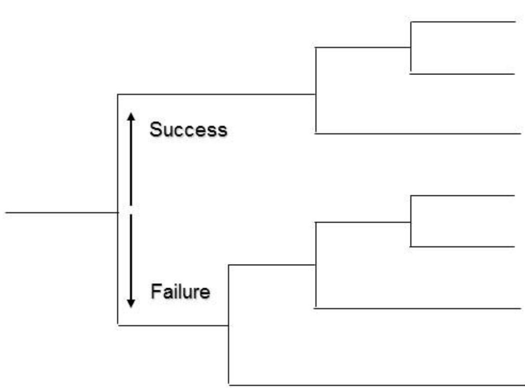


Event Tree Reduction and Simplification

- Single transient event tree can be drawn with specific IE dependencies included at the fault tree level
- Event tree structure can often be simplified by reordering top events
  - Example – Placing ADS before LPCI and CS on a BWR transient event tree
- Event tree development can be stopped if a partial sequence frequency at a branch point can be shown to be very small
- If at any branch point, the delineated sequences are identical to those in delineated in another event tree, the accident sequence can be transferred to that event tree (e.g., SORV sequences transferred to LOCA trees)
- Separate secondary event trees can be drawn for certain branches to simplify the analysis (e.g., ATWS tree)

System Level Event Tree Determines Sequence Logic

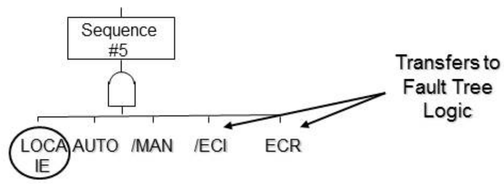
Initiating Event	*Rx Trip*	*Rx Trip*	*ST Core Cooling*	*LT Core Cooling*	*SEQ #*	*STATE*	*LOGIC*
LOCA	*AUTO*	*MAN*	*ECI*	*ECR*			



SEQ #	*STATE*	*LOGIC*
1	*OK*	
2	*LATE-CD*	*/AUTO*/ECI*ECR*
3	*EARLY-CD*	*/AUTO*ECI*
4	*OK*	
5	*LATE-CD*	*AUTO*/MAN*/ECI*ECR*
6	*EARLY-CD*	*AUTO*/MAN*ECI*
7	*ATWS*	*AUTO*MAN*

Sequence Logic Used to Combine System Fault Trees into Accident Sequence Models

- System fault trees (or cut sets) are combined, using Boolean algebra, to generate core damage accident sequence models.
  - CD seq. #5 = LOCA * AUTO * /MAN * /ECI * ECR



Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 55

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Sequence Cut Sets Generated From Sequence Logic

- Sequence cut sets generated by combining system fault trees (or cut sets) comprised by sequence logic
  - Cut sets can be generated from sequence #5 “Fault Tree”
    - Sequence #5 cut sets = (LOCA) * (AUTO cut sets) * (/MAN cut sets) * (/ECI cut sets) * (ECR cut sets)
    - Or, to simplify the calculation (via “delete term”)
      - Sequence #5 cut sets ≈ (LOCA) * (AUTO cut sets) * (ECR cut sets) - any cut sets that contain MAN + ECI cut sets are deleted

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 56

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Plant Damage State (PDS)

- Core Damage (CD) designation for end state not sufficient to support Level 2 analysis
  - Need details of core damage phenomena to accurately model challenge to containment integrity
- PDS relates core damage accident sequence to:
  - Status of plant systems (e.g., AC power operable?)
  - Status of RCS (e.g., pressure, integrity)
  - Status of water inventories (e.g., injected into RPV?)

Example Category Definitions for PDS Indicators

1. Status of RCS at onset of Core Damage

T	no break (transient)
A	large LOCA (6" to 29")
S1	medium LOCA (2" to 6")
S2	small LOCA (1/2" to 2")
S3	very small LOCA (less than 1/2")
G	steam generator tube rupture with SG integrity
H	steam generator tube rupture without SG integrity
V	interfacing LOCA

2. Status of ECCS

I	operated in injection only
B	operated in injection, now operating in recirculation
R	not operating, but recoverable
N	not operating and not recoverable
L	LPI available in injection and recirculation of RCS pressure reduced

3. Status of Containment Heat Removal Capability

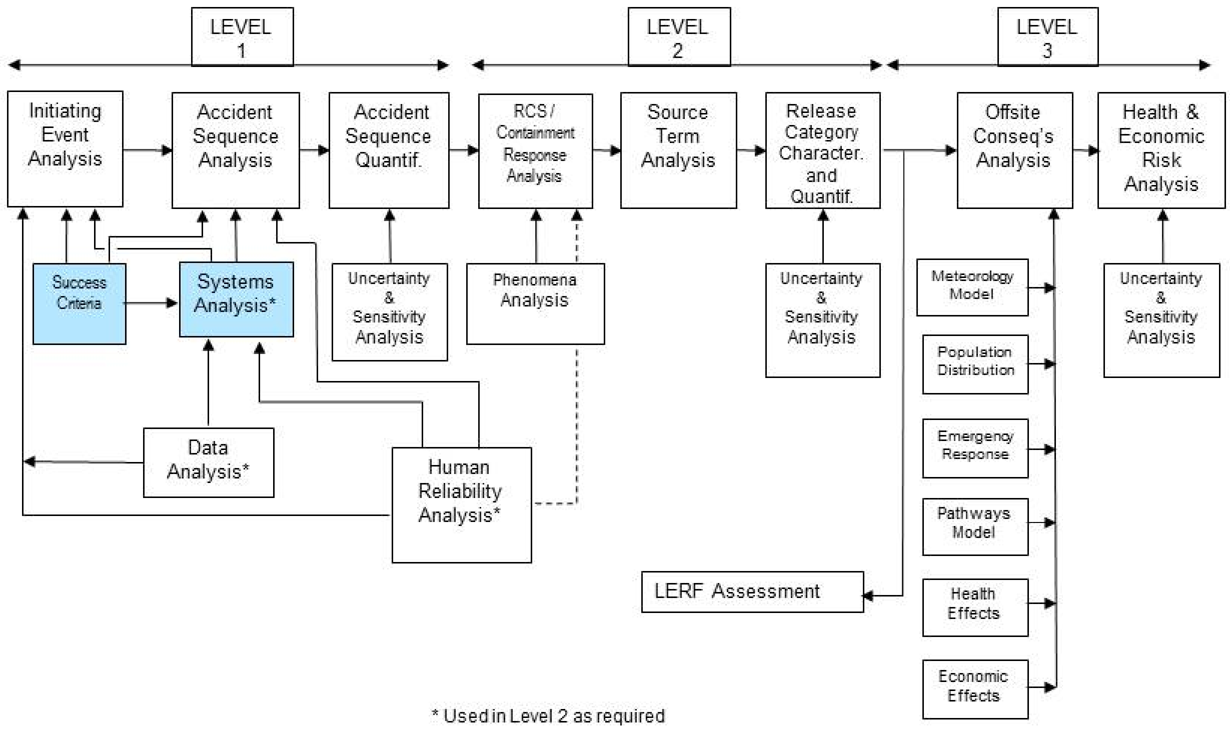
Y	operating or operable if/when needed
R	not operating, but recoverable
N	never operated, not recoverable

Systems Analysis

Systems Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



Systems (Fault Tree) Analysis

- **Purpose:** Students will learn purposes & techniques of fault tree analysis. Students will learn how appropriate level of detail for a fault tree analysis is established. Students will become familiar with terminology, notation, and symbology employed in fault tree analysis. In addition, a discussion of applicable component failure modes relative to the postulation of fault events will be presented.
- **Objectives:**
  - Provide a working knowledge of terminology, notation, and symbology of fault tree analysis
  - Demonstrate the method of fault tree analysis
  - Demonstrate the purposes and methods of fault tree reduction
- **References:**
  - NUREG-0492, Fault Tree Handbook
  - NUREG/CR-2300, PRA Procedures Guide
  - NUREG-1489, NRC Uses of PRA

Fault Tree Analysis Definition

*"An analytical technique, whereby an **undesired state** of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed **in the context of its environment and operation** to find all **credible** ways in which the undesired event can occur."*

NUREG-0492

Fault Trees

- Deductive analysis (event trees are inductive)
- Starts with undesired event definition
- Used to estimate system failure probability
- Explicitly models multiple failures
- Identify ways in which a system can fail
- Models can be used to find:
  - System “weaknesses”
  - System failure probability
  - Interrelationships between fault events

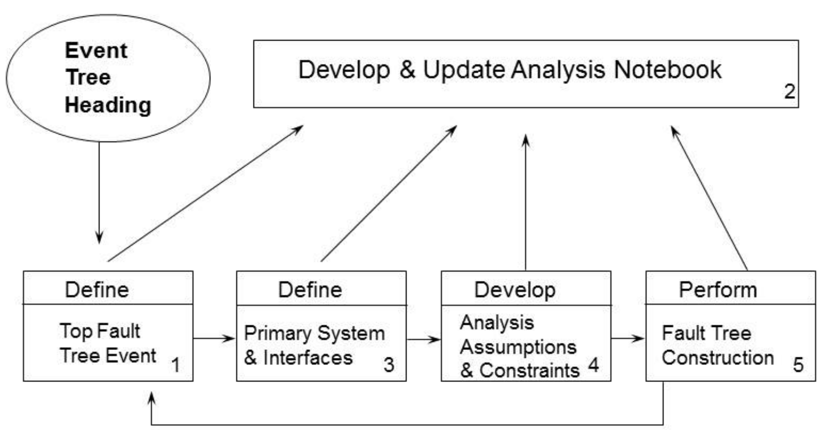
Fault Trees (cont.)

- Fault trees are graphic models depicting the various fault paths that will result in the occurrence of an undesired (top) event.
- Fault tree development moves from the top event to the basic events (or faults) which can cause it.
- Fault tree use gates to develop the fault logic in the tree.
- Different types of gates are used to show the relationship of the input events to the higher output event.
- Fault tree analysis requires thorough knowledge of how the system operates and is maintained.

System Mission Affects Model

- Demand based missions (binomial)
  - Normally in standby
  - Required to perform one (or more) times
  - e.g., actuation systems, relief valves
- Time based missions (Poisson)
  - Either in standby or normally operating
  - Required to operate for some length of time, which affects unreliability
  - e.g., ECCS, SWS

Fault Tree Development Process



1. Define Top Event

- Undesired event or state of system
  - Often corresponds to an event on an event tree
  - Based on success criterion for system
    - Typically initiating event dependent (e.g., HPI would have different success criteria for small LOCA vs. medium LOCA)
    - Can be sequence dependent
    - Success criteria determined from thermal/hydraulic calculations (i.e., computer code runs made to determine how much injection is needed to keep core covered given particular IE)
  - Success criterion used to determine failure criterion
    - Fault tree top event
  - Success criterion must be precise (e.g., "Uninterupted flow from 2/3 HPIS pumps for 24 hours through 2/4 injection lines"

2. Develop & Maintain Analysis Notebook

- Scope of analysis and system definition
- Notebook should include system design and operation information (normal and abnormal), support system requirements, instrumentation and control requirements, technical specifications, test and maintenance data, pertinent analytical assumptions, component locations.
- Notebook reflects the iterative nature of fault tree analysis.

3. Define Primary System & Interfaces

- A collection of discrete elements which interact to perform, in total or in part, a function or set of functions"
- System boundary definition depends on:
  - Information required from analysis
  - Level of resolution of data
- Clear documentation of system boundary definition is essential

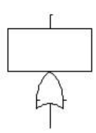
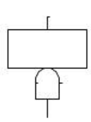
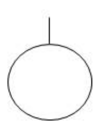
4. Develop Analysis Assumptions & Constraints

- Analytical assumptions must be developed to compensate for incomplete knowledge
- Rationale for assumptions should be specified and, wherever possible, supported by engineering analysis
- Document in notebook

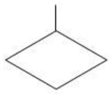
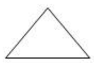
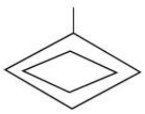
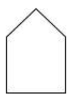
5. Fault Tree Construction

- Step-by-step postulation of system faults
- Utilization of standard symbology
- Postulation consistent with level of resolution of data & assumptions
- Iterative process

Fault Tree Symbols

Symbol		Description
	"OR" Gate	Logic gate providing a representation of the Boolean union of input events. The output will occur if at least one of the inputs occur.
	"AND" Gate	Logic gate providing a representation of the Boolean intersection of input events. The output will occur if all of the inputs occur.
	Basic Event	A basic component fault which requires no further development. Consistent with level of resolution in databases of component faults.

Fault Tree Symbols (cont.)

Symbol		Description
	Undeveloped Event	A fault event whose development is limited due to insufficient consequence or lack of additional detailed information
	Transfer Gate	A transfer symbol to connect various portions of the fault tree
	Undeveloped Transfer Event	A fault event for which a detailed development is provided as a separate fault tree and a numerical value is derived
	House Event	Used as a trigger event for logic structure changes within the fault tree. Used to impose boundary conditions on FT. Used to model changes in plant system status.

Event and Gate Naming Scheme

- A consistent use of an event naming scheme is required to obtain correct results
- Example naming scheme: XXX-YYY-ZZ-AAAA
- Where:
  - XXX is the system identifier (e.g., HPI)
  - YYY is the event and component type (e.g., MOV)
  - ZZ is the failure mode identifier (e.g., FS)
  - AAAAA is a plant component descriptor
- A gate naming scheme should also be developed and utilized - XXXaaa
  - XXX is the system identifier (e.g., HPI)
  - aaa is the gate number

Specific Failure Modes Modeled for Each Component

- Each component associated with a specific set of failure modes/mechanisms determined by:
  - Type of component
    - E.g., Motor-driven pump, air-operated valve
  - Normal/Standby state
    - Normally not running (standby), normally open
  - Failed/Safe state
    - Failed if not running, or success requires valve to stay open

Typical Component Failure Modes

- Active Components
  - Fail to Start
  - Fail to Run
  - Fail to Open/Close/Operate
  - Unavailability
    - Test or Maintenance Outage

Typical Component Failure Modes (cont.)

- Passive Components (Not always modeled in PRAs)
  - Rupture
  - Plugging (e.g., strainers/orifice)
  - Fail to Remain Open/Closed (e.g., manual valve)
  - Short (cables)

Component Boundaries

- Typically include all items unique to a specific component, e.g.,
  - Drivers for EDGs, MDPs, MOVs, AOVs, etc.
  - Circuit breakers for pump/valve motors
  - Need to be consistent with how data was collected
    - That is, should individual piece parts be modeled explicitly or implicitly
    - For example, actuation circuits (FTS) or room cooling (FTR)

Active Components Require "Support"

- Signal needed to "actuate" component
  - Safety Injection Signal starts pump or opens valve
  - Operator action may be needed to actuate
- Support systems might be required for component to function
  - AC and/or DC power
  - Service water or component water cooling
  - Room cooling

Definition of Dependent Failures

- Three general types of dependent failures:
  - Certain initiating events (e.g., fires, floods, earthquakes, service water loss) cause failure of multiple components
  - Intersystem dependencies including:
    - Functional dependencies (e.g., dependence on AC power)
    - Shared-equipment dependencies (e.g., HPCI and RCIC share common suction valve from CST)
    - Human interaction dependencies (e.g., maintenance error that disables separate systems such as leaving a manual valve closed in the common suction header from the RWST to multiple ECCS system trains)
  - Inter-component dependencies (e.g., design defect exists in multiple similar valves)
- The first two types are captured by event tree and fault tree modeling; the third type is known as common cause failure (i.e., the residual dependencies not explicitly modeled) and is treated parametrically

Common Cause Failures (CCFs)

- Conditions which may result in failure of more than one component, subsystem, or system
- Concerns:
  - Defeats redundancy and/or diversity
  - Data suggest high probability of occurrence relative to multiple independent failures

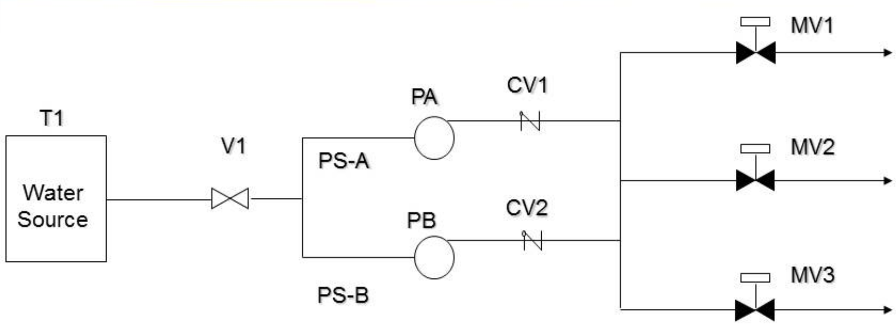
Common Cause Failure Mechanisms

- Environment
  - Radioactivity
  - Temperature
  - Corrosive environment
- Design deficiency
- Manufacturing error
- Test or Maintenance error
- Operational error

Two Common Fault Tree Construction Approaches

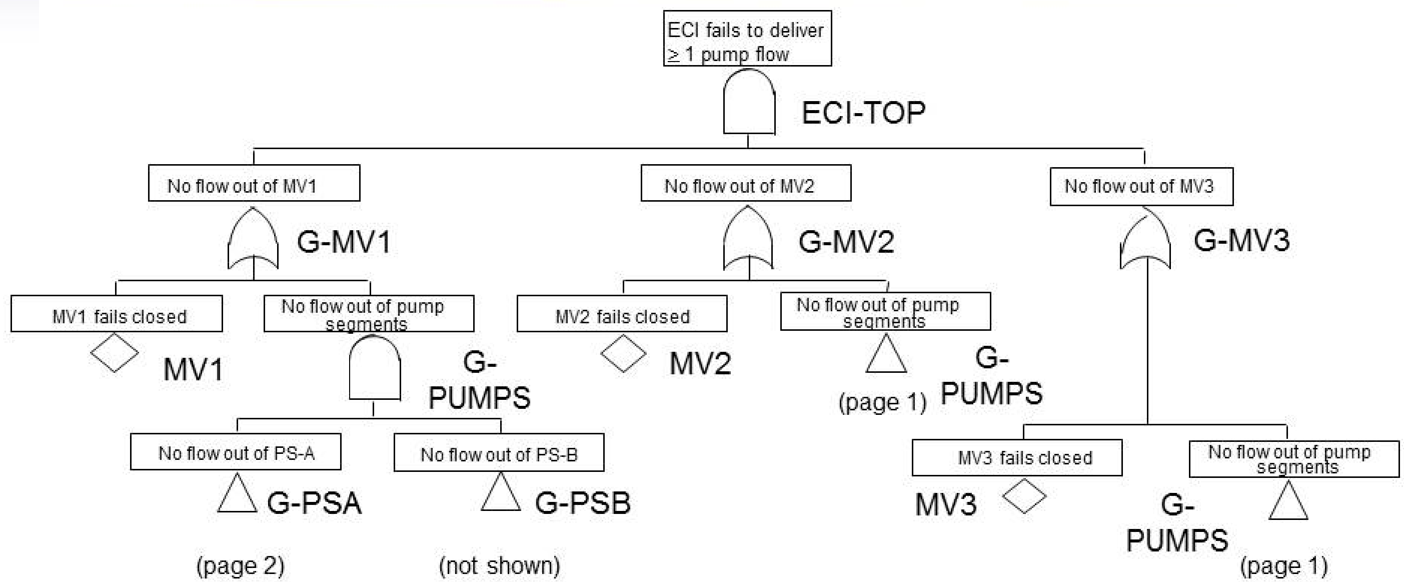
- "Sink to source"
  - Start with system output (i.e., system sink)
  - Modularize system into a set of pipe segments (i.e., group of components in series)
  - Follow reverse flow-path of system developing fault tree model as the system is traced
- Block diagram-based
  - Modularize system into a set of subsystem blocks
  - Develop high-level fault tree logic based on subsystem block logic (i.e., blocks configured in series or parallel)
  - Expand logic for each block

Example - ECI

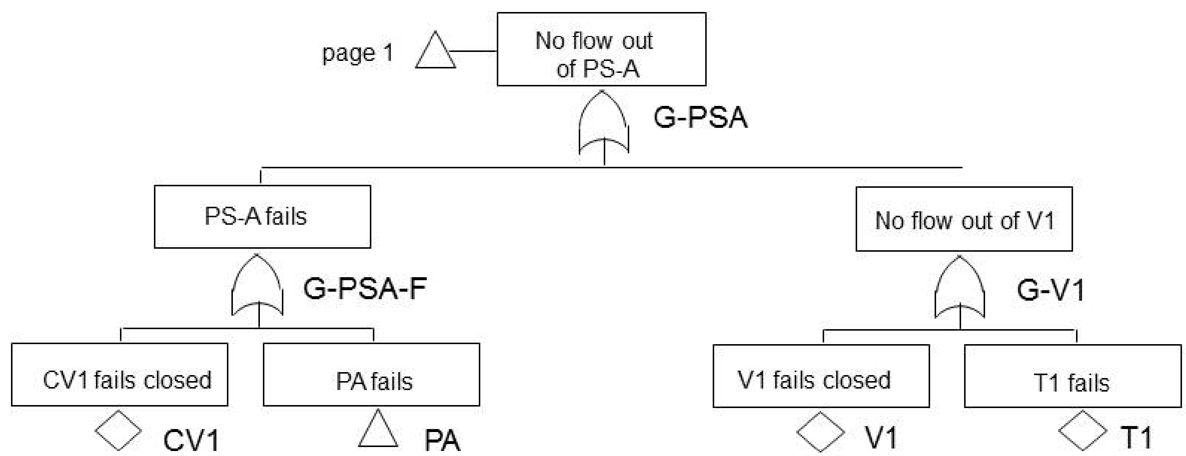


***Success Criteria**: Flow from any one pump through any one MV*
T_ tank
V_ manual valve, normally open
PS-_ pipe segment
P_ pump
CV_ check valve
MV_ motor-operated valve, normally closed

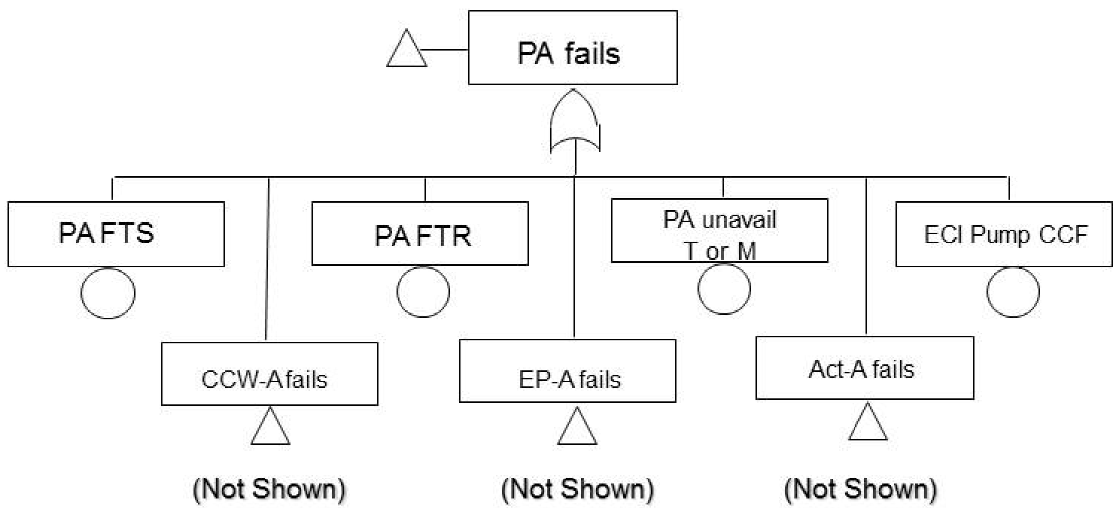
ECI System Fault Tree – "Sink to Source Method" (page 1)



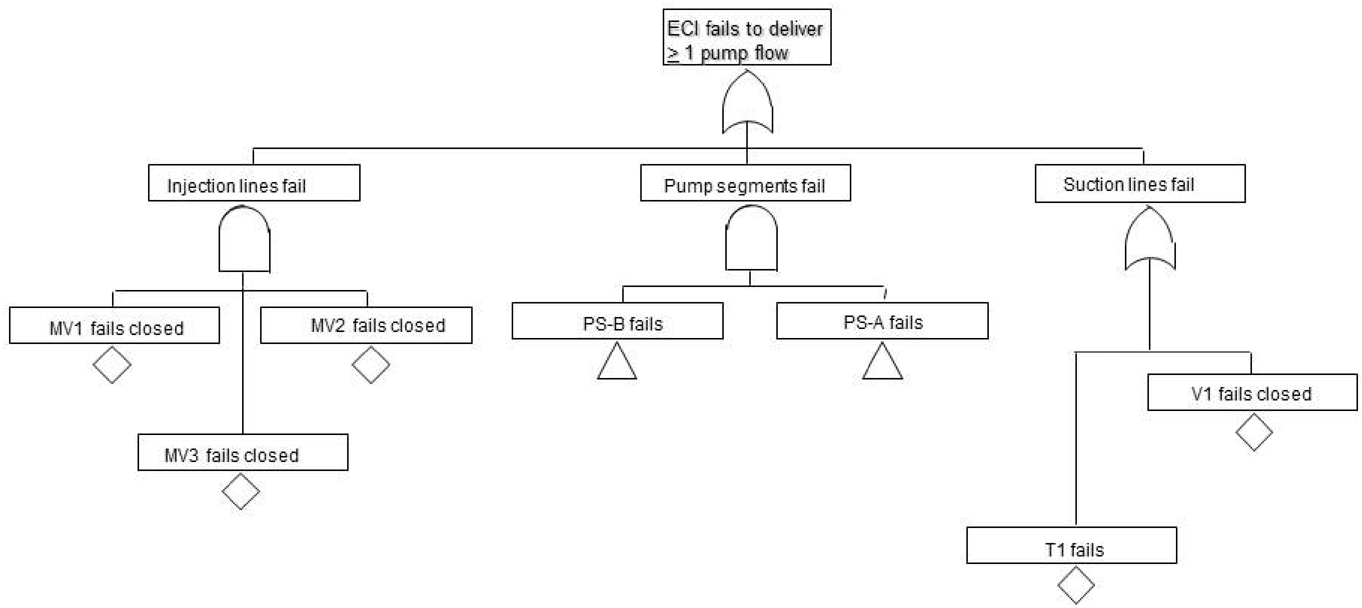
ECI System Fault Tree – “Sink to Source Method” (page 2)



ECI System Fault Tree – "Sink to Source Method" (page 3)



ECI System Fault Tree - Block Diagram Method



Boolean Fault Tree Reduction

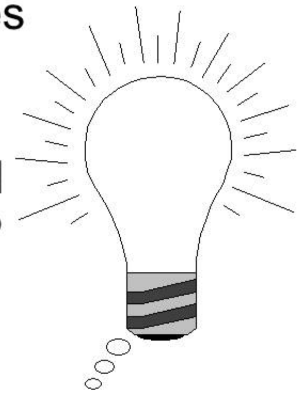
- Express fault tree logic as Boolean equation
- Apply rules of Boolean algebra to reduce terms
- Results in reduced form of Boolean equation

Rules of Boolean Algebra

Mathematical Symbolism	Engineering Symbolism		Designation
(1a) $X \cap Y = Y \cap X$ (1b) $X \cup Y = Y \cup X$	$X * Y = Y * X$ $X + Y = Y + X$	Algebra	Commutative Law
(2a) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ (2b) $X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X * (Y * Z) = (X * Y) * Z$ $X(YZ) = (XY)Z$ $X + (Y + Z) = (X + Y) + Z$		Associative Law
(3a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ (3b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X * (Y + Z) = (X * Y) + (X * Z)$ $X(Y+Z) = XY + XZ$ $X + (Y * Z) = (X + Y) * (X + Z)$		Distributive Law
(4a) $X \cap X = X$ (4b) $X \cup X = X$	**Important!** $\boxed{X * X = X \quad X + X = X}$	Important During Cut Set Generation	Idempotent Law
(5a) $X \cap (X \cup Y) = X$ (5b) $X \cup (X \cap Y) = X$	$X * (X + Y) = X$ $X + X * Y = X$		Law of Absorption
(6a) $X \cap X' = \Phi = 0$ (6b) $X \cup X' = \Omega = I$ (6c) $(X')' = X$	$X * /X = \Phi = 0$ $X + /X = \Omega = I$ $/(/X) = X$		Complementation
(7a) $(X \cap Y)' = X' \cup Y'$ (7b) $(X \cup Y)' = X' \cap Y'$	$/(X * Y) = /X + /Y$ $/(X + Y) = /X * /Y$		DeMorgan's Theorem

Minimal Cutset

A group of basic event failures (component failures and/or human errors) that are ***collectively necessary*** and ***sufficient*** to cause the TOP event to occur.



Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 91

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Reduction of Example Fault Tree

ECI-TOP = G-MV1 * G-MV2 * G-MV3.

Start Substituting

ECI-TOP = (MV1 + G-PUMPS) * (MV2 + G-PUMPS) * (MV3 + G-PUMPS)

ECI-TOP = (MV1 * MV2 * MV3) +
(MV1 * MV2 * G-PUMPS) +
(MV1 * G-PUMPS * MV3) +
(MV1 * G-PUMPS * G-PUMPS) +
(G-PUMPS * MV2 * MV3) +
(G-PUMPS * MV2 * G-PUMPS) +
(G-PUMPS * G-PUMPS * MV3) +
(G-PUMPS * G-PUMPS * G-PUMPS).

Keep substituting and Performing Boolean Algebra (e.g., X*X = X)

ECI-TOP = (MV1 * MV2 * MV3) +
(MV1 * MV2 * G-PUMPS) +
(MV1 * G-PUMPS * MV3) +
(MV1 * G-PUMPS) +
(G-PUMPS * MV2 * MV3) +
(G-PUMPS * MV2) +
(G-PUMPS * MV3) +
(G-PUMPS).

ECI-TOP = (MV1 * MV2 * MV3) +
(G-PUMPS).

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 92

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Reduction of Example Fault Tree (cont.)

```
ECI-TOP = (MV1 * MV2 * MV3) +
          (G-PSA * G-PSB).

ECI-TOP = (MV1 * MV2 * MV3) +
          ((G-PSA-F + G-V1) * (G-PSB-F + G-V1)).

ECI-TOP = (MV1 * MV2 * MV3) +
          (G-PSA-F * G-PSB-F) +
          (G-PSA-F * G-V1) +
          (G-V1 * G-PSB-F) +
          (G-V1).

ECI-TOP = (MV1 * MV2 * MV3) +
          (G-PSA-F * G-PSB-F) +
          (G-V1).

ECI-TOP = (MV1 * MV2 * MV3) +
          (PA + CV1) * (PB + CV2) +
          (V1 + T1).

ECI-TOP = MV1 * MV2 * MV3 +
          PA * PB +
          PA * CV2 +
          CV1 * PB +
          CV1 * CV2 +
          V1 +
          T1.
```


Fault Tree Pitfalls

- Inconsistent or unclear basic event names
  - X*X = X, so if X is called X1 in one place and X2 in another place, incorrect results are obtained
- Missing dependencies or failure mechanisms
  - An issue of completeness
- Unrealistic assumptions
  - Availability of redundant equipment
  - Credit for multiple independent operator actions
  - Violation of plant LCO
- Modeling T&M unavailability can result in illegal cutsets
- Putting recovery in FT might give optimistic results
- Logic loops

Logic Loops Result From Circular Support Function Dependencies

- **ECI pump requires AC power**
- **AC power supplied from either Offsite Power or Diesel Generators (DGs)**
- **DGs require Component Cooling Water (CCW) for cooling**
- **CCW pumps require AC power**

Results

- Sanity checks on cut sets
  - Symmetry
    - If Train-A failures appear, do Train-B failures also appear?
  - Completeness
    - Are all redundant trains/systems really failed?
    - Are failure modes accounted for at component level?
  - Realism
    - Do cut sets make sense (i.e., Train-A out for T&M ANDed with Train-B out for T&M)?
  - Predictive Capability
    - If system model predicts total system failure once in 100 system demands, is plant operating experience consistent with this?

Human Reliability Analysis

ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

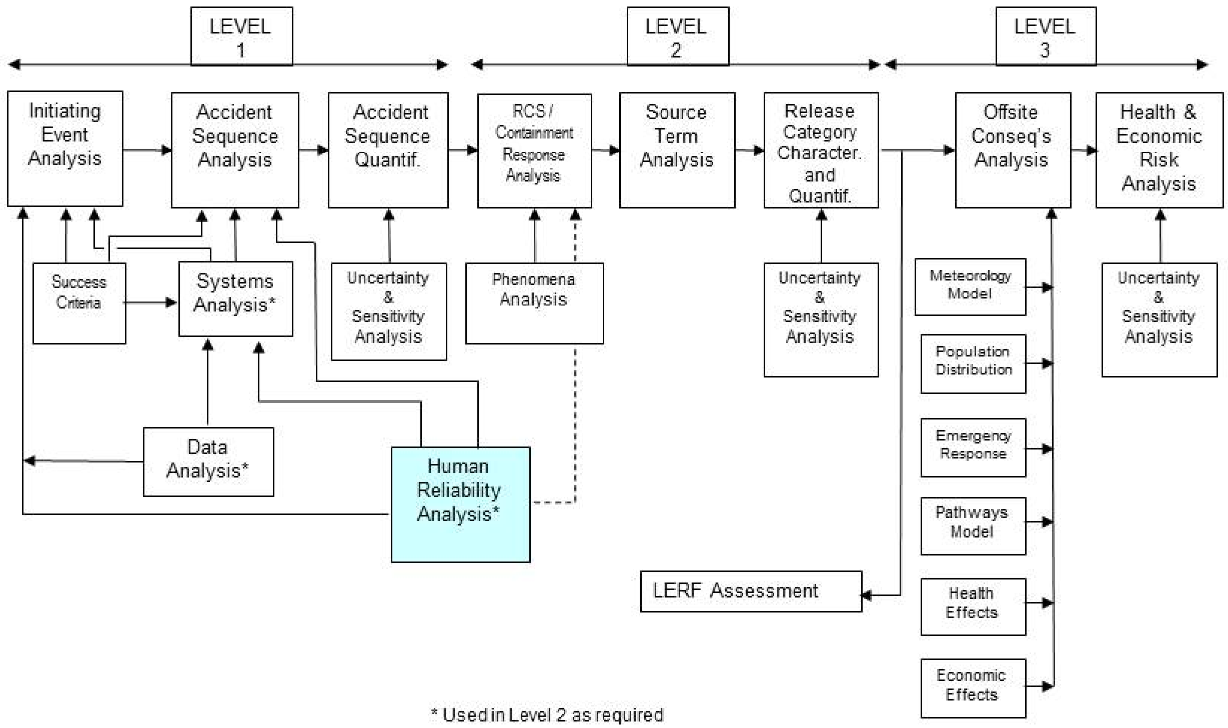
Curtiss Wright Flow Control Company SCIENTECH

SAIC From Science to Solutions™ Science Applications International Corporation

Human Reliability Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Human Reliability Analysis

Purpose: This session will provide a generalized, high-level introduction to the topic of human reliability and human reliability analysis in the context of PRA.

Objectives: Provide students with an understanding of:
- The goals of HRA and important concepts and issues
- The basic steps of the HRA process in the context of PRA
- Basic aspects of selected HRA methods

HRA Purpose

Why Develop a HRA?

– **PRA reflects the as-built, as-operated plant**
  - **HRA models the "as-operated" portion**

Definition of HRA

– A **structured approach** used to **identify** potential human failure events (HFEs) and to systematically **estimate the probability** of those errors using data, models, or expert judgment

HRA Produces

– Qualitative evaluation of the factors impacting human errors and successes

– Human error probabilities (HEPs)

Human Reliability Analysis

- Starts with the basic premise that the humans can be represented as either:.
  - A component of a system, or
  - A failure mode of a system or component.
- Identifies and quantifies the ways in which human actions initiate, propagate, or terminate fault & accident sequences.
- Human actions with both positive and negative impacts are considered in striving for realism.
- A difficult task in a PRA since need to understand the plant hardware response, the operator response, and the accident progression modeled in the PRA.

Human Reliability Analysis Objectives

Ensure that the **impacts of plant personnel** actions are reflected in the assessment of risk in such a way that:

a) both **pre-initiating event and post-initiating event** activities, including those modeled in support system initiating event fault trees, are addressed.

b) logic model elements are defined to represent the effect of such personnel actions on **system availability**/unavailability and on **accident sequence** development.

c) plant-specific and scenario-specific factors are accounted for, including those factors that influence either what activities are of interest or human performance.

d) human performance issues are addressed in an integral way so that **issues of dependency are captured**.

Ref: ASME/RA-Sb-2005

Modeling of Human Actions

- Human Reliability Analysis provides a structured modeling process
- HRA **process steps**:
  - Identification & Definition
    - Human interaction identified, then defined for use in the PRA as a Human Failure Event (HFE)
    - Includes HFE categorization as to the type of action
  - Qualitative analysis of context & performance shaping factors
  - Quantification of Human Error Probability (HEP)
  - Dependency
  - Documentation

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 103

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Categories Of Human Failure Events in PRA

- Operator actions can occur throughout the accident sequence
  - **Pre-initiator errors** (latent errors, unrevealed) occur before the initiating event.
    - May occur in or out of the main control room
    - Failure to restore from test/maintenance
    - Miscalibration
    - Often captured in equipment failure data
    - For HRA the focus is on equipment being left unavailable or not working exactly right.
  - Operator actions contribute or **cause initiating events**
    - Usually implicitly included in the data used to quantify initiating event frequencies.

Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 104

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Categories Of Human Failure Events in PRA (cont'd)

– **Post-initiator errors** occur after reactor trip. Examples:
  - Operation of components that have failed to operate automatically, or require manual operation.
  - "Event Tree top event" operator actions modeled in the event trees (e.g., failure to depressurize the RCS in accordance with the EOPs)
  - Recovery actions for hardware failures (example - aligning an alternate cooling system, subject to available time)
  - Recovery actions following crew failures (example - providing cooling late after an earlier operator action failed)
  - Operation of components from the control room or locally.

Categorization & Definition of Human Failure Events in PRA (cont'd)

- Additional "category", error of commission or aggravating errors of commission, typically out of scope of most PRA models.
  – Makes the plant response worse than not taking an action at all
- Within each operator action, there are generally, two types of error:
  – Diagnostic error (cognition) – failure of detection, diagnosis, or decision-making
  – Execution error (manipulation) – failure to accomplish the critical steps, once they have been decided, typically due to the following error modes.
    - Errors of omission (EOO, or Skip) -- Failure to perform a required action or step, e.g., failure to monitor tank level
    - Errors of commission (EOC, or Slip) -- Action performed incorrectly or wrong action performed, e.g., opened the wrong valve, or turned the wrong switch.

Human Reliability Analysis is the Combination of Three Basic Steps

Identification & Definition	Qualitative	Quantification
taxonomies context from event trees error producing conditions cognitive error errors of commission	Context from event trees & fault trees generic error models performance shaping factors	data availability databases simulation empirical approaches

- From about 1980 on, some 38 different HRA methods have been developed - almost all centered on quantification.
- There is no universally accepted HRA method (to date).
- The context of the operator action comes directly from the event trees and fault trees although some techniques have recently ventured beyond.

Identification & Definition Process

- **Identify** Human Failure Events (HFEs) to be considered in plant models.
  - Based on PRA event trees, fault trees, & procedures.
    - Includes front line systems & support systems.
  - Often done in conjunction with the PRA modelers (Qualitative screening)
  - Normal Plant Ops-- Identify potential errors involving miscalibration or failure to restore equipment by observing test and maintenance, reviewing relevant procedures and plant practices
    - Guidelines for pre-initiator qualitative screening
  - Post-Trip Conditions-- Determine potential errors in diagnosing and manipulating equipment in response to various accident situations

Identification & Definition Process (cont.)

- PRA model identifies component/system/function failures
- HRA requires **definition** of supporting information, such as:
  - for post-initiating events, the cues being used, timing and the emergency operating procedure(s) being used.
- ATHEANA – identify the "base case" for accident scenario
  - Expected scenario – including operator expectations for the scenario
  - Sequence and timing of plant behavior – behavior of plant parameters
  - Key operator actions

Identification Process (cont'd)

- Review emergency operating procedures to identify potential human errors
- Flow chart the EOPs to identify critical decision points and relevant cues for actions
- If possible, do early observations of simulator exercises
- List human actions that could affect course of events (qualitative screening)

Qualitative Analysis

- **Context**, a set of plant conditions based on the PRA model
  - Initiating event & event tree sequence
    - includes preceding hardware & operator successes/failures
  - Cues, Procedure, Time window
- Qualitatively examine factors that could influence performance (**Performance Shaping Factors, PSFs**) such as
  - Training/experience - Scenario timing
  - Clarity of cues - Workload
  - Task complexity - Crew dynamics
  - Environmental cond. - Accessibility
  - Human-machine interface
  - Management and organizational factors
- Note ATHEANA models "Error Forcing Context" consisting of plant context & scenario-specific factors that would influence operator response.

Performance Shaping Factors (PSFs)

- Are people-, task-, environmental-centered influences which could affect performance.
- Most HRA modeling techniques allow the analyst to account for PSFs during their quantification procedure.
- PSFs can Positively or Negatively impact human error probabilities
- PSFs are identified and evaluated in the human reliability task analysis

Quantifying the Human Error Probability

- Quantifying is the process of
  - selecting an HRA method then
  - calculating the Human Error Probability for a HFE
    - based on the qualitative assessment and
    - based on the context definition.
- The calculation steps depend on the methodology being used.
- Data sources – the input data for the calculations typically comes operator talk-throughs &/or simulations, while some methods the data comes from databanks or expert judgment.
- The result is typically called a Human Error Probability or HEP

Levels of Precision

- Conservative (screening) level useful for determining which human errors are the most significant contributors to overall system error
- Those found to be potentially significant contributors can be profitably analyzed in greater detail (which often lowers the HEP)

Screening

- Too many HFEs to do detailed quantification?
  - Trying to reduce level of effort, resources
  - Used during IPE era for initial model development
- ASME PRA Standard
  - Pre-initiators: screening pre-initiators is addressed in High Level Requirement HLR-HR-B
  - Post-initiators: screening is not addressed explicitly as a High Level Requirement
    - Supporting requirement HR-G1 limits the PRA to Capability Category I if conservative/screening HEPs used.
- Thus, screening is more appropriate to Fire PRA.

Detailed Quantification

- Point at which you bring all the information you have about each event
  - PSFs, descriptions of plant conditions given the sequence
  - Results from observing simulator exercises
  - Talk-throughs with operators/trainers
  - Dependencies
- Quantification Methods
  - Major problem is that none of the methods handle all this information very well
- Assign HEPs to each event in the models

HRA Methods

- Attempt to reflect the following characteristics:
  - plant behavior and conditions
  - timing of events and the occurrence of human action cues
  - parameter indications used by the operators and changes in those parameters as the scenario proceeds
  - time available and locations necessary to implement the human actions
  - equipment available for use by the operators based on the sequence
  - environmental conditions under which the decision to act must be made and the actual response must be performed
  - degree of training, guidance, and procedure applicability

Common HRA Methodologies in the USA

- Technique for Human Error Rate Prediction (THERP)
- Accident Sequence Evaluation Program (ASEP) HRA Procedure
- Cause-Based Decision Tree (CBDT) Method
- Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) Method
- Standardized Plant Analysis Risk HRA (SPAR-H) Method
- A Technique for Human Event Analysis (ATHEANA)

Caused Based Decision Tree (CBDT) Method (EPRI)

Series of decision trees address potential causes of errors, produces HEPs based on those decisions.

- Half of the decision trees involve the man-machine cue interface:
  - Availability of relevant indications (location, accuracy, reliability of indications);
  - Attention to indications (workload, monitoring requirements, relevant alarms);
  - Data errors (location on panel, quality of display, interpersonal communications);
  - Misleading data (cues match procedure, training in cue recognition, etc.);
- Half of the decision trees involve the man-procedure interface:
  - Procedure format (visibility and salience of instructions, place-keeping aids);
  - Instructional clarity (standardized vocabulary, completeness of information, training provided);
  - Instructional complexity (use of "not" statements, complex use of "and" & "or" terms, etc.); and
  - Potential for deliberate violations (belief in instructional adequacy, availability and consequences of alternatives, etc.).
- For time-critical actions, the CBDT is supplemented by a time reliability correlation

EPRI HRA Calculator

- Software tool
- Uses SHARP1 as the HRA framework
- Post-initiator HFE methods:
  - For diagnosis, uses CBDT (decision trees) and/or HCR/ORE (time based correlation)
  - For execution, THERP for manipulation
- Pre-Initiator HFE methods:
  - Uses THERP and ASEP to quantify pre-initiator HFEs

ATHEANA

- Experience-based (uses knowledge of domain experts, e.g., operators, pilots, trainers,etc.)
- Focuses on the error-forcing context
- Links plant conditions, performance shaping factors (PSFs) and human error mechanisms
- Consideration of dependencies across scenarios
- Attempts to address PSFs holistically (considers potential interactions)
- Structured search for problem scenarios and unsafe actions

Dependencies

Dependency refers to the extent to which failure or success of one action will influence the failure or success of a subsequent action.

1) Human interaction depends on the accident scenario, including the type of initiating event
2) Dependencies between multiple human actions modeled within the accident scenario,
3) Human interactions performed during testing or maintenance can defeat system redundancy,
4) Multiple human interactions modeled as a single human interaction may involve significant dependencies. (from SHARP1)

HRA Process Summary

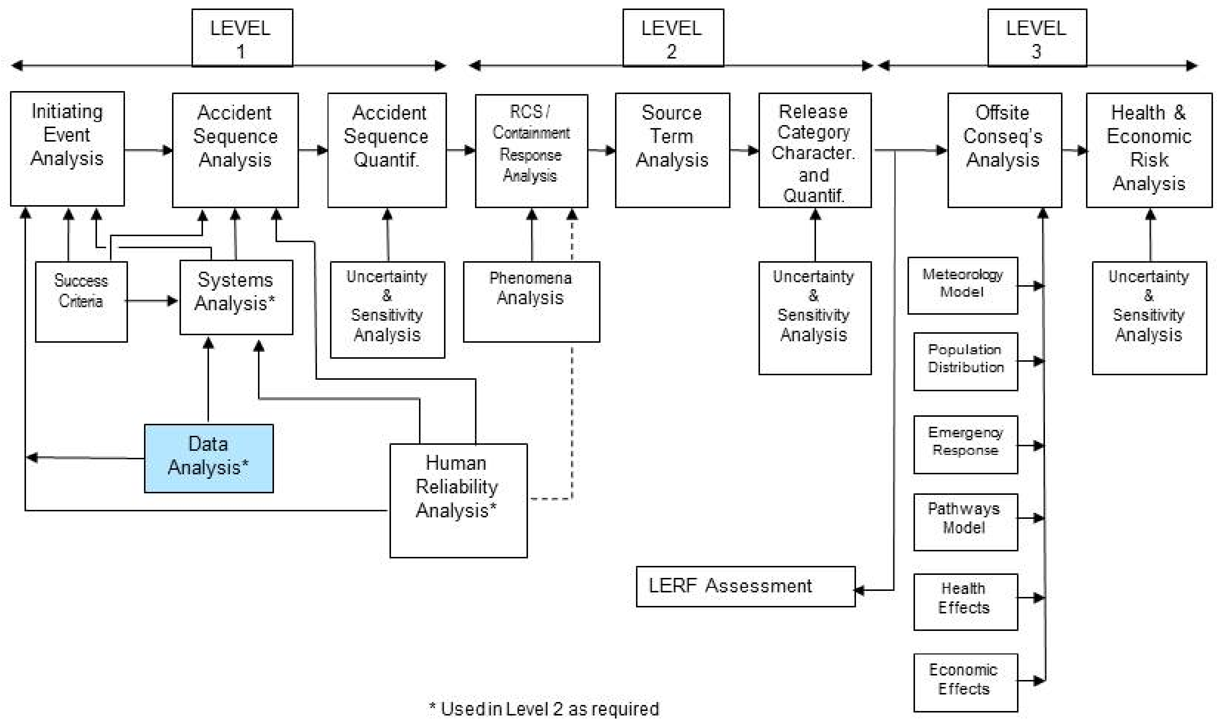
- Human Reliability Analysis provides a structured modeling process
- Human Interactions are incorporated as Human Failure Events in a PRA, **identification & definition** finds the HFEs
- Post-initiator operator actions consist of:
  - **Qualitative analysis** of Context and Performance Shaping Factors
    - Operator action must be feasible (for example, sufficient time, sufficient staff, sufficient cues, access to the area)
  - Then **Quantitative assessment (using an HRA method**)
    - Includes dependency evaluation
- Two Parts of the Each Human Failure Event (HFE)
  - Operator must recognize the need/demand for the action (**cognition**) AND
  - Operator must take steps (**execution**) to complete the actions.

Data Analysis

Data Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Data Analysis

- Purpose: Students will be introduced to sources of initiating event data; and hardware data and equipment failure modes, including common cause failure, that are modeled in PRAs.

- Objectives: Students will be able to:
  - Understand parameters typically modeled in PRA and how each is quantified.
  - Understand what is meant by the terms
    - Generic data
    - Plant-specific data
    - Bayesian updating
  - Describe what is meant by common-cause failure, why it is important, and how it is included in PRA

References

- NUREG/CR-6823 PRA Data Handbook
- NUREG/CR-5750 IE Frequency Data
- NUREG/CR-5500 Reliability Study (multiple systems)
- NUREG/CR-6928 IE and Component Data
- NUREG/CR-2300 PRA Procedures Guide
- NUREG-1489 (App. C) NRC Use of PRA
- NUREG/CR-5485, Guidelines on modeling Common-Cause failures in PRA
- NUREG/CR-5497, Common-Cause Failure Parameter Estimations
- NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Definition and Classification
- N. Siu and D. Kelly, "Bayesian Parameter Estimation in PRA," tutorial paper in Reliability Engineering and System Safety 62 (1998) 89-116.
- Martz and Waller, "*Bayesian Reliability Analysis*."

PRA Parameters

- Initiating Event Frequencies
- Basic Event Probabilities
  - Hardware
    - component reliability (fail to start/run/operate/etc.)
    - component unavailability (due to test or maintenance)
  - Common Cause Failures
  - Human Errors (discussed in previous session)

Categories of Data

- Two basic categories of data: plant-specific and generic
- Some guidance on the use of each category:
  - Not feasible or necessary to collect plant-specific data for all components in a PRA (extremely reliable components may have no failures)
  - Some generic data sources are non-conservative (e.g., LERS do not report all failures)
  - Inclusion of plant-specific data lends credibility to the PRA
  - Inclusion of plant-specific data allows comparison of plant equipment performance to industry averages
- Should use plant-specific data whenever possible, as dictated by the availability of relevant information

Initiating Event Frequencies

- Typically combination of:
  - Generic data for rare events (e.g., LOCAs)
  - Plant-specific data for more common events (most transients)
- An IE frequency is a failure rate (λ)
  - Poisson: prob(r failures in time t) = $(1/r!)\, e^{-\lambda t}(\lambda t)^r$
    prob(r >0, in time t) = $1-e^{-\lambda t} \approx \lambda t$ (for $\lambda t << 1$)
- Parameters required are number of plant scrams and total time
  - For at-power PRAs, time parameter is the number of years plant is critical

Basic Events Probabilities

- Probability of failure depends on mission and failure rate (i.e., the λ or p)
  - Typically modeled as either Poisson or binomial
  - Unavailability (e.g., T&M) calculated directly as a probability
    - However, T&M unavailability can be estimated as an unreliability (like binomial) as well
- Key feature (of data) is that set of failure events and set of demands (or time) must be consistent with each other

Failure Probability Models

- Demand Failures
  - Binomial: prob(r failures in n demands)

    $= \quad p^r(1-p)^{n-r}$

    prob(1 failure|1 demand) = $p = Q_d$
- Failures in Time
  - Poisson: prob(r failures in time t) = $(1/r!)\, e^{-\lambda t}(\lambda t)^r$

    prob(r >0, in time t) = $1-e^{-\lambda t} \approx \lambda t$ (for $\lambda t << 1$)

Q = Failure probability (unreliability or unavailability)	t_i = surveillance test interval
p = Failure rate (per demand)	λ_m = maintenance frequency
λ_s = Failure rate (per hour) standby	d_m = maintenance duration
λ_h = Failure rate (per hour) operating	t_{OOS} = total time out of service
t_m = mission time	t_{total} = total time

Component Failure Modes

- Demand failure
  - $Q_d = p$
  - Need number of failures and valid demands to estimate p
- Mission time failure (failure to run)
  - $Q_r = 1 - e^{-\lambda_h t_m}$
  - $Q_r \approx \lambda_h t_m$ (for small λt; when $\lambda t < 0.1$)
  - Need number of failures and run time to estimate λ_h
- Test and maintenance unavailability
  - $Q_m = \lambda_m d_m = t_{OOS}/t_{total}$
  - Need either
    - maintenance frequency (λ_m) and duration (d_m)
    - Out-of-Service (OOS) time (t_{OOS}) and total time (t_{total})
- Standby failure (alternative to demand failure model)
  - $Q_s \approx \lambda_s t_i/2$
  - Need number of failures and time in standby to estimate λ_s

Boundary Conditions and Modeling Assumptions Affect Form of Data

- Clear understanding of component boundaries and missions needed to accurately use raw data or generic failure rates. For example:
  - Do motor driven components include circuit breakers? (Are CB faults included in component failure rate?)
- Failure mode being modeled also impacts type and form of data needed to quantify the PRA.
  - FTR – failures while operating and operating time
  - FTS/FTO – failures and demands (successes)

Data Sources for Parameter Estimation

- Generic data
- Plant-specific data
- Bayesian updated data
  - Prior distribution
  - Updated estimate

Generic Data Sources

- NUREG-1150 supporting documents (NUREG/CR-4550 series, pre-1987)
- WASH-1400 (pre-1975)
- IEEE Standard 500 (1990)
- NUREG/CR-3862 for initiating events (pre-1986)
- NUREG/CR-5750 for initiating events (1987-1995)
- NUREG/CR-5500 for system reliability (1984-1998)
- NUREG/CR-6928 for components and initiating events (1998-2002)
- NUREG-1032 for loss of offsite power(pre-1988)
- NUREG-5496 loss of offsite power (1980-1996)
- SECY 04-0060 Loss-of-Coolant Accident Break Frequencies for the Option III Risk-Informed Reevaluation of 10 CFR 50.46, Appendix K to 10 CFR Part 50, and General Design Criteria (GDC) 35 (April 2004)
- NUREG-1829 Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process (June 2005)
- Institute of Nuclear Power Operations Nuclear Plant Reliability Data System (NPRDS) – archival only (no longer maintained)
- Institute of Nuclear Power Operations Equipment Performance Information Exchange (EPIX) – replaced NPRDS

Generic Data Issues

- Key issue is whether data is applicable for the specific plant being analyzed
  - Most generic component data is mid-1980s or earlier vintage
  - Some IE frequencies known to have decreased over the last decade
    - Frequencies updated in NUREG/CRs 5750 and 5496
  - Criteria for judging data applicability not well defined (do not forget important engineering considerations that could affect data applicability)
  - ASME PRA Standard requirements

Plant-Specific Data Sources

- Licensee Event Reports (LERs)
  - Can also be source of generic data
- Post-trip SCRAM analysis reports
- Maintenance reports and work orders
- System engineer files
- Control room logs
- Monthly operating status reports
- Test surveillance procedures

Plant-Specific IE and Component Data Collection and Analysis

- Gather data to obtain raw information needed for estimating event parameters
  - Determine period of time for obtaining plant data
    - Entire plant history can be used minus first year of operation
    - Most recent data should be used to represent current maintenance practices and component performance
    - Five to seven years of data is desirable
  - Collect plant information from plant records and documents listed on previously
  - Sort data by IE category; component, failure mode, and severity
    - Plant changes can affect the categorization of a scram event
  - Pool data from several like components in same system
  - Screen data
    - Events that can no longer occur due to plant change can be eliminated
  - Obtain exposure estimates
  - Interpret the information to obtain variables of interest (e.g., failures, demands, operating hours)
  - Estimate parameter values from data
  - Scram data can be used to estimate some conditional event probabilities (e.g., relief valve sticking open)

Component Failure Severity Classification

- Raw data is classified by severity of the component failure
- Example severity classes:
  - Catastrophic - the component would have failed to perform its function
  - Degraded – component degraded to point where it can not meet required success criteria and was taken out of operation for repair

  Incipient - component degraded but could still function and was taken out of operation for repair
- The class of failure severity determines if raw data is used in calculating a specific data parameter
  - Catastrophic and degraded failures are used in calculating failure rates and probabilities and maintenance outage unavailabilities
  - Incipient failures are used to calculate maintenance outage unavailabilities

Component Exposure Estimates

- "Exposures" refers to the amount of component operating time (failure rates) and the number of demands (failure probabilities)
- Sources of component exposure include:
  - Tests – Tech Specs, procedures, test records used to estimate frequency and duration of tests
  - Actuations – actual equipment usage
  - Failure-related actuations – operability test after maintenance event (ASME Standard says not to include this)
  - Interface-related actuations – increased test frequency per Tech Spec (e.g., DGs) and closure of valves to isolate failed components
  - Operation time meter

Plant-Specific Data Issues

- Combining data from different sources can result in:
  - double counting of the same failure events
  - inconsistent component boundaries
  - inconsistent definition of “failure”
- Plant-specific data is typically very limited
  - small statistical sample size
- Inaccuracy and non-uniformity of reporting
  - LER reporting rule changes
- Difficulty in interpreting “raw” failure data
  - administratively declared inoperable, does not necessarily equate to a “PRA” failure

Bayesian Methods Employed to Generate Uncertainty Distributions

- Two motivations for using Bayesian techniques
  - Generate probability distributions (classical methods generally only produce uncertainty intervals, not pdf’s)
  - Compensate for sparse data (e.g., no failures)
- In effect, Bayesian techniques combine an initial estimate (prior) with plant-specific data (likelihood function) to produce a final estimate (posterior)
- However, Bayesian techniques rely on (and incorporate) subjective judgement
  - different options for choice of prior distribution (i.e., the starting point in a Bayesian calculation)

Bayes' Theorem is Basis for Bayesian Updating of Data

- Typical use: sparse plant-specific data combined with generic data using Bayes' Theorem:

$$\pi_1(\theta \mid E) = \frac{L(E \mid \theta)\pi_0(\theta)}{\int L(E \mid \theta)\pi_0(\theta)\,d\theta}$$

- Where:
  - $\pi_o(\theta)$ is prior distribution (generic data)
  - $L(E|\theta)$ is likelihood function (plant-specific data)
  - $\pi_1(\theta|E)$ is posterior distribution (updated estimate)

Bayesian Technique Starts With Subjective Judgment

- Prior represents one's belief about a parameter before any data have been "observed"
- Prior can be either informative or non-informative
  - Three common priors
    - Non-informative (Jeffreys) prior
    - Informative prior (e.g., generic data)
    - Constrained non-informative prior

Non-Informative Prior

- Imparts little prior belief or information
- Minimal influence on posterior distribution
  - Except when updating with very sparse data
- Basically assumes 1/2 of a failure in one demand (for binomial, or in zero time for a Poisson process)
  - If update data is very sparse, mean of posterior will be pulled to 0.5

E.g.: for plant-specific data of 0/10 (failures/demands)

Update=> 0.5/1 (prior) + 0/10 (likelihood) = 0.5/11 (posterior)

Informative Prior

- Maximum utilization of <u>all</u> available data
- Prior usually based on generic or industry-wide data
- Avoids potential conservatism that can result from use of non-informative prior
- However, good plant-specific data can be overwhelmed by a large generic data set

  e.g., prior = 100/10000 (failures/demands) = 1E-2

  plant-specific = 50/100 (failures/demands) = 0.5

  posterior = 150/10100 = 1.5E-2 (basically the prior)

Constrained Non-informative Prior

- Combines certain aspects of informative and non-informative priors
  - Weights the prior as a non-informative (i.e., 1/2 of a failure)
  - However, constrains the mean value of the prior to some generic-data based value
- For example - generic estimate of previous example would be "converted" to a non-informative prior

  100/10000 => 0.5/50 (this then used as the prior)

  Update=> 0.5/50 + 50/100 = 50.5/150 = 0.34

Common Cause Failures (CCFs)

- Conditions which may result in failure of more than one component, subsystem, or system
- Common cause failures are important since they:
  - Defeats redundancy and/or diversity
  - Data suggest high probability of occurrence relative to multiple independent failures

Common Cause Failure Mechanisms

- Environment
  - Radioactivity
  - Temperature
  - Corrosive environment
- Design deficiency
- Manufacturing error
- Test or Maintenance error
- Operational error

Common Cause Modeling in PRA

- Three parametric models used
  - Beta factor (original CCF model)

$$\beta = \frac{\text{Number of common cause failures}}{\text{Total number of failures}}$$

  - Multiple Greek Letter (MGL) model
    - (β = 2 failures, $\gamma = 3$ failures, $\delta = 4$ failures)
  - Alpha factor model (addressed uncertainty concerns in MGL)
    - $\alpha_k \equiv$ conditional probability that a failure event involves k components failing due to a shared cause, given a failure event
- Apply to cut sets containing same failure mode for sample component type
  - Diesel generators
  - MOVs, AOVs, PORVs, SRVs
  - Pump
  - Batteries

Beta Factor Example

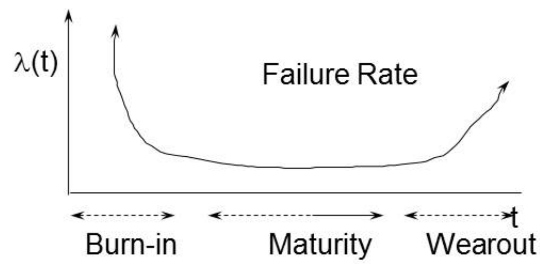
- High pressure pumps
  - β = 10 CCF ÷ 47 total failures ≈ 2.1E-1
  - Motor-driven pump fail to start = 3.0E-3 per demand
- Cut set: HPI-MDP-FS-A * HPI-MDP-FS-B
  - Independent failure ≈ 3E-3 * 3E-3 = 9E-6
- Cut set: HPI-MDP-CF-CCFAB
  - CCF = 3E-3 * β = 6E-4

Limitations of CCF Modeling

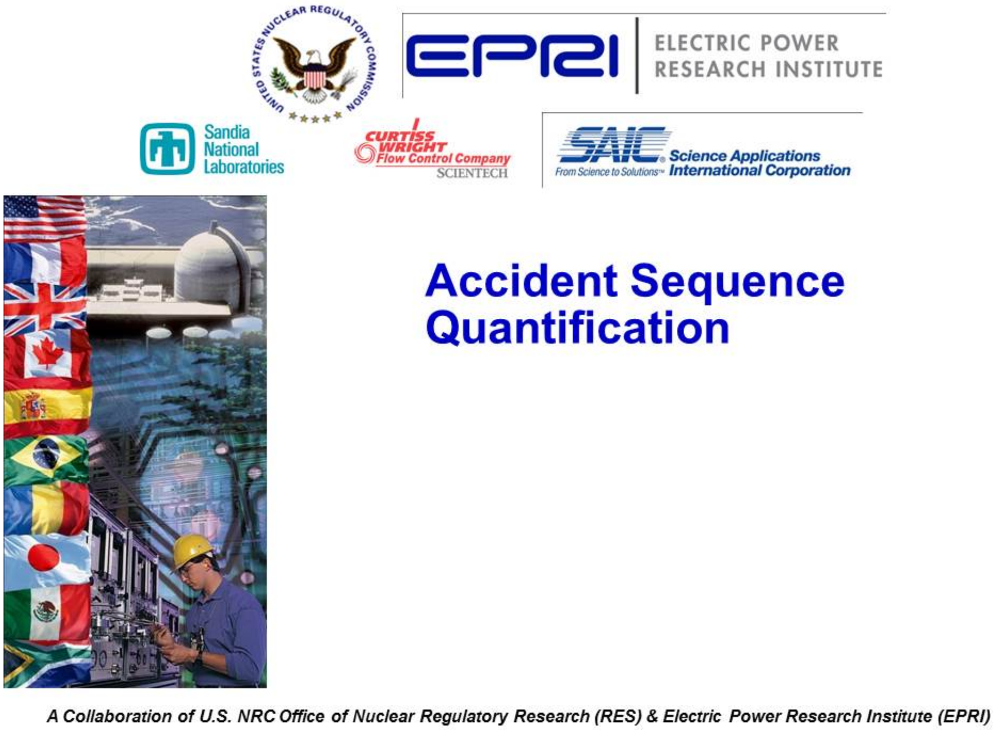
- Limited data, hence generic data often used
  - Applicability issue for specific plant
- Screening values may be used
  - Potential to skew the results
- Not typically modeled across systems since data is collected/analyzed for individual systems
- Not typically modeled for divers components (e.g., motor-driven pump/turbine-driven pump)
- Causes not explicitly modeled (i.e., each failure mechanism not explicitly modeled)

Component Data Not Truly Time Independent

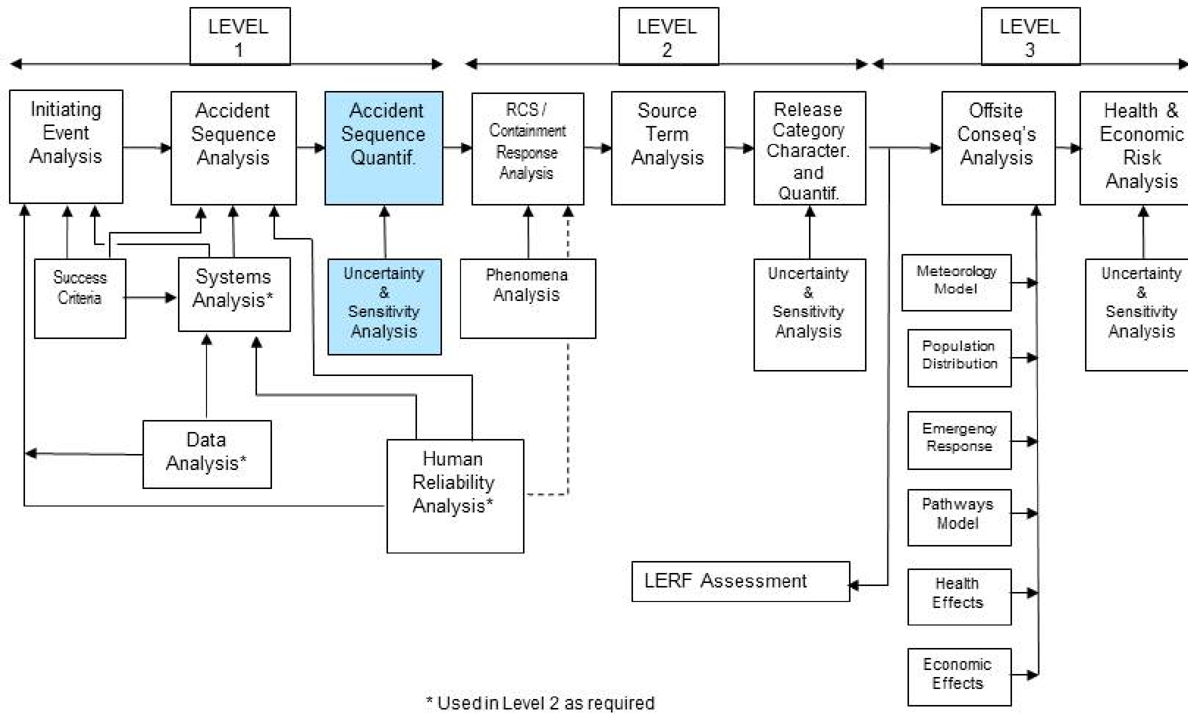
- PRAs typically assume time-independence of component failure rates
  - One of the assumptions for a Poisson process (i.e., failures in time)
- However, experience has shown aging of equipment does occur
  - Failure rate (λ) = $\lambda(t)$
  - "Bathtub" curve



Accident Sequence Quantification



Principal Steps in PRA



* Used in Level 2 as required

Purpose and Objectives

- Purpose
  - Present elements of accident sequence quantification and importance analysis and introduce concept of plant damage states
- Objectives
  - Become familiar with the:
    - process of generating and quantifying cut sets
    - different importance measures typically calculated in a PRA
    - impact of correlation of data on quantification results
    - definition of plant damage states
- References: NUREG/CR-2300 and NUREG/CR-2728

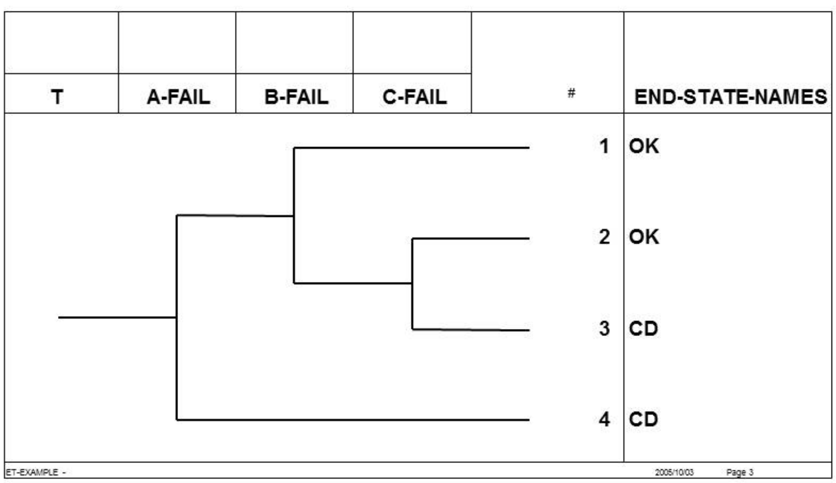
Prerequisites for Generating and Quantifying Accident Sequence Cut Sets

- Initiating events and frequencies
- Event trees to define accident sequences
- Fault trees and Boolean expressions for all systems (front line and support)
- Data (component failures and human errors)

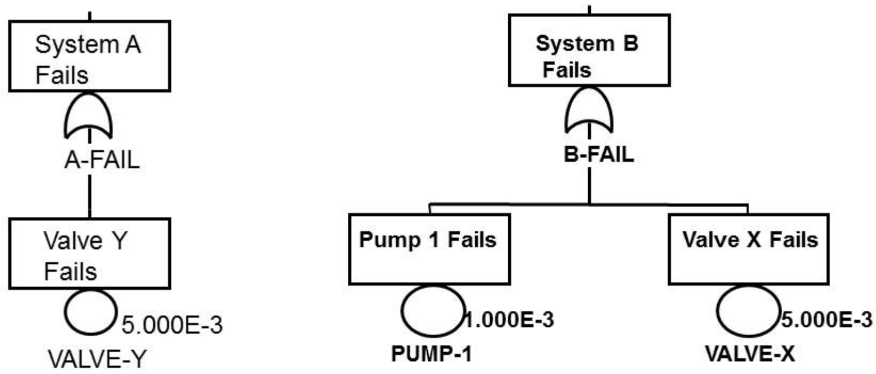
Accident Sequence Quantification (Fault-Tree Linking Approach)

- Link fault tree models on a sequence level using event trees (i.e., generate sequence logic)
- Generate minimal cut sets (Boolean reduction) for each sequence
- Quantify sequence minimal cut sets with data
- Eliminate inappropriate cut sets, add operator recovery actions, and requantify
- Determine dominant accident sequences
- Perform sensitivity, importance, and uncertainty analysis

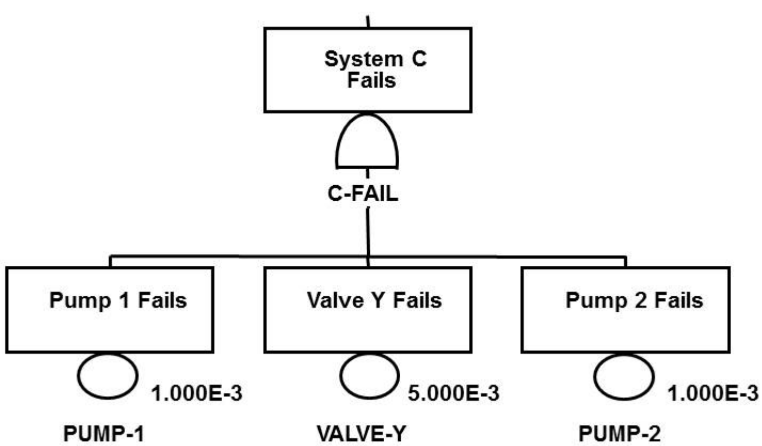
Example Event Tree



Example Fault Trees



Example Fault Trees (Concluded)



Generating Sequence Logic

- Fault trees are linked using sequence logic from event trees. From the example event tree two sequences are generated:
  - Sequence # 3: T * /A-FAIL * B-FAIL * C-FAIL
  - Sequence #4: T * A-FAIL

Generate Minimal Cut Sets for Each Sequence

- A ***cut set*** is a combination of events that cause the sequence to occur
- A minimal cut set is the smallest combination of events that causes to sequence to occur
- Cut sets are generated by "ANDing" together the failed top event fault trees, and then, if necessary, eliminating (i.e., deleting) those cut sets that contain failures that would prevent successful (i.e., complemented) top events from occurring. This process of elimination is called *Delete Term*
- Each cut set represents a failure scenario that must be "ORed" together with all other cut sets for the sequence when calculating the total frequency of the sequence

Sequence Cut Set Generation Example

- Sequence #3 logic is T * /A-FAIL * B-FAIL * C-FAIL
- ANDing failed top events yields

  B-FAIL * C-FAIL = (PUMP-1 + VALVE-X) * (PUMP-1 * VALVE-Y * PUMP-2)
  = (PUMP-1 * PUMP-1 * VALVE-Y * PUMP-2) + (VALVE-X * PUMP-1 * VALVE-Y * PUMP-2)
  = (PUMP-1 * VALVE-Y * PUMP-2) + (VALVE-X * PUMP-1 * VALVE-Y * PUMP-2)
  = PUMP-1 * VALVE-Y * PUMP-2
- Using Delete Term to remove cut sets with events that would fail top event A-FAILS (i.e., VALVE-Y) results in the elimination of all cut sets
- Sequence #4 logic is T * A-FAIL, resulting in the cut set T *VALVE-Y

Quantification of Sequence Cut Sets

- Exact Solution for Top = A + B:

  P(Top) = P(A + B) = P(A) + P(B) - P(AB)
  - Cross terms become unwieldy for large lists of cut sets.
- Thus, sequences typically quantified using either:
  - Rare-Event Approximation
    - P(Top) = sum of probabilities of individual minimal cut sets (MCSs) = P(A) + P(B)
    - P(AB) judged sufficiently small (rare) that it can be ignored (i.e., cross-terms are simply dropped)

    $$\mathbf{P(Top\ Event)} \leq \sum \mathbf{P(MCS_k)}$$

    Or
  - Minimal Cut Set Upper Bound (min-cut) Approximation
    - P(Top) = 1 - product of cut set success probabilities

    $$\mathbf{P(Top\ Event)} \leq \mathbf{1-} \Pi\mathbf{(1-P\{MCS_k\})}$$

Comparison of Quantification Methods for P(A+B)

	Small values for P(A) & P(B), A & B independent	Large values for P(A) & P(B), A & B independent	A & B dependent
Values	P(A) = 0.01 P(B) = 0.03	P(A) = 0.4 P(B) = 0.6	B = /A P(A) = 0.4 P(B) = P(/A) = 0.6
Exact	0.01 + 0.03 - (0.01 * 0.03) = 0.0397	0.4 + 0.6 - (0.4 * 0.6) = 0.76	0.4 + 0.6 - P(A*/A) = 1.0
Rare Event	0.01 + 0.03 = 0.04	0.4 + 0.6 = 1.0	0.4 + 0.6 = 1.0
MinCut UB	1 - [(1-0.01) * (1-0.03)] = 0.0397	1 - [(1-0.4) * (1-0.6)] = 0.76	1 - [(1-0.4) * (1-0.6)] = 0.76

Eliminating "Inappropriate" Cut Sets

- When solving fault trees to generate sequence cut sets it is likely that "inappropriate" cut sets will be generated
- "Inappropriate" cut sets are those containing *invalid* combinations of events. An example would be:
  - … SYS-A-TRAIN-1-TEST * SYS-A-TRAIN-2-TEST ….
- Typically eliminated by searching for combinations of invalid events and then deleting the cut sets containing those combinations

Adding "Recovery Actions" to Cut Sets

- Cut sets are examined to determine whether the function associated with a failed event can be restored; thus "recovering" from the loss of function
- If the function associated with an event can be restored, then a "Recovery Action" is ANDed to the cut set to represent this restoration
- The probability assigned to the "Recovery Action" will be the probability that the operators fail to perform the action or actions necessary to restore the lost function
- Probabilities are derived either from data (e.g., recovery of off-site power) or from human reliability analysis (e.g., manually opening an alternate flow path given the primary flow path is failed)

Dominant Accident Sequences (Examples)

Surry (NUREG-1150)

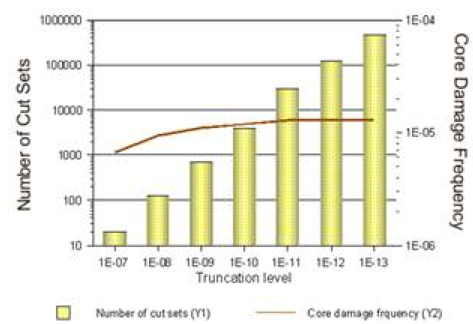
Seq	Description	% CDF	Cum
1	Station Blackout (SBO) - Batt Depl.	26.0	26.0
2	SBO - RCP Seal LOCA	13.1	39.1
3	SBO - AFW Failure	11.6	50.7
4	SBO - RCP Seal LOCA	8.2	58.9
5	SBO - Stuck Open PORV	5.4	64.3
6	Medium LOCA - Recirc Failure	4.2	68.5
7	Interfacing LOCA	4.0	72.5
8	SGTR - No Depress - SG Integ'ty Fails	3.5	76.0
9	Loss of MFW/AFW - Feed & Bleed Fail	2.4	78.4
10	Medium LOCA - Injection Failure	2.1	80.5
11	ATWS - Unfavorable Mod. Temp Coeff.	2.0	82.5
12	Large LOCA - Recirculation Failure	1.8	84.3
13	Medium LOCA - Injection Failure	1.7	86.0
14	SBO - AFW Failure	1.6	87.6
15	Large LOCA - Accumulator Failure	1.6	89.2
16	ATWS - Emergency Boration Failure	1.6	90.8
17	Very Small LOCA - Injection Failure	1.5	92.3
18	Small LOCA - Injection Failure	1.1	93.4
19	SBO - Battery Depletion	1.1	94.5
20	SBO - Stuck Open PORV	0.8	95.3

Grand Gulf (NUREG-1150)

Seq	Description	% CDF	Cum
1	Station Blackout (SBO) With HPCS And RCIC Failure	89.0	89.0
2	SBO With One SORV, HPCS And RCIC Failure	4.0	93.0
3	ATWS - RPS Mechanical Failure With MSIVs Closed, Operator Fails To Initiate SLC, HPCS Fails And Operator Fails To Depressurize	3.0	96.0

Truncation Issues Affect Quantification

- Two types of truncation
  - Cut set frequency
  - Cut set order
    - Truncating on number of basic events in a cut set generally limited to vital area analyses
- Becoming less of a concern with increased computer/software capabilities
- Low probability events can accumulate
  - 1,000 cut sets at 1E-9 each = 1E-6
  - 10,000 cut sets at 1E-9 each = 1E-5



Truncation cutoff value should be decreased until change in total frequency becomes stable

Importance Measures for Basic Events

- Provide a quantitative perspective on risk and sensitivity of risk to changes in input values
- Three are encountered most commonly:
  - Fussell-Vesely (F-V)
  - Birnbaum
  - Risk Reduction (RR)
  - Risk Increase (RI) or Risk Achievement (RA)

Importance Measures
(Layman Definitions)

- Risk Achievement Worth (RAW)
  - Relative risk increase assuming failure
- Risk Reduction Worth (RRW)
  - Relative risk reduction assuming perfect performance
- Fussell-Vesely (F-V)
  - Fractional reduction in risk assuming perfect performance
- Birnbaum
  - Difference in risk between perfect performance and assumed failure

Importance Measures
(Mathematical Definitions)

R = Baseline Risk

R(1) = Risk with the element always failed or unavailable

R(0) = Risk with the element always successful

RAW = R(1)/R or R(1) - R

RRW = R/R(0) or R - R(0)

F-V = [R-R(0)]/R

Birnbaum = R(1) – R(0)

Limitations of Importance Measures

- Risk rankings are not always well-understood in terms of their issues and engineering interpretations
  - That is, high importance does not necessarily mean dominant contributor to CDF
- RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured
  - That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error
- F-V and RAW rankings can differ significantly when using different risk metrics
  - Such as, core damage frequency due to internal events versus external events, shutdown risk, etc.
- Individual F-V or RAW measures cannot be combined to obtain risk importance for combinations of events

Uncertainty Must be Addressed in PRA

- Uncertainty arises from many sources:
  - Inability to specify initial and boundary conditions precisely
    - Cannot specify result with deterministic model
    - Instead, use probabilistic models (e.g., tossing a coin)
  - Sparse data on initiating events, component failures, and human errors
  - Lack of understanding of phenomena
  - Modeling assumptions (e.g., success criteria)
  - Modeling limitations (e.g., inability to model errors of commission)
  - Incompleteness (e.g., failure to identify system failure mode)

PRAs Identify Two Types of Uncertainty

- Distinction between aleatory and epistemic uncertainty:
  - "Aleatory" from the Latin Alea (dice), of or relating to random or stochastic phenomena. Also called "random uncertainty or variability."
  - "Epistemic" of, relating to, or involving knowledge; cognitive. [From Greek episteme, knowledge]. Also called "state-of-knowledge uncertainty."

Aleatory Uncertainty

- Variability in or lack of precise knowledge about underlying conditions makes events unpredictable. Such events are modeled as being probabilistic in nature. In PRAs, these include initiating events, component failures, and human errors.
- For example, PRAs model initiating events as a Poisson process, similar to the decay of radioactive atoms
- Poisson process characterized by frequency of initiating event, usually denoted by parameter λ

Epistemic Uncertainty

- Value of λ is not known precisely
- Could model uncertainty in estimate of λ using statistical confidence interval
  - Can't propagate confidence intervals through PRA models
  - Can't interpret confidence intervals as probability statements about value of λ
- PRAs model lack of knowledge about value of λ by assigning (usually subjectively) a probability distribution to λ
  - Probability distribution for λ can be generated using Bayesian methods.

Types of Epistemic Uncertainties

- Parameter uncertainty
- Modeling uncertainty
  - System success criteria
  - Accident progression phenomenology
  - Health effects models (linear versus nonlinear, threshold versus non-threshold dose-response model)
- Completeness
  - Complex errors of commission
  - Design and construction errors
  - Unexpected failure modes and system interactions
  - All modes of operation not modeled

Addressing Epistemic Uncertainties

- Parameter uncertainty addressed by propagating parameter uncertainty distributions through model
- Modeling uncertainty usually addressed through sensitivity studies
  - Research ongoing to examine more formal approaches
- Completeness addressed through comparison with other studies and peer review
  - Some issues (e.g., design errors) are simply acknowledged as limitations
  - Other issues (e.g., errors of commission) are topics of ongoing research

Prerequisites for Performing a Parameter Uncertainty Analysis

- Cut sets for individual sequence or groups of sequences (e.g., by initiator or total plant model) exist
- Failure probabilities for each basic event, including distribution and correlation information (for those events that are uncertain or are modeled as having uncertainty)
- Frequencies for each initiating event, including distribution information

Performing A Parameter Uncertainty Analysis

- Select cut sets
- Select sampling strategy
  - Monte Carlo: simple random sampling process/technique
  - Latin Hypercube: stratified sampling process/technique
- Select number of observations (i.e., number of times a variable's distribution will be sampled)
- Perform calculation

Correlation: Effect on Results

- Correlating data produces wider uncertainty in results
  - Without correlating a randomly selected high value will usually be combined with randomly selected lower values (and vice versa), producing an averaging effect
    - Reducing calculated uncertainty in the result
  - Mean value of probability distributions that are skewed right (e.g. lognormal, commonly used in PRA) is increased when uncertainty is increased

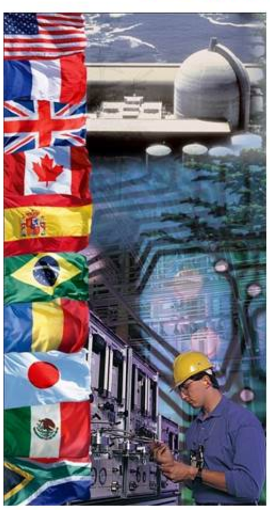
Fire PRA Workshop 2012, Bethesda, MD
PRA Fundamentals and Overview

Slide 184

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

LEVEL 2/LERF Analysis

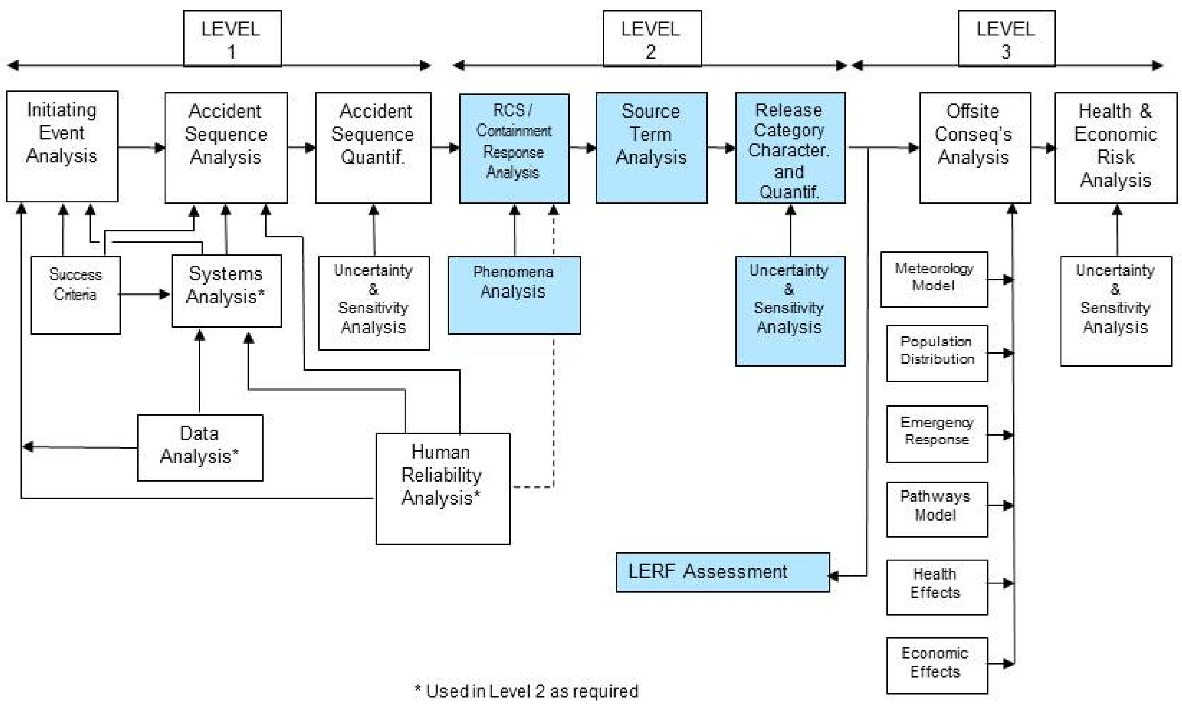
ELECTRIC POWER RESEARCH INSTITUTE



LEVEL 2/LERF Analysis

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Principal Steps in PRA



* Used in Level 2 as required

Purpose and Objectives

- Purpose: Students receive a brief introduction to accident progression (Level 2 PRA).
- Objectives: At the conclusion of this topic, students will be able to:
  - List primary elements which comprise accident phenomenology
  - Explain how accident progression analysis is related to full PRA
  - Explain general factors involved in containment response
- Reference: NUREG/CR-2300, NUREG-1489 (App. C)

Level 2 PRA Risk Measures

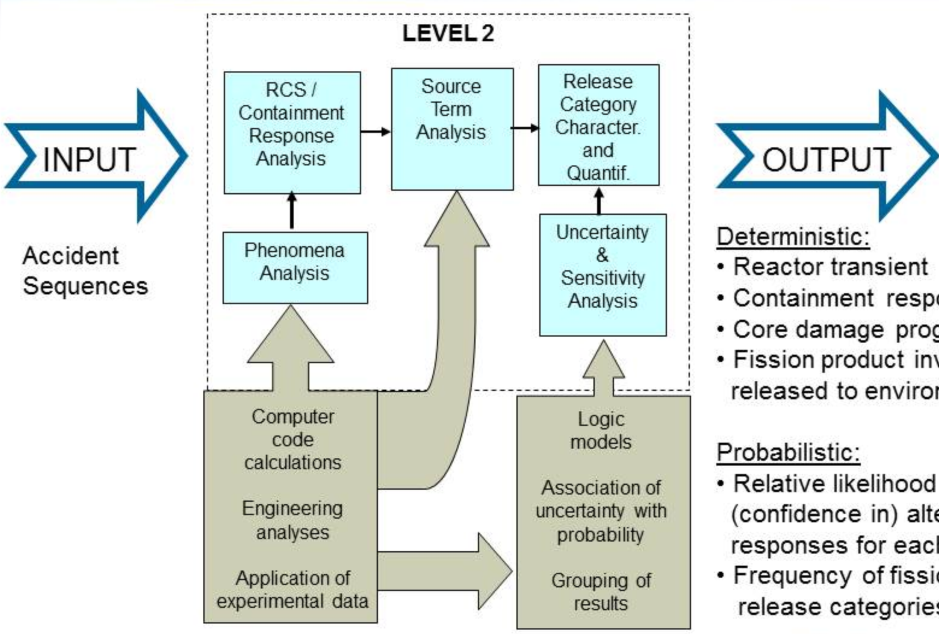
- Current NRC emphasis on LERF
  - Risk-informed Decision-Making for Currently Operating Reactors
  - Broader view expected for new reactors
- Some discussion of alternative risk acceptance criteria
  - Goals for frequency of various release magnitudes
  - Release often expressed in units of activity (not health consequences)
- Full-scope Level 2 offers Complete Characterization of Releases to Environment
  - Frequency of large/small, early/late releases

LERF Definition

- A LERF definition is provided in the PSA Applications Guide:

  Large, Early Release: A radioactive release from the containment which is both large and early. Large is defined as involving the rapid, unscrubbed release of airborne aerosol fission products to the environment. Early is defined as occurring before the effective implementation of the off-site emergency response and protective actions.

Level 2 PRA is a Systematic Evaluation of Plant Response to Core Damage Sequences



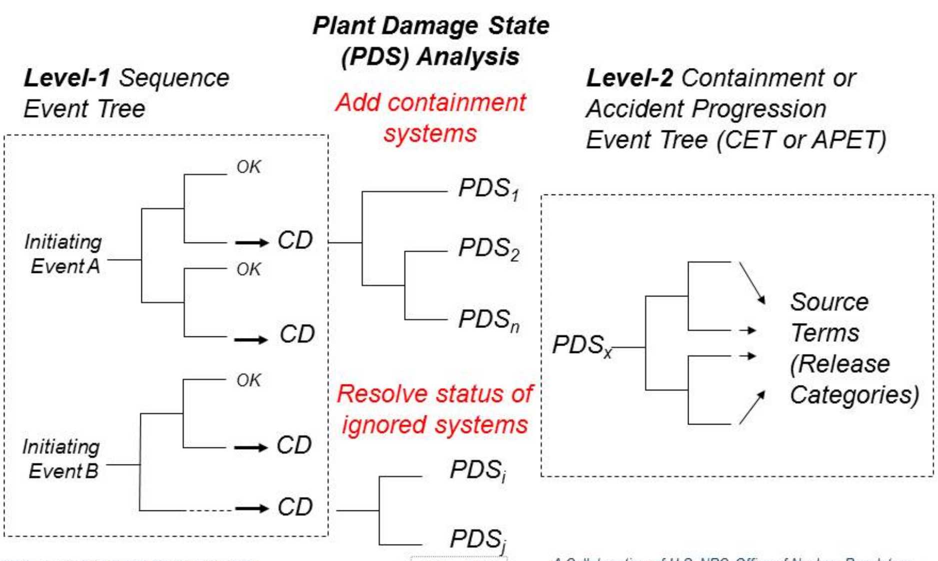
<u>Deterministic:</u>
- Reactor transient
- Containment response
- Core damage progression
- Fission product inventory released to environment

<u>Probabilistic:</u>
- Relative likelihood of (confidence in) alternative responses for each sequence
- Frequency of fission product release categories

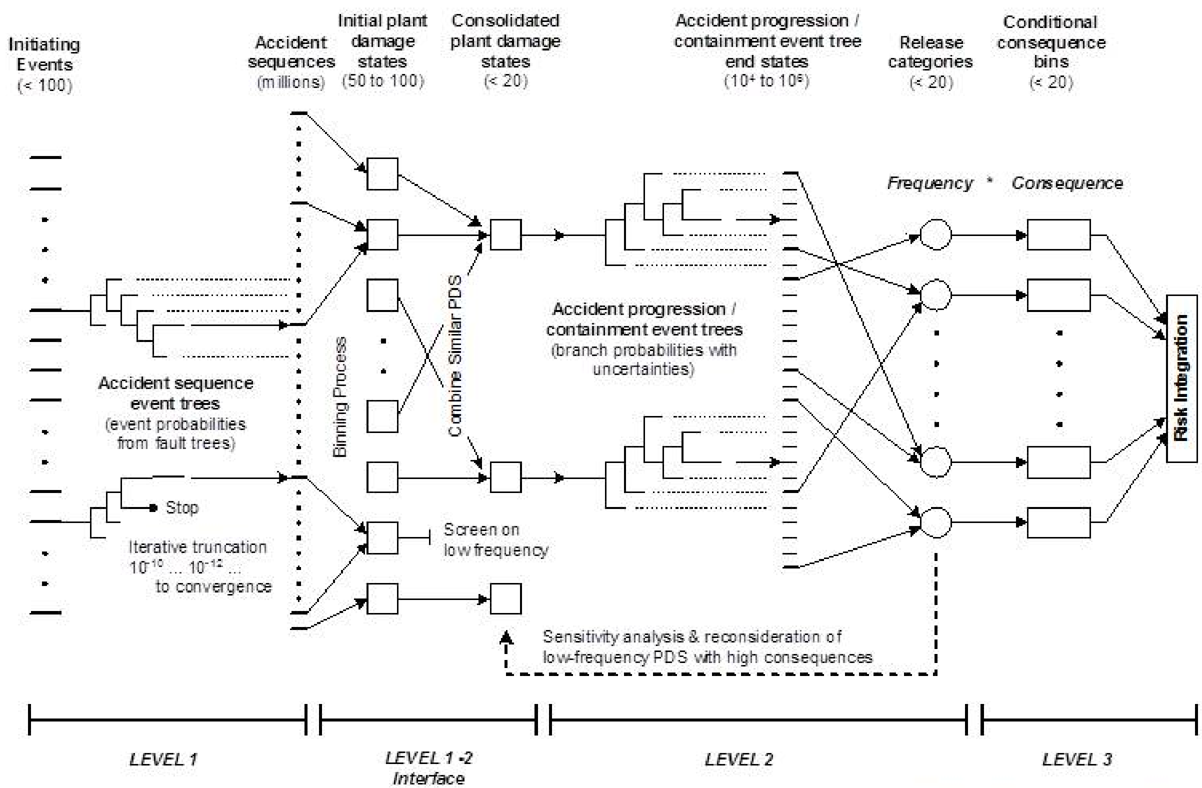
Some Subtle Features of the Level 2 PRA Process

- Level 2 Requires More Information than a Level 1 PRA Generates
  - Containment safeguards systems not usually needed to determine ‘core damage’
  - Level 1 event trees built from success criteria can ignore status of front-line systems that influence <u>extent of</u> core damage
- Event Trees Create Very Large Number of Scenarios to Evaluate
  - Grouping of similar scenarios is a practical necessity
- Quantification Involves Considerable Subjective Judgment
  - Uncertainty, Sensitivity and Uncertainty in Uncertainty

Additional Work is Often Required to Link Level 1 Results to Level 2



Typical Steps in Level 2 Probabilistic Model



Major Tasks:

- Plant Damage State (PDS) Analysis
  - Link to Level 1
- Deterministic Assessments of Plant Response to Severe Accidents
  - Containment performance assessment
  - Accident progression & source term analysis
- Probabilistic Treatment of Epistemic Uncertainties
  - Account for phenomena not treated by computer codes
  - Characterize relative probability of alternative outcomes for uncertain events
- Couple Frequency with Radiological Release
  - Link to Level 3

Major Steps of Level 2 Analysis

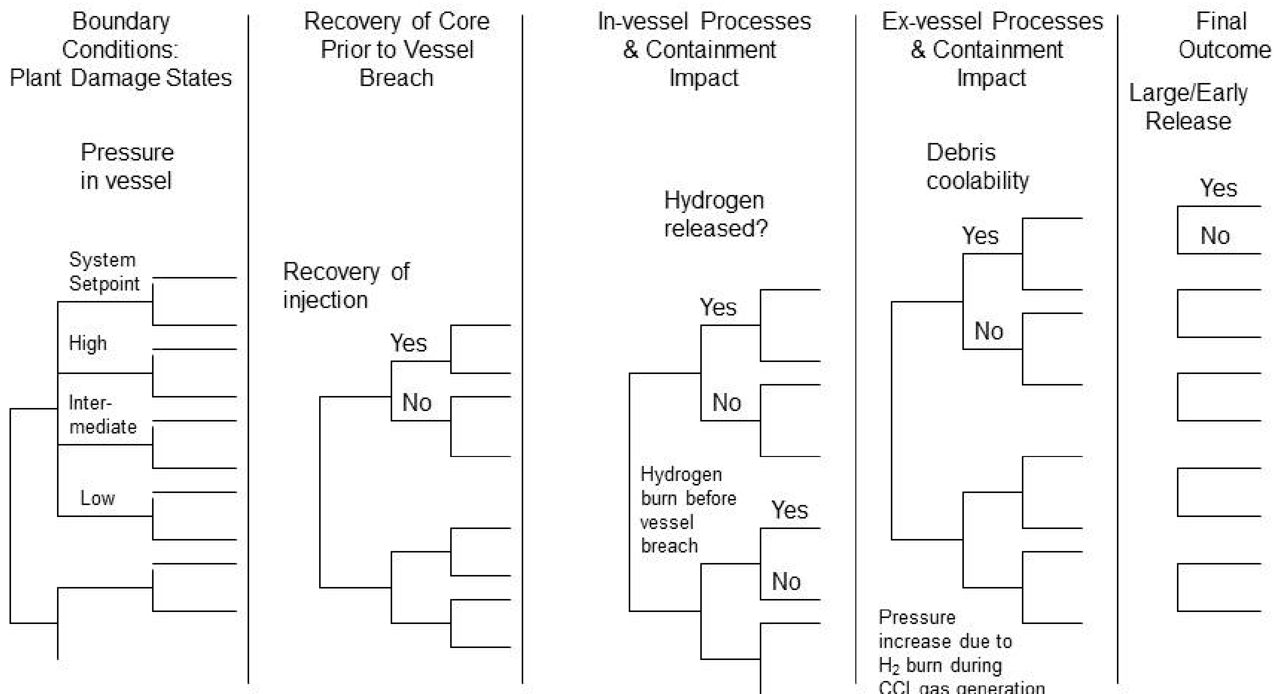
- Level 1 -2 Interface
  - Enhance Level 1 accident sequence models to meet Level 2 needs
  - Group cut sets into "plant damage state" (PDS) bins.
  - Output - Frequency of each PDS bin (5 to 25 PDSs).
- Accident Progression Analysis
  - Run preliminary MELCOR runs to establish source term Release Categories
  - Build Containment Event Tree (CET)
    - Sequence of events that lead to containment failure and fission product release.
  - Run PDSs through CET
  - Output - Frequency of each CET end-state.
- Source Term Binning
  - Develop criteria for source term binning of CET end-states
  - Run additional MELCOR runs to refine source term Release Categories
  - Group CET end-states into source term "Release Categories"
  - Output - Frequency of each Release Category.

Level 1-2 Interface

- Enhance Level 1 accident sequence models to address Level 2 information needs
  - Add front line systems excluded from core damage sequences but relevant to the progression of core damage.
  - Add containment system response to Level 1 models
  - Requantify Level 1 results
  - Accomplished using either a Containment Safeguards Tree or Bridge Tree

- Consolidate Level 1 results for Level 2 (PDS Analysis)
  - Identify post-core damage attributes important to containment response
  - Group Level 1 Sequences (or cut sets) into bins defined in terms of common accident attributes relevant to containment response.
  - Output - Frequency of PDSs.

Schematic of Accident Progression Event Tree



Source: NUREG-1150

Accident Progression Analysis

- There are 4 major steps in Accident Progression Analysis
  - 1. Develop the Accident Progression Event Trees (APETs)
  - 2. Perform structural analysis of containment
  - 3. Quantify APET issues
  - 4. Group APET sequences into accident progression bins

Severe Accident Analysis

Computer Code (e.g., MAAP or MELCOR) Calculations Provide Foundation Information for Design-Specific Information --

- Thermal-hydraulic response/success criteria
  - Primary coolant inventory management, reactor pressure control & heat removal
- Time of major events
  - Onset of core damage
  - Time to exceed containment failure criteria
  - Available time for operator actions
- Evolution of severe accident phenomena
  - RCS & containment pressure/temperature signatures
  - Fission product release/transport (source term)
- Containment Ultimate Pressure

Containment Response

- How does the containment system deal with physical conditions resulting from the accident?
  - Pressure
  - Heat sources
  - Fission products
  - Steam and water
  - Hydrogen
  - Other non-condensables
- Typical failure modes:
  - Isolation failure or bypass
  - Over-pressure (global)
  - Creep (axial growth)
  - Corium-concrete interaction
  - Blowdown reaction forces
  - Local heating of pressure boundary penetrations or seals
  - Localized dynamic loads

Deterministic Analysis Results Useful for APET/CET Quantification

- Probability of containment failure at vessel breach hinges on likelihood of hydrogen ignition in containment.
  - Possibilities for ignition sources?
  - Flame propagation from drywell?
  - Debris transport from pedestal?

  Questions the APET/CET should consider
- Containment over-pressure from large burn can also fail drywell wall
  - Suppression pool bypass for late in-vessel F.P. releases
- Reactor vessel failure at low pressure depends on failure of safety valve
  - Valve failure criteria?
  - Single cycling valve?

  Questions the APET/CET should consider

APET/CET Quantification

- System failure events quantified in manner consistent with Level 1
  - Most system issues handled prior to PDS Analysis
- Dependencies and Data (Aleatory) Uncertainties Accompanying Level 1 systems analysis must be carried forward through PDS:
  - Support system failures, if any.
  - Prior operator performance, if any.
  - PDS frequency as distribution, if any.
- Most CET events cannot be quantified as randomly occurring events
  - Fundamental nature of uncertainty is NOT stochastic (random) behavior of the 'system'
  - Epistemic or 'state-of-knowledge' uncertainty
  - Probability represents analysts' degree of confidence that a particular outcome is true
  - Evidence may point to one outcome over another
- Many events are quantified using engineering judgment

Uncertainty Analysis in Level 2 PRA

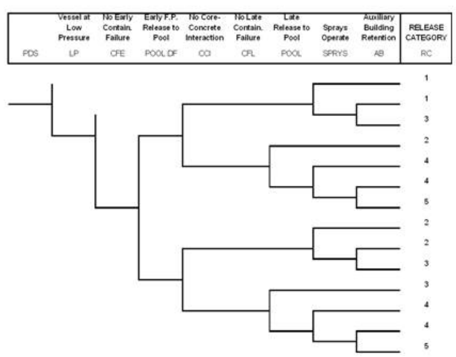
- Event Quantification in CET Predominantly Reflects Epistemic Uncertainty
  - Subjective judgment about a particular outcome
- Most CET probabilities are estimated as point estimates:
  - From deterministic calculations, or
  - Engineering judgment.
- Distributions Can Be Defined and Sampled to model epistemic uncertainties

Issues to Tackle in Propagating Uncertainty through Level 2 APET/CET

- Large Values of Probability (> 0.1) Are Common
  - Eliminates Use of Some Quantification Techniques common to Level 1.
- Correlation Among Events Can be Complicated
  - Event chronology:
    - Example: Hydrogen Combustion
      - Probability of early burn correlated with in-vessel generation
      - Probability of burn at vessel breach correlated with early burn
      - Probability of late burn correlated with all earlier burns
  - Circular Dependence
    - H2 Generation → RPV Pressure → SRV Behavior → H2 Generation

Source Term Binning

- **Rather than calculate a source term for each end-state of the CET, rules are generated to group end-states with similar source terms.**
  - **Each group is referred to as a source term 'bin' or release category**
  - **Rules (binning criteria) are based on knowledge gained from multiple source term calculations**



Process similar to PDS analysis

- **Define binning criteria from results of calculations**
- **Link each CET end-state to a unique Category**

Typical Source Term Binning Characteristics

- Timing, size & location of containment failure
- Plant or accident features that attenuate airborne fission product concentration
  - Release path through auxiliary building(s)
  - Atmosphere sprays
- Effectiveness of ex-vessel debris cooling
- Availability of water after RPV lower head failure
  - Cover debris with pool of water (scrubbing)
  - Cool RPV surfaces reduces revolatilization

Release Fraction as a Measure for Comparing Source Terms

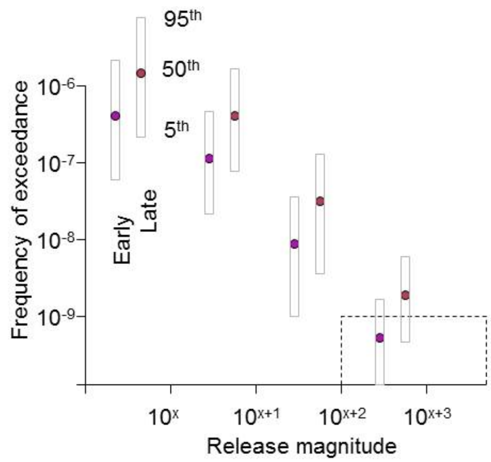
- "Bin" or group calculated source terms into broad classes based on magnitude and timing of release to the environment
  - Release fractions for Iodine (I-131) and Cesium (Cs-137) are established measures of early and long-term health effects, respectively
  - Binning criteria can be based on one, or both measures

Fractional Release of Initial Core Inventory

Release Category	Lower Bound	Upper Bound
RC1	1.0	0.1
RC2	0.1	0.01
RC3	1.E-2	1.E-3
RC4	1.E-3	1.E-4
RC5	1.E-4	1.E-5
RC6	1.E-5	1.E-6
RC7	1.E-6	1.E-7
RC8	No release	

Full Scope Level 2 PRA: Wide Range of Possible Accidental Releases to Environment

- Characterization of Releases to the Environment of all Types
  - Large/Small
  - Early/Late
  - Energetic/Protracted
  - Elevated/Ground level
- Frequency of Each Type Describes Full Spectrum of Releases Associated with Core Damage Events



Bounding or Screening Models for U.S. Risk-Informed Applications (LERF)

- NUREG/CR- 6595 (Brookhaven 2004)
  - Provides simplified approach designed to supplement Level-I PRAs submitted in support of risk-informed decision making.
  - Accident sequence information provided in the Level-I PRA is used to estimate the frequencies of various containment failure modes."
- A Simplified Model Can Be Used to Estimate Bounding Value of LERF
  - Simple method outlined in NUREG/CR-6595
  - Pre-quantified "CETs" with paths leading to LERF
  - Avoids expensive of plant-specific deterministic analysis
  - Avoids source term (MELCOR) calculations
  - Only useful if bounding values for conditional containment failure probability are tolerable

4

MODULE 1 FIRE PROBABILISTIC RISK ASSESMENT

The following is a short description of the Fire PRA technical tasks covered in Module 1. For further details, refer to the individual task descriptions in Volume 2 of EPRI 1011989, NUREG/CR-6850.

- ***Fire PRA Component Selection (Task 2).*** The selection of components that are to be credited for plant shutdown following a fire is a critical step in any Fire PRA. Components selected would generally include many components credited in the 10 CFR 50 Appendix R post-fire SSD analysis. Additional components will likely be selected, potentially including any and all components credited in the plant's internal events PRA. Also, the proposed methodology would likely introduce components beyond either the 10 CFR 50 Appendix R list or the internal events PRA model. Such components are often of interest due to considerations of multiple spurious actuations that may threaten the credited functions and components.
- ***Qualitative Screening (Task 4).*** This task identifies fire analysis compartments that can be shown to have little or no risk significance without quantitative analysis. Fire compartments may be screened out if they contain no components or cables identified in Tasks 2 and 3, and if they cannot lead to a plant trip due to either plant procedures, an automatic trip signal, or technical specification requirements.
- ***Plant Fire-Induced Risk Model (Task 5).*** This task discusses steps for the development of a logic model that reflects plant response following a fire. Specific instructions have been provided for treatment of fire-specific procedures or preplans. These procedures may impact availability of functions and components, or include fire-specific operator actions (e.g., self-induced-station-blackout).
- ***Quantitative Screening (Task 7).*** A Fire PRA allows the screening of fire compartments and scenarios based on their contribution to fire risk. This approach considers the cumulative risk associated with the screened compartments (i.e., the ones not retained for detailed analysis) to ensure that a true estimate of fire risk profile (as opposed to vulnerability) is obtained.
- ***Post-Fire Human Reliability Analysis (Task 12).*** This task considers operator actions for manipulation of plant components. Task 12 is covered in **limited detail** in the PRA/Systems module. In particular, those aspects of Task 12 that deal with identifying and incorporating human failure events (HFEs) into the plant response model are discussed. Methods for quantifying human error probabilities (HEPs) are deferred to Module 4.
- ***Fire Risk Quantification (Task 14).*** The task summarizes what is to be done for quantification of the fire risk results.
- ***Uncertainty and Sensitivity Analyses (Task 15).*** This task describes the approach to follow for identifying and treating uncertainties throughout the Fire PRA process. The treatment may vary from quantitative estimation and propagation of uncertainties where

possible (e.g., in fire frequency and non-suppression probability) to identification of sources without quantitative estimation. The treatment may also include one-at-a-time variation of individual parameter values or modeling approaches to determine the effect on the overall fire risk (sensitivity analysis).

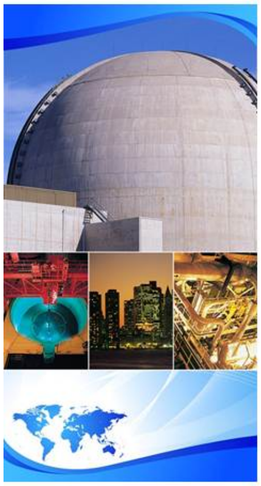
Introduction and Overview: The Scope and Structure of PRA/Systems Analysis Module

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

SAIC Science Applications International Corporation
From Science to Solutions



EPRI/NRC-RES FIRE PRA METHODOLOGY
Introduction and Overview: the Scope and Structure of PRA/Systems Analysis Module

Jeff LaChance – Sandia National Laboratories
Rick Anoba – Anoba Consulting Services, LLC

Joint RES/EPRI Fire PRA Training Workshop 2012
Bethesda MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

What we'll cover in the next four days
An overview…

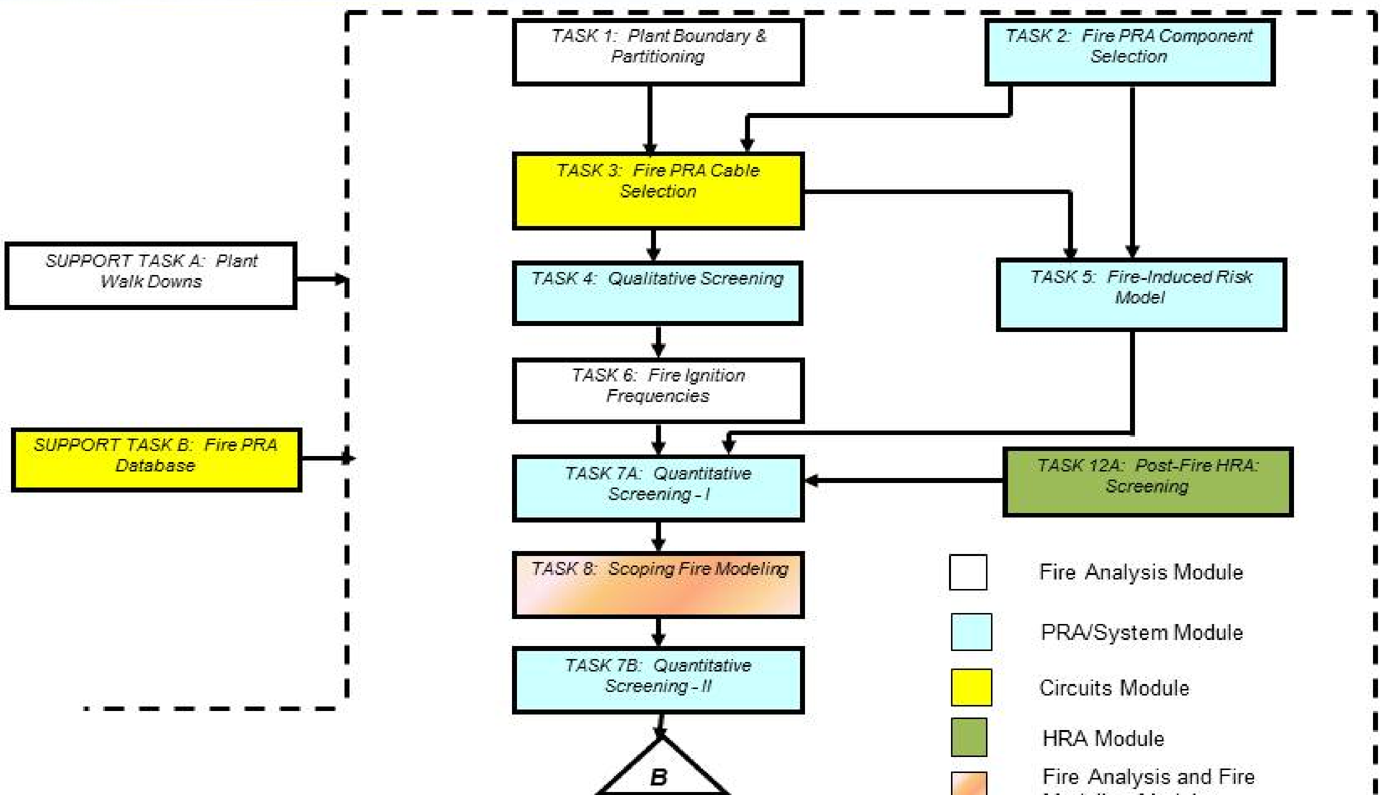
- The purpose of this presentation is to provide an Overview of the Module 2 – PRA/Systems Analysis
  - Scope of this module relative to the overall methodology
    - Which tasks fall under the scope of this module
  - General structure of the each technical task in the documentation
  - Quick introduction to each task covered by this module:
    - Objectives of each task
    - Task input/output
    - Task interfaces

Training Objectives

- Our intent:
  - To deliver practical implementation training
  - To illustrate and demonstrate key aspects of the procedures

- We expect and want significant participant interaction
  - Class size should allow for *questions and discussion*
  - We will take questions about the *methodology*
  - We *cannot* answer questions about a *specific application*
  - *We* will moderate discussions, and *we* will judge when the course must move on

Recall the overall fire PRA structure
Module 2 covers the "blue" tasks

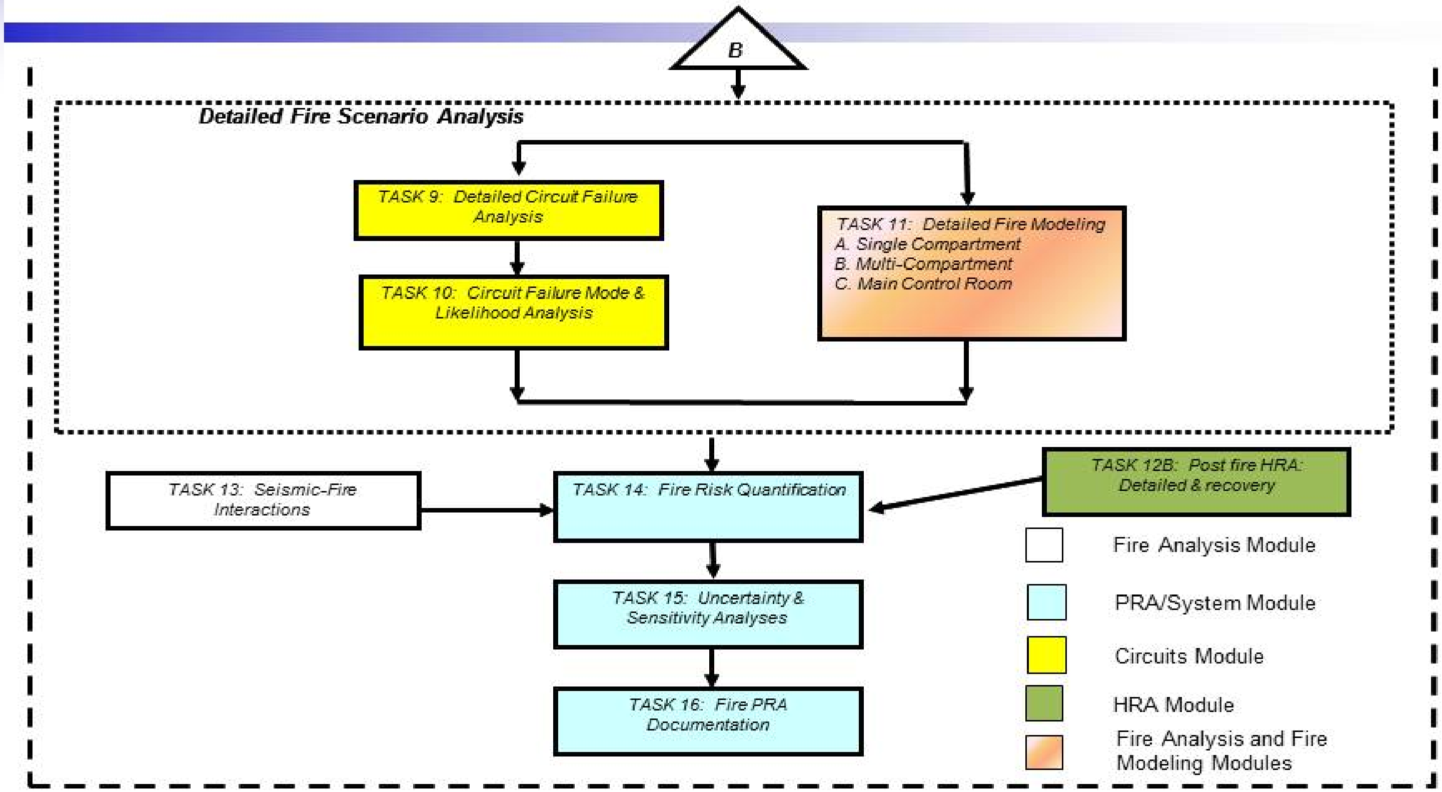


Fire PRA Training, 2012, Bethesda MD
Module 1 PRA/Systems – Introduction and Overview

Slide 4

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Recall the overall fire PRA structure (2)
Module 2 covers the "blue" tasks



Each technical task has a common structure as presented in the guidance document

1. Purpose
2. Scope
3. Background information: General approach and assumptions
4. Interfaces: Input/output to other tasks, plant and other information needed, walk-downs
5. Procedure: Step-by-step instructions for conduct of the technical task
6. References

Appendices: Technical bases, data, examples, special models or instructions, tools or databases

Scope of Module 1: PRA/Systems Analysis

- This module will cover all aspects of the plant systems accident response modeling, integration of human actions into the plant model, and quantification tasks
- Specific tasks covered are:
  - Task 2: Equipment Selection
  - Task 4: Qualitative Screening
  - Task 5: Fire-Induced Risk Model
  - Task 7: Quantitative Screening
  - Task 15: Risk Quantification
  - Task 16: Uncertainty Analysis

Task 2: Equipment Selection (1 of 2)

Module 1

- Objective: To decide what subset of the plant equipment will be modeled in the FPRA
- FPRA equipment will be drawn from:
  - Equipment from the internal events PRA
    - We do assume that an internal events PRA is available!
  - Equipment from the Post-Fire Safe Shutdown analysis
    - e.g., the Appendix R analysis or the Nuclear Safety Analysis under NFPA-805
  - Other "new" equipment not in either of these analyses

Task 2: Equipment Selection (2 of 2)

Module 1

- Many choices to be made in this task, many factors will influence these decisions
  - Fire-induced failures that might cause an initiating event
  - Mitigating equipment and operator actions
  - Fire-induced failures that adversely impact credited equipment
  - Fire-induced failures that could lead to inappropriate or unsafe operator actions
- Choices are important in part because "selecting" equipment implies a burden to *Identify and Trace* cables
  - Cable selection is Task 3 (Module 2)…

Task 4: Qualitative Screening (1 of 2)

Module 1

- Objective: To identify fire compartments that can be screened out as insignificant risk contributors without quantitative analysis

- This is an *Optional* task
  - You may choose to bypass this task which means that all fire compartments will be treated quantitatively to some level of analysis (level may vary)

Task 4: Qualitative Screening (2 of 2)

Module 1

- Qualitative screening criteria consider:
  - Trip initiators
  - Presence of selected equipment
  - Presence of selected cables

- Note that any compartment that is "screened out" in this step is reconsidered in the multi-compartment fire analysis as a potential source of multi-compartment fires
  - See Module 3, Task 11c

Task 5: Fire-Induced Risk Model

Module 1

- Objective: Construct the FPRA plant response model reflecting:
  – Functional relationships among selected equipment and operator actions
- Covers both CDF and LERF
- Begins with internal events model but more than just a "tweak"
  – Adds fire unique equipment – various reasons/sources
  – May delete equipment not to be credited for fire
  – Adds fire-specific equipment failure modes
    - e.g., spurious actuations (Task 9)
  – Adds fire-specific human failure events (Task 12)

Task 7: Quantitative Screening (1 of 2)

Module 1

- Objective: To identify compartments that can be shown to be insignificant contributors to fire risk based on limited quantitative considerations
- This task is *Optional*
  – Analyst may choose to retain all compartments for more detailed analysis

Task 7: Quantitative Screening (2 of 2)

Module 1

- Screening may be performed in stages of increasing complexity
- Consideration is given to:
  - Fire ignition frequency
  - Screening of specific fire sources as non-threatening (no spread, no damage)
  - Impact of fire-induced equipment and cable failures
    - conditional core damage probability (CCDP)
- A word of caution: quantitative screening criteria should consider the PRA standard and Reg. Guide 1.200
  - 6850/1011989 criteria are obsolete, but approach is unchanged

Task 14: Fire Risk Quantification

Module 1

- Objective: To quantify fire-induced CDF and LERF
- Covered in limited detail
- Relatively straight-forward roll-up for fire scenarios considering
  - Ignition frequency
  - Scenario-specific equipment and cable damage
  - Equipment failure modes and likelihoods
  - Credit for fire mitigation (detection and suppression)
  - Fire-specific HEPs
  - Quantification of the FPRA plant response model

Task 15: Uncertainty and Sensitivity

Module 1

- Objective: Provide a process for identifying and quantifying uncertainties in the FPRA and for identifying sensitivity analysis cases
- Covered in limited detail
- Guidance is based on potential strategies that might be taken, but choices are largely left to the analyst
  - e.g., what uncertainties will be characterized as distributions and propagated through the model?

Any questions before we move on?

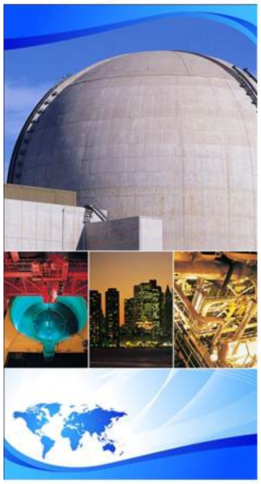
Sample Plant Description

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

SAIC Science Applications International Corporation
From Science to Solutions



EPRI/NRC-RES FIRE PRA METHODOLOGY

Sample Plant Description

Joint RES/EPRI Fire PRA Workshop
July and September, 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Sample Problems / Sample Plant

- Fire PRA module will involve hands-on exercises
  - Intent: To illustrate *key aspects* of the methodology through a cohesive set of sample problems
- All exercises are built around a common sample plant – the Simple Nuclear Power Plant (SNPP)
- The exercises are designed such that taking all modules together presents a fairly complete picture of the FPRA methodology
  - Not every task is covered by the SNPP sample problems
  - Not every aspect of covered tasks are illustrated

Fire PRA Training 2012, Bethesda MD
Introduction and Overview

Slide 2

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

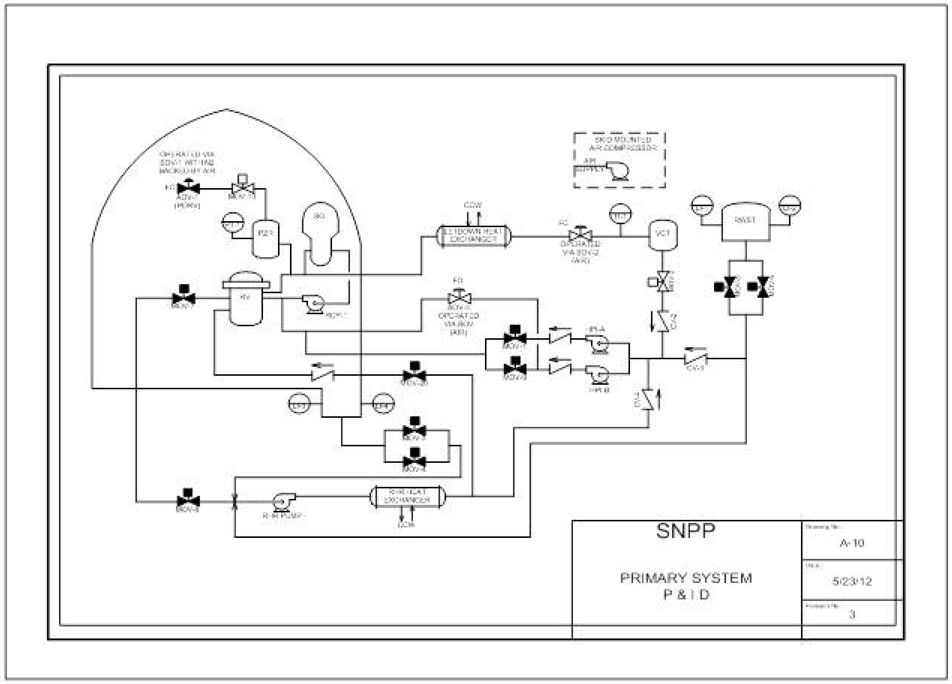
The SNPP: Intent and Approach

- The SNPP is not intended to reflect either regulatory compliance or good engineering practice
  - It is purely an imaginary construct intended to highlight key aspects of the methodology – nothing more!
- The SNPP has been kept as simple as possible while still serving the needs of the training modules
- Aspects of the plant are assumed for purposes of the training exercises, e.g.:
  - BOP equipment not covered in detail
  - Some systems are assumed to remain available

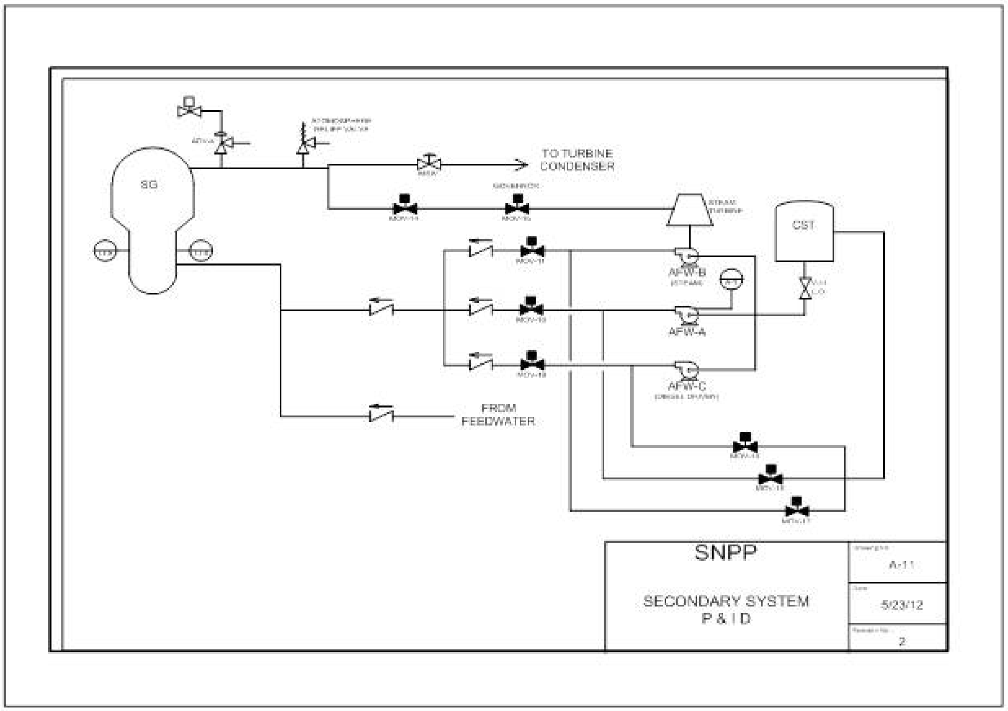
The SNPP: Plant Characteristics

- PWR with one primary coolant loop
  - One steam generator, one RCP, one pressurizer
  - Chemical volume control/high-pressure injection system
  - Residual heat removal system
- Secondary side includes:
  - Main steam and feedwater loop for the single steam generator (not modeled)
  - Multiple train auxiliary feedwater system to provide decay heat removal
- Support systems includes:
  - CCW (not modeled)
  - Instrument air
  - AC and DC power
  - Instrumentation
- See Chapter 2 for complete plant description

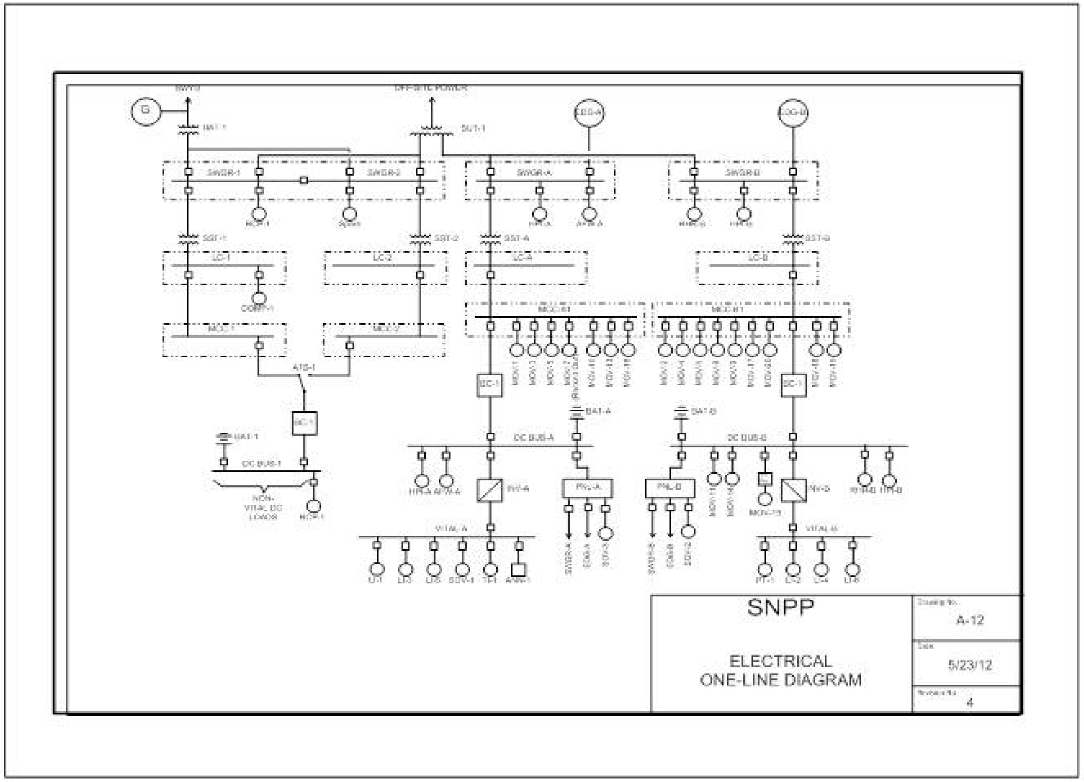
The SNPP: Primary Systems P&ID



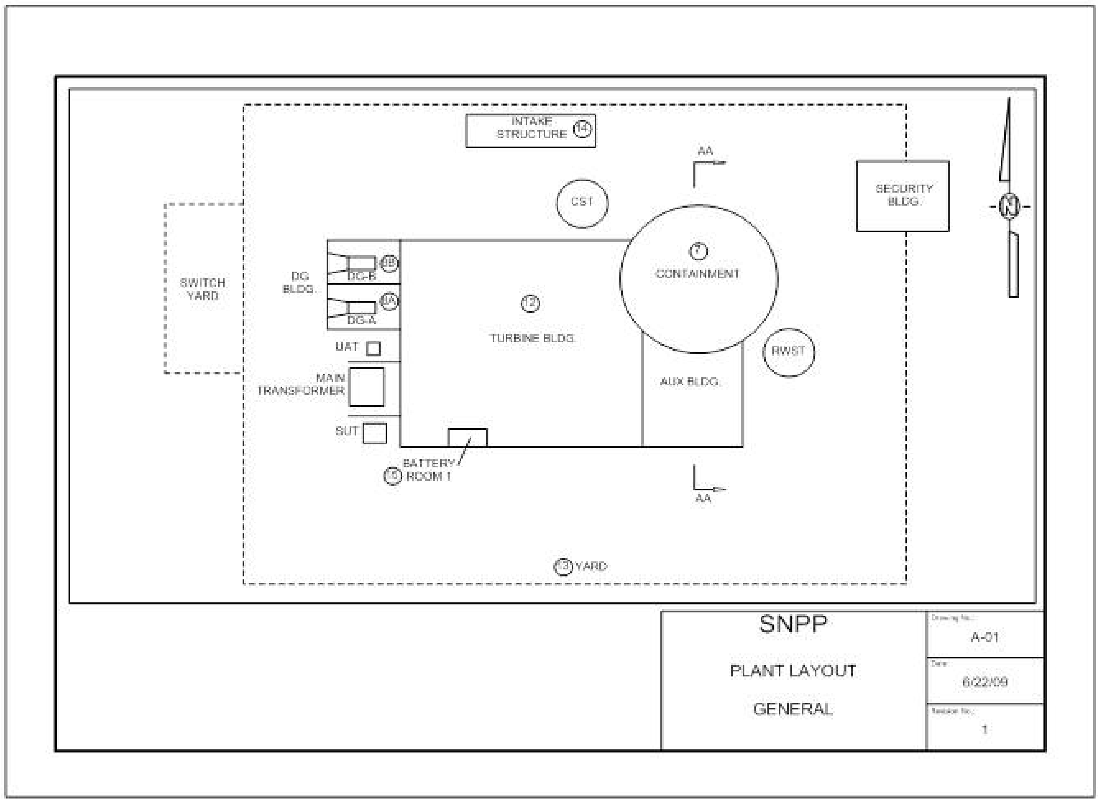
The SNPP: Secondary Systems P&ID



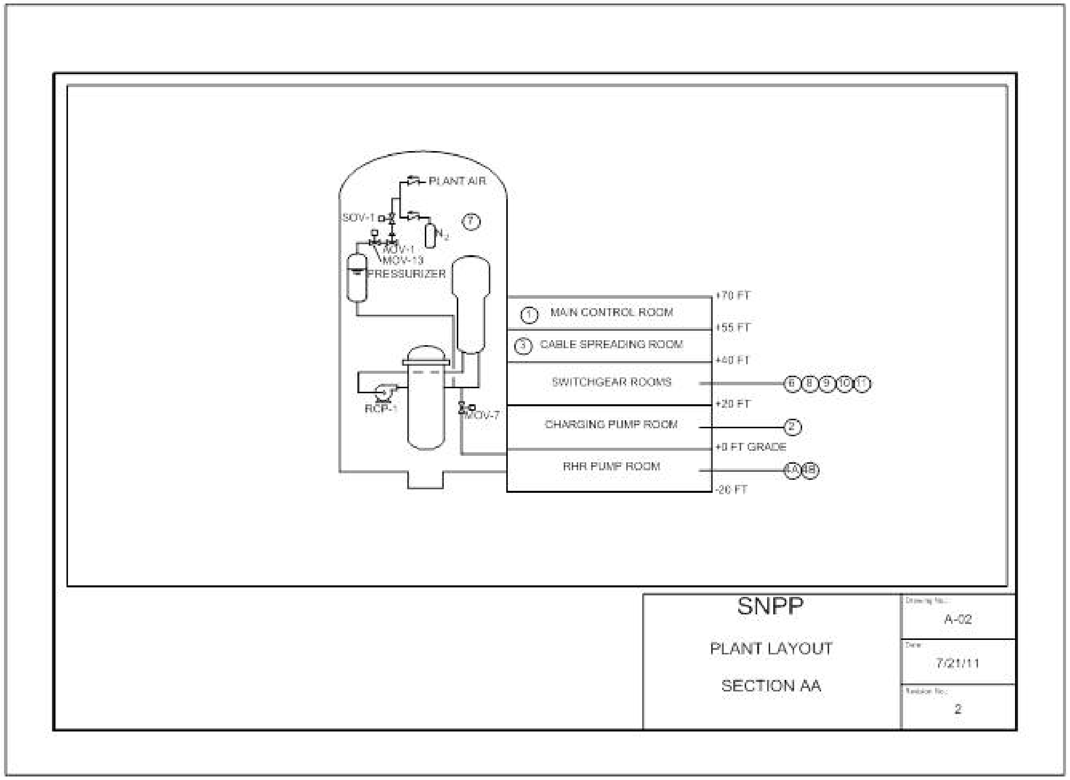
The SNPP: Electrical One-Line Diagram



The SNPP: General Plant Layout - Plan



The SNPP: Plant Layout – Elevation Containment and Auxiliary Building

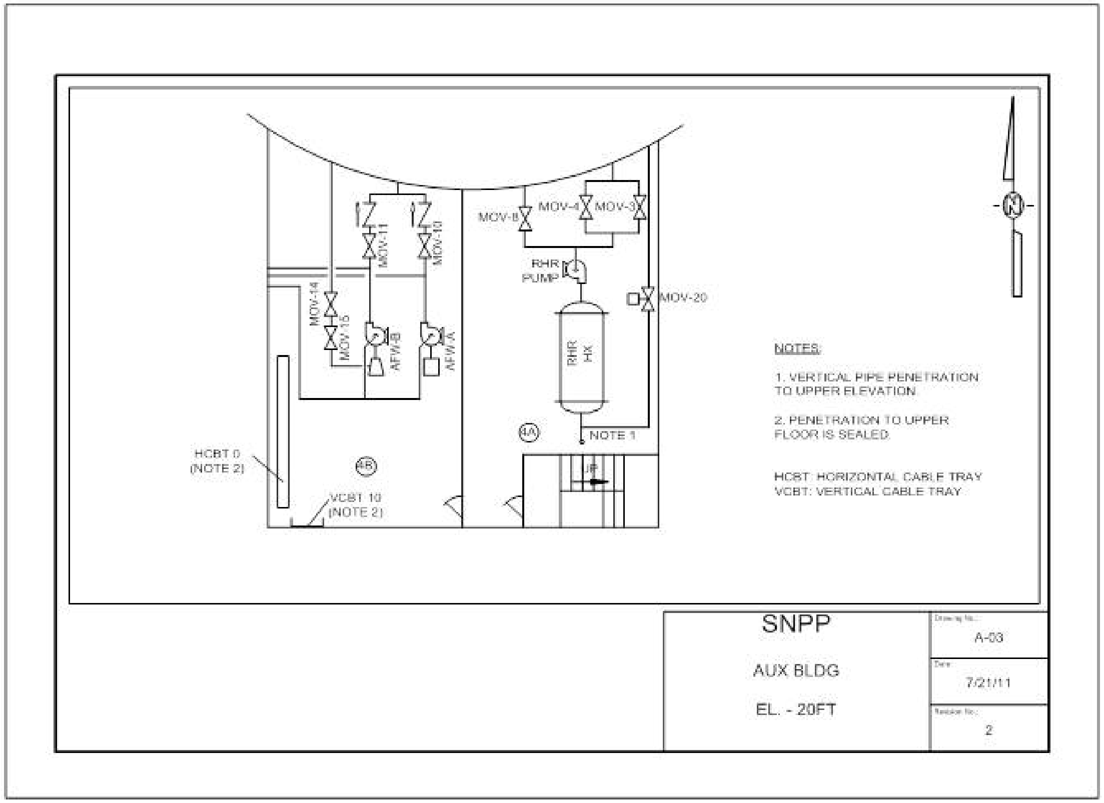


Fire PRA Training 2012, Bethesda MD
Introduction and Overview

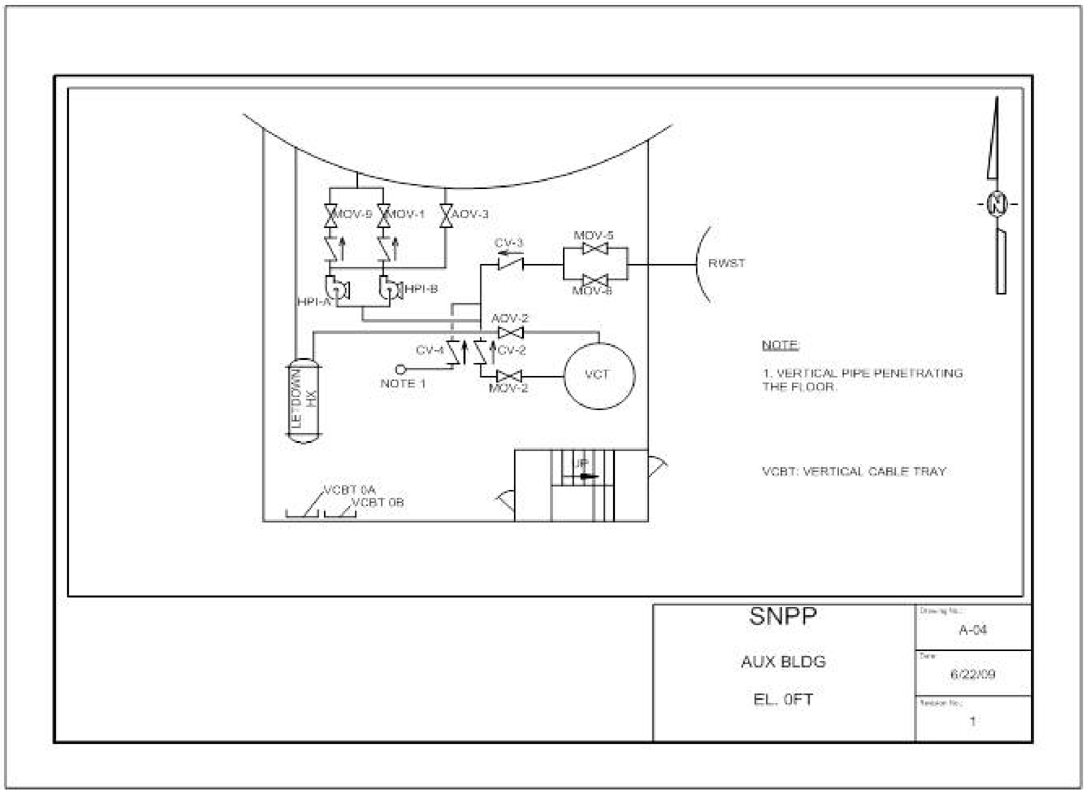
Slide 9

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

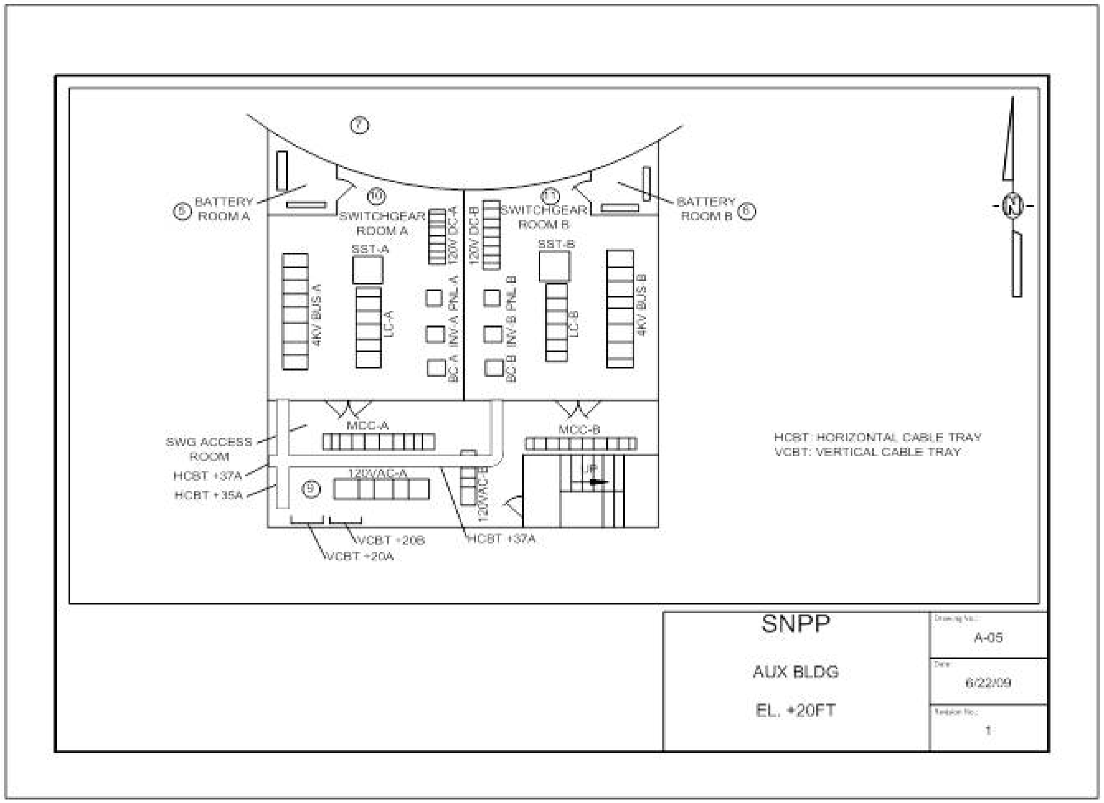
The SNPP: Aux. Bld. – RHR Pump Room



The SNPP: Aux. Bld. – Charging Pump Rm.



The SNPP: Aux. Bld. – Switchgear Rooms

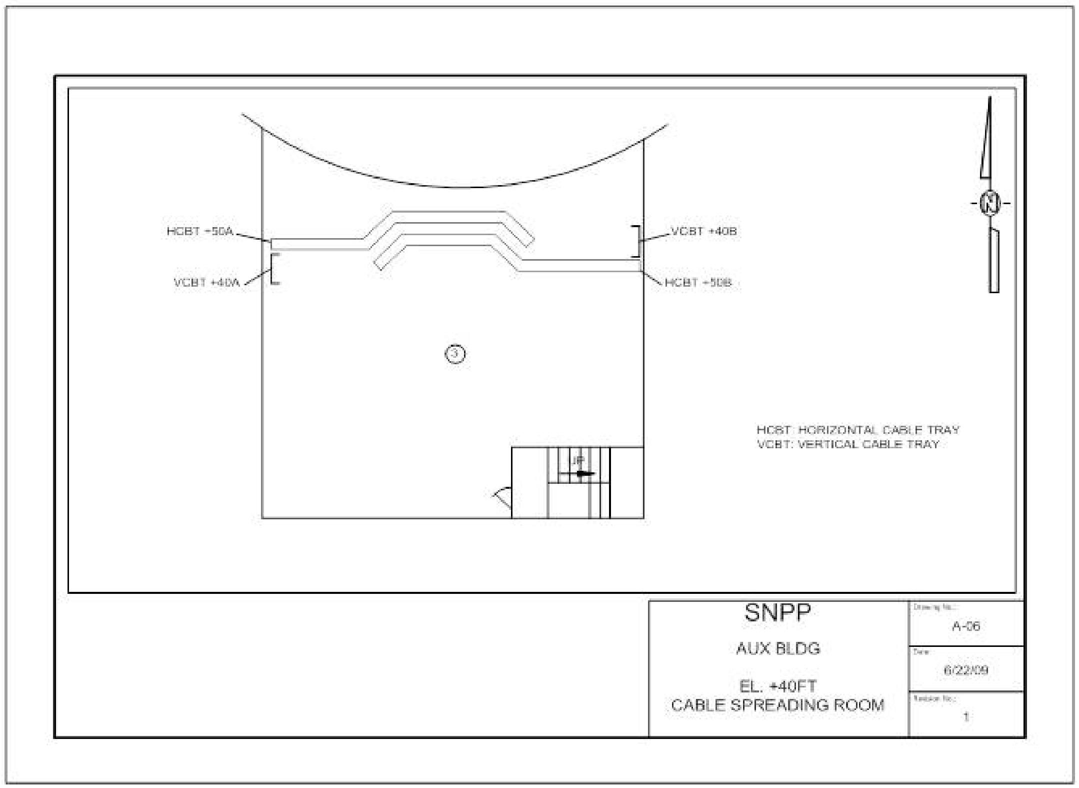


Fire PRA Training 2012, Bethesda MD
Introduction and Overview

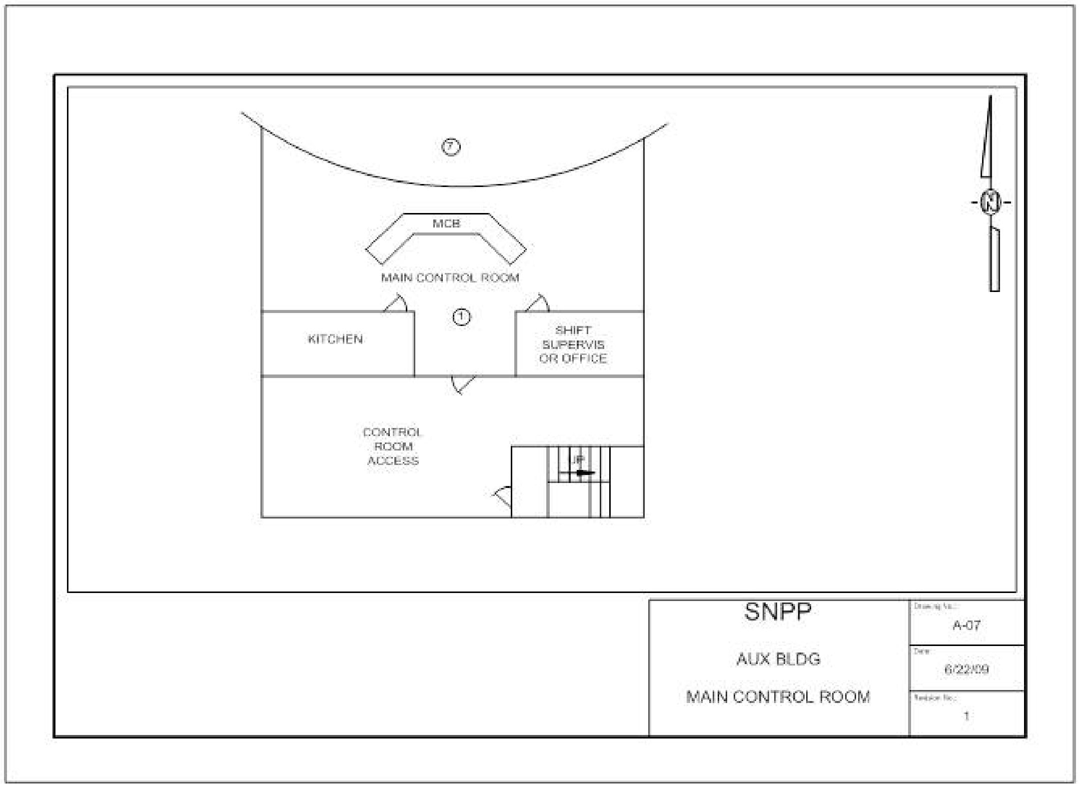
Slide 12

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

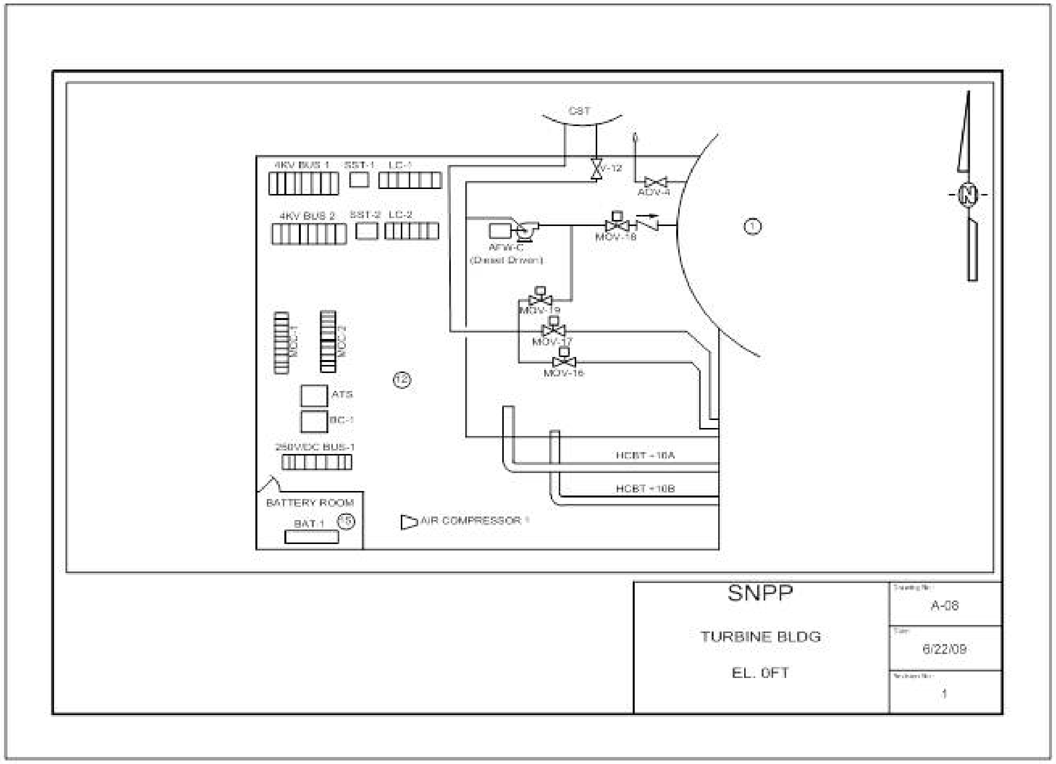
The SNPP: Aux. Bld. – Cable Spreading Rm.



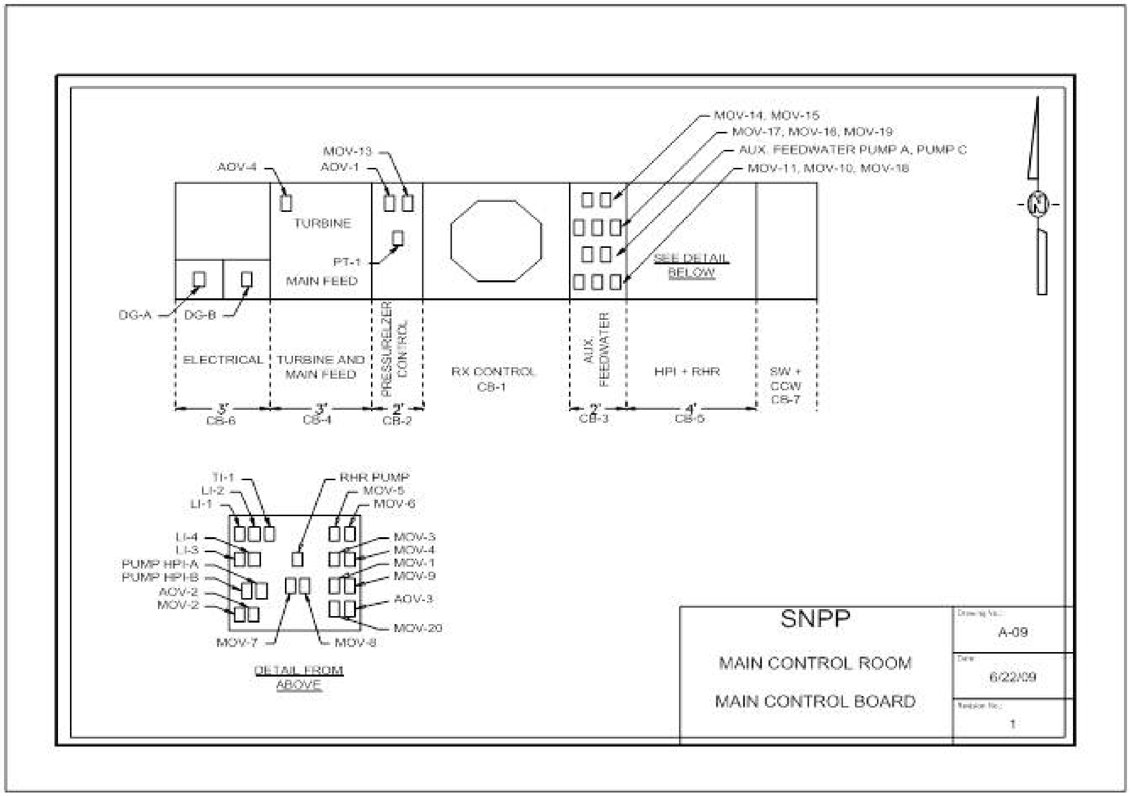
The SNPP: Aux. Bld. – Main Control Room



The SNPP: Turbine Building



The SNPP: Main Control Board Layout



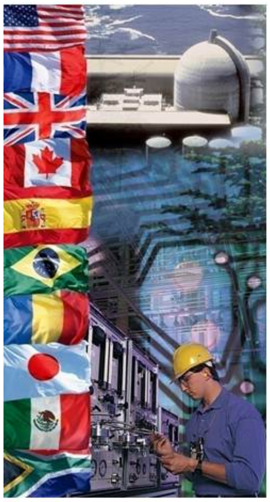
A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2 –Fire PRA Component Selection

ELECTRIC POWER RESEARCH INSTITUTE

Science Applications International Corporation

Sandia National Laboratories



EPRI/NRC-RES FIRE PRA METHODOLOGY

Task 2 - Fire PRA Component Selection

Jeff LaChance – Sandia National Laboratories
Rick Anoba – Anoba Consulting Services, LLC

Joint RES/EPRI Fire PRA Training Workshop 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Component Selection
Purpose (per 6850/1011989)

- Purpose: describe the procedure for selecting plant components to be modeled in a Fire PRA
- Fire PRA Component List
  - Key source of information for developing Fire PRA Model (Task 5)
    - Used to identify cables that must be located (Task 3)
- Process is iterative to ensure appropriate agreement among fire PRA Component List, Fire PRA Model, and cable identification

Corresponding PRA Standard Element

- Primary match is to element ES - Equipment Selection
  - ES Objective (as stated in the PRA standard):

    "Select plant equipment that will be included/credited in the fire PRA plant response model."

HLRs (per the PRA Standard)

- HLR-ES-A: The Fire PRA shall identify equipment whose failure caused by an initiating fire including spurious operation will contribute to or otherwise cause an initiating event (6 SRs)
- HLR-ES-B: The Fire PRA shall identify equipment whose failure including spurious operation would adversely affect the operability/functionality of that portion of the plant design to be credited in the Fire PRA (5 SRs)
- HLR-ES-C: The Fire PRA shall identify instrumentation whose failure including spurious operation would impact the reliability of operator actions associated with that portion of the plant design to be credited in the Fire PRA (2 SRs)
- HLR-ES-D: The Fire PRA shall document the fire PRA equipment selection, including that information about the equipment necessary to support the other fire PRA tasks (e.g. equipment identification, equipment type, normal, desired, failed states of equipment) in a manner that facilitates fire PRA applications, upgrades, and peer review (1 SR)

Task 2: Fire PRA Component Selection
Scope (per 6850/1011989)

Fire PRA Component List should include the following major categories of equipment:

- Equipment whose fire-induced failure (including spurious actuation) causes an initiating event
- Equipment needed to perform mitigating safety functions and to support operator actions
- Equipment whose fire-induced failure or spurious actuation may adversely impact credited mitigating safety functions
- Equipment whose fire-induced failure or spurious actuation may cause inappropriate or unsafe operator actions

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 5

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Component Selection
Approach (per 6850/1011989)

- Step 1: Identify Internal Events PRA sequences to include in fire PRA Model (necessary for identifying important equipment)
- Step 2: Review Internal Events PRA model against the Fire Safe Shutdown (SSD) Analysis and reconcile differences in the two analyses (including circuit analysis approaches)
- Step 3: Identify fire-induced initiating events based on equipment affected
- Step 4: Identify equipment subject to fire-induced spurious operation that may challenge the safe shutdown capability
- Step 5: Identify additional mitigating, instrumentation, and diagnostic equipment important to human response
- Step 6: Include "potentially high consequence" related equipment
- Step 7: Assemble the Fire PRA Component List

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 6

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Component Selection
General Observations

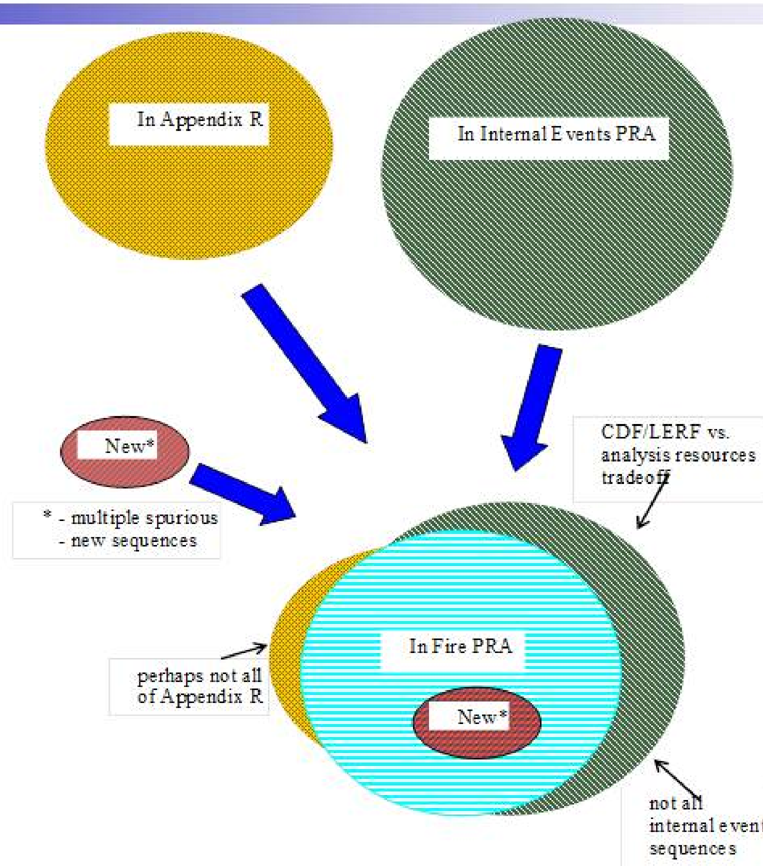
- Two major sources of existing information are used to generate the Fire PRA Component List:
    - Internal Events PRA model
    - Fire Safe Shutdown Analysis (Appendix R assessment)
- Just "tweaking" your Internal Events PRA is probably NOT sufficient – requires additional effort
    - Consideration of fire-induced spurious operation of equipment
    - Potential for undesirable operator actions due to spurious alarms/indications
    - Additional operator actions for responding to fire (e.g., opening breakers to prevent spurious operation)
- Just crediting Appendix R components may NOT be conservative
    - True that all other components in Internal Events PRA will be assumed to fail, but:
        - May be missing components with adverse risk implications (e.g., event initiators or complicatd SSD response)
        - May miss effects of non-modeled components on credited (modeled) systems/components and on operator performance
        - Still need to consider non-credited components as sources of fires

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 7

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection
Overview of Scope



Task 2: Fire PRA Component Selection
Assumptions

The following assumptions underlie this procedure:

- A good quality Internal Events PRA and Appendix R Safe Shutdown (SSD) analysis are available
- Analysts have considerable collective knowledge and understanding of plant systems, operator performance, the Internal Events PRA, and Appendix R SSD analysis
- Steps 4 thru 6 are applied to determine an appropriate number of spurious actuations to consider
  - Configurations, timing, length of sustained spurious actuation, cable material, etc., among reasons to limit what will be modeled
  - Note that HS duration is a current FAQ topic…

From: Lessons Learned and Insights
In-process FAQs …

- FAQ 08-0051
  - Issue:
    - The guidance does not provide a method for estimating the duration of a hot short once formed
    - This could be a significant factor for certain types of plant equipment that will return to a "fail safe" position if the hot short is removed or if MSO concurrence could trigger adverse impacts
  - General approach to resolution:
    - Analyze the cable fire test data to determine if an adequate basis exists to establish hot short duration distributions
  - Status:
    - Approved, but limited to AC hot shorts only
    - Will be revisited with lessons learned from DESIREE-FIRE test results for DC hot shorts (NUREG/CR-7100)

Task 2: Fire PRA Component Selection
Inputs/Outputs

Task inputs and outputs:

- Inputs from other tasks: equipment considerations for operator actions from Task 12 (Post-Fire HRA)
- Inputs from the MSO Expert Panel Reviews
- Could use inputs from other tasks to show equipment does not have to be modeled (e.g., Task 9 – Detailed Circuit Analysis or Task 11 - Fire Modeling to show an equipment item cannot spuriously fail or be affected by possible fires)
- Outputs to Task 3 (Cable Selection) and Task 5 (Risk Model)
- Choices made in this task set the overall analysis scope

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 1: Identify sequences to include and exclude from Fire PRA

- Some sequences can generally be excluded
  - Sequences requiring passive/mechanical failures that can not be initiated by fires (e.g., pipe-break LOCAs, SGTR, vessel rupture)
  - Sequences that can be caused by a fire but are low frequency (e.g., ATWS in a PWR)
  - It may be decided to not model certain systems (i.e., assume failed for Fire PRA) thereby excluding some sequences (e.g., main feedwater as a mitigating system not important)
- Possible additional sequences (recommend use of expert panel to address plant specific considerations)
  - Sequences associated with spurious operation (e.g., vessel/SG overfills, PORV opening, letdown or other pressure/level control anomalies)
  - MCR abandonment scenarios and other sequences arising from Fire Emergency Procedures (FEPs) and/or use of local manual actions

- Corresponding PRA Standard SRs: PRM-B5,B6

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 2: Review the internal events PRA model against the fire safe shutdown analysis

- Identify and reconcile:
  - differences in functions, success criteria, and sequences (e.g., Appendix R - no feed/bleed; PRA - feed/bleed)
  - front-line and support system differences (e.g., App. R - need HVAC; PRA - do not need HVAC)
  - system and equipment differences due to end state and mission considerations (e.g., App. R - cold shutdown; PRA - hot shutdown)
  - other miscellaneous equipment differences.
- Include review of manual actions (e.g., actions needed for safe shutdown) in conjunction with Task 12 (HRA)
- Corresponding PRA Standard SRs: ES-A3(a), ES-B1,B3

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 13

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 3: Identify fire-induced initiating events based on equipment affected

- Consider equipment whose failure (including spurious actuation) will cause automatic plant trip
- Consider equipment whose failure (including spurious actuation) will likely result in manual plant trip, per procedures
- Consider equipment whose failure (including spurious actuation) will invoke Technical Specification Limiting Condition of Operation (LCO) necessitating a forced shutdown while fire may still be present (prior EPRI guidance recommended consideration of <8 hr LCO)
- Compartments with none of the above need not have initiator though can conservatively assume simple plant trip
- Corresponding PRA Standard SRs: ES-A1,A3 & PRM-B3,B4,B5,B6

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

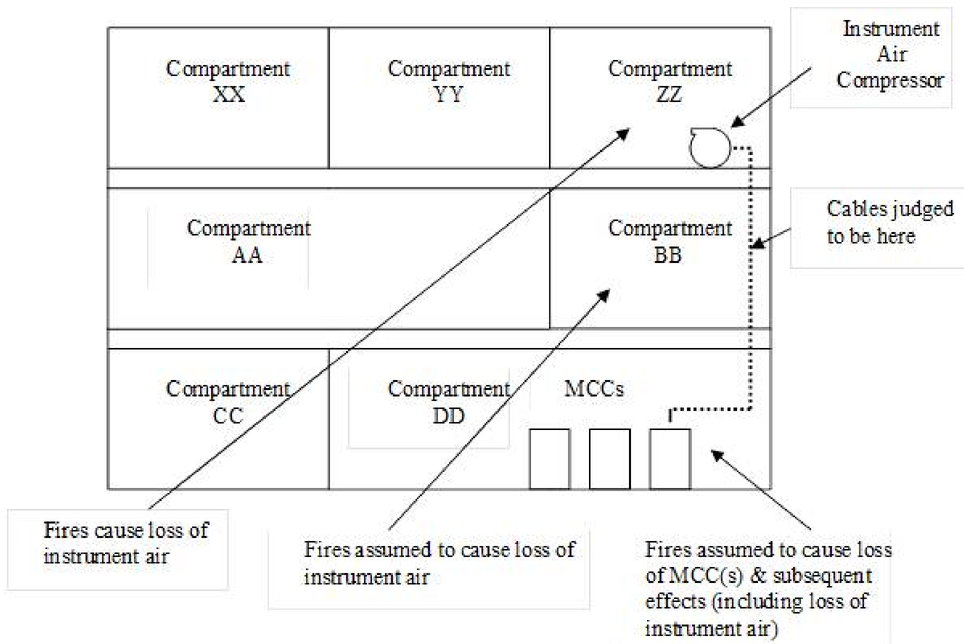
Slide 14

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

- Since not all equipment/cable locations in the plant (e.g., all Balance of Plant systems) may be identified, judgment involved in identifying 'likely' cable paths
  - Need a basis for any case where routing is not verified
  - Routing by exclusion (e.g., from a fire area, compartment, raceway…) is a common and acceptable approach
- Should consider spurious event(s) contributing to initiators
- Related PRA standard SR: CS-A11

Task 2: Fire PRA Component Selection
Steps In Procedure/Details



Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 4: Identify equipment whose spurious actuation may challenge the safe shutdown capability

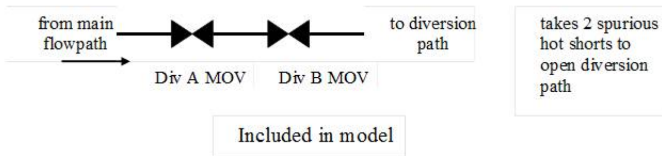
- Examine multiple spurious events within each system considering success criteria
  - PRA standard has specific requirements for multiple spurious events
- Review system P&IDs, electrical single lines, and other drawings
- Focus on equipment or failure modes not already on the component list (e.g., flow diversion paths)
- Review/Incorporate PRA related scenarios identified by the MSO Expert Panel to identify new components/failure modes
- Review Internal Events System Notebooks to identify components/failure modes screened based on low probability combinations

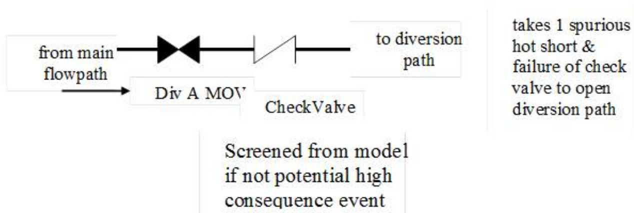
Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 4: Identify equipment whose spurious actuation may challenge the safe shutdown capability (Continued)

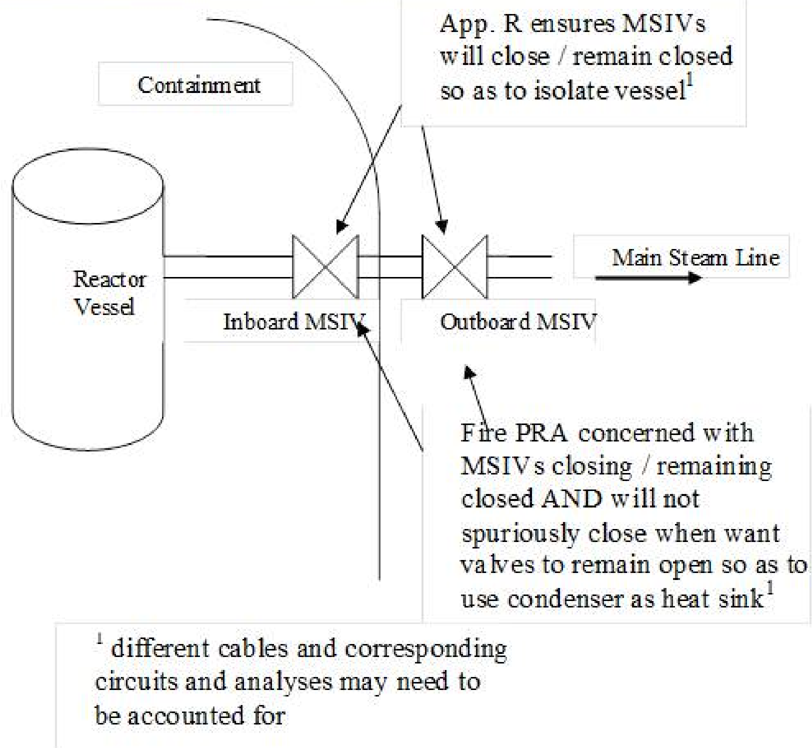
- Be aware of any failure combinations that could cause or contribute to an initiating event.
- Any new failure combinations that could cause or contribute to an initiating event should be addressed in Step 3.
- Any new equipment/failure modes should be added to component list for subsequent cable-tracing and circuit analysis
- Corresponding PRA Standard SRs: ES-B2,B3

Task 2: Fire PRA Component Selection
Flow Diversion Path Examples





Task 2: Fire PRA Component Selection
Example of a *New Failure Mode of a Component*



Task 2: Fire PRA Component Selection MSO Expert Panel

- This approach *complements* but is *not* part of the published consensus methodology (6850/1011989)

Reference Documents

- NEI 00-01, Revision 2, "Guidance for Post-Fire Safe Shutdown Circuit Analysis", May 2009
  - ❑ Focused on use of the generic list of MSOs provided in Appendix G, and the guidance provided in Section 4.4, "Expert Panel Review of MSOs"
- NEI 04-02 Frequently Asked Question (FAQ) 07-0038, Lessons Learned on Multiple Spurious Operations
- WCAP-16933-NP, Revision 0, "PWR Generic List of Fire-Induced Multiple Spurious Operation Scenarios", April 2009
- NRC Regulatory Guide 1.205, Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants, Revision 1, December 2009

Task 2: Fire PRA Component Selection MSO Expert Panel

Purpose

- Perform a systematic and complete review of credible spurious and MSO scenarios, and determine whether or not each individual scenario is to be included or excluded from the plant specific list of MSOs to be considered in the plant specific post-fire Fire PRA and Safe Shutdown Analysis (SSA).
- Involves group "what-if" discussions of both general and specific scenarios that may occur.

Task 2: Fire PRA Component Selection MSO Expert Panel

Expert Panel Membership:

- Fire Protection
- Fire Safe Shutdown Analysis: This expert should be familiar with the SSA input to the expert panel and with the SSA documentation for existing spurious operations.
- PRA: This expert should be familiar with the PRA input to the expert panel.
- Operations
- System Engineering
- Electrical Circuits

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 23

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection MSO Expert Panel

Process Overview

- Process is based on a diverse review of the Safe Shutdown Functions. Panel focuses on system and component interactions that could impact nuclear safety
- Review and discuss the potential failure modes for each safe shutdown function
- Identify MSO combinations that could defeat safe shutdown through those failure mechanisms
- Outputs are used in later tasks to identify cables and potential locations where vulnerabilities could exist
- MSOs determined to be potentially significant may be added to the PRA model and SSA

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 24

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection MSO Expert Panel

Supporting Plant Information for Reviews

- Flow Diagrams
- Control Wiring Diagrams
- Single and/or Three Line Diagrams
- Safe Shutdown Logic Diagrams
- PRA Event Sequence Diagrams
- Post-Fire Safe Shutdown Analysis
- Fire PRA models, analyses and cut-sets
- Plant operating experience

Task 2: Fire PRA Component Selection MSO Expert Panel

MSO Selection

- Review existing Safe Shutdown Analysis (SSA) list
- Expand existing MSO's to include all possible component failures
- Verify SSA assumptions are maintained
- Review generic list of MSO's (NEI 00-01 Revision 2, Appendix G)
- Screen MSO's that do not apply to your plant (i.e., components or system do not exist)

Task 2: Fire PRA Component Selection MSO Expert Panel

MSO Selection (Continued)

- Place all non-screened MSO's on plant specific list of MSO's
- Evaluate each MSO to determine if it can be screened due to design or operational features that would prevent it from occurring (i.e., breaker racked out during normal operation)
- Review the generic MSO list for similar or additional MSO's
- Develop and evaluate list of new MSO's

Task 2: Fire PRA Component Selection MSO Expert Panel

MSO Development

- Identify MSO combinations that could defeat safe shutdown through the previously identified failure mechanisms
  - The panel will build these MSO combinations into fire scenarios to be investigated
  - The scenario descriptions that result should include the identification of specific components whose failure or spurious operation would result in a loss of a safe shutdown function or lead to core damage

Task 2: Fire PRA Component Selection MSO Expert Panel

MSO Development (Continued)

- The expert panel systematically reviews each system (P&IDs, etc) affecting safe shutdown and the core, for the following Safe Shutdown Functions:
  - ❑Reactivity Control
  - ❑Decay Heat Removal
  - ❑Reactor Coolant
  - ❑Inventory Control
  - ❑Pressure Control
  - ❑Process Monitoring
  - ❑Support Functions

Task 2: Fire PRA Component Selection MSO Expert Panel

Typical Generic PWR MSOs

Scenario	Description
Loss of all RCP Seal Cooling	Spurious isolation of seal injection header flow, ***AND*** *Spurious isolation of CCW flow to Thermal Barrier Heat Exchanger (TBHX)*
RWST Drain Down via Containment Sump	Spurious opening of multiple series containment sump valves

Task 2: Fire PRA Component Selection MSO Expert Panel

Typical Generic BWR MSOs

RPV coolant drain through the Scram Discharge Volume (SDV) vent and drain	MSO opening of the solenoid valves which supply control air to the air operated isolation valves
Spurious Operations that creates RHR Pump Flow Diversion from RHR/LPCI, including diversion to the Torus or Suppression Pool.	RHR flow can be diverted to the containment through the RHR Torus or Suppression Pool return line isolation valves (E11-F024A, B and E11-F028A, B).

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 31

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection MSO Expert Panel

Outputs and Documentation

- Plant specific list of MSO's
- MSO Expert Panel Review Report
- The MSO Expert Panel is a living entity and the Plant Specific list of MSO's is a living document
- MSO components that could have PRA impact are addressed in Task 2
- MSO scenarios that have PRA impact are addressed in Task 5.

Fire PRA Workshop 2012, Bethesda MD
Task 2: Component Selection

Slide 32

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 2: Fire PRA Component Selection
Steps In Procedure/Details (per 6850/1011989)

Step 5: Identify additional instrumentation/diagnostic equipment important to operator response (level of redundancy matters!)

- Identify human actions of interest in conjunction with Task 12 (HRA)
- Identify instrumentation and diagnostic equipment associated with credited and potentially harmful human actions considering spurious indications related to each action
  - Is there insufficient redundancy to credit desired actions in EOPs/FEPs/ARPs in spite of failed/spurious indications?
  - Can a spurious indication(s) cause an undesired action because action is dependent on an indication that could be 'false'?
  - If yes – put indication on component list for cable/circuit review
- See new/expanded guidance developed by the RES/EPRI fire HRA collaboration.

- Corresponding PRA Standard SRs: ES-C1,C2

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Guidance on identification of harmful spurious operating instrumentation and diagnostic equipment:

- Assume instrumentation is in its normal configuration
- Focus on instrumentation with little redundancy
  - Note that fire PRA standard has language on this subject (i.e., verification of instrument redundancy in fire context)
- When verification of a spurious indication is required (and reliably performed), it may be eliminated from consideration
- When multiple and diverse indications must spuriously occur, those failures can be eliminated if the HRA shows that such failures would not likely cause a harmful operator action
- Include spurious operation of electrical equipment that would cause a faulty indication and harmful action
- Include inter-system effects

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 6: Include "potentially high consequence" related equipment

- High consequence events are one or more related failures at least partially caused by fire that:
  - by themselves cause core damage and large early release, or
  - single component failures that cause loss of entire safety function and lead directly to core damage
- Example of first case: spurious opening of two valves in high-pressure/low pressure RCS interface, leading to ISLOCA
- Example of second case: spurious opening of single valve that drains safety injection water source

- Corresponding PRA Standard SR: ES-A6

Task 2: Fire PRA Component Selection
Steps In Procedure/Details

Step 7: Assemble Fire PRA component list. Should include following information:

- Equipment ID and description (may be indicator or alarm)
- System designation
- Equipment type and location (at least compartment ID)
- PRA event ID and description
- Normal and desired position/status
- Failed electrical/air position
- References, comments, and notes

- Note: development of an actual/physical fire PRA component list is not a requirement of the PRA Standard

Sample Problem Exercise for Task 2, Step 1

- Distribute blank handout for Task 2, Step 1
- Distribute completed handout for Task 2, Step 1
- Question and Answer Session

Sample Problem Exercise for Task 2, Steps 2 and 3

- Distribute blank handout for Task 2, Step 2
- Distribute completed handout for Task 2, Step 2 Question and Answer Session
- Discuss Step 3
- Question and Answer Session

Sample Problem Exercise for Task 2, Steps 4 through 6

- Distribute blank handout for Task 2, Steps 4 through 6
- Distribute completed handout for Task 2, Steps 4 through 6
- Question and Answer Session

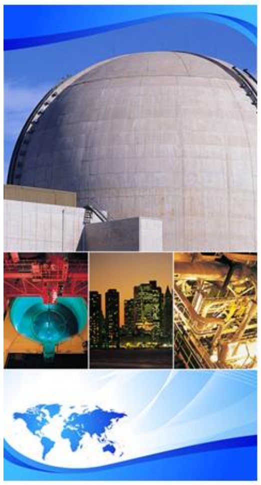
Sample Problem Exercise for Task 2, Step 7

- Distribute blank handout for Task 2, Step 7
- Distribute completed handout for Task 2, Step 7
- Question and Answer Session

Mapping HLRs & SRs for the ES technical element to NUREG/CR-6850, EPRI TR 1011989

Technical element	HLR	SR	6850/1011989 sections that cover SR	Comments
ES	A	The Fire PRA shall identify equipment whose failure caused by an initiating fire including spurious operation will contribute to or otherwise cause an initiating event.		
		1	2.5.3	
		2	3.5.3	Covered in "Cable Selection" chapter
		3	2.5.3	
		4	2.5.1, 2.5.4	
		5	2.5.4	
		6	2.5.6	
	B	The Fire PRA shall identify equipment whose failure including spurious operation would adversely affect the operability/functionality of that portion of the plant design to be credited in the Fire PRA.		
		1	2.5.2	
		2	2.5.4	
		3	5.5.1	Covered in "Fire-Induced Risk Model" chapter
		4	3.5.3	Covered in "Cable Selection" chapter
		5	n/a	Exclusion based on probability is not covered in 6850/1011989
	C	The Fire PRA shall identify instrumentation whose failure including spurious operation would impact the reliability of operator actions associated with that portion of the plant design to be credited in the Fire PRA.		
		1	2.5.5	
		2	2.5.5	
	D	The Fire PRA shall document the Fire PRA equipment selection, including that information about the equipment necessary to support the other Fire PRA tasks (e.g., equipment identification; equipment type; normal, desired, failed states of equipment; etc.) in a manner that facilitates Fire PRA applications, upgrades, and peer review.		
		1	n/a	Documentation not covered in 6850/1011989

Task 5 – Fire-Induced Risk Model Development



EPRI/NRC-RES FIRE PRA METHODOLOGY

Task 5 - Fire-Induced Risk Model Development

Joint RES/EPRI Fire PRA Workshop 2012
Bethesda MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Fire PRA Risk Model
Purpose (per 6850/1011989)

- Purpose: describe the procedure for developing the Fire PRA model to calculate CDF, CCDP, LERF, and CLERP for fire ignition events.
- Fire Risk Model
  - Key input for Quantitative Screening (Task 7)
    - Used to quantify CDF/CCDP and LERF/CLERP
- Process is iterative to ensure appropriate agreement among fire PRA Component List, Fire PRA Model, cable identification, and quantitative screening

Fire PRA Workshop 2012, Bethesda MD
Task 5 - Fire-Induced Risk Model Development
Slide 2
A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Fire PRA Risk Model
Corresponding PRA Standard Element

- Primary match is to element PRM - Equipment Selection
  - PRM Objectives (as stated in the PRA standard):

    "(a) to identify the initiating events that can be caused by a fire event and develop a related accident sequence model. (b) to depict the logical relationships among equipment failures (both random and fire induced) and human failure events (HFEs) for CDF and LERF assessment when combined with the initiating event frequencies."

Fire PRA Risk Model
HLRs (per the PRA Standard)

- HLR-PRM-A: The Fire PRA shall include the Fire PRA plant response model capable of supporting the HLR requirements of FQ.
- HLR-PRM-B: The Fire PRA plant response model shall include fire-induced initiating events, both fire induced and random failures of equipment, fire-specific as well as non–fire-related human failures associated with safe shutdown, accident progression events (e.g., containment failure modes), and the supporting probability data (including uncertainty) based on the SRs provided under this HLR that parallel, as appropriate, Part 2 of this Standard, for Internal Events PRA.
- HLR-PRM-C: The Fire PRA shall document the Fire PRA plant response model in a manner that facilitates Fire PRA applications, upgrades, and peer review.

Fire PRA Risk Model
Scope (per 6850/1011989)

- Task 5: Fire-Induced Risk Model Development
  - Constructing the PRA model
  - Step 1–Develop the Fire PRA CDF/CCDP Model.
  - Step 2–Develop the Fire PRA LERF/CLERP Model

Fire PRA Risk Model
General Comment/Observation

- Task 5 does not represent any changes from past practice, but what is modeled is largely based on Task 2 with HRA input from Task 12
- Bottom line – just "tweaking" your Internal Events PRA is probably NOT sufficient

Task 5: Fire Risk Model Development
General Objectives

Purpose: Configure the Internal Events PRA to provide fire risk metrics of interest (primarily CDF and LERF).

- Based on standard state-of-the-art PRA practices
- Intended to be applicable for any PRA methodology or software
- Allows user to quantify CDF and LERF, or conditional metrics CCDP and CLERP
- *Conceptually, nothing "new" here – need to "build the PRA model" reflecting fire induced initiators, equipment and failure modes, and human actions of interest*

Task 5: Fire Risk Model Development
Inputs/Outputs

Task inputs and outputs:

- Inputs from other tasks: [Note: inclusion of spatial information requires cable locations from Task 3]
  - Sequence considerations, initiating event considerations, and components from Task 2 (Fire PRA Component Selection),
  - Unscreened fire compartments from Task 4 (Qualitative Screening),
  - HRA events from Task 12 (Post-Fire HRA)
- Output to Task 7 (Quantitative Screening) which will further modify the model development
- Can always iterate back to refine aspects of the model

Task 5: Fire Risk Model Development
Steps in Procedure

Two major steps:

- Step 1: Develop CDF/CCDP model

- Step 2: Develop LERF/CLERP model

Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1 (2): Develop CDF/CCDP (LERF/CLERP) models

Step 1.1 (2.1): Select fire-induced initiators and sequences and incorporate into the model.

- Corresponding SRs: PRM-A1, A2, A3, B1-B15

- Fire initiators are generally defined in terms of compartment fires or fire scenarios

- Each fire initiator is mapped to one or more internal event initiators to mimic the fire-induced impact to the plant.

Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1.1 (2.1) – continued

- Initiating events previously screened in the internal events analysis may have to be reconsidered for the Fire PRA
- Final mapping of fire initiator to internal events initiators is based on cable routing information (task 3)
- The structure of Internal Events PRA should be reviewed to determine proper mapping of fire initiators

Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1.1 (2.1) – continued

- The Internal Events PRA should have the capability to quantify CDF and LERF sequences
- Internal events sequences form bulk of sequences for Fire PRA, but a search for new sequences should be made (see Task 2). Some new sequences may require new logic to be added to the PRA model

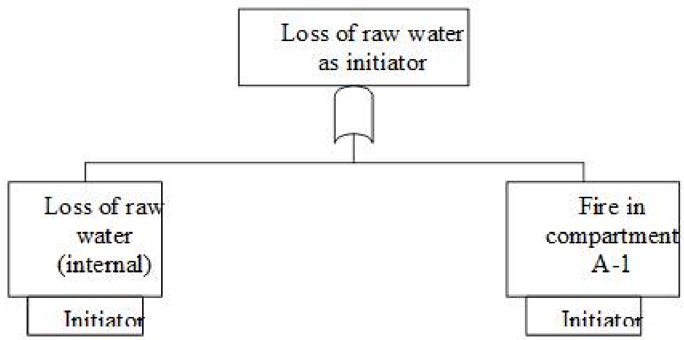
Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1.1 (2.1) - continued

- Plants that use fire emergency procedures (FEPs) may need special models to address unique fire-related actions (e.g., pre-defined fire response actions and MCR abandonment).

- Some human actions may induce new sequences not covered in Internal Events PRA and can “fail” components
  - Example: SISBO, or partial SISBO

Task 5: Fire Risk Model Development
Steps in Procedure/Details



Example of new logic with a fire-induced loss of raw water initiating event

Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1.2 (2.2): Incorporate fire-induced equipment failures

– Corresponding SRs: PRM-A4, B3, B6, B9

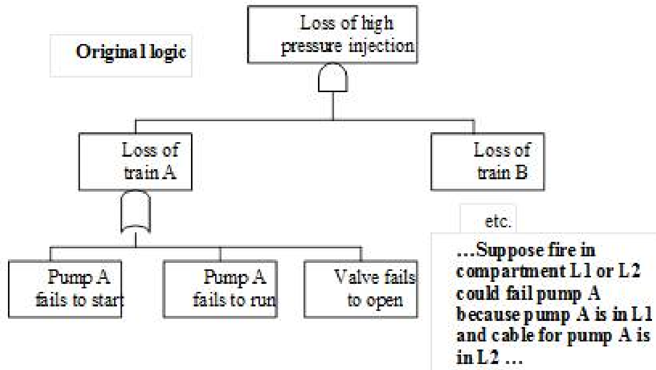
- Fire PRA database documents list of potentially failed equipment for each fire compartment
- Basic events for fire-induced spurious operations are defined and added to the PRA model (FAQ 08-0047)
- Inclusion of spatial information requires equipment and cable locations
  - May be an integral part of model logic, or handled with manipulation of a cable location database, etc.

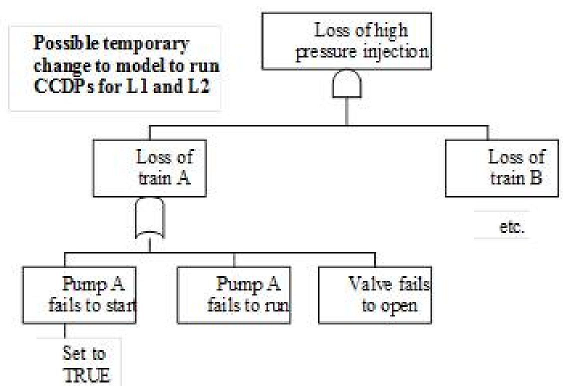
Fire PRA Workshop 2012, Bethesda MD
Task 5 - Fire-Induced Risk Model Development

Slide 15

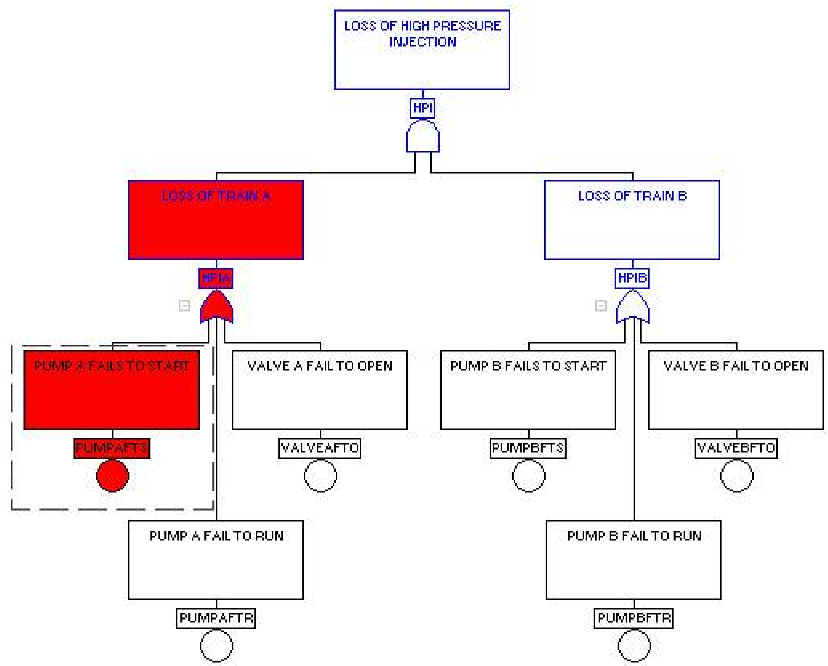
A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 5: Fire Risk Model Development
Steps in Procedure/Details

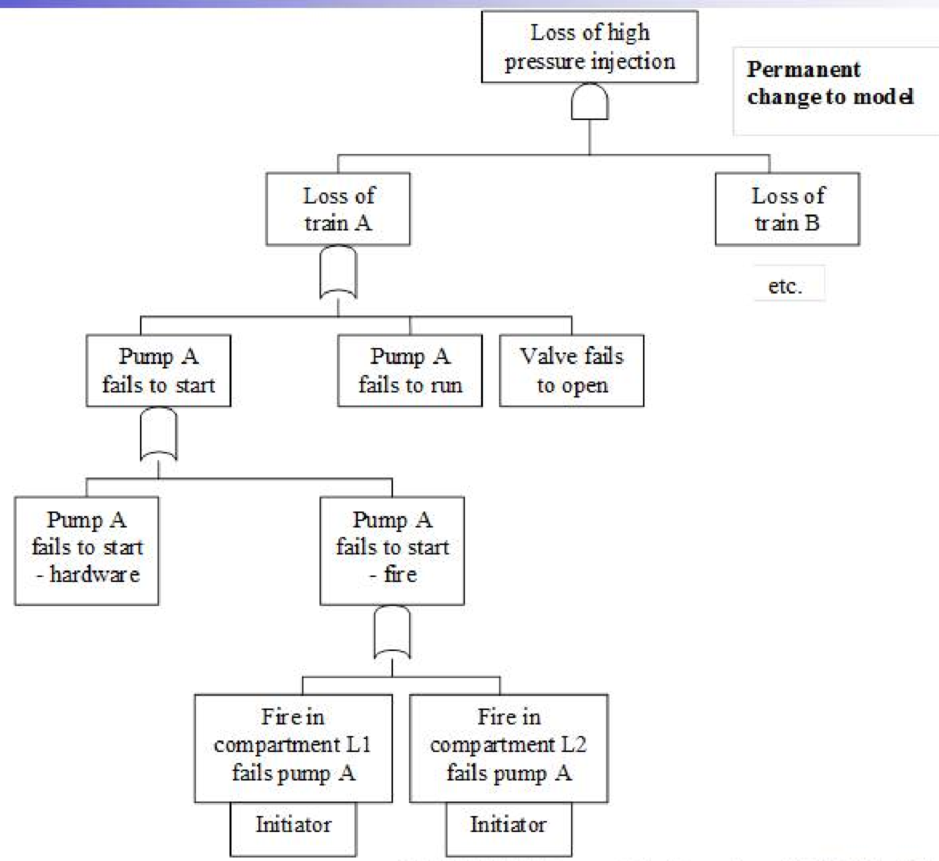




Task 5: Fire Risk Model Development
Steps in Procedure/Details

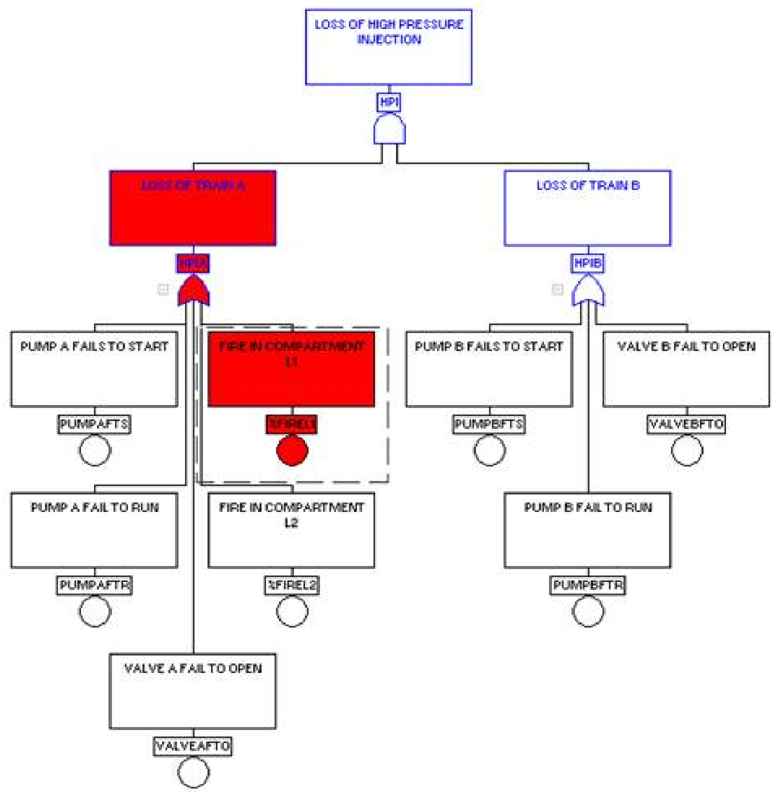


Task 5: Fire Risk Model Development
Steps in Procedure/Details



Task 5: Fire Risk Model Development

Steps in Procedure/Details



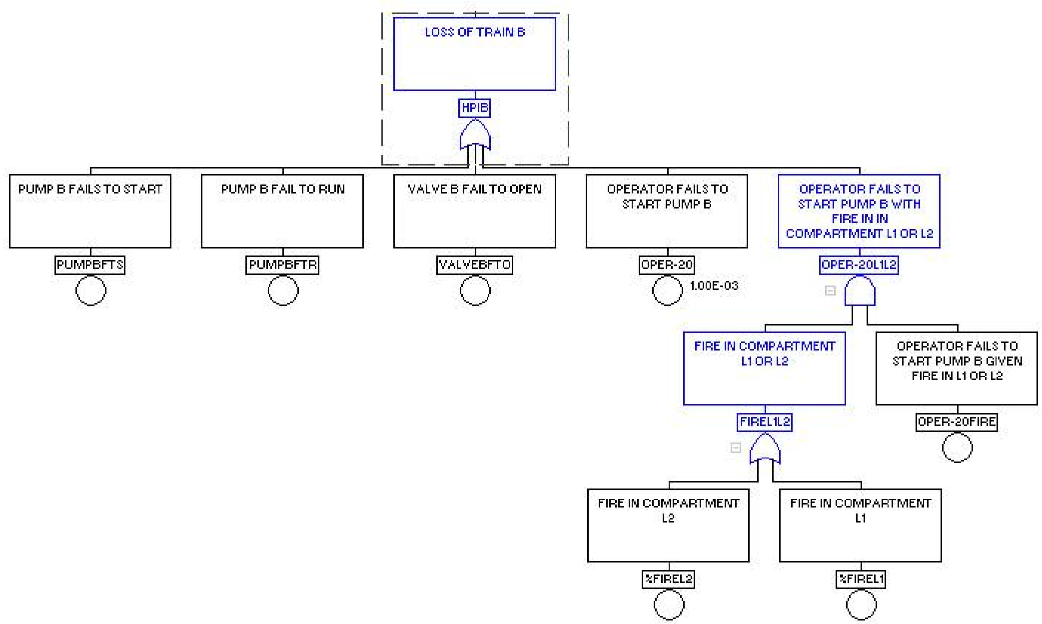
Task 5: Fire Risk Model Development
Steps in Procedure/Details

Step 1.3 (2.3): Incorporate fire-induced human failures

– Corresponding SRs: PRM-B9, B11

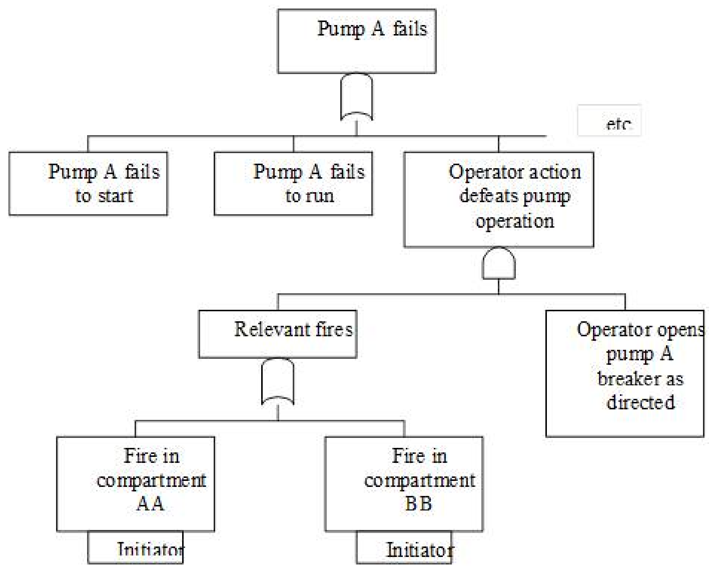
- New fire-specific HFEs may have to be added to the model to address actions specified in FEPs [Note: all HFEs will be set at screening values at first, using Task 12 guidance]
- Successful operator actions may temporarily disable ("fail") components

Task 5: Fire Risk Model Development
Steps in Procedure/Details



Task 5: Fire Risk Model Development
Steps in Procedure/Details

Suppose a proceduralized manual action carried out for fires in compartments AA & BB defeats Pump A operation by de-energizing the pump (opening its breaker drawer)…



Sample Problem Exercise for Task 5

- Distribute blank handout for Task 5, Steps 1 and 2
- Distribute completed handout for Task 5, Steps 1 and 2
- Question and Answer Session

Mapping HLRs & SRs for the PRM technical element to NUREG/CR-6850, EPRI TR 1011989

Technical element	HLR	SR	6850/1011989 sections that cover SR	Comments
PRM	A	The Fire PRA shall include the Fire PRA plant response model capable of supporting the HLR requirements of FQ.		
		1	5.5.1.1, 5.5.2.1	
		2	5.5.1.1, 5.5.2.1	
		3	5.5.1.1, 5.5.2.1	
		4	5.5.1.1, 5.5.1.2, 5.5.2.1, 5.5.2.2	

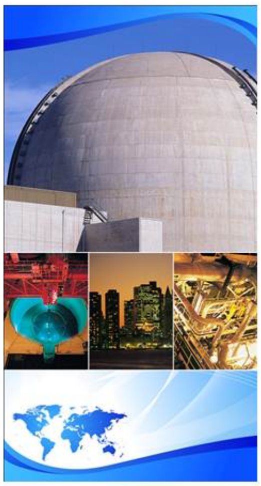
Mapping HLRs & SRs for the PRM technical element to NUREG/CR-6850, EPRI TR 1011989

Technical element	HLR	SR	6850/1011989 sections that cover SR	Comments
PRM	B	The Fire PRA plant response model shall include fire-induced initiating events, both fire induced and random failures of equipment, fire-specific as well as non–fire-related human failures associated with safe shutdown, accident progression events (e.g., containment failure modes), and the supporting probability data (including uncertainty) based on the SRs provided under this HLR that parallel, as appropriate, Part 2 of this Standard, for Internal Events PRA.		
		1	5.5.1.1, 5.5.2.1	
		2	5.5.1.1, 5.5.2.1	
		3	5.5.1.1, 5.5.1.2, 5.5.2.1, 5.5.2.2	
		4	5.5.1.1, 5.5.2.1	
		5	5.5.1.1, 5.5.2.1	
		6	5.5.1.1, 5.5.1.2, 5.5.2.1, 5.5.2.2	
		7	5.5.1.1, 5.5.2.1	
		8	5.5.1.1, 5.5.2.1	
		9	5.5.1.1, 5.5.1.2, 5.5.1.3, 5.5.2.1, 5.5.2.2, 5.5.2.3	
		10	5.5.1.1, 5.5.2.1	
		11	5.5.1.1, 5.5.1.3, 5.5.2.1, 5.5.2.3	
		12	5.5.1.1, 5.5.2.1	
		13	5.5.1.1, 5.5.2.1	
		14	5.5.1.1, 5.5.2.1	
		15	5.5.1.1, 5.5.2.1	
		12	5.5.1.1, 5.5.2.1	
		13	5.5.1.1, 5.5.2.1	
		14	5.5.1.1, 5.5.2.1	
		15	5.5.1.1, 5.5.2.1	

Mapping HLRs & SRs for the PRM technical element to NUREG/CR-6850, EPRI TR 1011989

Technical element	HLR	SR	6850/1011989 sections that cover SR	Comments
	C	The Fire PRA shall document the Fire PRA plant response model in a manner that facilitates Fire PRA applications, upgrades, and peer review.		
		1	n/a	Documentation not covered in 6850/1011989

Task 4 - Qualitative Screening



EPRI/NRC-RES FIRE PRA METHODOLOGY

Task 4 - Qualitative Screening
Task 7 - Quantitative Screening

Joint RES/EPRI Fire PRA Workshop 2012

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Qualitative / Quantitative Screening
Scope (per 6850/1011989)

- Task 4: Qualitative Screening
  - First chance to identify very low risk compartments
- Task 7: Quantitative Screening
  - Running the Fire PRA model to iteratively screen / maintain modeled sequences at different levels of detail

Fire PRA Workshop 2012, Bethesda MD
Task 4 & 7 – Qualitative/Quantitative Screening

Slide 2

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Qualitative Screening - Corresponding PRA Standard Element

- Primary match is to element QLS – Qualitative Screening
  - QLS Objectives (as stated in the PRA standard):

"(a) The objective of the qualitative screening (QLS) element is to identify physical analysis units whose potential fire risk contribution can be judged negligible without quantitative analysis.

(b) In this element, physical analysis units are examined only in the context of their individual contribution to fire risk. The potential risk contribution of all physical analysis units is reexamined in the multicompartment fire scenario analysis regardless of the physical analysis unit's disposition during qualitative screening."

Qualitative Screening – HLRs (per the PRA Standard)

- **HLR-QLS-A: The Fire PRA shall identify those physical analysis units that screen out as individual risk contributors without quantitative analysis (4 SRs).**
- **HLR-QLS-B: The Fire PRA shall document the results of the qualitative screening analysis in a manner that facilitates Fire PRA applications, upgrades, and peer review (3 SRs).**

Task 4: Qualitative Screening
Objectives and Scope

- The objective of Task 4 is to identify those fire compartments that can be shown to have a negligible risk contribution without quantitative analysis
  - This is where you exclude the office building inside the protected area
- Task 4 *only* considers fire compartments as individual contributors
  - Multi-compartment scenarios are covered in Task 11(b)
  - Compartments that screen out qualitatively need to be re-considered as potential Exposing Compartments in the multi-compartment analysis (but not as the Exposed Compartment)

Task 4: Qualitative Screening
Required Input and Task Output

- To complete Task 4 you need the following input:
  - List of fire compartments from Task 1
  - List of Fire PRA equipment from Task 2 including location mapping results
  - List of Fire PRA cables from Task 3 including location mapping results
- Task Output: A list of fire compartments that will be screened out (no further analysis) based on qualitative criteria
  - Unscreened fire compartments are used in Task 6 and further screened in Task 7

Task 4: Qualitative Screening
A Note….

- Qualitative Screening is OPTIONAL!
  - You may choose to retain any number of potentially low-risk fire compartments (from one to all) without formally conducting the Qualitative Screening Assessment for the compartment
    - However, to eliminate a compartment, you must exercise the screening process for the compartment
  - *Example 1*: Many areas will never pass qualitative screening, so simply keep them
  - *Example 2*: If you are dealing with an application with limited scope (e.g. NFPA 805 Change Evaluation) a formalized Qualitative Screening may be pointless

Task 4: Qualitative Screening
Screening Criteria (per 6850/1011989)

- A Fire Compartment may be screened out** if:
  - No Fire PRA equipment or cables are located in the compartment, and
  - No fire that remains confined to the compartment could lead to:
    - An automatic plant trip, or
    - A manual trip *as specified by plant procedures*, or
    - A *near-term* manual shutdown due to violation of plant Technical Specifications*

    *In the case of tech spec shutdown, consideration of the time window is appropriate
      - No firm time window is specified in the procedure – rule of thumb: consistent with the time window of the fire itself
      - Analyst must choose and justify the maximum time window considered

(**Note: screened compartments are re-considered as fire source compartments in the multi-compartment analysis - Task 11c)

Corresponding PRA Standard SRs: QLS-A1, A2

Mapping HLRs & SRs for the QLS technical element to NUREG/CR-6850, EPRI TR 1011989

Technical Element	HLR	SR	6850/1011989 section that covers SR	Comments
QLS	A	**The Fire PRA shall identify those physical analysis units that screen out as individual risk contributors without quantitative analysis**		
		1	4.5	
		2	4.5	
		3	4.5	
		4	n/a	Additional screening not covered in 6850/1011989
	B	**The Fire PRA shall document the results of the qualitative screening analysis in a manner that facilitates Fire PRA applications, upgrades, and peer review**		
		1	n/a	Documentation is discussed in Section 16.5 of 6850/1011989
		2	n/a	Documentation is discussed in Section 16.5 of 6850/1011989
		3	n/a	Documentation is discussed in Section 16.5 of 6850/1011989

Task 7 - Quantitative Screening

Task 7: Quantitative Screening
General Objectives (per 6850/1011989)

Purpose: allow (i.e., optional) screening of fire compartments and scenarios based on contribution to fire risk. Screening is primarily compartment-based (Tasks 7A/B). Scenario-based screening (Tasks 7C/D) is a further refinement (optional).

- Screening criteria not the same as acceptance criteria for regulatory applications (e.g., R.G. 1.174)
- Screening does not mean "throw away" – screened compartments/scenarios will be quantified (recognized to be conservative) and carried through to Task 14 as a measure of the residual fire risk

Quantitative Screening - Corresponding PRA Standard Element

- Primary match is to element QNS – Quantitative Screening
  - QNS Objective (as stated in the PRA standard):

  "The objective of the quantitative screening (QNS) element is to screen physical analysis units from further (e.g., more detailed quantitative) consideration based on preliminary estimates of fire risk contribution and using established quantitative screening criteria."

Quantitative Screening – HLRs (per the PRA Standard)

- **HLR-QNS-A: If quantitative screening is performed, the Fire PRA shall establish quantitative screening criteria to ensure that the estimated cumulative impact of screened physical analysis units on CDF and LERF is small (1 SR).**
- **HLR-QNS-B: If quantitative screening is performed, the Fire PRA shall identify those physical analysis units that screen out as individual risk contributors (2 SRs).**
- **HLR-QNS-C: VERIFY that the cumulative impact of screened physical analysis units on CDF and LERF is small (1 SR).**
- **HLR-QNS-D: The Fire PRA shall document the results of quantitative screening in a manner that facilitates Fire PRA applications, upgrades, and peer review (2 SRs).**

Task 7: Quantitative Screening
Inputs/Outputs

- Inputs from other tasks for compartment-based screening (7A/B):
  - Fire ignition frequencies from Task 6,
  - Task 5 (Fire-Induced Risk Model),
  - Task 12 (Post-Fire HRA Screening), and
  - Task 8 (Scoping Fire Modeling) (7B only)

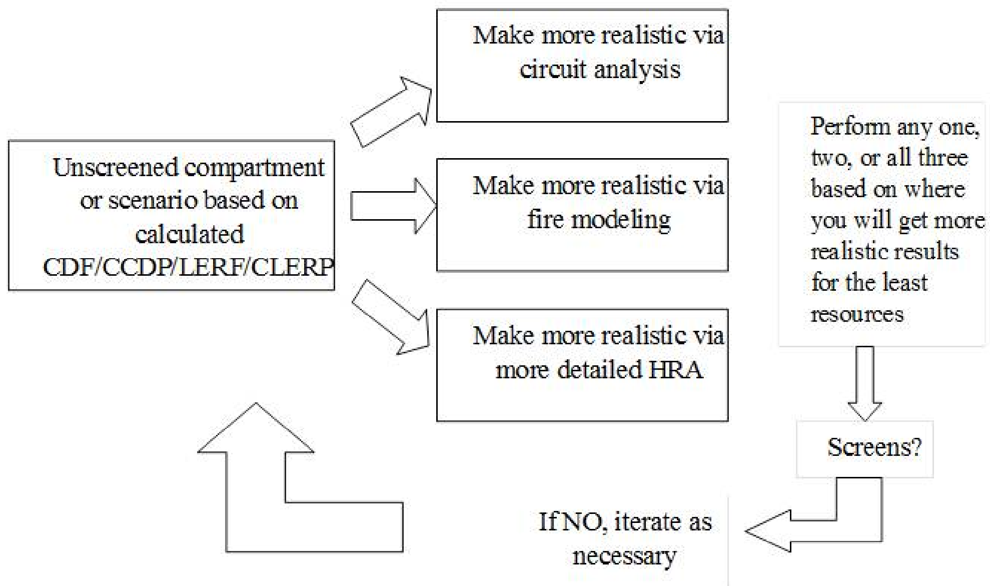
Task 7: Quantitative Screening
Inputs/Outputs (cont'd)

- Inputs from other tasks for scenario-based screening (7C/D) include inputs listed above plus:
  - Task 9 (Detailed Circuit Failure Analysis) and/or
  - Task 11 (Detailed Fire Modeling) and/or
  - Task 12 (Detailed Post-Fire HRA), and
  - Task 10 (Circuit Failure Mode Likelihood Analysis) (7D only)

Task 7: Quantitative Screening
Inputs/Outputs (cont'd)

- Outputs to other tasks:
  - Unscreened fire compartments from Task 7A go to Task 8 (Scoping Fire Modeling),
  - Unscreened fire compartments from Task 7B go to Task 9 (Detailed Circuit Failure Analysis) and/or Task 11 (Detailed Fire Modeling) and/or Task 12 (Detailed Post-Fire HRA),
  - Unscreened fire scenarios from Task 7C/D go to Task 14 (Fire Risk Quantification) for best-estimate risk calculation

Task 7: Quantitative Screening
Overview of the Process



Task 7: Quantitative Screening
Steps in Procedure

Three major steps in the procedure:

- Step 1: Quantify CDF/CCDP model
- Step 2: Quantify LERF/CLERP model
- Step 3: Quantitative screening

Task 7: Quantitative Screening
Steps in Procedure/Details

Step 1: Quantify CDF/CCDP models.

- Step 1.1: Quantify CCDP model
  - Fire-induced initiators are set to TRUE (1.0) for each fire compartment, CCDP calculated for each compartment
  - This step can be bypassed, if desired, by using fire frequencies in the model directly and calculating CDF

Task 7: Quantitative Screening
Steps in Procedure/Details

Step 1: Quantify CDF/CCDP models.

- Step 1.2: Quantify CDF
  - Compartment fire-induced initiator frequencies combined with compartment CCDPs from Step 1.1 to obtain compartment CDFs
- Step 1.3: Quantify ICDP (optional)
  - ICDP includes unavailability of equipment removed from service routinely
  - Recommend this be done if will use PRA for configuration management

Task 7: Quantitative Screening
Steps in Procedure/Details

Step 2: Develop LERF/CLERP models.

- Exactly analogous to Step 1 but now for LERF, CLERP
- Like ICDP, ILERP is optional

Task 7: Quantitative Screening
Establishing Quantitative Screening Criteria

- This is an area that has evolved beyond 6850/1011989
- 6850/1011989 *cumulative* screening criteria are based in part on screening against a fraction of the internal events risk results
  - Published PRA standard echoes 6850/1011989 (SR QNS-C1)
- Regulatory Guide 1.200 took exception to SR QNS-C1
  - NRC staff position: "screening criteria … should relate to the total CDF and LERF for the fire risk, not the internal events risk."
  - That is, screening should be within the hazard group (e.g., fire)
- An update to the PRA standard is pending and will *likely* revise QNS-C1 to reflect NRC staff position
- Bottom line: If you plan to use your fire PRA in regulatory applications, pay attention to RG 1.200 and watch for the PRA standard update

Task 7: Quantitative Screening
Screening Criteria for Single Fire Compartment

Step 3: Quantitative screening, Table 7.2 from NUREG/CR-6850

Quantification Type	CDF and LERF Compartment Screening Criteria	ICDP and ILERP Compartment Screening Criteria (Optional)
Fire Compartment CDF	CDF < 1.0E-7/yr	
Fire Compartment CDF With Intact Trains/Systems Unavailable		ICDP < 1.0E-7
Fire Compartment LERF	LERF < 1.0E-8/yr	
Fire Compartment LERF With Intact Trains/Systems Unavailable		ILERP < 1.0E-8

Note: The standard and RG 1.200 do not establish screening criteria for individual fire compartments – only cumulative criteria (see next slide…)

Task 7: Quantitative Screening
Screening Criteria For All Screened Compartments

Quantification Type	6850/1011989 Screening Criteria	NRC Staff Position per RG 1.200 for Cat II	NRC Staff Position per RG 1.200 for Cat III
Sum of CDF for all screened-out fire compartments	< 10% of internal event average CDF	the sum of the CDF contribution for all screened fire compartments is **<10%** of the estimated total CDF for **fire** events	the sum of the CDF contribution for all screened fire compartments is **<1%** of the estimated total CDF for **fire** events
Sum of LERF for all screened-out fire compartments	< 10% of internal event average LERF	the sum of the LERF contributions for all screened fire compartments is **<10%** of the estimated total LERF for **fire** events	the sum of the LERF contributions for all screened fire compartments is **<1%** of the estimated total LERF for **fire** events
Sum of ICDP for all screened-out fire compartments	< 1.0E-6	n/a	n/a
Sum of ILERP for all screened-out fire compartments	< 1.0E-7	n/a	n/a

Sample Problem Demonstration for Task 7

- On-line demonstration of Task 7
- Question and Answer Session

Mapping HLRs & SRs for the QNS technical element to NUREG/CR-6850, EPRI TR 1011989

Technical Element	HLR	SR	6850/101198 9 section that covers SR	Comments
QNS	A	**If quantitative screening is performed, the Fire PRA shall establish quantitative screening criteria to ensure that the estimated cumulative impact of screened physical analysis units on CDF and LERF is small**		
		1	7.5.3	Specific screening criteria are identified in 6850/1011989
	B	**If quantitative screening is performed, the Fire PRA shall identify those physical analysis units that screen out as individual risk contributors**		
		1	7.5.1, 7.5.2	
		2	7.5.1, 7.5.2	
	C	**Verify that the cumulative impact of screened physical analysis units on CDF and LERF is small**		
		1	7.5.3	Specific screening criteria are identified in 6850/1011989
	D	**The Fire PRA shall document the results of quantitative screening in a manner that facilitates Fire PRA applications, upgrades, and peer review**		
		1	n/a	Documentation is discussed in Section 16.5 of 6850/101198
		2	n/a	Documentation is discussed in Section 16.5 of 6850/101198

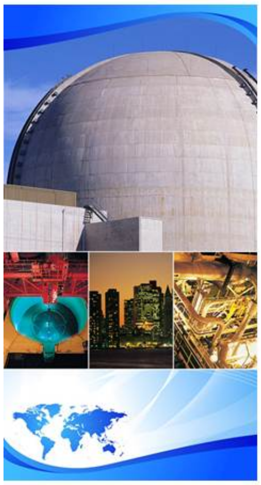
Task 14 – Fire Risk Quantification

ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

Science Applications International Corporation

From Science to Solutions



EPRI/NRC-RES FIRE PRA METHODOLOGY

Task 14 – Fire Risk Quantification

Fire PRA Workshop 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Fire Risk Quantification
Purpose (per 6850/1011989)

- Purpose: describe the procedure for performing fire risk quantification.
- Provides a general method for quantifying the final Fire PRA Model to generate the final fire risk results

Fire PRA Workshop 2012, Bethesda MD
Task 14 – Fire Risk Quantification

Slide 2

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Fire Risk Quantification
Corresponding PRA Standard Element

- Primary match is to element FQ – Fire Risk Quantification
  - FQ Objectives (as stated in the PRA standard):

    (a) quantify the fire-induced CDF and LERF contributions to plant risk.(b) understand what are the significant contributors to the fire-induced CDF and LERF."

Fire Risk Quantification
HLRs (per the PRA Standard)

- HLR-FQ-A: Quantification of the Fire PRA shall quantify the fire-induced CDF
- HLR-FQ-B: The fire-induced CDF quantification shall use appropriate models and codes and shall account for method-specific limitations and features.
- HLR-FQ-C: Model quantification shall determine that all identified dependencies are addressed appropriately.
- HLR-FQ-D: The frequency of different containment failure modes leading to a fire-induced large early release shall be quantified and aggregated, thus determining the fire-induced LERF.

Fire Risk Quantification
HLRs (per the PRA Standard)

- HLR-FQ-E: The fire-induced CDF and LERF quantification results shall be reviewed, and significant contributors to CDF and LERF, such as fires and their corresponding plant initiating events, fire locations, accident sequences, basic events (equipment unavailabilities and human failure events), plant damage states, containment challenges, and failure modes, shall be identified. The results shall be traceable to the inputs and assumptions made in the Fire PRA.
- HLR-FQ-F: The documentation of CDF and LERF analyses shall be consistent with the applicable SRs.

Fire Risk Quantification
Scope (per 6850/1011989)

- Task 14: Fire Risk Quantification
  - Obtaining best-estimate quantification of fire risk
  - Step 1–Quantify Final Fire CDF Model
  - Step 2–Quantify Final Fire LERF Model
  - Step 3–Conduct Uncertainty Analysis

Task 14: Fire Risk Quantification
General Objectives

Purpose: perform final (best-estimate) quantification of fire risk

- Calculate CDF/LERF as the primary risk metrics
- Include uncertainty analysis / sensitivity results (see Task 15)
- Identify significant contributors to fire risk
- Carry along insights from Task 13 to documentation but this is not an explicit part of "quantifying" the Fire PRA model
- Carry along residual risk from screened compartments and scenarios (Task 7); both (final fire risk and residual risk) are documented in Task 16 to provide total risk perspective

Task 14: Fire Risk Quantification
Inputs/Outputs

Task inputs:

- Inputs from other tasks:
  - Task 5 (Fire-Induced Risk Model) as modified/run thru Task 7 (Quantitative Screening),
  - Task 10 (Circuit Failure Mode Likelihood Analysis),
  - Task 11 (Detailed Fire Modeling), and
  - Task 12 (Post-Fire HRA Detailed Analysis)

Task 14: Fire Risk Quantification
Inputs/Outputs

- Output is the quantified fire risk results including the uncertainty and sensitivity analyses directed by Task 15 (Uncertainty and Sensitivity Analysis), all of which is documented per Task 16 (Fire PRA Documentation)

Task 14: Fire Risk Quantification
Steps in Procedure

Four major steps in the procedure*:

- Step 1: Quantify CDF
- Step 2: Quantify LERF
- Step 3: Perform uncertainty analyses including propagation of uncertainty bounds as directed under step 4 of Task 15
- Step 4: Perform sensitivity analyses as directed under step 4 of Task 15

* In each case, significant contributors are also identified

Task 14: Fire Risk Quantification
Quantification Process

Characteristics of the quantification process:

- Procedure is "general"; i.e., not tied to a specific method (event tree with boundary conditions, fault tree linking…)
- Can calculate CDF/LERF directly by explicitly including fire scenario frequencies or first calculate CCDP/CLERP and then combine with fire scenario frequencies
- Quantify consistent with relevant ASME-ANS PRA Standard (RA-Sa-2009) supporting requirements
  - Many cross-references from FQ to internal events section (Part 2) for most aspects of risk quantification

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 1 (2): Quantify Final Fire CDF/LERF Model

Step 1.1 (2.1): Quantify Final Fire CCDP/CLERP Model

- Corresponding SRs: FQ-A1, A2, A3, A4, B1, C1, D1, E1

- Final HRA probabilities including dependencies
- Final cable failure probabilities
- Final cable impacts

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 1.2 (2.2): Quantify Final Fire CDF/LERF Frequencies

– Corresponding SRs: FQ-A1-A4, B1, C1, D1, E1

- Final compartment frequencies
- Final scenario frequencies
- Final fire modeling parameters (i.e., severity factors, non-suppression probabilities, etc)

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 1.3 (2.3): Identify Main Contributors to Fire CDF/LERF

- Corresponding SRs: FQ-A1-A3, E1

- Contributions by fire scenarios, compartments where fire ignition occurs, plant damage states, post-fire operator actions, etc.

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 3: Propagate Uncertainty Distributions

- Probability distributions of epistemic uncertainties propagated through the CDF and LERF calculations
- Monte Carlo or Latin hypercube protocols

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 4.1: Identification of Final Set of Sensitivity Analysis Cases

- Review sensitivity cases identified in Task 15
- Finalize sensitivity cases for Step 4.2

Task 14: Fire Risk Quantification
Steps in Procedure/Details

Step 4.2: CDF and/or LERF Computations and Comparison

- Mean CDF/LERF values computed for each sensitivity analysis case considered in Step 4.1
- The results should be compared with the base-case considered in Steps1 and 2

Mapping HLRs & SRs for the FQ technical element to NUREG/CR-6850, EPRI TR 1011989

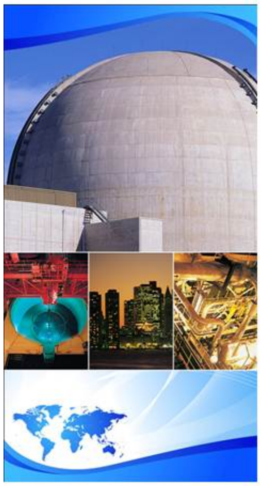
Technical element	HLR	SR	6850/1011989 sections that cover SR	Comments
FQ	A	Quantification of the Fire PRA shall quantify the fire-induced CDF.		
		1	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2, 14.5.2.3	
		2	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2, 14.5.2.3	
		3	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2, 14.5.2.3	
		4	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2	
	B	The fire-induced CDF quantification shall use appropriate models and codes and shall account for method-specific limitations and features.		
		1	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2	
	C	Model quantification shall determine that all identified dependencies are addressed appropriately.		
		1	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2	
	D	The frequency of different containment failure modes leading to a fire-induced large early release shall be quantified and aggregated, thus determining the fire-induced LERF		
		1	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2	
	E	The fire-induced CDF and LERF quantification results shall be reviewed, and significant contributors to CDF and LERF, such as fires and their corresponding plant initiating events, fire locations, accident sequences, basic events (equipment unavailabilities and human failure events), plant damage states, containment challenges, and failure modes, shall be identified. The results shall be traceable to the inputs and assumptions made in the Fire PRA		
		1	14.5.1.1, 14.5.1.2, 14.5.2.1, 14.5.2.2, 14.5.2.3	
	F	The documentation of CDF and LERF analyses shall be consistent with the applicable SRs.		
		1	n/a	Documentation not covered in 6850/1011989
		2	n/a	Documentation not covered in 6850/1011989

Task 15 – Uncertainty and Sensitivity Analysis

ELECTRIC POWER RESEARCH INSTITUTE

Sandia National Laboratories

Science Applications International Corporation



EPRI/NRC-RES FIRE PRA METHODOLOGY

Task 15 – Uncertainty and Sensitivity Analysis

Fire PRA Workshop 2012
Bethesda, MD

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 15:Uncertainty and Sensitivity Analysis
Purpose (per 6850/1011989)

Purpose: Provide a process for identifying and treating uncertainties in the Fire PRA, and identifying sensitivity analysis cases

- Many of the inputs to the Fire PRA are uncertain
- Important to identify sources of uncertainty and assumptions that have the strongest influence on the final results
- Fire risk can be quantified without explicit quantification of uncertainties, but the risk results cannot be considered as complete without it
- Sensitivity analysis is an important complement to uncertainty assessment

Fire PRA Workshop 2012, Bethesda MD
Task 15 - Uncertainty and Sensitivity Analysis

Slide 2

A Collaboration of U.S. NRC Office of Nuclear Regulatory Research (RES) & Electric Power Research Institute (EPRI)

Task 15:Uncertainty and Sensitivity Analysis
Scope

Scope of Task 15 includes:

- Background information on uncertainty
- Classification of the types of uncertainty
- A general approach on treating uncertainties in Fire PRA

Uncertainty and Sensitivity Analysis - Corresponding PRA Standard Element

- Primary match is to element UNC – Uncertainty and Sensitivity Analysis
- UNC Objectives (as stated in the PRA standard):

"(a) identify sources of analysis uncertainty

(b) characterize these uncertainties

(c) assess their potential impact on the CDF and LERF estimates"

Uncertainty and Sensitivity Analysis – HLRs (per the PRA Standard)

- **HLR-UNC-A: The Fire PRA shall identify sources of CDF and LERF uncertainties and related assumptions and modeling approximations. These uncertainties shall be characterized such that their potential impacts on the results are understood.**

Task 15:Uncertainty and Sensitivity Analysis
Types of Uncertainty

- Distinction between aleatory and epistemic uncertainty:
  - "Aleatory" - from the Latin alea (dice), of or relating to random or stochastic phenomena. Also called "random uncertainty or variability."
    - Reflected in the Fire PRA models as a set of interacting random processes involving a fire-induced transient, response of mitigating systems, and corresponding human actions
  - "Epistemic" - of, relating to, or involving knowledge; cognitive. [From Greek episteme, knowledge]. Also called "state-of-knowledge uncertainty."
    - Reflects uncertainty in the parameter values and models (including completeness) used in the Fire PRA – addressed in this Task

Task 15:Uncertainty and Sensitivity Analysis
Inputs and Outputs

- Inputs from other Tasks:
  - Identification of sources of epistemic uncertainties from Tasks 1 through 13 worthy of uncertainty/sensitivity analysis (i.e., key uncertainties)
  - Quantification results from Task 14 including risk drivers used to help determine key uncertainties
  - Proposed approach for addressing each of the identified uncertainties including sensitivity analyses
- Outputs to other Tasks:
  - Sensitivity analyses performed in Task 14
  - Results of uncertainty and sensitivity analysis are reflected in documentation of Fire PRA (Task 16)

Task 15:Uncertainty and Sensitivity Analysis
General Procedure (per 6850/1011989)

Addresses a process to be followed rather than a pre-defined list of epistemic uncertainties and sensitivity analyses, since these could be plant specific

- Step 1: Identify uncertainties associated with each task
- Step 2: Develop strategies for addressing uncertainties
- Step 3: Review uncertainties to decide which uncertainties to address and how
- Step 4: Perform uncertainty and sensitivity analyses
- Step 5: Include results of uncertainty and sensitivity analyses in Fire PRA documentation

Task 15: Uncertainty and Sensitivity Analysis
Steps in Procedure/Details

See Appendix U to NUREG/CR-6850 for background on uncertainty analysis. See Appendix V for details for each task.

Step 1: Identify epistemic uncertainties for each task

- Initial assessment of uncertainties to be treated is provided in Appendix V to NUREG/CR-6850 (but consider plant specific analysis for other uncertainties such as specific assumptions)
- From a practical standpoint, characterize uncertainties as modeling and data uncertainties
- Outcome is a list of issues, by task, leading to potentially important uncertainties (both modeling and data uncertainty)

Related SRs:

- PRM-A4, FQ-F1, IGN-A10, IGN-B5, FSS-E3, FSS-E4, FSS-H5, FSS-H9, and CF-A2 for sources of uncertainty

Task 15: Uncertainty and Sensitivity Analysis
Steps in Procedure/Details

Step 2: Develop strategies for addressing uncertainties

- Strategy can range from no action to explicit quantitative modeling
- Each task analyst is expected to provide suggested strategies
- Possible strategies include propagation of data uncertainties, developing multiple models, addressing uncertainties qualitatively, quality review process, and basis for excluding some uncertainties
- Basis for strategy should be noted and may include importance of uncertainty on overall results, effects on future applications, resource and schedule constraints

Task 15:Uncertainty and Sensitivity Analysis
Steps in Procedure/Details

Step 3: Review uncertainties to decide which uncertainties to address and how

- Review carried out by team of analysts familiar with issues, perhaps meeting more than once

- Review has multiple objectives:
  - Identify uncertainties that will not be addressed, and reasons why
  - Identify uncertainties to be addressed, and strategies to be used
  - Identify uncertainties to be grouped into single assessment
  - Identify issues to be treated via sensitivity analysis
  - Instruct task analysts who perform the analyses

Task 15:Uncertainty and Sensitivity Analysis
Sensitivity Analysis

- Sensitivity analysis can provide a perspective that cannot be obtained from a review of significant risk contributors.

  - Each task analyst can provide a list of parameters that had the strongest influence in their part of the analysis

  - Experiment with modified parameters to demonstrate impact on the final risk results

  - Modeling uncertainties can be demonstrated through sensitivity analysis

  - Sensitivities should be performed for individual uncertainties as well as for appropriate logical groups of uncertainties

Task 15:Uncertainty and Sensitivity Analysis
Steps in Procedure/Details

Step 4: Perform uncertainty and sensitivity analyses

- Uncertainty analyses may involve:
  - Quantitative sampling of parameter distributions
  - Manipulation of models to perform sensitivity analyses
  - Qualitative evaluation of uncertainty

- Following items should be made explicit:
  - Uncertainties being addressed
  - Strategy being followed
  - Specific methods, references, computer programs, etc. being used (to allow traceability)
  - Results of analyses, including conclusions relative to overall results of Fire PRA
  - Potential impacts on anticipated applications of results

Task 15:Uncertainty and Sensitivity Analysis
Steps in Procedure/Details

Step 5: Include results in PRA documentation

- Adequate documentation of uncertainties and sensitivities is as important as documentation of baseline results

- Adequate documentation leads to improved decision-making

- Documentation covered more fully under Task 16

Task 15:Uncertainty and Sensitivity Analysis *Expectations*

- Minimum set of uncertainties expected to have a formal treatment:
  - Fire PRA model structure itself, representing the uncertainty with regard to how fires could result in core damage and/or large early release outcomes (Tasks 5/7)
  - Uncertainty in each significant fire ignition frequency (Task 6)
  - Uncertainty in each significant circuit failure mode probability (Task 10)
  - Uncertainty in each significant target failure probability (Task 11)
    - Heat release rate
    - Suppression failure model and failure rate
    - Position of the target set vs. ignition sources
  - Uncertainty in each significant human error probability (Task 12)
  - Uncertainty in each core damage and large early release sequence frequency based on the above inputs as well as uncertainties for other significant equipment failures/modes (Task 14)

Task 15:Uncertainty and Sensitivity Analysis *Expectations*

- Other uncertainties may be relevant to address
  - Other activities related to uncertainty are underway
  - You might need to consult other resources for information (e.g., NUREG-1855, EPRI TR 1016737)
- Sensitivity analyses should be performed where important to show robustness in results (i.e., demonstrate where results are / are not sensitive to reasonable changes in the inputs)
- While not really a source of uncertainty, per se, technical quality issues and recommended reviews are also addressed

Mapping HLRs & SRs for the UNC technical element to NUREG/CR-6850, EPRI TR 1011989

Technical Element	HLR	SR	6850/101198 9 section that covers SR	Comments
	A	**The Fire PRA shall identify sources of CDF and LERF uncertainties and related assumptions and modeling approximations. These uncertainties shall be characterized such that their potential impacts on the results are understood**		
		1	15.5.1	
		2	15.5.5	Documentation is discussed in Section 16.5 of 6850/101198

NRC FORM 335 (12-2010) NRCMD 3.7 U.S. NUCLEAR REGULATORY COMMISSION **BIBLIOGRAPHIC DATA SHEET** *(See instructions on the reverse)*	1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.) NUREG/CP-0303, Volume 1 EPRI 3002005205
2. TITLE AND SUBTITLE Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES)-2012 Volume 1 Module 1:Probabilistic Risk Analysis (PRA)	3. DATE REPORT PUBLISHED MONTH: April YEAR: 2016 4. FIN OR GRANT NUMBER
5. AUTHOR(S) K. Wright; P. Smith; F. Gonzalez; K. Hamburger; T. Rivera; D. Stroup	6. TYPE OF REPORT Technical 7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Risk Analysis
U. S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research (RES)
Washington, DC 20555-0001

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, CA 94304

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

10. SUPPLEMENTARY NOTES

NRC–RES/EPRI Fire PRA Workshop conducted July 16–20, 2012, and September 24–28, 2012 in Bethesda, MD

11. ABSTRACT (200 words or less)

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) and the Electric Power Research Institute (EPRI) working under a memorandum of understanding (MOU) jointly conducted two sessions of the NRC–RES/EPRI Fire Probabilistic Risk Assessment (PRA) Workshop on July 16–20, 2012, and September 24–28, 2012, at the Bethesda Marriott in Bethesda, MD. The purpose of the workshop was to provide detailed, hands-on training on the fire PRA methodology described in the technical document, NUREG/CR-6850 (EPRI 1011989) entitled "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities." This fire PRA methodology document supports implementation of the risk-informed, performance-based rule in Title 10 of the Code of Federal Regulations (10 CFR) 50.48(c) endorsing National Fire Protection Association (NFPA) Standard 805, as well as other applications such as exemptions or deviations to the agency's current regulations and fire protection significance determination process (SDP) phase 3 applications.

This NUREG/CP documents both of the two sessions of the NRC-RES/EPRI Fire PRA Workshop delivered in 2012 and includes the slides and handout materials delivered in each module of the course as well as video recordings of the training that was delivered. This NUREG/CP can be used as an alternative training method for those who were unable to physically attend the training sessions. This report can also serve as a refresher for those who attended one or more training sessions and could also be useful preparatory material for those planning to attend future sessions.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)	13. AVAILABILITY STATEMENT
fire, risk-informed regulation, fire hazard analysis (FHA), fire safety, fire protection, nuclear power plant, probabilistic risk assessment (PRA), Fire modeling, circuit analysis, human reliability analysis	unlimited
	14. SECURITY CLASSIFICATION
	(This Page) unclassified
	(This Report) unclassified
	15. NUMBER OF PAGES
	16. PRICE

NUREG/CP-0303, Vol. 1 Methods for Applying Risk Analysis to Fire Scenarios (MARIAFIRES) – 2012 April 2016

Module 1: PRA