

**BSC**

**Design Calculation or Analysis Cover Sheet**

1. QA: QA

2. Page 1

Complete only applicable items.

3. System Monitored Geologic Repository		4. Document Identifier 000-PSA-MGR0-00900-000-00A					
5. Title Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis							
6. Group Preclosure Safety Analyses							
7. Document Status Designation <input type="checkbox"/> Preliminary <input checked="" type="checkbox"/> Committed <input type="checkbox"/> Confirmed <input type="checkbox"/> Cancelled/Superseded							
8. Notes/Comments See Page 2 for list of authors.							
Attachments							Total Number of Pages
Attachment A. Event Trees							69
Attachment B. System/Pivotal Event Analysis – Fault Trees							96
Attachment C. Active Component Reliability Data Analysis							51
Attachment D. Passive Equipment Failure Analysis							92
Attachment E. Human Reliability Analysis							70
Attachment F. Fire Analysis							29
Attachment G. Event Sequence Quantification Summary Tables							2
Attachment H. Excel Spreadsheet, SAPHIRE Model, and Supporting Files							2 + CD
<b>RECORD OF REVISIONS</b>							
9. No.	10. Reason For Revision	11. Total # of Pgs.	12. Last Pg. #	13. Originator (Print/Sign/Date)	14. Checker (Print/Sign/Date)	15. EGS (Print/Sign/Date)	16. Approved/Accepted (Print/Sign/Date)
00A	Initial issue	619	H-2	Dawn Martin-Miller/ See page 2 <i>Dawn</i> <i>Ma</i> 3/12/2008	See Page 3	M. Frank <i>M. Frank</i> 3/12/2008	M. Wisenberg <i>M. Wisenberg</i> 3/12/2008

**DISCLAIMER**

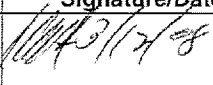
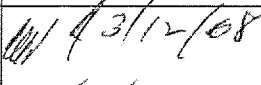

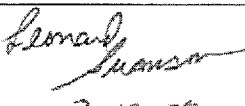
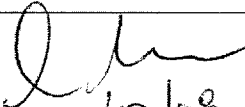

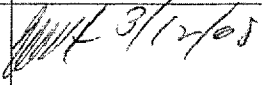
The analysis contained in this document was developed by Bechtel SAIC Company, LLC (BSC) and is intended solely for the use of BSC in its work for the Yucca Mountain Project (YMP).



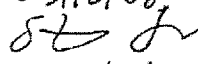
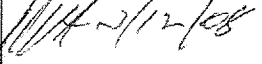
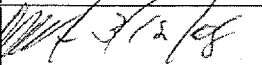
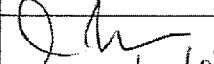
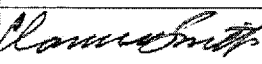
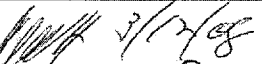
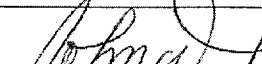
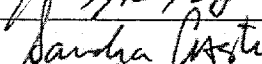

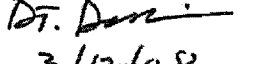
Section	Section Name	Originator	Signature/Date
1	PURPOSE	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
2	REFERENCES	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
3	ASSUMPTIONS	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
4	METHODOLOGY	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
4.1	QUALITY ASSURANCE	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
4.2	USE OF SOFTWARE	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
4.3	DESCRIPTION OF ANALYSIS METHODS	Paul Amico David Bradley Dan Christman Erin Collins Phuoc Le Dawn Martin-Miller Joe Minarick Doug Orvis Mary Presley  3/12/2008 <i>DM</i> Pierre Macheret <i>PNacht</i>	<i>[Signatures]</i> 3/12/08 3/12/08 3/12/08 3/12/08 3/12/08 3/12/08 3/12/08 3/12/08 3/12/08
5	LIST OF ATTACHMENTS	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
6	BODY OF ANALYSIS	N/A	
6.0	INITIATING EVENT SCREENING	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
6.1	EVENT TREE ANALYSIS	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
6.2	INITIATING AND PIVOTAL EVENT ANALYSIS	Dan Gallagher	<i>[Signature]</i> 3/12/2008
6.3	DATA UTILIZATION	David Bradley (6.3.2.3 and 6.3.2.4 only)	<i>[Signature]</i> 3/12/08
		Dan Christman (6.3.2.1, 6.3.2.2, and 6.3.2.5 only)	<i>[Signature]</i> 3/12/08
		Erin Collins	<i>[Signature]</i> 3/12/08
6.4	HUMAN RELIABILITY ANALYSIS	Paul Amico	<i>[Signature]</i> 3/12/08
		Mary Presley	<i>[Signature]</i> 3/12/08
		Erin Collins	<i>[Signature]</i> 3/12/08
		Doug Orvis	<i>[Signature]</i> 3/12/08
6.5	FIRE ANALYSIS	Paul Amico	<i>[Signature]</i> 3/12/08
		Laura Plumb (under the supervision of Paul Amico)	<i>[Signature]</i> 3/12/08
6.6	(NOT USED)		
6.7	EVENT SEQUENCE QUANTIFICATION	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
6.8	EVENT SEQUENCE GROUPING AND CATEGORIZATION	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
6.9	DEFINED ITS SSCs AND PROCEDURAL SAFETY CONTROLS REQUIREMENTS	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
7	RESULTS AND CONCLUSIONS	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
Att A	EVENT TREES	Dawn Martin-Miller	<i>[Signature]</i> 3/12/2008
Att B	SYSTEM/PIVOTAL EVENT ANALYSIS - FAULT TREES	Dan Gallagher Daryl Kepler Bill Schwinkendorf	<i>[Signatures]</i> 3/12/08 3/12/08 3/12/08
Att C	ACTIVE COMPONENT RELIABILITY DATA ANALYSIS	Erin Collins	<i>[Signature]</i> 3/12/08

Section	Section Name	Originator	Signature/Date
Att D	PASSIVE EQUIPMENT FAILURE ANALYSIS	David Bradley (Section D2) Dan Christman (Sections D1 and D3)	<i>[Signature]</i> 3/12/08
Att E	HUMAN RELIABILITY ANALYSIS	Paul Amico Mary Presley Erin Collins Doug Orvis	<i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08
Att F	FIRE ANALYSIS	Paul Amico Laura Plumb (under supervision of Paul Amico)	<i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08
Att G	EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES	Dawn Martin-Miller Dan Gallagher	<i>[Signature]</i> 3/12/2008 <i>[Signature]</i> 3/12/2008
Att H	EXCEL SPREADSHEET, SAPHIRE MODEL, AND SUPPORTING FILES	Dawn Martin-Miller Dan Gallagher	<i>[Signature]</i> 3/12/2008 <i>[Signature]</i> 3/12/2008

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

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Andrew Burningham	<i>[Signature]</i> 3/12/08	Section 1-7; Attachments A, C, F, G, and H	Administrative check	Perform checks on the Calculations and Analyses Checklist (Attachment 6 to EG-PRO-3DP-G04B-00037) that are administrative in nature (e.g., format, procedural compliance, links in InfoWorks, DIRS, reference format, document numbering, confirmation of SAPHIRE validation, tracking number, etc.)
Amy Primmer	<i>[Signature]</i> 3/12/08	Attachments B, D, and E		
Shyang-Fenn <del>(Alex) Deng</del> (Alex) Deng AKK 3/12/08	<i>[Signature]</i> 3/12/08	Sections 1, 3, 4, and 7	Overall approach and methodology	Check that the standard approach and methodology includes changes to the methodology resulting from input from industry reviewers.
Phuoc Le	<i>[Signature]</i> 3/12/08	Section 6.0 through 6.8 and Attachments A through H	Cut set check	Initiating Event Screening-Section 6.0 and cut set check. Section 6.0 through 6.8 and Attachments A through H.
Kathryn Ashley	<i>[Signature]</i> 3/12/08	Section 6.9	Specialty check	Check Section 6.9.
Daniel Christman	<i>[Signature]</i> 3/12/08	Section 6.5 and Attachment F	Specialty check:	Fire Initiating Events - Section 6.5 and Attachment F.
Doug Orvis	<i>[Signature]</i> 3/12/08	Section 6.0	Specialty Check; Section 6.0 – 6.0.9, excluding 6.0.5	Initiating event screening Section 6.0.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
W. Guy Rhoden	 3/12/08	Section 6.0.5	Specialty Check; Section 6.0.5	Initiating event screening – screening of diesel fuel oil storage tank (Area 70A) and tanker truck explosions
Laura Plumb <i>working for Reliability</i>	 3/12/08	Section 6.3.3 Miscellaneous Data	Specialty check	Section 6.3.3 miscellaneous data and supporting reference and cross-reference to other sections.
Ching Chan	 3/12/2008	Attachment B-1 Site Prime Mover Fault Tree Analysis	Design Concurrence	Check fault tree description. -Design accurately described. -Basic events have basis in latest issued for LA information. -Success criteria accurate. -Basic events clearly phrased. -References to Engineering documents correct and up to date.
Len Swanson	 3-12-08	Attachment B-2 Site Transporter Fault Tree Analysis	Design Concurrence	Check fault tree description. -Design accurately described -Basic events have basis in latest issued for LA information. -Success criteria accurate. -Basic events clearly phrased. -References to Engineering documents correct and up to date.
Phuoc Le (covered in cut set check) ASR 3/12/08	 3/12/08	Attachment B-3 Conveyance Collides with Facility Door fault tree	Design Concurrence	Check fault tree description. -Design accurately described. -Basic events have basis in latest issued for LA information. -Success criteria accurate. -Basic events clearly phrased. -References to Engineering documents correct and up to date.
Stephen Skochko for Karim Vakhshoori	 for Karim Vakhshoori 3/12/08	Attachment B-4 System Pivotal Events Analyses - Fault Tree Analysis – Horizontal Cask Tractor and Trailer	Design Concurrence	Check fault tree description. -Design accurately described. -Basic events have basis in latest issued for LA information. -Success criteria accurate. -Basic events clearly phrased. -References to Engineering documents correct and up to date.
Dan Christman	 3/12/08	Attachment C Active Component Reliability Data Analysis	Specialty check	Check Attachment C including the Mathcad file for Bayesian update of reliability values.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Doug Smith Stephen Skochko for Karim Vakhshoori Stephen Skochko	 03/12/08  for Karim Vakhshoori 03/12/08  03/12/08	Attachment C Active Component Reliability Data Analysis	Detailed references and numerical inputs	This check traced input data back to references for Attachment C.
Daniel Christman	 2/12/08	Attachment D Passive Equipment Failure Analysis	Specialty check	Check Section D2, 6.3.2.3, and 6.3.2.4.
David Bradley	 3/12/08	Attachment D Passive Equipment Failure Analysis	Specialty check	Check Sections D1, D3, 6.3.2.1, 6.3.2.2, and 6.3.2.5.
Phuoc Le	 3/12/08	Attachment E Human Reliability Analysis	Specialty check	Section 6.4 and Attachment E.
Clarence Smith	 3/12/08	Attachment E Human Reliability Analysis	Design concurrence	Check that the basic scenarios in Attachment E are consistent with the concept of operations.
Dan Christman	 3/12/08	Attachment F Fire Analysis and Section 6.5	Specialty check	Check the fire analysis calculation.
John Wang John ASR 3/12/08	 3/12/08	Section 6.0 through 6.9 and Attachments E and F	Detailed references and numerical inputs	Check that references in the main body are <del>references to</del> references to the appropriate documents. <del>documents</del> ASR 3/12/08
Sandra Castro ASR 3/12/08	 3/12/08	Section 2.1 <sup>ASR</sup> 3/12/08	References	Check that all references to engineering documents are correct and up to date. ASR 3/12/08
John Wang Jabo Tang ASR 3/12/08	 3/12/2008	All sections of main body and attachments	Detailed references and numerical inputs	Check that data in <del>body</del> body of analysis has been accurately copied from the sources in attachments.
Dale Dexheimer	 3/12/08	Section 6.8	Specialty check	Check consistency with Preclosure Consequence Analyses.

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Jabo Tang		All sections of main body and attachments	Detailed References and numerical Inputs	Check that data in body of analysis has been accurately copied from the sources in attachments.
Dale Dexheimer		Section 6.8	Specialty Check	Check consistency with Preclosure Consequence Analyses.

*see previous page*

*[Signature]*  
3/12/2008

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	12
1. PURPOSE .....	15
2. REFERENCES .....	19
2.1 PROJECT PROCEDURES/DIRECTIVES .....	19
2.2 DESIGN INPUTS .....	19
2.3 DESIGN CONSTRAINTS .....	27
2.4 DESIGN OUTPUTS .....	28
2.5 ATTACHMENT REFERENCES .....	28
3. ASSUMPTIONS .....	29
3.1 ASSUMPTIONS REQUIRING VERIFICATION .....	29
3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION .....	29
4. METHODOLOGY .....	30
4.1 QUALITY ASSURANCE .....	30
4.2 USE OF SOFTWARE .....	31
4.3 DESCRIPTION OF ANALYSIS METHODS .....	33
5. LIST OF ATTACHMENTS .....	95
6. BODY OF ANALYSIS .....	96
6.0 INITIATING EVENT SCREENING .....	96
6.1 EVENT TREE ANALYSIS .....	115
6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS .....	125
6.3 DATA UTILIZATION .....	133
6.4 HUMAN RELIABILITY ANALYSIS .....	165
6.5 FIRE INITIATING EVENTS .....	171
6.6 NOT USED .....	173
6.7 EVENT SEQUENCE FREQUENCY RESULTS .....	173
6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION .....	178
6.9 IMPORTANT TO SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS AND PROCEDURAL SAFETY CONTROL REQUIREMENTS .....	192
7. RESULTS AND CONCLUSIONS .....	205
ATTACHMENT A EVENT TREE ANALYSIS .....	A-1
ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS–FAULT TREES .....	B-1
ATTACHMENT C ACTIVE COMPONENT RELIABILITY DATA ANALYSIS .....	C-1
ATTACHMENT D PASSIVE EQUIPMENT FAILURE ANALYSIS .....	D-1
ATTACHMENT E HUMAN RELIABILITY ANALYSIS .....	E-1
ATTACHMENT F FIRE ANALYSIS .....	F-1

**CONTENTS (Continued)**

	<b>Page</b>
ATTACHMENT G EVENT SEQUENCE QUANTIFICATION SUMMARY TABLE .....	G-1
ATTACHMENT H EXCEL SPREADSHEET, SAPHIRE MODEL, AND SUPPORTING FILES .....	H-1



## FIGURES

	<b>Page</b>
4.3-1. Event Sequence Analysis Process.....	33
4.3-2. Preclosure Safety Assessment Process .....	38
4.3-3. Portion of a Simplified Example Process Flow Diagram for Typical Intra-Site Operations.....	39
4.3-4. Event Sequence Diagram to Event Tree Relationship.....	41
4.3-5. Excel Spreadsheet Example Emphasizing ISO-ESD02-TAD, Sequence 3-3 for a TAD Canister Drop Resulting in an Unfiltered Radiological Release .....	46
4.3-6. Grouped Event Sequences for ESD-02, TAD Canisters.....	49
4.3-7. Example Fault Tree.....	50
4.3-8. Concept of Uncertainty in Load and Resistance.....	53
4.3-9. Point Estimate Load Approximation Used in PCSA .....	55
4.3-10. Component Failure Rate “Bathtub Curve” Model.....	62
4.3-11. Incorporation of Human Reliability Analysis within the PCSA.....	72
6.1-1. Example of a Self-Contained Event Tree .....	118
6.1-2. Example of an Initiator Event Tree.....	120
6.1-3. Example of a System Response Event Tree .....	121
6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line) .....	137

**TABLES**

	<b>Page</b>
4.3-1. Criticality Control Parameter Summary .....	90
6.0-1. Retention Decisions from External Events Hazards Screening Analysis.....	100
6.0-2. Bases for Screening Internal Initiating Events.....	101
6.0-3. Parameters Used to Estimate Stand-Off Distances for Explosion Involving the Area 70A or a Tanker Truck.....	106
6.0-4. Additional Inputs Used for Quantitative Evaluation of a Fuel Tank Explosion .....	108
6.0-5. Estimated Stand-Off Distances for Area 70A and a Tanker Resupply Truck.....	113
6.1-1. Waste Form Throughputs over the Preclosure Period .....	122
6.1-2. Figure Locations for Initiator Event Trees and System Response Event Trees.....	123
6.2-1. Summary of Top Event Quantification for the SPM .....	129
6.2-2. Summary of Top Event Quantification for the Site Transporter .....	131
6.2-3. Summary of Top Event Quantification for the Cask Tractor and Cask Transfer Trailer .....	132
6.2-4. Top Level and Linking Fault Trees .....	133
6.3-1. Active Component Reliability Data Summary .....	139
6.3-2. Failure Probabilities Due to Drops and Other Impacts.....	146
6.3-3. Failure Probabilities Due to Miscellaneous Events .....	146
6.3-4. Failure Probabilities for Collision Events.....	149
6.3-5. Summary of Canister Failure Probabilities in Fire.....	151
6.3-6. Probabilities of Loss of Shielding.....	154
6.3-7. Summary of Passive Event Failure Probabilities.....	156
6.3-8. Passive Failure Basic Events used in Intra-Site Operations Event Sequence Analysis.....	157
6.3-9. Fire Analysis Frequencies.....	158
6.3-10. Miscellaneous Data Used in the Reliability Analysis.....	159
6.4-1. Human Failure Event Probability Summary.....	169
6.5-1. Fire Initiating Event Frequency Distributions .....	172
6.7-1. Example Event Sequence Quantification Summary Table.....	175
6.8-1. Bounding Category 2 Event Sequences.....	178

**TABLES (Continued)**

6.8-2.	Category 1 Final Event Sequences Summary .....	184
6.8-3.	Category 2 Final Event Sequences Summary .....	185
6.8-4.	Off-Normal Events Not Analyzed for Categorization .....	191
6.9-1.	Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs .....	193
6.9-2.	Summary of Procedural Safety Controls for Intra-Site Operations .....	204
7-1.	Key to Results .....	205
7-2.	Summary of Category 2 End States .....	206

## ACRONYMS AND ABBREVIATIONS

### Acronyms

ATHEANA	a technique for human event analysis
BOP	balance of plant
BSC	Bechtel SAIC Company, LLC
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
DHLW	defense high-level radioactive waste
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EFC	error forcing context
ESD	event sequence diagram
FEA	finite element analysis
FEM	finite element modeling
FTA	fault tree analysis
GROA	geologic repository operations area
HAM	horizontal aging module
HAZOP	hazard and operability
HCTT	cask tractor and cask transfer trailer (used only for SAPHIRE fault tree codes)
HDPC	horizontal dual-purpose canister
HEPA	high-efficiency particulate air filter
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HSTC	horizontal shielded transfer cask
HVAC	heating, ventilation, and air conditioning
IET	initiator event tree
IHF	Initial Handling Facility
ITC	important to criticality
ITS	important to safety

**ACRONYMS AND ABBREVIATIONS (Continued)**

LLW	low-level radioactive waste
LLWF	Low-Level Waste Facility
LOS	loss of shielding
LS-DYNA	Livermore Software–Dynamic Finite Element Program
MLD	master logic diagram
N/A	not applicable
NAICS	North American Industry Classification System
NFPA	National Fire Protection Association
NRC	U.S. Nuclear Regulatory Commission
PCSA	Preclosure Safety Analysis
PDF	probability density function
PEFA	passive equipment failure analysis
PFD	process flow diagram
PRA	probabilistic risk assessment
PSC	procedural safety controls
PSF	performance-shaping factor
QA	quality assurance
RF	Receipt Facility
SFTM	spent nuclear fuel transfer machine
SLS	steel/lead/steel
SNF	spent nuclear fuel
SPM	site prime mover
SRET	system response event tree
SSC	structure, system, or component
SSCs	structures, systems, and components
TAD	transportation, aging, and disposal
TEV	transport and emplacement vehicle
TNT	trinitrotoluene
TYP-FM	type and failure mode
WHF	Wet Handling Facility
WPTT	waste package transfer trolley
YMP	Yucca Mountain Project

## ACRONYMS AND ABBREVIATIONS (Continued)

### Abbreviations

AC	alternating current
BTU	British Thermal Unit
°C	degree Celsius
ft	foot, feet
ft <sup>3</sup>	cubic foot
hr	hour
K	Kelvin
k <sub>eff</sub>	effective neutron multiplication factor
kPa	kilopascal
kV	kilovolt
lb	pound
lb-mol	pound-mole
m <sup>2</sup>	square meter
psi	pound per square inch
°R	degree Rankine
V	volt
yr	year

## 1. PURPOSE

This document and its companion document entitled *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29) constitute a portion of the preclosure safety analysis (PCSA) that is described in its entirety in the safety analysis report that will be submitted to the U.S. Nuclear Regulatory Commission (NRC) as part of the Yucca Mountain Project (YMP) license application. These documents are part of a collection of analysis reports that encompass all waste handling activities and facilities of the geologic repository operations area (GROA) from the beginning of operation to the end of the preclosure period. The *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29) describes the identification of initiating events and the development of potential event sequences that emanate from them. This analysis uses the resulting event sequences to perform a quantitative analysis of the event sequences for the purpose of categorization per the definition provided by 10 CFR 63.2 (Ref. 2.3.2).

The PCSA uses probabilistic risk assessment (PRA) technology derived from both nuclear power plant and aerospace methods and applications in order to perform analyses to comply with the risk informed aspects of 10 CFR 63.111 and 63.112 (Ref. 2.3.2) and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report* (Ref. 2.2.69). The PCSA, however, limits the use of PRA technology to identification and development of event sequences that might lead to direct exposure of workers or onsite members of the public; radiological releases that may affect the workers or public (onsite and offsite) and criticality.

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

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

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

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

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

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

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

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



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

Other boundary conditions used in the PCSA include:

- Plant operational state. The initial state of the facility is normal with each system operating within its vendor-prescribed operating conditions.
- No other simultaneous initiating events. It is standard practice to not consider the occurrence of other initiating events (human-induced or naturally occurring) during the time span of an event sequence because (a) the probability of two simultaneous initiating events within the time window is small and, (b) each initiating event will cause operations to be terminated, which further reduces the conditional probability of the occurrence of a second initiating event, given that the first has occurred.
- Equipment failure mode. The failure mode of a structure, system, or component (SSC) corresponds to that required to make the initiating or pivotal event occur.
- Fundamental to the basis for the use of industry-wide reliability parameters within the PCSA, such as failure rates, is the use of SSCs within the GROA that conform to NRC accepted consensus codes and standards, and other regulatory guidance.
- Intentional malevolent acts, such as sabotage and other security threats, are not addressed in this analysis.

As stated, the scope of the PCSA is limited to internal initiating events originating within the GROA boundary and external initiating events that have their origin outside the GROA boundary, but can affect buildings and/or equipment within the GROA. External event analyses are documented in other PCSA documents (e.g., *External Events Hazards Screening Analysis* (Ref. 2.2.26)). Internal event identification (using a master logic diagram (MLD) and hazard and operability (HAZOP) evaluation), event sequence development and grouping, and related facility details are provided in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29), which also documents the methodology and process employed and initiates the analysis that is completed here.

This document uses event trees from the event sequence development analysis (Ref. 2.2.29) to quantify the event sequences for each waste form. Quantification refers to the process of obtaining the mean frequency of each event sequence for the purpose of categorization. This document shows the categorization of each event sequence based on:

- Mean frequency associated with the event sequence frequency distribution.
- Uncertainty associated with the event sequence frequency distributions.

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

Other PCSA documents, which are not referenced here, cover the reliability and categorization of external events and summarize PSCs and nuclear safety design bases.

## 2. REFERENCES

### 2.1 PROJECT PROCEDURES/DIRECTIVES

- 2.1.1 EG-PRO-3DP-G04B-00037, REV 10. *Calculations and Analyses*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0001.
- 2.1.2 EG-PRO-3DP-G04B-00046, Rev. 10. *Engineering Drawings*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080115.0014.
- 2.1.3 IT-PRO-0011, REV 7. *Software Management*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: DOC.20070905.0007.
- 2.1.4 LS-PRO-0201, REV 5. *Preclosure Safety Analysis Process*. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071010.0021.

### 2.2 DESIGN INPUTS

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

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

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

- 2.2.1 \*Ahrens, M. 2000. *Fires in or at Industrial Chemical, Hazardous Chemical and Plastic Manufacturing Facilities, 1988-1997 Unallocated Annual Averages and Narratives*. Quincy, Massachusetts: National Fire Protection Association. TIC: 259997.
- 2.2.2 AIChE (American Institute of Chemical Engineers) 2000. *Guidelines for Chemical Process Quantitative Risk Analysis*. 2nd Edition. New York, New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers. ISBN: 0-8169-0720-X. TIC: 251253.
- 2.2.3 \*ANSI/ANS-58.23-2007. 2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.
- 2.2.4 \*Apostolakis, G. and Kaplan, S. 1981. "Pitfalls in Risk Calculations." *Reliability Engineering*, 2, 135-145. Barking, England: Applied Science Publishers. TIC: 253648.

- 2.2.5 ASCE/SEI 7-05. 2006. *Minimum Design Loads for Buildings and Other Structures*. Including Supplement No. 1. Reston, Virginia: American Society of Civil Engineers. TIC: 258057. ISBN: 0-7844-0809-2.
- 2.2.6 ASME (American Society of Mechanical Engineers) 2002. RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.
- 2.2.7 ASME 2004. *2004 ASME Boiler and Pressure Vessel Code*. 2004 Edition. New York, New York: American Society of Mechanical Engineers. TIC: 256479.
- 2.2.8 \*Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.
- 2.2.9 \*Battelle 2001. *Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report*. Washington, D.C.: U.S. Department of Transportation, Federal Motor Carrier Safety Administration. ACC: MOL.20080228.0002.
- 2.2.10 \*Benhardt, H.C.; Eide, S.A.; Held, J.E.; Olsen, L.M.; and Vail, R.E. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)*. WSRC-TR-93-581. Aiken, South Carolina: Westinghouse Savannah River Company, Savannah River Site. ACC: MOL.20061201.0160.
- 2.2.11 Bjorkman, G.; Chuang, T-J.; Einziger, R.; Malik, S.; Malliakos, A.; Mitchell, J.; Navarro, C.; Ryder, C.; Shaukat, S.; Ulses, A.; and Zigh, G. 2007. *A Pilot Probabilistic Risk Assessment of a Dry Cask Storage System at a Nuclear Power Plant*. NUREG-1864. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20070913.0518.
- 2.2.12 BSC 2005. *Thermal Performance of Spent Nuclear Fuel During Dry Air Transfer-Initial Calculations*. 000-00C-DSU0-03900-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20050110.0003.
- 2.2.13 \*BSC 2006. *Low-Level Waste Management Plan*. 000-30R-MW00-00100-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061218.0016.
- 2.2.14 BSC 2007. *Aging Facility Cask Tractor Mechanical Equipment Envelope*. 170-MJ0-HAT0-00601-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070910.0016.
- 2.2.15 BSC 2007. *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope*. 170-MJ0-HAT0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070518.0002.

- 2.2.16 BSC 2007. *Basis of Design for the TAD Canister-Based Repository Design Concept*. 000-3DR-MGR0-00300-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0042.
- 2.2.17 BSC 2007. *Cask Transfer Trolley and Site Transporter Sliding/Rocking Calculation*. 000-MJC-H000-00200-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071201.0010.
- 2.2.18 \*BSC 2007. *Diesel Fuel Oil Storage Diesel Fuel Oil System Piping and Instrumentation Diagram*. 70A-M60-PS00-00103-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070904.0003.
- 2.2.19 BSC 2007. *GROA External Dose Rate Calculation*. 000-PSA-MGR0-01300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071023.0003.
- 2.2.20 BSC 2007. *Mechanical Handling Design Report-Site Transporter*. 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.
- 2.2.21 BSC 2007. *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert*. 000-00C-DNF0-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071017.0001.
- 2.2.22 BSC 2007. *Shielding Requirements and Dose Rate Calculations for WHF and LLW*. 050-00C-WH00-00300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0017.
- 2.2.23 BSC 2007. *Waste Form Throughputs for Preclosure Safety Analysis*. 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.
- 2.2.24 \*BSC 2007. *Yucca Mountain Project Drainage Report and Analysis*. 000-CDC-MGR0-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070924.0043.
- 2.2.25 BSC 2007. *Yucca Mountain Project Engineering Specification Cask Tractor and Cask Transfer Trailers*. 000-3PS-HAT0-00300-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0004.
- 2.2.26 BSC 2008. *External Events Hazards Screening Analysis*. 000-00C-MGR0-00500-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080219.0001.
- 2.2.27 \*BSC 2008. *Geologic Repository Operations Area Aging Pad Site Plan*. 170-C00-AP00-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080129.0005.

- 2.2.28 \*BSC 2008. *Geologic Repository Operations Area North Portal Site Plan*. 100-C00-MGR0-00501-000 REV 00F. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080125.0007.
- 2.2.29 BSC 2008. *Intra-Site Operations and BOP Event Sequence Development Analysis*. 000-PSA-MGR0-00800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0004.
- 2.2.30 BSC 2008. *Preclosure Consequence Analyses*. 000-00C-MGR0-00900-000-00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080129.0006.
- 2.2.31 BSC 2008. *Preclosure Criticality Safety Analysis*. TDR-MGR-NU-000002 REV 01. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0007.
- 2.2.32 BSC 2008. *Seismic and Structural Container Analyses for the PCSA*. 000-PSA-MGR0-02100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080220.0003.
- 2.2.33 \*Cote, A.E. and Linville, J.L., eds. 1986. *Fire Protection Handbook*. 16th Edition. Quincy, Massachusetts: National Fire Protection Association. TIC: 256296. ISBN: 978-0-87765-315-8.
- 2.2.34 \*CRA (Corporate Risk Associates Limited) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique*. CRA-BEGL-POW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.
- 2.2.35 \*Denson, W.; Chandler, G.; Crowell, W.; Clark, A; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995*. NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.
- 2.2.36 DOE 2007. *Software Independent Verification and Validation Change in Operating System Version Report for: SAPHIRE v7.26*. Document ID: 10325-COER-7.26-01. Las Vegas, Nevada: U.S. Department of Energy, Office of Repository Development. ACC: MOL.20070607.0263. (DIRS 184933)
- 2.2.37 DOE 2007. *Transportation, Aging and Disposal Canister System Performance Specification*. WMO-TADCS-000001, Rev. 0. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070614.0007.
- 2.2.38 \*DOT (U.S. Department of Transportation) [n.d.]. "Summary Tables." *Large Truck Crash Causation Study*. [Washington, D.C.]: U.S. Department of Transportation. ACC: MOL.20080227.0020. internet accessible URL: <http://www.ai.fmcsa.dot.gov/LTCCS/>
- 2.2.39 \*DOT 2000. "Speeding Counts...on All Roads!" Washington, D.C.: U.S. Department of Transportation, Federal Highway Administration. ACC: MOL.20080228.0001.

- 2.2.40 \*DOT 2004. Traffic Safety Facts 2002: *A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System*. DOT HS 809 620. Washington, D.C.: U.S. Department of Transportation, National Highway Traffic Safety Administration. ACC: MOL.20080228.0003.
- 2.2.41 \*Ellingwood, B.; Galambos, T.V.; MacGregor, J.G.; and Cornell, C.A. 1980. *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures*. SP 577. Washington, D.C.: National Bureau of Standards, Department of Commerce. ACC: MOL.20061115.0081.
- 2.2.42 EPRI (Electric Power Research Institute) and NRC (U.S. Nuclear Regulatory Commission) 2005. *Summary & Overview. Volume 1 of EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0061.
- 2.2.43 EPRI and NRC 2005. *Detailed Methodology*. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI TR-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0062.
- 2.2.44 \*Federal Emergency Management Agency (FEMA) [n.d.]. *Handbook of Chemical Hazard Analysis Procedures*. Washington, D.C.: FEMA. ACC: MOL.20080311.0022.
- 2.2.45 \*Fischer, L.E.; Chou, C.K.; Gerhard, M.A.; Kimura, C.Y.; Martin, R.W.; Mensing, R.W.; Mount, M.E.; and Witte, M.C. 1987. *Shipping Container Response to Severe Highway and Railway Accident Conditions*. NUREG/CR-4829. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: NNA.19900827.0230; NNA.19900827.0231.
- 2.2.46 \*Fleming, K.N. 1975. *A Reliability Model for Common Mode Failures in Redundant Safety Systems*. GA-A13284. San Diego, California: General Atomic Company. ACC: MOL.20071219.0221.
- 2.2.47 \*Fragola, J.R. and McFadden, R.H. 1995. "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom." *Reliability Engineering and System Safety*, 47, 255-273. New York, New York: Elsevier. TIC: 259675. ISSN: 0951-8320.
- 2.2.48 \*Gertman, D.I.; Gilbert, B.G.; Gilmore, W.E.; and Galyean, W.J. 1989. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations*. NUREG/CR-4639, Vol. 5, Part 4, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252112.
- 2.2.49 \*Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-042848-7.

- 2.2.50 Iqbal, N. and Salley, M.H. 2004. Fire Dynamics Tools (FDT): *Quantitative Fire Hazard Analysis Methods for the U.S. Nuclear Regulatory Commission Fire Protection Inspection Program*. NUREG-1805. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050725.0071.
- 2.2.51 \*Kumamoto, H.; Henley, E.J. 1996. *Probabilistic Risk Assessment and Management for Engineers and Scientists*. 2nd Edition. New York, New York: IEEE Press. ISBN: 0-7803-1004-7.
- 2.2.52 \*Lion Oil Company. 2002. *Material Safety Data Sheet for Low Sulfur Diesel Fuel*. MSDS No. LO0270. El Dorado, Arizona: Lion Oil Company. ACC: MOL.20070904.0031.
- 2.2.53 \*Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.
- 2.2.54 \*Lopez Droguett, E.; Groen, F.; and Mosleh, A. 2004. "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety*, Vol. 83, 311–321. New York, New York: Elsevier. TIC: 259380.
- 2.2.55 \*Marshall, F.M.; Rasmuson, D.M.; and Mosleh, A. 1998. *Common-Cause Failure Parameter Estimations*. NUREG/CR-5497. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0105.
- 2.2.56 \*Martz, H.F. and Waller, R.A. 1991. *Bayesian Reliability Analysis*. Malabar, Florida: Krieger Publishing Company. TIC: 252996. ISBN: 0-89464-395-9.
- 2.2.57 \*Mosleh, A. 1993. *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*. NUREG/CR-5801. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 245473.
- 2.2.58 \*Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques. Volume 2 of Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.
- 2.2.59 \*Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1988. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106. ISBN: 0-408-10604-2.
- 2.2.60 \*Nolan, D.P. 1996. *Handbook of Fire and Explosion Protection Engineering Principles for Oil, Gas, Chemical and Related Facilities*. Westwood, New Jersey: Noyes Publications. TIC: 256119. ISBN: 978-0-81551-394-0.



- 2.2.61 \*Nowlen, S.P. 1986. *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report*. NUREG/CR-4680. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0099.
- 2.2.62 \*Nowlen, S.P. 1987. *Quantitative Data on the Fire Behavior of Combustible Materials Found in Nuclear Power Plants: A Literature Review*. NUREG/CR-4679. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0100.
- 2.2.63 NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.
- 2.2.64 \*NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants. Final Report*. NUREG/CR-2300. Two volumes: Refer to HQS.19880517.3290 (Volume 1) and HQS.19880517.2505 (Volume 2). Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.
- 2.2.65 NRC 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.
- 2.2.66 NRC 1997. *Standard Review Plan for Dry Cask Storage Systems*. NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.
- 2.2.67 NRC 2000. *Standard Review Plan for Transportation Packages for Spent Nuclear Fuel*. NUREG-1617. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249470.
- 2.2.68 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624, REV 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.
- 2.2.69 NRC 2003. *Yucca Mountain Review Plan, Final Report*. NUREG-1804, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards. TIC: 254568.
- 2.2.70 NRC 2007. *Interim Staff Guidance HLWRS-ISG-02. Preclosure Safety Analysis – Level of Information and Reliability Estimation*. HLWRS-ISG-02. Washington, DC: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.
- 2.2.71 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, DC. U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0230.

- 2.2.72 \*Owen, A.B. 1992. "A Central Limit Theorem for Latin Hypercube Sampling." *Journal of the Royal Statistical Society: Series B, Statistical Methodology*, 54, (2), 541-551. London, England: Royal Statistical Society. TIC: 253131.
- 2.2.73 Regulatory Guide 1.174, Rev. 1. 2002. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington, D.C.: U. S. Nuclear Regulatory Commission. ACC: MOL.20080215.0049. Internet Accessible.
- 2.2.74 Regulatory Guide 1.91, Rev. 1. 1978. *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 2774.
- 2.2.75 SAIC (Science Applications International Corporation) 2002. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*. SAIC-01/2650. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20080115.0138.
- 2.2.76 SAPHIRE V. 7.26. 2007. VMware/WINDOWS XP. STN: 10325-7.26-01. (DIRS 183846)
- 2.2.77 \*SFPE (Society of Fire Protection Engineers) 2002. *SFPE Handbook of Fire Protection Engineering*. 3rd Edition. Quincy, Massachusetts: National Fire Protection Association. TIC: 255463. ISBN: 0-87765-451-4.
- 2.2.78 \*Siu, N.O. and Kelly, D.L. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment." *Reliability Engineering and System Safety*, 62, 89-116. New York, New York: Elsevier. TIC: 258633. ISSN: 09518320.
- 2.2.79 \*Smith, C. 2007. *Master Logic Diagram*. Bethesda, Maryland: Futron Corporation. ACC: MOL.20071105.0153; MOL.20071105.0154.
- 2.2.80 \*Snow, S.D. 2007. *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations*, EDF-NSNF-085, Rev. 0. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0062.
- 2.2.81 \*Snow, S.D. and Morton, D.K. 2007. *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository*. EDF-NSNF-087, Rev. 0. Idaho Falls, Idaho: Idaho National Laboratory. ACC: MOL.20080206.0063.
- 2.2.82 \*Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; and Yoshimura, H.R. 2000. *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672; SAND2000-0234. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20001010.0217.

- 2.2.83 \*Swain, A.D. and Guttman, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*. NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.
- 2.2.84 \*Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. PhD Dissertation. Espoo, Finland: VTT Technical Research Centre of Finland. TIC: 259928. ISBN: 951-38-6392-1.
- 2.2.85 \*Tooker, D.W. 2008. "Reference Information for Processing of Spent Pool Water Treatment System, Spent Clean-Up Filters, and Spent Resin Generated in the Wet Handling Facility." Interoffice memorandum from D.W. Tooker (BSC) to Distribution, January 11, 2008, 0110082493. ACC: CCU.20080111.0011.
- 2.2.86 \*U.S. Census Bureau 3/21/2000. "1997 Economic Census: Summary Statistics for the United States 1997 NAICS Basis." Washington, DC: U.S. Census Bureau. Accessed 12/11/2007. URL: <http://www.census.gov/epcd/ec97/ustotals.htm>. ACC: MOL.20080310.0082.
- 2.2.87 Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook*. NUREG-0492. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 208328.
- 2.2.88 Weast, R.C., ed. 1978. *CRC Handbook of Chemistry and Physics*. 59th Edition. West Palm Beach, Florida: CRC Press. TIC: 246814. ISBN: 0-8493-0549-8.
- 2.2.89 \*Weisstein, Eric W. [n.d.] "Normal Sum Distribution." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/NormalSumDistribution.html>. ACC: MOL.20080307.0161.
- 2.2.90 \*Williams, J.C. 1986. "HEART - A Proposed Method for Assessing and Reducing Human Error." *9th Advances in Reliability Technology Symposium - 1986*. Bradford, England: University of Bradford. TIC: 259862.

## 2.3 DESIGN CONSTRAINTS

- 2.3.1 10 CFR 50. 2007. Energy: Domestic Licensing of Production and Utilization Facilities. U.S. Nuclear Regulatory Commission.
- 2.3.2 10 CFR 63. 2007. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. U.S. Nuclear Regulatory Commission.
- 2.3.3 10 CFR 71. 2007. Energy: Packaging and Transportation of Radioactive Material. U.S. Nuclear Regulatory Commission. ACC: MOL.20070829.0114.

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

## **2.4 DESIGN OUTPUTS**

- 2.4.1 BSC 2008. *ITS SSC/Non-ITS SSC Interactions Analysis*. 000-PSA-MGR0-02300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company
- 2.4.2 BSC 2008. *Preclosure Nuclear Safety Design Bases*. 000-30R-MGR0-03500-000-000. Las Vegas, Nevada: Bechtel SAIC Company
- 2.4.3 BSC 2008. *Preclosure Procedural Safety Controls*. 000-30R-MGR0-03600-000-000 REV 00. Las Vegas, Nevada: Bechtel SAIC Company
- 2.4.4 BSC 2008. *Seismic Event Sequence Quantification and Categorization*. 000-PSA-MGR0-01100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company.

## **2.5 ATTACHMENT REFERENCES**

Attachment A: references are cited in Section 2.2 of main body

Attachment B: references are cited in Section B1.1, B2.1, and B3.1

Attachment C: references are cited in Section C5

Attachment D: references are cited in Section D4

Attachment E: references are cited in Section E8

Attachment F: references are cited in Section F2

Attachment G: references are cited in Sections 2.2 and 2.4 of main body

Attachment H: none

### 3. ASSUMPTIONS

#### 3.1 ASSUMPTIONS REQUIRING VERIFICATION

None used.

#### 3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION

##### 3.2.1 General Analysis Assumptions

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

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

## 4. METHODOLOGY

### 4.1 QUALITY ASSURANCE

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

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

**Documentation of suitability for intended use of “QA: N/A” drawings:** Engineering drawings are prepared using the “QA: QA” procedure *Engineering Drawings* (Ref. 2.1.2). They are checked by an independent checker and reviewed for constructability and coordination before review and approval by the engineering group supervisor and the discipline engineering manager (Ref. 2.1.2, Section 3.2.2, and Attachments 3 and 5). The check, review, and approval process provides assurance that these drawings accurately document the design and operational philosophy of the facility. For this reason, they are suitable for their intended use as sources of input to this analysis.

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

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

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

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

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

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

1. Some inputs are cited as sources of the methods used in the analysis. These inputs are suitable for their intended uses because they represent commonly accepted methods of analysis among safety analysis practitioners or, more generally, among scientific and engineering professionals.
2. Some inputs are cited as examples of applications of methods of analysis by others. These inputs are suitable for their intended uses because they illustrate applicable methods of analysis.
3. Some inputs are cited as sources of historical safety-related data. These inputs are suitable for their intended uses because they represent historical data that is commonly accepted among safety analysis practitioners.
4. Some inputs are cited as sources of accepted practices as recommended by codes, standards, or review plans. These inputs are suitable for their intended uses because they represent codes, standards, or review plans that are commonly accepted by practitioners of the affected professional disciplines.
5. Some inputs provide information specific to the Yucca Mountain Repository that was produced by organizations other than BSC. These inputs are suitable for their intended uses because they provide information that was developed for the Yucca Mountain Repository under procedures that apply to the organization that produced the information.

## **4.2 USE OF SOFTWARE**

### **4.2.1 Level 1 Software**

This section addresses software used in this analysis as Level 1 software, as defined in *Software Management* (Ref. 2.1.3, Attachment 12). SAPHIRE V. 7.26 STN 10325-7.26-01 (Ref. 2.2.76) is used in this analysis for PRA simulation and analyses. The SAPHIRE software is used on a personal computer running Windows XP inside a VMware virtual machine; it is also listed in the

current *Qualified and Controlled Software Report*, and was obtained from Software Configuration Management. The SAPHIRE software is specifically designed for PRA simulation and analyses and has been verified to show that this software produces precise solutions for encoded mathematical models within the defined limits for each parameter employed (Ref. 2.2.36). Therefore, SAPHIRE version 7.26 is suitable for use in this analysis.

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

#### 4.2.2 Level 2 Software

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

- Word 2003, a component of Microsoft Office Professional 2003, and Visio Professional 2003 are listed in the current Level 2 Usage Controlled Software Report. Word 2003 and Visio 2003 are used in this analysis for the generation of graphics and text. The accuracy of the resulting graphics and text is verified by visual inspection. The precise means of verification is left to the discretion of the checker in compliance with applicable procedures.
- Excel 2003, a component of Microsoft Office Professional 2003, and Mathcad version 13.0 and 14.0 are listed in the current Level 2 Usage Controlled Software Report. Crystal Ball version 7.3.1, a commercial, off-the-shelf, Excel-based risk analysis tool, is listed on the Controlled Software Report and is registered for Level 2 usage. Excel 2003 is used for this analysis to produce noncomplex reliability models (described in Section 6), to calculate probability distributions for selected SAPHIRE inputs, and to graphically display information. Mathcad 13.0 and 14.0 and Crystal Ball 7.3.1 are also used for calculating probability distributions for SAPHIRE and for graphics. Graphical representations are verified by visual inspection. The calculations are documented in sufficient detail to allow an independent replication of the computations. The user-defined formulas and inputs are verified by visual inspection. The results are in some cases verified by independent replication of the computations; however, in some cases (e.g., for some Excel calculations and Mathcad 13.0 and 14.0 calculations), the results are verified by visual inspection. The precise means of verification is left to the discretion of the checker in compliance with applicable procedures.
- WinZip 9.0, a file compression utility for Windows, is listed in the current Level 2 Usage Controlled Software Report. WinZip 9.0 is used in this analysis to compress files for presentation on compact disc in Attachment H.

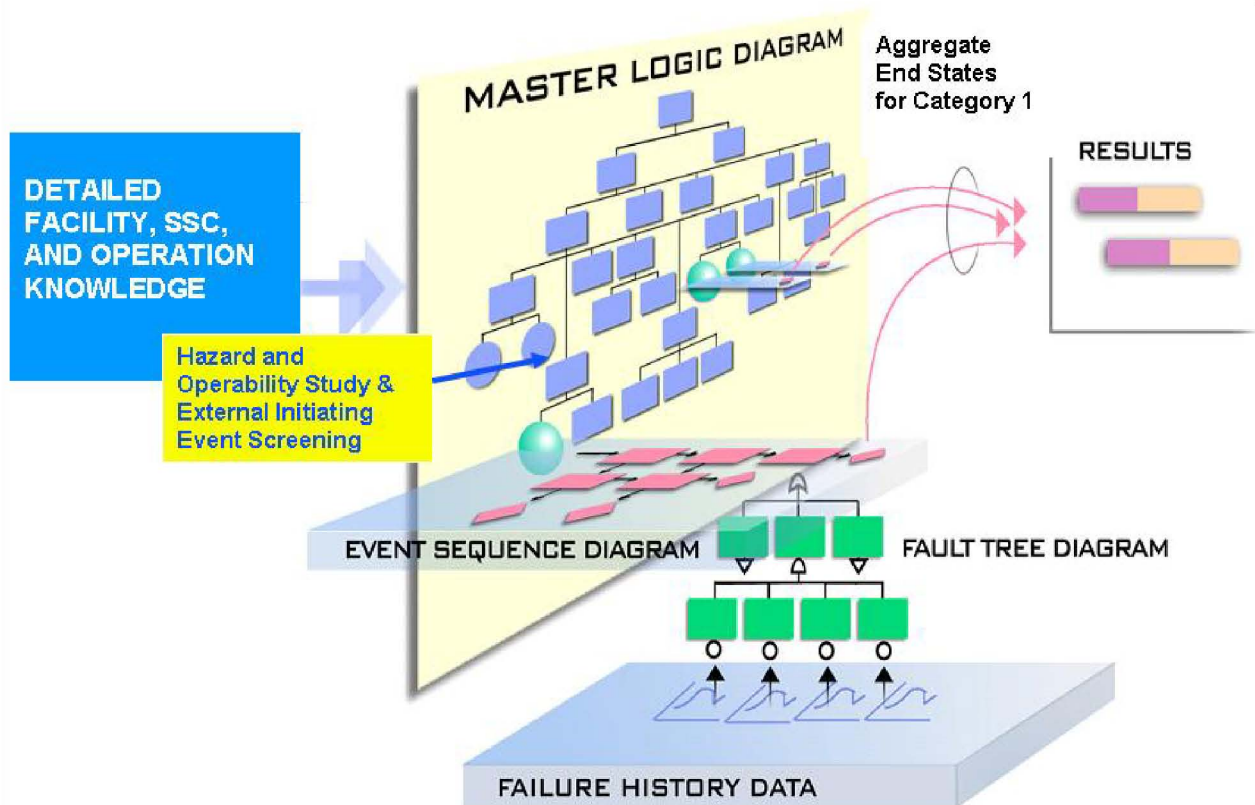


### 4.3 DESCRIPTION OF ANALYSIS METHODS

This section presents the PCSA approach and analysis methods in the context of overall repository operations. As such, it includes a discussion of operations that may not apply to Intra-Site Operations and balance of plant (BOP) facilities. Specific features and operations of Intra-Site Operations are not discussed until Section 6, where the methods described here are applied. The PCSA uses the technology of PRA as described in references such as *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6). The PRA answers three questions:

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

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



Source: Modified from (Ref. 2.2.79).

Figure 4.3-1. Event Sequence Analysis Process

The PCSA starts with analysts obtaining sufficient knowledge of the designs and operations of facility, equipment, and SSCs to understand how the YMP waste handling is conducted. This is largely performed and documented in the precedent event sequence development analysis (Ref. 2.2.29). An understanding of how a facility operates is a prerequisite for developing event sequences that depict how it would fail. *Success criteria* are important additional inputs to the PCSA. A success criterion states the minimum functionality that constitutes acceptable, safe performance. For example, a success criterion for a crane is to pick-up, transport, and put-down a cask without dropping it. The complementary statement of a success criterion is a failure mode (e.g., crane drops cask).

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

1. “OK”—Indicates the absence of the other end states.
2. Direct Exposure, Degraded Shielding—Applies to event sequences where an SSC providing shielding is not breached, but the shielding function is jeopardized. An example is a lead-shielded transportation cask that is dropped from a height great enough for the lead to slump toward the bottom of the cask at impact, leaving a partially shielded path for radiation to stream. This excludes radionuclide release from containment and an indication of a reactivity increase.
3. Direct Exposure, Loss of Shielding (LOS)—Applies to event sequences where an SSC providing shielding fails, leaving a direct path for radiation to stream. For example, this end state applies to a breached transportation cask, with the dual-purpose canister (DPC) or transportation, aging, and disposal (TAD) canister inside maintaining its containment function. In another example, this end state applies to shield doors inadvertently opened. This excludes radionuclide release from containment and an indication of a reactivity increase.
4. Radionuclide Release, Filtered—Indicates a release of radioactive material from its containment, through a filtered path, to the environment. The release is filtered when it is confined and filtered through the successful operation of the heating, ventilation, and air-conditioning (HVAC) system over its mission time. This excludes nuclear reactivity increases.

5. Radionuclide Release, Unfiltered—Indicates a release of radioactive material from its confinement, through an unfiltered path, to the environment. This excludes nuclear reactivity increases.
6. Radionuclide Release, Filtered, Also Important to Criticality—For dry operations with canistered SNF, this end state refers to a situation in which a breach of a canister has occurred (resulting in a radionuclide release), and a moderator, such as unborated water, has entered the canister. For dry operations with uncanistered commercial spent nuclear fuel (UCSNF), this end state refers to a situation in which a breach of a transportation cask has occurred (resulting in a radionuclide release), and a moderator, such as unborated water, has entered the cask. The release of the radioactive material to the environment is through a filtered path.
7. Radionuclide Release, Unfiltered, Also Important to Criticality—This end state refers to a situation in which an unfiltered radionuclide release occurs and (unless the associated event sequence is beyond Category 2) a criticality investigation is indicated.
8. Important to Criticality—This end state refers to a situation in which there has been no radionuclide release and (unless the associated event sequence is beyond Category 2) a criticality investigation is indicated.

The end states Radionuclide Release (filtered or unfiltered), also Important to Criticality and Important to Criticality segregate event sequences for which some of the conditions leading to a criticality event have been met. This does not imply, however, that a criticality event is inevitable.

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

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

Criticality analyses are performed to ensure that any Category 1 and Category 2 event sequences that terminate in end states that are ITC would not result in a criticality. In order to determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity of variations in each of the parameters ITC during the preclosure period. The parameters are: waste form characteristics, reflection, interaction, neutron absorbers (fixed and

soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor to variations in any of these parameters as a function of the other parameters. The deterministic sensitivity analysis covers all reasonably achievable repository configurations that are ITC. Section 4.3.9 provides a detailed discussion of the treatment of criticality in event sequences.

The third question, “How likely is it?” is answered by the estimation of event sequence frequencies. The PCSA uses *failure history* records (for example, *Nonelectronic Parts Reliability Data 1995* (Ref. 2.2.35) and *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)* NUREG/CR-4639 (Ref. 2.2.48)), structural reliability analysis, thermal stress analysis, and engineering and scientific knowledge about the design as the basis for estimation of probabilities and frequencies. These sources coupled with the techniques of probability and statistics, for example, *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, NUREG/CR-6823 (Ref. 2.2.8), are used to estimate frequencies of initiating events and event sequences and the conditional probabilities of pivotal events.

The PCSA uses *event sequence diagrams* (ESDs), *event trees*, and *fault trees* to develop and quantify event sequences. The ESDs and event trees are described and developed in the event sequence development analyses (Ref. 2.2.29). The present analysis uses fault trees to disaggregate an SSC or equipment item to a level of detail that is supported by available reliability information from failure history records. Various techniques of probability and statistics are employed to estimate failure frequencies of mechanical, electrical, electro-mechanical, and electronic equipment. Such frequencies, or *active component* unreliabilities, provide inputs to the fault tree models of equipment items. Fault trees are used to model initiating events and, in some instances, to model pivotal events.

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

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

The frequency of occurrence of an event sequence is the product of the frequency of its initiating event and the conditional probabilities of its pivotal events. This is true whether or not the frequency and probabilities are expressed as single points or probability distributions. The frequencies of event sequences within the same ESD that result in the same end state are

summed to group together event sequences for the purpose of categorization. The concept of *aggregating event sequences* to obtain aggregated end state results is depicted in Figure 4.3-1.

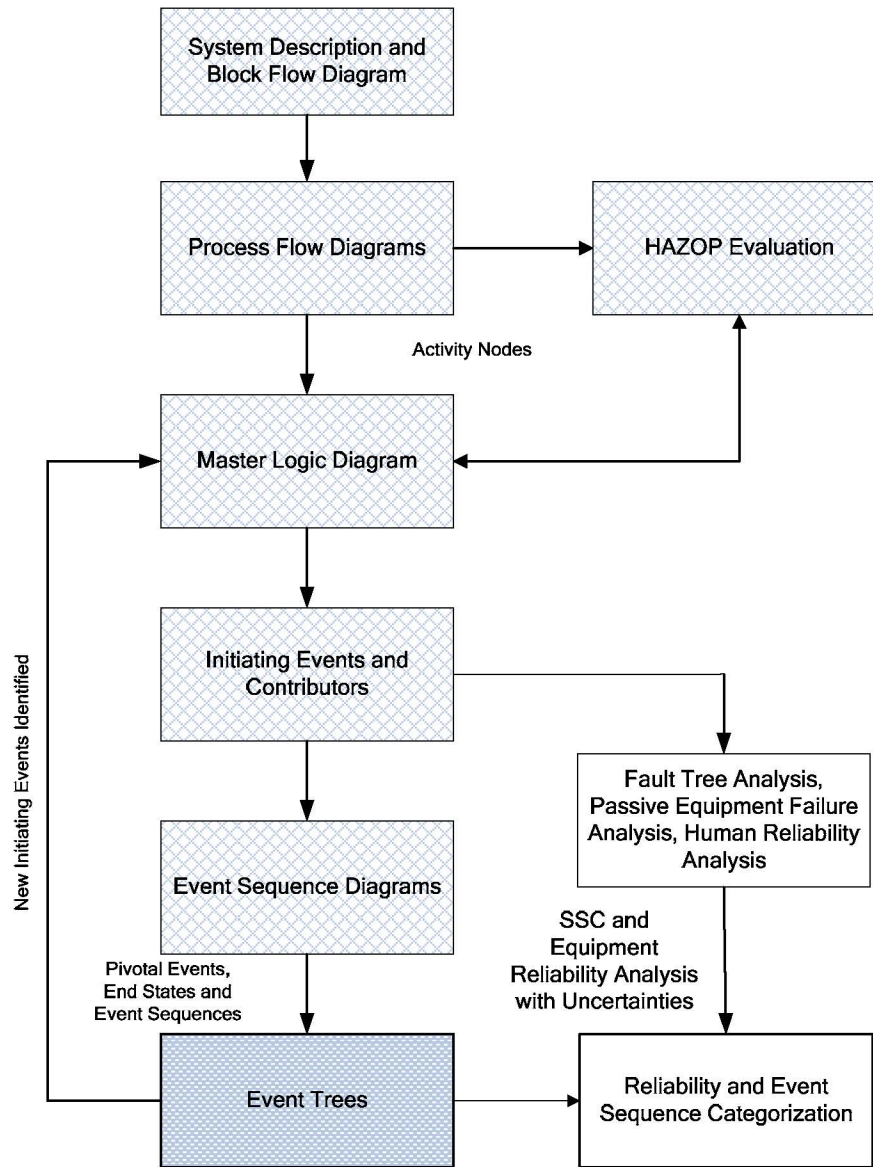
The PCSA is described above as a system simulation. This is important in that any simulation or model is an approximate representation of reality. Approximations may lead to uncertainties regarding the frequencies of event sequences. The event sequence quantification presented in this document propagates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

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

1. Quantify the frequency of each initiating event that is identified in the event sequence development analysis (Ref. 2.2.29).
2. Quantify the conditional probability of the pivotal events in each event sequence.
3. Calculate the frequency of each event sequence (i.e., calculate the product of the initiating event frequency and pivotal event conditional probabilities).
4. Calculate the frequencies of the aggregated event sequences.
5. Categorize the aggregated event sequences for further analysis.

The activities required to accomplish these objectives are illustrated in Figure 4.3-2. The cross-hatched boxes review the process steps performed for the event sequence development analysis (Ref. 2.2.29). The interface between the event sequence development analysis and this categorization analysis is the set of event trees, as represented by the darkly shaded box. The event trees from the event sequence development analysis are passed as input into this analysis. The unshaded boxes represent the analysis performed in this study, the methods of which are described later in Section 4.

The event sequences that are categorized in this analysis can be more fully understood by consulting the event sequence development analysis (Ref. 2.2.29). The remainder of this subsection presents a brief overview of the event sequence development process.

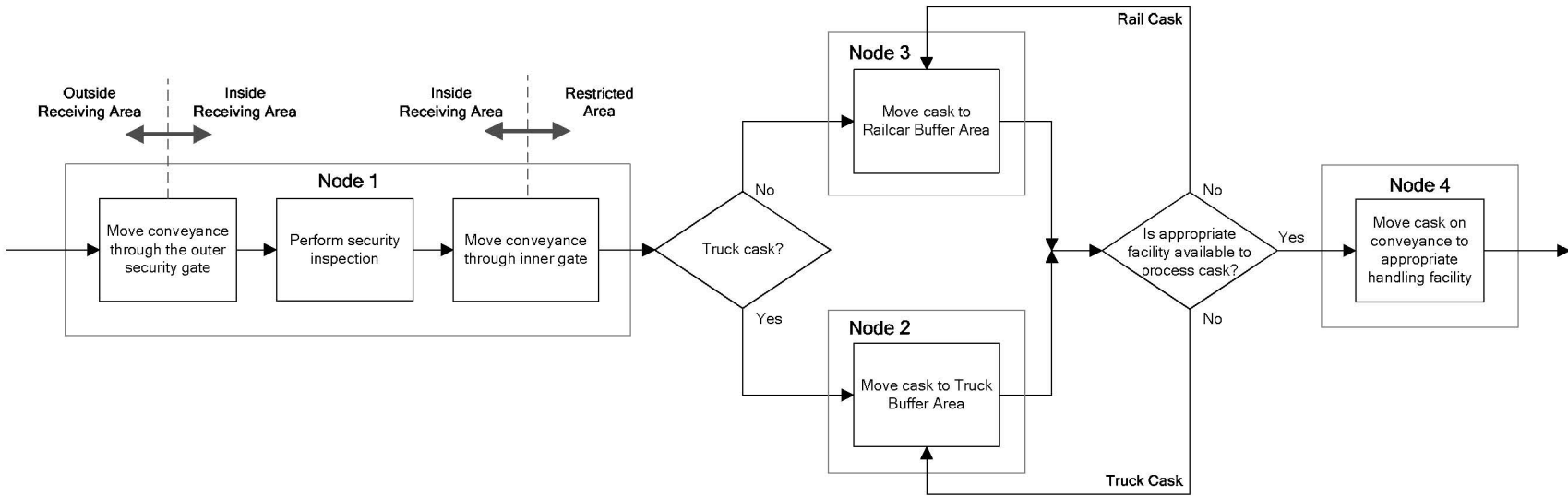


NOTE: HAZOP = hazard and operability; SSC = structure, system, or component.

Source: Modified from *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29, Figure 2).

Figure 4.3-2. Preclosure Safety Assessment Process

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



39

NOTE: This diagram illustrates a small portion of the overall handling operations for typical site transportation operations.  
TC = transportation cask.

Source: Original

Figure 4.3-3. Portion of a Simplified Example Process Flow Diagram for Typical Intra-Site Operations

March 2008

Development of the MLD is accomplished by deriving specific failures from a generalized statement of the undesired state. As a “top-down” analysis, the MLD starts with a top event, which represents a generalized undesired state. The top event includes direct exposure to radiation or exposure as result of a release of radioactive material. The basic question answered by the MLD is “How can the top event occur?” Each successively lower level in the MLD hierarchy divides the identified ways in which the top event can occur with the aim of eventually identifying specific initiating events that may cause the top event. In the MLD, the initiating events are shown at the next-to-lowest level. The lowest level provides an example of contributors to the initiating event. This process for the PCSA is presented in detail in the event sequence development analysis (Ref. 2.2.29, Section 4.3.1.2).

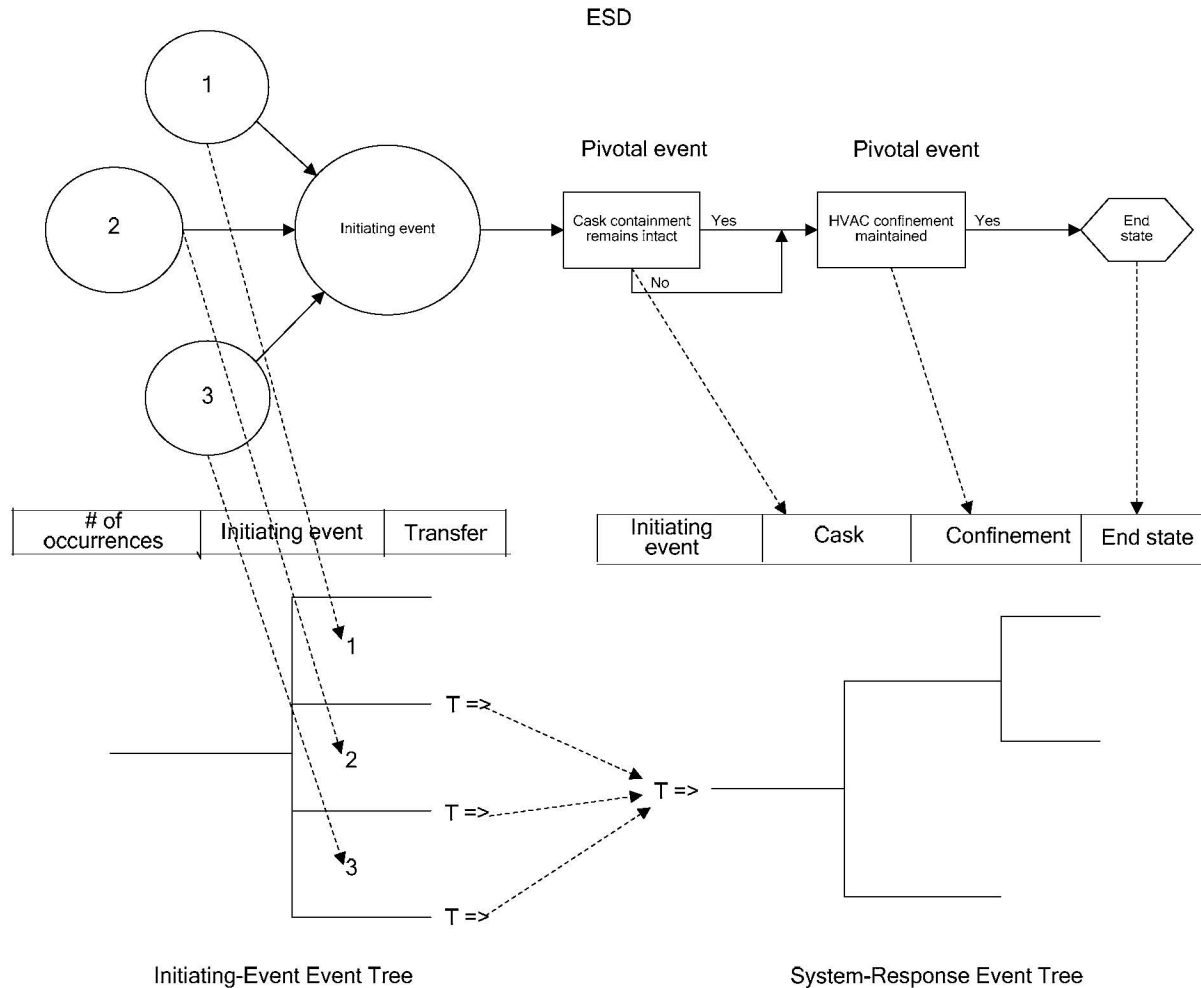
The HAZOP evaluation focuses on identifying potential initiators that are depicted in the lower levels of the MLD. It is a “bottom-up” approach that supplements the “top-down” approach of the MLD. Based on the PFD, the HAZOP evaluation includes a systematic study of repository operations during the preclosure phase. As an early step in the performance of the HAZOP evaluation, the intended function, or intention, of each node in the PFD is defined. The intention is a statement of what the node is supposed to accomplish as part of the overall operation. The HAZOP analysts work their way through the PFD, node by node, and postulate deviations from normal operations. A deviation is any out-of-tolerance variation from the normal values of parameters specified for the intention.

Although the repository is to be the first of its kind in some ways, the planned operations are based on established technologies, such as transportation cask movement by truck and rail; crane transfers of casks and canisters; rail-based trolleys; air-based conveyances; robotic welding; and SNF pool operations. The team assembled for the HAZOP evaluation (and available on call as questions arose) had experience with such technologies and was well equipped to perform the evaluation.

The MLD and HAZOP evaluation are strongly interrelated. The MLD is cross-checked to the HAZOP evaluation. That is, the MLD is modified to include any initiators and contributors identified in the HAZOP evaluation that are not already included in the MLD. The entire process (Figure 4.3-2) is iterative in nature with insights from succeeding steps often feeding back to predecessors. The top-down MLD and the bottom-up HAZOP evaluation provide a diversity of viewpoints that add confidence that no important initiating events have been omitted. Details on implementation of the HAZOP evaluation are presented in the event sequence development analysis (Ref. 2.2.29, Section 4.3.1.3).

An overview of the pertinent human and SSC responses to an initiating event is depicted in an ESD. As shown in Figure 4.3-4, an ESD represents event sequences in terms of initiating events, pivotal events, and end states. Because the future is uncertain, the analyst does not know which of the alternative scenarios might occur. The ESD depicts the alternative scenarios as paths that can be traced through the diagram. Each alternative path from initiating event to an end state represents an event sequence. The events that may occur after the initiating event are identified by asking and answering the question “What can happen next?” Typically, questions about the integrity of radionuclide containment (e.g., cask, canister, or waste package) and confinement (e.g., HVAC) become pivotal events in the ESD.





Source: Original

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

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

For example, all initiating events that challenge the containment function of a cask would include pivotal events that question the containment integrity of the cask and the shielding integrity. The knowledge to develop such ESDs and appropriately group the initiating events comes from a detailed knowledge of the SSCs and operations derived from developing the PFD,

MLD, and HAZOP evaluation. The pivotal event conditional probabilities are the same for all initiating events grouped in a little bubble. All initiating events represented by the big bubble have the same human and SSC responses and, therefore, may be represented by the same event sequences. However, the conditional probability for each pivotal event is not necessarily the same for each little bubble.

#### 4.3.1 Event Tree Analysis and Categorization

Also illustrated in Figure 4.3-4 is the relationship of the YMP ESDs to their equivalent event trees. Event trees contain the same information as ESDs but in a form suitable to be used by software such as SAPHIRE (Ref. 2.2.36), which ultimately stores event trees, fault trees, and reliability data, and can be used to quantify complex event sequences. (SAPHIRE was used on for fault tree quantification of initiating events for Intra-Site Operations and Subsurface Operations, because the systems and operations involved were not as complex as those in the waste handling facilities.)

Event tree depiction of ESDs provides little new information. In an event tree, each event sequence has its separate line so that the connections between initiating events and end states is more explicit than in ESDs (Ref. 2.2.64, Section 3.4.4.2). Any path from left to right that begins with the initiating event and terminates with an end state is an event sequence. Every path must ultimately terminate at an end state. As illustrated in the event tree portion of Figure 4.3-4, each intersection of a horizontal and vertical line is a node (or branch point). Each node is associated with a conditional probability of following the vertical (downward) branch. The complement is the probability of taking the vertical (upward) branch, that is, the probability of success. By convention, the description of each branch is stated as a success, and the downward branch indicates a failure. To quantify the event sequence, the initiating event frequency (or expected number of occurrences) is multiplied by the conditional probability of each subsequent pivotal event node in the event sequence until an end state is reached.

The YMP PCSA uses the concept of linked event trees (Ref. 2.2.64). Each facility has its own set of event trees. The first event tree simply represents the little bubbles, one horizontal line per little bubble. This is called the initiator event tree (IET). The second event tree contains the pivotal events and end states. This is called the system response event tree (SRET). An event sequence starts with each of the horizontal lines as if it were the initiating event on the SRET, as indicated in Figure 4.3-4. Each set of event trees is quantified for each waste container type (e.g., DPCs, TAD canisters, or DOE SNF) handled by the YMP. The event in the IET labeled “# of occurrences” represents the number of handlings (i.e., demands) for that initiating event. For example, each movement of an aging overpack between a handling facility and the Aging Facility provides an opportunity for a drop or collision. An event sequence quantification includes: the frequency (or number of occurrences) of each end state (e.g., radionuclide release), associated with a single lift, and multiplies it by the number of lifts to obtain the expected number of drops over the preclosure period. This approach is consistent with a binomial model of reliability.

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

Because each event sequence is associated with a mean number of occurrences over the preclosure period, categorization is straightforward. Those event sequences that are expected to occur one or more times before permanent closure of the GROA are Category 1 event sequences. Other event sequences that have at least one chance in 10,000 of occurring but less than one occurrence before permanent closure are Category 2 event sequences. Sequences that have less than one chance in 10,000 of occurring before permanent closure are identified as beyond Category 2. As described in Section 4.3.6, event sequence quantification considers uncertainties, and categorization is performed on the basis of an event sequence mean value of the underlying probability distribution. The preclosure period lasts 100 years but actual emplacement operations occupy 50% of this time (Ref. 2.2.16, Section 2.2.2.7).

An initiating event for an event sequence may have the potential to affect several waste form types, such as a high-level radioactive waste (HLW) canister and a DOE standardized canister, or a TAD canister and a DPC. For example, the seismically induced event sequence leading to a collapse of a surface facility could cause the breach of all the waste containers inside that facility. Similarly, a large fire affecting an entire facility affects all the waste containers inside the facility. The number of occurrences over the preclosure period of an event sequence that affects more than one type of waste container is equal to the number of occurrences of the event sequence, evaluated for one of the waste form types, multiplied by the probability that the other waste form types are present at the time the initiating event occurs. Because a probability is less than or equal to one, the resulting product is not greater than the number of occurrences of the event sequence before multiplication by the probability. The number of occurrences of an event sequence is calculated for a given waste form type, without adjustment for the probability of presence of other waste form types.

The results of the event sequence categorization (Section 6.8.3) show that the event sequences that have the potential to cause personnel exposure to radiation from more than one type of waste form are either Category 2 event sequences resulting in a direct exposure, or beyond Category 2 event sequences resulting in a radionuclide release. In the first case, doses from direct radiation after a Category 2 event sequence have no effect on the public because of the great distances from the locations of offsite receptors. In the second case, beyond Category 2 event sequences do not require a consequence calculation. Thus, the demonstration that the performance objectives of 10 CFR 63.111 (Ref. 2.3.2) are met is not dependent on the waste form at risk in the event sequences that may involve more than one type of waste form. It is appropriate, therefore, to evaluate event sequences separately for each relevant type of waste form.

Although event trees were developed in the event sequence development analysis (Ref. 2.2.29), detailed event tree analysis using SAPHIRE software was not carried out. Instead, the event sequence logic is extracted from the set of IETs and SRETs and modeled in an Excel spreadsheet. Subsequently, data for initiating event frequencies and pivotal event conditional probabilities obtained via fault tree analysis (FTA) or derived from empirical data are incorporated into the spreadsheet. FTA is performed using SAPHIRE. When the spreadsheet is fully populated, event sequence quantification begins, followed by event sequence grouping and categorization. The method for obtaining the initiating and pivotal event data is described in Section 4.3.2. How the Excel spreadsheet is used for quantification is described in Section 4.3.1.1.

#### 4.3.1.1 Quantification using Excel

This section presents a summary of how the quantification is performed for Intra-Site Operations using a combination of Excel (for event tree and event sequence quantification) and SAPHIRE fault tree quantification (to produce probability and uncertainty values for the calculation).

Internal event sequences that are based on the event trees presented in Attachment A and fault trees presented in Section 6.2 and Attachment B are quantified using Excel and SAPHIRE (refer also to discussion on software usage in Section 4.2). The quantification of an event sequence consists of calculating its number of occurrences over the preclosure period, which is generated by combining a frequency for each initiating event with the conditional probabilities of pivotal events that comprise the sequence. The quantification results are presented as an expression of the mean number of occurrences of each event sequence over the preclosure period and the uncertainty for the number of occurrences (i.e., standard deviation). The frequency of occurrence is the product of the following:

- *Number of times the waste handling operation or activity that gives rise to the event sequence is performed over the preclosure period:* An example of this value would be the total number of TAD canisters in aging overpacks to be sent to the Aging Facility combined with the number of transfers between a waste handling facility and the Aging Facility over the preclosure period.
- *Probability of occurrence of the initiating event, per waste handling operation, for the event sequence considered:* Continuing with the previous example, this could be the probability of dropping an aging overpack containing a TAD canister being conveyed by a site transporter between a surface facility and the Aging Facility. The initiating event probability is entered into Excel as parameters of the distribution (mean, median, and standard deviation), which are either produced from a fault tree in SAPHIRE or are based on a basic event value (e.g., empirical data on forklift collisions).
- *Conditional probability of each of the pivotal events of the event sequence (shown graphically in the SRET for each ESD):* The conditional probabilities used in this analysis are point values that represent a passive failure (Section 6.3.2), for example, breach of a TAD canister inside an aging overpack due to a drop.

Uncertainties in the initiating event probabilities are propagated through the event sequence logic to quantify the uncertainty in the event sequence quantification. The uncertainty associated with the initiating event probabilities provided by the fault trees are produced by SAPHIRE using the built-in Monte Carlo method. Each fault tree top event was analyzed using 10,000 trials and a seed value of 1234. The number of trials is considered sufficient to ensure accurate results for the distribution parameters.

The event sequence logic (graphically shown in Attachment A, Section A5) follows a transfer to a SRET, which provides the basis for quantifying the rest of the sequence through the use of the pivotal events. (The pivotal events are detailed in Attachment A, and the values used for them are presented in Section 6.3.) The IETs and the SRETs developed in SAPHIRE for the event sequence development analysis (Ref. 2.2.29) provide a graphical representation for model development in the Excel spreadsheet. An example of the Excel spreadsheet is provided in Figure 4.3-5.

TADs	Event Tree / Sequence No.													
		ISO-ESD02-TAD	No. of AOs	No. of moves (each)	IE mean	IE median	IE std dev	TRANSCASK	CANISTER	SHIELDING	MODERATOR	Calc'd Mean	Calc'd Median	Calc'd StdDev
ST collision	2-1	8,143	2	5.00E-03	2.00E-03	1.00E-03	N/A	1.00E+00	1.00E+00		8.E+01	3.E+01	2.E+01	OK
sm. bub1	2-2							1.00E+00	1.00E-05		8.E-04	3.E-04	2.E-04	DEL
	2-3							1.00E-08		1.00E+00	8.E-07	3.E-07	2.E-07	RRU
	2-4							1.00E-08		0.00E+00	0.E+00	0.E+00	0.E+00	RUC
ST drops AC	3-1	8,143	2	4.00E-08	2.00E-08	1.00E-07	N/A	1.00E+00	1.00E+00		6.5E-04	3.3E-04	1.6E-03	OK
sm. bub2	3-2							1.00E+00	5.00E-06		3.3E-09	1.6E-09	8.1E-09	DEL
	3-3							1.00E-05		1.00E+00	6.5E-09	3.3E-09	1.6E-08	RRU
	3-4							1.00E-05		0.00E+00	0.0E+00	0.0E+00	0.0E+00	RUC

	Total TAD Sequence ID	Mean	Median	StdDev
OK	ISO02-TAD-SEQ1-OK	8.1E+01	3.3E+01	1.6E+01
DE-SHIELD	ISO02-TAD-SEQ2-DEL	8.1E-04	3.3E-04	1.6E-04
RR-UNFIL	ISO02-TAD-SEQ3-RRU	8.2E-07	3.3E-07	1.6E-07
RR-UNFIL	ISO02-TAD-SEQ4-RUC	0.0E+00	0.0E+00	0.0E+00

Initial Categ.

Cat2

BC2

BC2

46

NOTE: AO = aging overpack; BC2 = beyond Category 2; Cat2 = Category 2; DEL = direct exposure, loss of shielding; ESD = event sequence diagram; IE = initiating event; RRU = unfiltered radionuclide release, not important to criticality; RUC = unfiltered radionuclide release, important to criticality; SEQ = sequence; ST = site transporter; StdDev = standard deviation; TAD = transportation, aging, and disposal.

Source: Original

Figure 4.3-5. Excel Spreadsheet Example Emphasizing ISO-ESD02-TAD, Sequence 3-3 for a TAD Canister Drop Resulting in an Unfiltered Radiological Release

The calculation is illustrated in Figure 4.3-5 as an event sequence (Event Tree/Sequence No. 3-3) initiated by a drop of a TAD canister in an aging overpack during a transfer to the Aging Facility via a site transporter, followed by the breach of the canister, without potential for moderator entry into the canister.

The event sequence, which leads to an unfiltered radionuclide release that is not ITC (RRU), starts with an IET that depicts the number of TAD canisters in aging overpacks that are transported to and from the Aging Facility over the preclosure period. Based on *Waste Form Throughputs for Preclosure Safety Analysis* (Ref. 2.2.23, Table 4), there are 16,286 such movements (i.e., 8,143 waste forms × 2 trips each). The branch on the IET that deals with the drop of a canister is followed. Multiplying the number of TAD canister movements by the probability of a drop yields the number of occurrences of this initiating event over the preclosure period.

The breach of the canister given a drop (Event Tree/Sequence No. 3-3), is first evaluated under the pivotal event called “CANISTER” (data labeled in spreadsheet as “CANISTER\_AO\_IMPACT”), which has a failure probability of 1E-08. The next pivotal event is “MODERATOR”, which has a probability value of “1”, indicating that moderator is not present. In the event sequence analyzed, no moderator entry occurs; that is, the success branch is followed.

The parameters to define a distribution are calculated for each event sequence by multiplying each parameter (mean, median, and standard deviation) by the scalar values for the number of occurrences, the number of movements, and the conditional probability point estimates. This method is valid because multiplying a distribution by one or more constants is a linear operation. That is, it is simply a translation of the moments of the distribution. An additional check of this method was made to ensure the results generated were consistent with the other PCSA analyses, which required complex modeling in SAPHIRE. Test cases were run in SAPHIRE, and the results were the same as those generated in the Excel spreadsheet.

For categorization, the single-line event sequences are aggregated (summed) for each end state, as described previously in Section 4.3. After multiplying the distribution parameters by the applicable scalar values as described above, the single-line event sequences still represent a probability distribution, for which the mean values can be directly summed, as described in Equation 1 (Ref. 2.2.89):

Summing mean values for a given distribution:

$$\mu_{X+Y} = \mu_X + \mu_Y \quad (\text{Eq. 1})$$

where

$X$  and  $Y$  are independent variates

$\mu_X$  is the mean value for one distribution

$\mu_Y$  is the mean value for a second distribution

The standard deviation ( $\sigma$ ) for the aggregated event sequence is calculated as the square root of the sum of the squares, based on the following property for combining variance,  $\sigma^2$ , of two distributions in Equation 2 (Ref. 2.2.89):

$$\sigma_{X+Y}^2 = \sigma_X^2 + \sigma_Y^2 \quad (\text{Eq. 2})$$

where

$X$  and  $Y$  are independent variates

$\sigma_X^2$  is the variance for one distribution

$\sigma_Y^2$  is the variance for the second distribution

Therefore, taking the square root of the variance to obtain the standard deviation, results in Equation 3:

$$\sqrt{\sigma_{X+Y}^2} = \sqrt{\sigma_X^2 + \sigma_Y^2} \quad (\text{Eq. 3})$$

That is, the standard deviation for the combined distribution is the square root of the sum of the squares of each distribution's value for standard deviation.

The median for each aggregated sequence is calculated based on the mean and variance using Equation 4 (reordered to solve for the median) (Ref. 2.2.51, Table 11.2).

$$\sigma^2 = \mu^2 \left[ \left( \frac{\mu}{m} \right)^2 - 1 \right] \quad (\text{Eq. 4})$$

$$m = \mu^2 \left[ \frac{1}{\sqrt{\mu^2 + \sigma^2}} \right]$$

where

$\sigma^2$  is the variance (standard deviation squared)

$\mu$  is the mean

$m$  is the median

The resulting values are the parameters that define the estimated probability distributions for each aggregated event sequence. The mean value for each aggregated sequence is compared to the performance objectives for categorization (Ref. 2.3.2). Figure 4.3-6 shows an example of the aggregated event sequence frequencies. The aggregated event sequence that results in direct exposure (DE-SHIELD-LOSS) has a mean value of 8.1E-04. This is greater than 1E-04 but less than 1, therefore, this is a Category 2 event sequence. The event sequence that ends in a non-ITC unfiltered radiological release (RR-UNFILTERED) is less than 1E-04 and is thus beyond



Category 2. The event sequence that ends in an unfiltered radiological release ITC (RR-UNFILTERED-ITC) is “0”, because moderator is not present in this event; therefore, the potential for criticality cannot exist.

	Total TAD Sequence ID	Mean	Median	StdDev	Initial Categ.
OK	ISO02-TAD-SEQ1-OK	8.1E+01	3.3E+01	1.6E+01	
DE-SHIELD-LOSS	ISO02-TAD-SEQ2-DEL	8.1E-04	3.3E-04	1.6E-04	Cat2
RR-UNFILTERED	ISO02-TAD-SEQ3-RRU	8.2E-07	3.3E-07	1.6E-07	BC2
RR-UNFILTERED-ITC	ISO02-TAD-SEQ4-RUC	0.0E+00	0.0E+00	0.0E+00	BC2

NOTE: DEL = direct exposure due to shield loss; RRU = unfiltered radionuclide release; RUC = unfiltered radionuclide release also important to criticality; SEQ = sequence; StdDev = standard deviation; TAD = transportation, aging, and disposal.

Source: Original

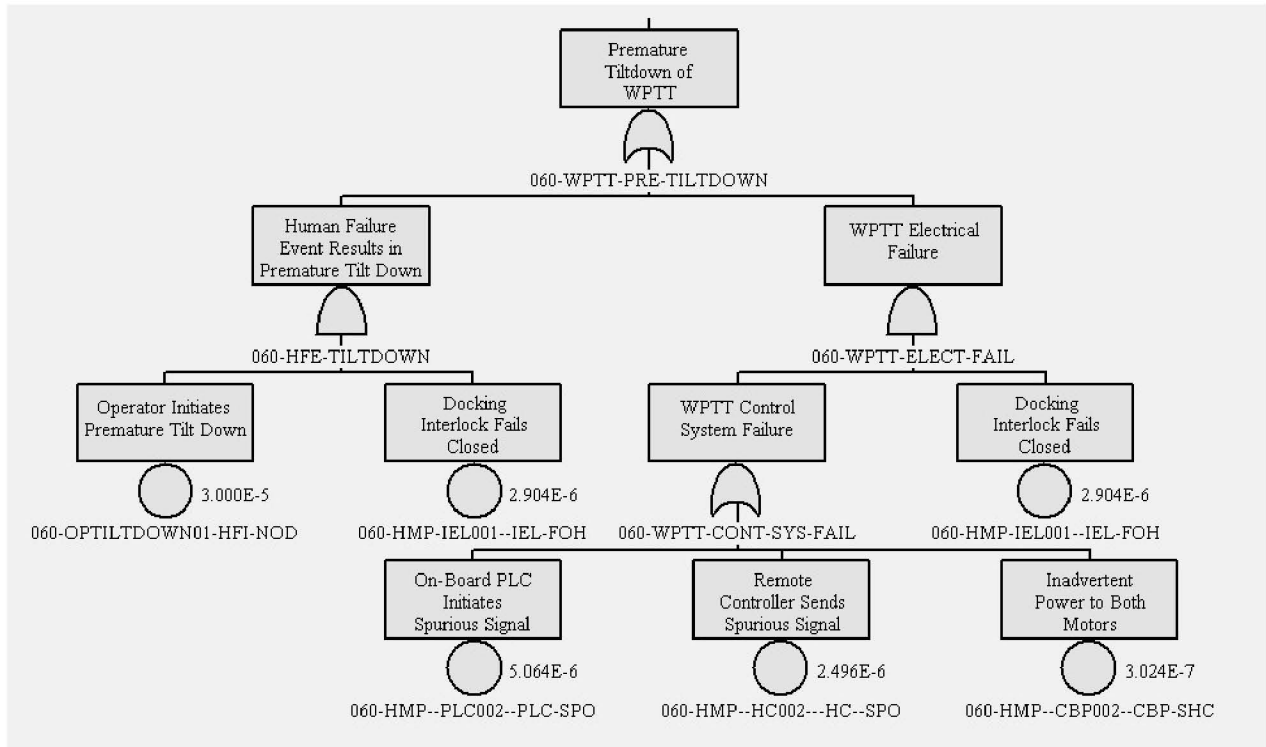
Figure 4.3-6. Grouped Event Sequences for ESD-02, TAD Canisters

### 4.3.2 Initiating and Pivotal Event Analysis

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

### 4.3.2.1 Fault Tree Analysis

Construction of a fault tree is a deductive reasoning process that answers the question “What are all combinations of events that can cause the top event to occur?” Figure 4.3-7 demonstrates this:



NOTE: This fault tree is presented for illustrative purposes only and is not intended to represent results of the present analysis.

PLC = programmable logic controller; WPTT = waste package transfer trolley.

Source: Original

Figure 4.3-7. Example Fault Tree

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

As the name implies, fault tree events are typically failures or faults. Fault trees use logic or Boolean gates. Figure 4.3-7 shows the two types of gates: the AND gate (mound-shaped symbol with a flat bottom) and the OR gate (mound-shaped symbol with a concave bottom). An AND gate flows output up the tree if *all* events immediately attached to it occur. An AND gate is often used to represent components or system features that back each other up, that is, if one fails then the other continues to adequately perform the function. An OR gate flows output up the tree if *any one or more* events immediately attached to it take place. The success criterion of the SSC or equipment being analyzed is important in determining the appropriate use of gates.

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

Fault trees are Boolean-reduced to “minterm” form, which expresses the top event in terms of the union of minimal cut sets. Minimal cut sets, which are groups of basic events that must all occur to cause the top event in the fault tree, result from applying the Boolean Idempotency and Absorption laws. FTA, as used in the PCSA, is well described in the *Fault Tree Handbook* NUREG-0492 (Ref. 2.2.87). Each minimal cut set represents a single basic event or a combination of two or more basic events (e.g., a logical intersection of basic events) that could result in the occurrence of the event sequence. Minimal cut sets are minimal in the sense that they contain no redundant basic events (i.e., if any basic event were removed from a minimal set, the remaining basic events together would not be sufficient to cause the top event). Section 4.3.6 continues the discussion about utilization of minimal cut sets in the quantification of event sequences.

The organization of the fault trees in the PCSA is developed to emphasize two primary elements, which together result in the occurrence of the top event: (1) human failure events (HFEs), and (2) equipment failures. The HFEs include postulated unintended crew actions and omissions of crew actions. Identification and quantification of HFEs are performed in phases. Initial identification of HFEs lead to design changes either to eliminate them or to reduce the probability that they would cause the fault tree top event. For example, adding an electro-mechanical interlock to a piece of equipment would make it so a crew error of commission and failure of the interlock must both take place for an initiating event to occur.

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

#### **4.3.2.2 Passive Equipment Failure Analysis**

Passive equipment (e.g., transportation casks, storage canisters, waste packages) may fail from manufacturing defects, material variability, defects introduced by handling, long-term effects such as corrosion, and normal and abnormal use. Industry codes such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.5) and “General Requirements for Division 1 and Division 2” Section III, Subsection NCA of *2004 ASME Boiler and Pressure Vessel Code* (Ref. 2.2.7) establish design load combinations for passive structures (such as building supports) and components (such as canisters). These codes specify design basis load combinations and provide the method to establish allowable stresses. Typical load combinations for buildings

involve snow load, dead (mass) load, live occupancy load, wind load, and earthquake load. Typical load combinations for canisters and casks are found in *2004 ASME Boiler and Pressure Vessel Code* (Ref. 2.2.7) and would include, for example, preloads or pre-stresses, internal pressurization and drop loads, which are specified in terms of acceleration. Design basis load combinations are purposefully specified to conservatively encompass anticipated normal operational conditions as well as uncertainties in material properties and analysis. Therefore, passive components, when designed to codes and standards and in the absence of significant aging, generally fail because of load combinations or individual loads that are much more severe than those anticipated by the codes. Fortunately, the conservative nature of establishing the design basis coupled with the low probability of multiple design basis loads occurring concurrently often means a significant margin or factor of safety exists between the design point and actual failure. The approach used in the PCSA takes advantage of the design margins (or factor of safety).

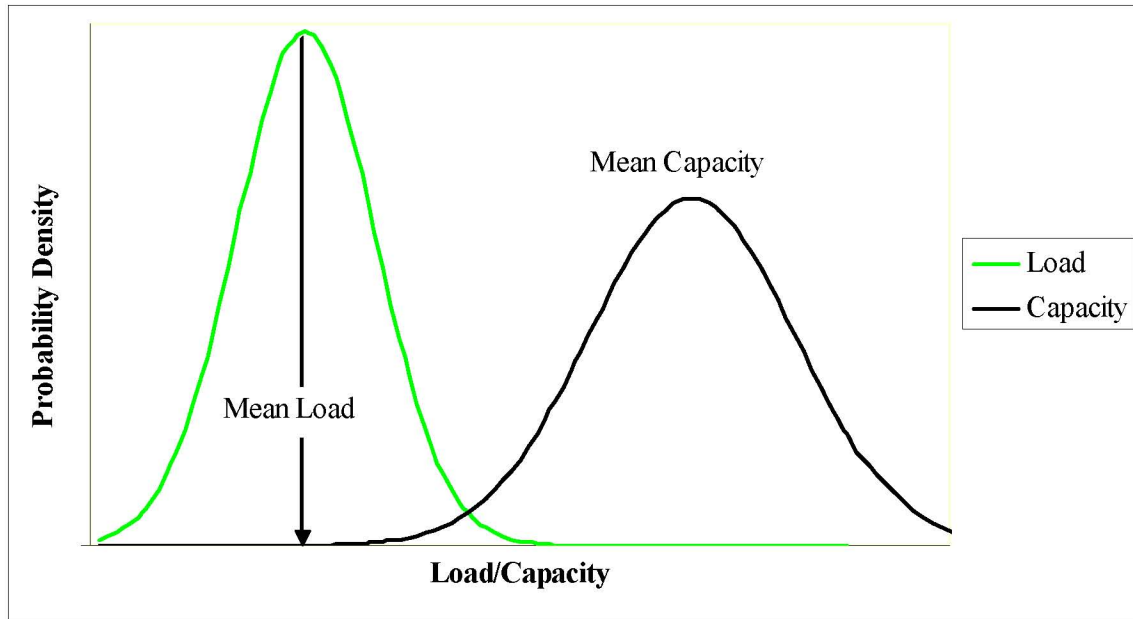
The development of code requirements for minimum design loads in buildings and other structures in the late 1970s considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures* (Ref. 2.2.41). This document refers to classic structural reliability theory. In this theory, each structure has a limit state (e.g., yield or ultimate), such that, loads and resistances are characterized by Equation 5:

$$g(x_1, x_2, \dots, x_i, \dots, x_n) = 0 \quad (\text{Eq. 5})$$

In Equation 5,  $g$  is termed the limit-state variable where failure is defined as  $g < 0$  and the  $x_i$  are resistance (sometimes called capacity or fragility) variables or load (sometimes called stress or demand) variables. The probability of failure of a structure is given, in general, by Equation 6:

$$P_f = \int \dots \int f_x(x_1, x_2, \dots, x_i, \dots, x_n) dx_1 dx_2 \dots dx_n \quad (\text{Eq. 6})$$

Where  $f_x$  is the joint probability density function (PDF) of  $x_i$  and the integral is over the region in which  $g < 0$ . The fact that these variables are represented by probability distributions implies that absolutely precise values are not known. In other words, the variable values are uncertain. This concept is illustrated in Figure 4.3-8. Codes and standards such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.5) guide the process of designing structures such that there is a factor of safety between the load and capacity. The factor of safety is established in recognition that quantities, methods used to evaluate them, and tests used to ascertain material strength give rise to uncertainty. A heuristic measure of the factor of safety is the distance between the mean values of the two curves.



Source: Original

Figure 4.3-8. Concept of Uncertainty in Load and Resistance

In the case in which Equations 5 and 6 are approximated by one variable representing capacity and the other representing load, each of which is a function of the same independent variable  $y$ , the more familiar load-capacity interference integral results as shown in Equation 7.

$$P_f = \int F(y)h(y)dy \quad (\text{Eq. 7})$$

$P_f$  is the mean probability of failure and is appropriate for use when comparing to a probability criterion such as one in a million. In Equation 7,  $F(y)$  represents the cumulative density function of structural capacity and  $h(y)$  represents the PDF of the load. The former is sometimes called the fragility function and the later is sometimes called the hazard function.

To analyze the probability of breach of a dropped canister,  $y$  is typically in units of strain,  $F$  is typically a fragility function, which provides the conditional probability of breach given a strain, and  $h$  is the PDF of the strain that would emerge from the drop. For seismic risk analysis,  $h$  represents the seismic motion input,  $y$  is in units of peak ground acceleration, and  $F$  is the seismic fragility. The seismic analysis of the YMP structures is documented in a separate PCSA analysis. Degradation of shielding owing to impact loads uses a strain to failure criterion within the simplified approach of Equation 8, described below. For analysis of the conditional probability of breach owing to fires,  $y$  is temperature,  $F$  is developed from fire data for non-combustible structures, and  $h$  is developed using probabilistic heat transfer calculations.

If load and capacity are known, then Equations 6 and 7 provide a single valued result, which is the mean probability of failure. Each function in Figure 4.3-8 is characterized by a mean value,  $\bar{L}$  (for load) and  $\bar{C}$  (for capacity), and a measure of the uncertainty, generally the standard deviation, usually denoted by  $\sigma_L$  and  $\sigma_R$  for L and C, respectively. The spread of the functions

may be expressed, alternatively, by the corresponding coefficient of variation (V) given by the ratio of standard deviation to mean, or  $V_L = \sigma_L/\bar{L}$  and  $V_R = \sigma_R/\bar{C}$  for load and capacity, respectively. The coefficient of variation may be thought of as a measure of dispersion expressed in terms of the number of means.

In the PCSA, the capacity curve for developing the fragility of casks and canisters against drops was constructed by a statistical fit to tensile elongation to failure tests (Ref. 2.2.32). The load curve may be constructed by varying drop height. A cumulative distribution function may be fit to a locus of points each of which is the product of drop height frequency and strain given drop height.

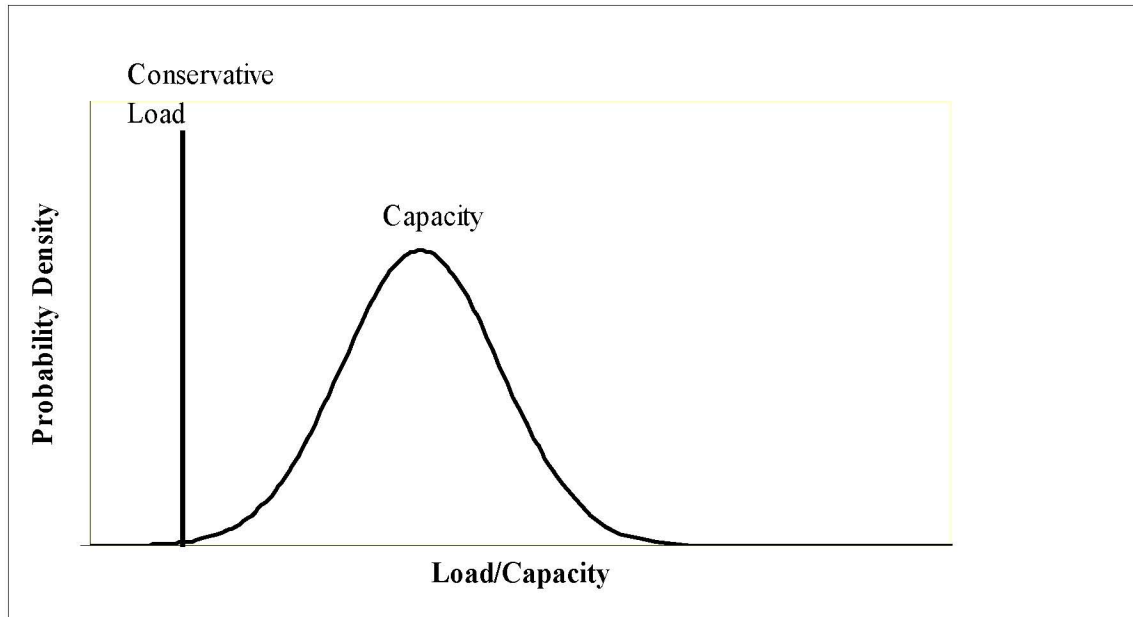
#### 4.3.2.2.1 Impact Events Associated with Containment Breach

A simplification of Equation 7, consistent with *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.70) and shown in Equation 8, is used in the PCSA. It is illustrated in Figure 4.3-9.

$$P_f = \int_0^h F(y)dy \quad (\text{Eq. 8})$$

In Equation 8,  $h$  is a single value conservative load.

The load is a single value estimated by performing a calculation for a condition more severe than the mean. For example, if the normal lift height of the bottom of a canister in a handling facility is 23 feet, a drop height of 32.5 feet is more severe and may be conservatively applied to all drop heights equal to or below this height. This can be conservatively applied to all drop heights equal to or below this height, such as for the maximum drop heights for railcars, truck trailers, or cask transfer trailers used during Intra-Site Operations. The conditional probability of breach is an increasing function of drop height. Strain resulting from drops is calculated by dynamic finite element analysis (FEA) using LS-DYNA for canisters and transportation cask drops (Ref. 2.2.32). Therefore, use of a higher than mean drop height for the load for all drop heights results in a conservative estimate of breach probability. As an additional conservatism, a lower limit of breach probability of 1E-05 was placed on drops of casks, canisters, and waste packages. To perform the analyses, representative canisters and casks were selected from the variety of available designs in current use which were relatively thin walled on the sides and bottom. This added another conservative element.



Source: Original

Figure 4.3-9. Point Estimate Load Approximation Used in PCSA

The PCSA applies PEFAs to a wide variety of event sequences including those associated with:

- Canister drops
- Canister collisions with other objects and structures
- Other objects dropped on canisters
- Transportation cask drops and subsequent sladdowns (analyzed without impact limiters)
- Conveyance derailments and collisions when carrying transportation casks and canisters (conveyances would be trucks, railcars, cask transfer trailers, and site transporters)
- Other objects dropped on transportation casks
- Waste package drops
- Waste package collisions with other waste packages
- TEV collisions with structures or another TEV when carrying a waste package
- Objects dropped on waste packages
- Objects dropped on TEV.

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

#### 4.3.2.2.2 Shielding Degradation Events

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

The shielding degradation analysis is based primarily on results of finite element modeling (FEM) performed for four generic transportation cask types for transportation accidents, as reported in *Reexamination of Spent Fuel Shipment Risk Estimates*, NUREG/CR-6672 (Ref. 2.2.82). The results of the FEM analysis were used to estimate threshold drop heights and thermal conditions at which LOS may occur in repository event sequences. The four cask types include one steel monolith rail cask, one steel/depleted uranium truck cask, one steel/lead/steel (SLS) truck cask, and one SLS rail cask. The study performed structural and thermal analyses for both failure of containment boundaries and LOS for accident scenarios involving rail and truck casks impacting unyielding targets at various impact speeds from 30 mph to greater than 120 mph. Impact orientations included side, corner, and end. The study also correlated the damage to impacts on real targets, including soil and concrete.

NUREG/CR-6672 (Ref. 2.2.82) addresses two modes of shielding degradation in accident scenarios: deformations of lid and closure geometry that permit direct streaming of radiation; and/or reductions in cask wall thickness or relocation of the depleted uranium or lead shielding. The shielding degradation due to lid/closure distortion can be accompanied by airborne releases if the inner shell of the cask is also breached.

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

Principal insights reported in *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672 (Ref. 2.2.82) include the following:

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

Therefore, this analysis focuses on SLS casks to estimate the drop or collision conditions that could result in shielding degradation from lead slumping. Since it is not possible to predict at



this time the fraction of casks to be delivered during the preclosure period that will be of the steel-lead-steel type, all transportation casks are analyzed as described below.

The document *Shipping Container Response to Severe Highway and Railway Accident Conditions*, NUREG/CR-4829 (Ref. 2.2.45) defines three levels of cask response, characterized by the maximum effective plastic strain within the inner shell of a transportation cask. Of these, level S3 has strain levels between 2.0% and 30% which produces large distortions, seal leakage likely and lead slump likely. The minimum strain level associated with S3 was applied to the strain versus impact speed results from the FEM (Ref. 2.2.82) to establish a median threshold impact speed for the onset of shielding degradation. The threshold speeds are translated into equivalent drop heights, using calculated bottom corner drops for impact loads onto real concrete targets, not idealized rigid targets. Use of a conservative coefficient of variation, coupled with the median, allowed a lognormal fragility curve as a function of drop height (or equivalently impact speed), to be developed. Each event sequence may be characterized by a conservative impact speed. For example, the maximum speed of onsite vehicles involved in moving and handling waste forms is 2.5 mph by design (except for the site prime mover (SPM) which is limited to 9 mph), and a cask drop height of 15 feet is unlikely, by design, to be exceeded. Using Equation 8, the fragility curve was combined with the maximum, or a conservative estimate of, impact speed (or equivalent drop height).

#### **4.3.2.2.3 Fire Events Associated with Possible Containment Breach**

Fire initiated events are included in the PCSA, which probabilistically analyzes the full range of possible fires that can occur, as well as variations in the dynamics of the heat transfer and uncertainties in the failure temperature of the target. This analysis focuses on fires that might directly impact the integrity of cask, canister, and waste package containment. Equation 7 is used for this purpose. The fragility analysis includes the uncertainty in the temperature that containment will be breached, and the uncertainty in the thermal response of the canister to the fire. In calculating the thermal response of the canister, variations in the intensity and duration of the fire are considered along with conditions that control the rate of heat transfer to the container, e.g., convective heat transfer coefficients, view factors, emissivities, etc. In calculating the failure temperature of the canister, variations in the material properties of the canister are considered, along with, variations in the loads that lead to failure. The load or demand is associated with uncertainty in the fire severity.

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

#### **4.3.2.2.4 Uncertainty in Fire Severity**

An uncertainty distribution for the fire duration is developed by considering test data and analytical results reported in several different sources; some specific to the YMP facilities and

some providing more generic information. In general, the fire durations are found to depend upon the amount, type, and configuration of the available combustible material.

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

Uncertainty in fire duration was developed from:

- *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. 2.2.84)
- *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report*. NUREG/CR-4680 (Ref. 2.2.61)
- *Quantitative Data on the Fire Behavior of Combustible Material in Nuclear Power Plants: A Literature Review*. NUREG/CR-4679 (Ref. 2.2.62).

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

The fire temperature used in this calculation is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. 2.2.77, p. 2-56). Fires inside a YMP facility may involve both combustible solid and liquid materials. A probability distribution for the fire temperature was derived by combining fire severity information for compartment fires discussed in *SFPE Handbook of Fire Protection Engineering* (Ref. 2.2.77, Section 2, Chapter 2) with information about liquid hydrocarbon pool fires. The derivation of this distribution is described in Attachment D, Section D2.1.2. The fire temperature distribution is normally distributed with a mean of 1,072 K (799°C) and a standard deviation of 172 K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C specified in 10 CFR 71.73 (Ref. 2.3.3).

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

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

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

The total radiant energy deposited in the container can be roughly estimated using Equation 9:

$$Q_{rad} = \varepsilon F_{cf} \sigma (T_{fire})^4 A t \quad (\text{Eq. 9})$$

where

$Q_{rad}$	=	incident radiant energy over the fire duration (J)
$\varepsilon$	=	emissivity of the container
$F_{cf}$	=	container-to-fire view factor
$\sigma$	=	Stefan-Boltzmann constant ( $\text{W/m}^2 \text{K}^4$ )
$T_{fire}$	=	equivalent blackbody fire temperature (K)
$A$	=	container surface area ( $\text{m}^2$ )
$t$	=	duration of the fire (s).

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

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

1. *Creep-Induced Failure.* Creep is the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load. This mode of failure is possible for long duration fires.
2. *Limit Load Failure.* This failure mode occurs when the load exerted on a material exceeds its structural strength. As the temperature of the canister increases, its strength decreases. Failure is generally predicted at some fraction (usually around 70%) of the ultimate strength.

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

Equation 7, along with the heat transfer equations, are solved using Monte Carlo simulation (described in Section 4.3.6) with the above described fragility and target fire severity probability distributions, and distributions for the uncertain heat transfer factors. For each Monte Carlo trial, the calculated maximum canister temperature is compared to the sampled target failure temperature. If the maximum temperature of the target exceeds the sampled failure temperature, then target failure is counted. The failure probability in this method is equal to the fraction of the samples for which failure is calculated.

Uncertainty in the calculated canister failure probability is given by a calculated mean and standard deviation, where the mean is simply the number of failures divided by the total number of samples and the standard deviation is given by Equation 10 for the standard deviation of a binomial distribution:

$$\sigma = \sqrt{\frac{\frac{n_{\text{fail}}}{N} \left( \frac{N - n_{\text{fail}}}{N} \right)}{N}} \quad (\text{Eq. 10})$$

where  $n_{\text{fail}}$  is the number of trials in which failure occurs and  $N$  is the total number of Monte Carlo trials.

#### 4.3.2.2.5 Fire Event Associated with Shielding Degradation

The thermal analyses in NUREG/CR-6672 (Ref. 2.2.82) indicates that the probability of shielding degradation in a fire scenario should be based on the probability of having a fire equivalent to a 1,000°C engulfing fire lasting more than a half-hour. However, shielding degradation does not occur unless there is a coincident puncture or breach in the cask that allows a pathway for melted lead to flow out of its usual configuration. These threshold conditions apply to all cask types and would result in radiation streaming from the cask.

The transportation cask is present within the YMP facilities in only three areas: vestibules, preparation rooms, and unloading rooms. Transportation casks are also present outside of buildings within the GROA. The fire ignition frequencies of these areas are summed up in Section 6.5 and Attachment F, Section F4.3. Furthermore, the method described above for obtaining the probability distribution of fire severity from input distributions of fire temperature and fire duration, resulted in an estimate of the conditional probability of the threshold fire given a fire ignition. The joint frequency of having a fire in these areas that is at or above the threshold was obtained and found to be very small (described in Attachment D). This is a conservative calculation because it did not include the conditional probability that a puncture or failure through the wall to the lead shielding must also occur for shielding degradation.

#### 4.3.2.2.6 Other Thermal Events Associated with Possible Breach

The PCSA focuses on the potential of cask, canister, and waste package breach associated with fires. As described above, the fires of most interest were those that surround the target containment. However, one heat-up associated with loss of building cooling is also considered. Such events are not relevant to the Intra-Site Operations analysis, but discussion is included here to show continuity of the methods used.

The analysis of loss of building cooling on containment integrity takes a conservative, analytical approach. A bounding set of conditions and configurations are postulated, and then using the ANSYS code (Ref. 2.2.12), the maximum steady state temperature is compared to the temperature at which the component would be expected to fail. In no case is a containment barrier found to be near its failure threshold from loss of building cooling.

#### **4.3.2.2.7 Fires that Occur Outside of Building Structures (Intra-Site Operations Only)**

Fires associated waste forms for Intra-Site Operations occur outside of the main process buildings. With regard to the frequency of such fires, based on historical fire ignition frequencies from other facilities, the fire frequency across the site is proportional to the number of main process buildings on the site. That is, the number of opportunities for fires outside buildings is affected by the number of main process buildings being serviced. There are six main process buildings in the GROA: Initial Handling Facility (IHF), Receipt Facility (RF), WHF, and three CRCFs).

The frequency of outside fires at the YMP is expected to be similar to those from other industrial facilities. The specific type of facility, the type of construction of the buildings, and other features are not considered relevant to the frequency of outside fires because the ignition sources that exist outside of the buildings are considered to be generic to any industrial facility. The assessment of fire severity is performed as already described. Fire severity is addressed in Attachment D, Section D2.1.

Outside fire initiating events are considered for the potential to directly affect one or more waste forms, causing a breach or shield degradation that would result in a release. The fire analysis, therefore, focuses on this potential. The steps of this process include identifying areas onsite where waste forms can be present, correlating these areas with historical industry-wide databases, and defining the initiating events.

In order to assess the total fire frequency, two pieces of information are required from the industry-wide databases: the number of facilities and the number of fires at these facilities. The assessment of this data yields the fire frequencies for outside areas, which is then used as input to the fire initiating event frequency analysis.

The frequency is expressed in terms of facility-year. Therefore, the overall frequency of outside fires for the GROA will be the frequency per facility-year times the number of main process buildings (six): IHF, WHF, RF, and three CRCFs.

A suitable uncertainty distribution is applied to the results of the initiating event frequency analysis to represent the significant uncertainty that results from the application of this methodology.

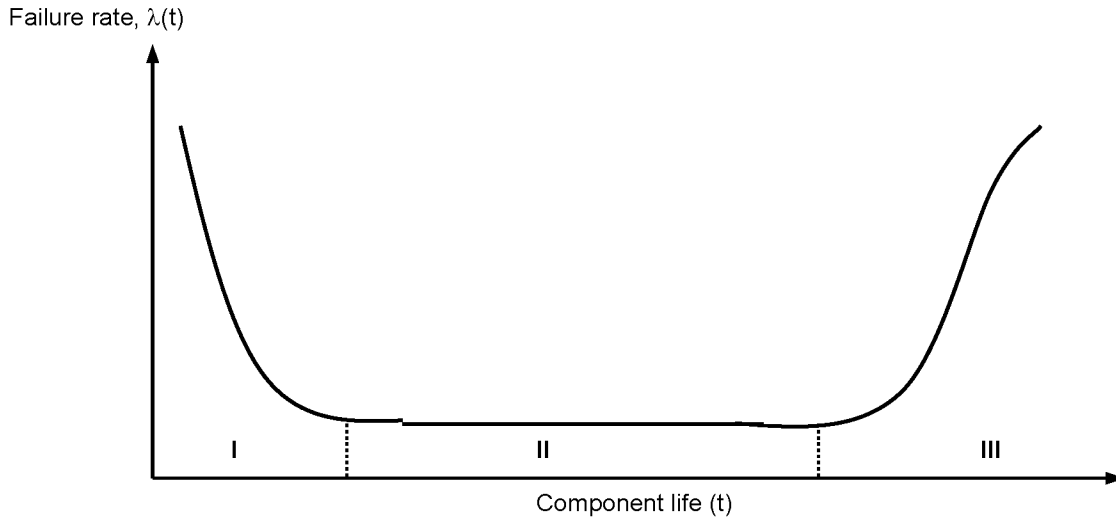
### **4.3.3 Utilization of Industry-Wide Reliability Data**

#### **4.3.3.1 Use of Population Variability Data**

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

As presented in NUREG-0492 (Ref. 2.2.87), the typical model of failure probability for a component is depicted as a “bathtub curve” illustrated in Figure 4.3-10. The curve is divided into three distinct phases. Phase I represents the component failure probability during the “burn-

in” period. Phase II corresponds to the “constant failure rate function” where the exponential distribution can be applied to calculate the probability of failure within a specified “mission time.” Toward the end of the component life or the wear-out period, that is represented by Phase III of the curve, the probability of failure increases.



Source: NUREG-0492 (Ref. 2.2.87, Figure X-8, p. X-23)

Figure 4.3-10. Component Failure Rate “Bathtub Curve” Model

As is usually done in PRA, the PCSA uses Phase II because Phase I failures are identified by burn-in testing of equipment before repository operations occur and Phase III failures are eliminated by preventive maintenance which includes manufacturer recommended replacement intervals. In Phase II, the component time-to-failure probability can be represented with the exponential distribution. The probability of failure of a given component (or system) depends on the value of the constant failure rate,  $\lambda$ , and the mission time,  $t_m$ , as follows in Equation 11:

$$P_F(\lambda, t_m) = 1 - \exp(-\lambda t_m) \quad (\text{Eq. 11})$$

When the product  $\lambda t_m$  is small ( $<0.1$ ), the failure probability may be calculated by the following Equation 12 approximation, which introduces less than a 10% error:

$$P_F(\lambda, t_m) \cong \lambda t_m \quad (\text{Eq. 12})$$

The PCSA also uses the concept of unavailability to estimate basic event probabilities. This applies to standby equipment, such as the emergency diesel generators and fire suppression. In accordance with reliability theory, after each test the component or system is considered to be “good as new,” with a “resetting” of the time-to-failure “clock” for the exponential failure model. The unavailability factor is evaluated as the probability of failure during the time between tests,  $\tau$ . The average unavailability factor, or failure on demand of the standby unit,  $q_d$ , is calculated as shown in Equation 13:

$$q_d(\lambda, \tau) = \frac{1}{2}(\lambda \tau) \quad (\text{Eq. 13})$$

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

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

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

1. Historical performance of successes and failures of an identical piece of equipment under identical environmental conditions and stresses that are being analyzed (e.g., operational experience).
2. Historical performance of successes and failures of an identical piece of equipment under conditions other than those being analyzed (e.g., test data).
3. Historical performance of successes and failures of a similar piece of equipment or similar category of equipment under conditions that may or may not be those under analysis (e.g., another program's test data or data from handbooks or compilations).
4. General engineering or scientific knowledge about the design, manufacture, and operation of the equipment or an expert's experience with the equipment.

The YMP repository has not yet operated, and test information on prospective equipment has not yet been developed. It is assumed that equipment and SSCs designed and purchased for the Yucca Mountain repository will be of the population of equipment and SSCs represented in U.S. industry-wide reliability information sources (Assumption 3.2.1). Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population. Attachment C, Section C1, contains the list of industry-wide reliability information sources used in the PCSA.

The lack of actual operating experience, the use of industry-wide data, and the consideration of uncertainties (Ref. 2.2.70) suggested that a Bayesian approach was appropriate for the PCSA. A Bayesian approach and the use of judgment in expressing the state-of-knowledge of basic event unreliability is a well-recognized and accepted practice (Ref. 2.2.56), (Ref. 2.2.8), and (Ref. 2.2.64). Furthermore, to paraphrase HLWRS-ISG-02 (Ref. 2.2.70), reliability estimates for high reliability SSCs may include the use of engineering judgment, supported by sufficient technical basis, and empirical reliability analyses of a SSC could include values based on industry experience and judgment.

Let  $\lambda_j$  be one failure rate of a set of possible failure rates of a component and  $E$  be a new body of evidence. Knowledge of the probability of  $\lambda_j$  given  $E$ , is represented by  $P(\lambda_j/E)$ . For a failure rate, frequency, or probability of active equipment, Bayes' theorem is stated as follows in Equation 14:

$$P(\lambda_j / E) = \frac{P(\lambda_j)L(E / \lambda_j)}{\sum_j P(\lambda_j)P(E / \lambda_j)} \quad (\text{Eq. 14})$$

In summary, this states that the knowledge of the “updated” probability of  $\lambda_j$ , given the new information  $E$ , equals the “prior” probability of  $\lambda_j$ , before any new information, times the likelihood function,  $L(E/\lambda_j)$ . The likelihood function is a probability that the new information really could be observed, given the failure rate,  $\lambda_j$ . The numerator in Equation 14 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of  $\lambda_j$  equals unity. If there is actual operational experience available, then the steps in an application of Bayes’ theorem would be as follows: (1) estimate the prior probability using one or more of the four reliability data types; (2) obtain new information in the form of tests or experiments; (3) characterize the test information in the form of a likelihood function; and (4) perform the calculation in accordance with Equation 14 to infer the updated probability.

The PCSA used industry-wide reliability data to develop Bayesian prior distributions for each active equipment/component failure mode in the fault trees. Updates per Equation 14 await actual test and operations. The following summarizes the methods used to develop the Bayesian prior distributions.

Using multiple reliability databases typically causes a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution,  $g$ , representing the source-to-source variability, also called population variability, of the component reliability (Ref. 2.2.8, Section 8.1). In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. The population-variability distributions developed in this analysis attempt to encompass the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the PCSA. As indicated in “Bayesian Parameter Estimation in Probabilistic Risk Assessment” (Ref. 2.2.78, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example, the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

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



For each data source, the reliability information about a component's failure rate or failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. 2.2.78, Section 4.2). When no exposure data is available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution (Ref. 2.2.78, Section 4.4) and (Ref. 2.2.54, pp. 312, 314, and 315).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. 2.2.8, Section 8.2.1), which have the advantage of resulting in relatively simpler calculations. This technique, however, is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of "The Combined Use of Data and Expert Estimates in Population Variability Analysis" (Ref. 2.2.54, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the population-variability distribution in its lognormal form is noted  $g(x, \nu, \tau)$ , where  $x$  is the reliability parameter for the component (failure rate or failure probability), and  $\nu$  and  $\tau$ , the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided that in the latter case any tail truncation above  $x=1$  has a negligible effect (Ref. 2.2.78, p. 99).

The validity of this can be confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1 of Attachment C, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98% of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

To determine  $\nu$  and  $\tau$ , it is first necessary to express the likelihood for each data source as a function of  $\nu$  and  $\tau$  only, (i.e., unconditionally on  $x$ ). This is done by integrating, over all possible values of  $x$ , the likelihood function evaluated at  $x$ , weighted by the probability of observing  $x$ , given  $\nu$  and  $\tau$ . For example, if the data source  $i$  indicates that  $r$  failures of a component occurred out of  $n$  demands, the associated likelihood function  $L_i(\nu, \tau)$ , unconditional on the failure probability  $x$ , is as follows in Equation 15:

$$L_i(\nu, \tau) = \int_0^1 \text{Binom}(x, r, n) \times g(x, \nu, \tau) dx \quad (\text{Eq. 15})$$

where  $Binom(x, r, n)$  represents the binomial distribution evaluated for  $r$  failures out of  $n$  demands, given a failure probability equal to  $x$ , and  $g(x, \nu, \tau)$  is defined as previously indicated. This equation is similar to that shown in “Bayesian Parameter Estimation in Probabilistic Risk Assessment” (Ref. 2.2.78, Equation 37). If the component reliability is expressed in terms of a failure rate and the data source provides exposure data, the binomial distribution in Equation 15 would be replaced by a Poisson distribution. If the data source provided expert opinion only (i.e., no exposure data), then the binomial distribution in Equation 15 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine  $\nu$  and  $\tau$  ((Ref. 2.2.78), p. 101). The maximum likelihood estimators for  $\nu$  and  $\tau$  are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each data source (Ref. 2.2.54, Equation 4). To find the maximum likelihood estimators for  $\nu$  and  $\tau$ , it is equivalent and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of  $\nu$  and  $\tau$  completely determines the population-variability distribution  $g$  for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution  $g$ , which are calculated using the formulas given in NUREG/CR-6823 (Ref. 2.2.8, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to  $\exp(\nu + \tau^2/2)$  and the error factor is equal to  $\exp(1.645 \times \tau)$ . A discussion of the adequacy of the empirical Bayes method for the YMP analysis is provided in Attachment C, Section C2.1.

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, “External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom” ((Ref. 2.2.47), Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between 2E-08/hr (5th percentile) and 6E-05/hr (95th percentile). Using the definition of the error factor given in NUREG/CR-6823 (Ref. 2.2.8, Section A.7.3), this corresponds to an error factor of  $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$ . Therefore, in the PCSA, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55, are too diffuse to adequately represent the population-variability distribution of a component. In such instances (i.e., the two cases in the entire PCSA database when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution, and therefore is unaffected by the value taken by the error factor. Based on NUREG/CR-6823 (Ref. 2.2.8, Section A.7.3), the median is calculated as  $\exp(\nu)$ , where  $\nu$  is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the PCSA is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in NUREG/CR-6823 (Ref. 2.2.8, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for a component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the PDF of the lognormal distribution, and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using the data source that yields the most diffuse likelihood using one of the two methods described in the next paragraph.

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean, and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data, i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities, the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffreys' non-informative prior distribution. As indicated in NUREG/CR-6823 (Ref. 2.2.8, Section 6.2.2.5.2), this non-informative prior conveys little preceding belief or information, thus allowing the data to speak for itself.

#### 4.3.3.2 Dependent Events

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

1. **Functional dependence** is present when one component or system relies on another to supply vital functions. An example of a functional dependence in this analysis is electric power supply to HVAC. Functional dependence is explicitly modeled in the event tree and fault tree logic.
2. **Environmental dependence** is in play when system functionality relies on maintaining an environment within designed or qualified limits. Here, an example is material property change as a result of temperature change. Environmental effects are modeled in the system reliability analyses as modifications (e.g., multiplying factors) to system- and component-failure probabilities and are also included in the passive equipment failure analyses. External events such as earthquakes, lightning strikes, and

high winds that can degrade multiple SSCs are modeled explicitly as initiating events and are discussed in other PCSA documents.

3. **Spatial dependence** is at work when one SSC fails by virtue of close proximity to another. For example, during an earthquake one SSC may impact another because of close proximity. Another example is inadvertent fire suppression actuation which wets SSCs below it. Spatial dependences are identified by explicitly looking for them in the facility layout drawings. Inadvertent fire suppression is modeled explicitly in the event trees and fault trees.
4. **Human dependence** is present when a structure, system, component, or function fails because humans intervene inappropriately or failed to intervene. In the YMP, most human errors are associated with initiating events (inadvertent actuation) or are pre-initiator failures (failure to restore after maintenance). The PCSA includes an extensive HRA which is described later in this section, in Section 6.4 and in Attachment E. The results of the HRA are integrated into the event tree and fault tree models for a complete characterization of event sequence frequency.

#### 4.3.3.3 Common-Cause Failures

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

Because CCFs are relatively uncommon, it is difficult to develop a statistically significant sample from monitoring only one system or facility, or even several systems. The development of CCF techniques and data, therefore, rely on a national data collection effort that monitors a large number of nuclear power systems. Typically, the fraction of component failures associated with common causes leading to multiple failures ranges between 1% and 10% (Ref. 2.2.46), (Ref. 2.2.59), and (Ref. 2.2.55). This fraction depends on the component; level of redundancy (e.g., two, three, or four); duty cycle; operating and environmental conditions; maintenance interventions; and testing protocol, among others. For example, equipment that is operated in cold standby mode (i.e., called to operate occasionally on demand) with a large amount of preventive maintenance intervention tends to have a higher fraction of CCFs than systems that continuously run.

It is not practical to explicitly identify all CCFs in a fault tree or event tree. Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. 2.2.46), the Multiple Greek Letter method (Ref. 2.2.58), which is an extension of the beta factor method, and the Alpha Factor method (Ref. 2.2.59). These methods do not require an explicit knowledge of the dependence failure mode.

The PCSA uses the Alpha Factor method NUREG/CR-5485 (Ref. 2.2.59), which is summarized below. After identifying potential CCF events from the fault trees, appropriate alpha factors are identified according to the procedure described in NUREG/CR-5801 (Ref. 2.2.57). The general equations for estimating the probability of a CCF event in which  $k$  of  $m$  components fail are as follows in Equations 16, 17, and 18:

$$Q(k,m) = \frac{k}{\binom{m-1}{k-1}} \alpha_k Q_t \quad \text{for staggered test} \quad (\text{Eq. 16})$$

$$Q(k,m) = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad \text{for non-staggered test} \quad (\text{Eq. 17})$$

where  $\alpha_k$  denotes the alpha factor for size  $k$ ,  $Q_t$  denotes the total failure probability, and:

$$\alpha_t = \sum_{k=1}^m k \alpha_k \quad (\text{Eq. 18})$$

Generic alpha factors used in the PCSA are taken from NUREG/CR-5801 (Ref. 2.2.57). The process of applying these alpha factors is explained further in Attachment C, Section C3.

#### 4.3.4 Human Reliability Analysis

Human interactions that are typically associated with the operation, test, calibration, or maintenance of an SSC (e.g., drops from a crane when using slings) are implicit in the empirical data. If this is the case, empirical data may be used, provided human errors that cause the SSC failures are explicitly enumerated and determined to be applicable to YMP operations. When this was the case in the PCSA, the appropriate method of Section 4.3.3.1 was applied. Otherwise, an HRA was performed, the methodology of which is summarized in this section. The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6) and incorporates the guidance in HLWRS-ISG-04 (Ref. 2.2.71). It emphasizes a comprehensive qualitative analysis and uses applicable quantitative models.

The HRA task identifies, models, and quantifies HFEs postulated for YMP operations to assess the impact of human actions on event sequences modeled in the PCSA. YMP operations differ from those of traditional nuclear power plants, and the HRA reflects these differences. Appendix

E.IV of Attachment E includes further discussion of these differences and how they influence the choice of methodology.

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

#### **4.3.4.1 HRA Boundary Conditions**

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

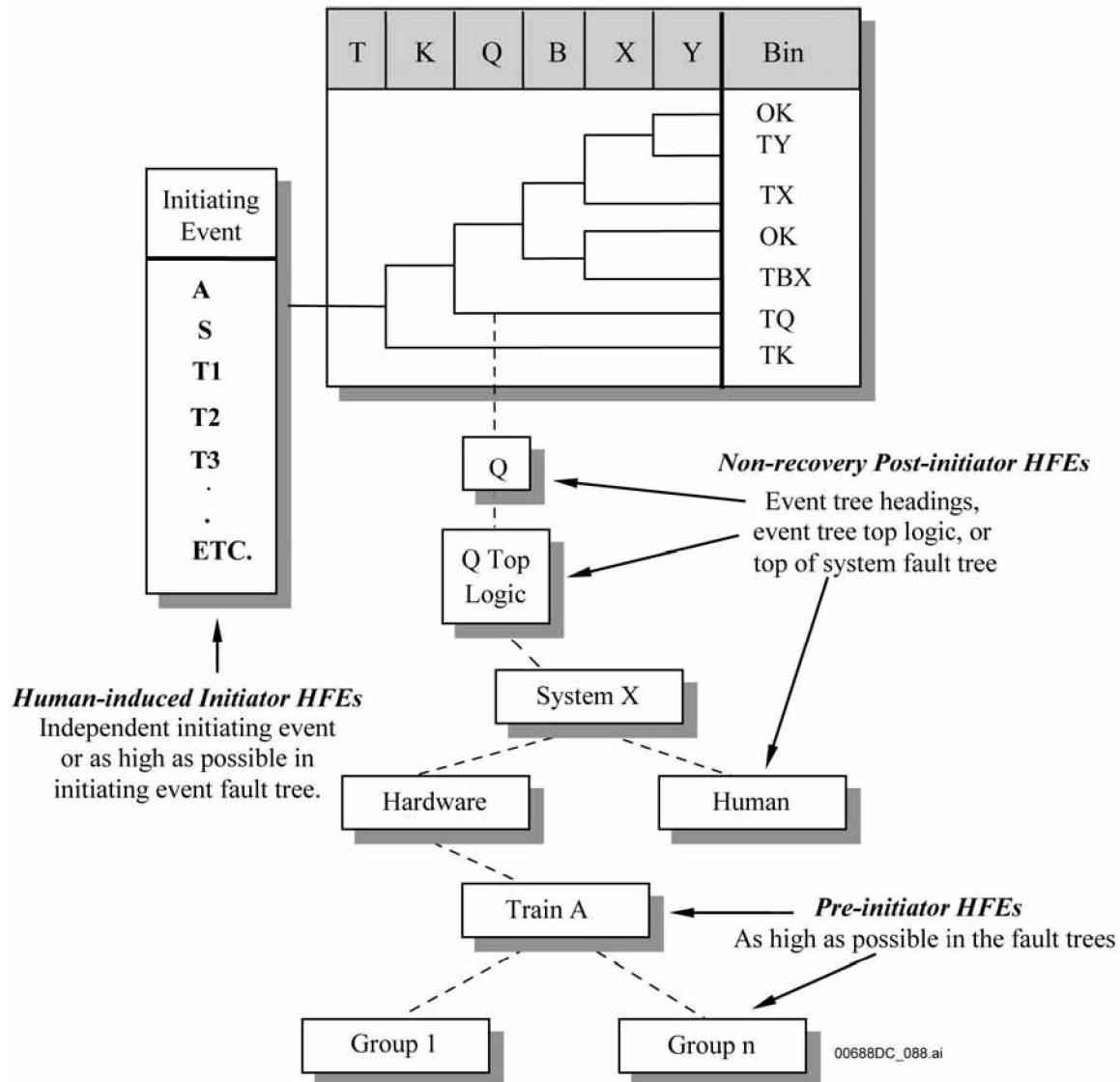
1. Only HFES made in the performance of assigned tasks are considered. Malevolent behavior, deliberate acts of sabotage, and the like are not considered in this task.
2. All personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard operating procedures is made because the employee believes their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.
3. Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include SNF handling at reactor sites having independent SNF storages, chemical munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the GROA facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.
4. The YMP is initially operating under normal conditions and is designed to the highest quality human factor specifications. The level of operator stress is optimal unless the analyst determines that the human action in question cannot be accommodated in such a manner as to achieve optimal stress.
5. In performing the operations, the operator does not need to wear protective clothing unless it is an operation similar to those performed in comparable facilities where protective clothing is required.

6. The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are to be experienced and have functioned in their present positions for a sufficient amount of time to be proficient.
7. The environment inside each YMP facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination, and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made regarding optimal weather conditions.
8. While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

#### **4.3.4.2 HRA Methodology**

The HRA consists of several steps that follow the intent of ASME RA-S-2002 (Ref. 2.2.6) and the process guidance provided in *Technical Basis and Implementation Guidelines for Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. 2.2.68). The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt material that is based on nuclear power plants to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. 2.2.68). Section 10.3 of NUREG-1624 (Ref. 2.2.68) provides an overview of the method for incorporating HFEs into a PRA. Figure 4.3-11 illustrates this integration method.



NOTE: HFE = human failure event.

Source: Original

Figure 4.3-11. Incorporation of Human Reliability Analysis within the PCSA

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

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



**Step 3: Identify and Define HFEs of Concern**—Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then becomes the error-forcing context (EFC) for a specific HFE. As defined by ATHEANA (Ref. 2.2.68), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses. The analyses performed in later steps (e.g., Steps 6 and 7) may identify the need to define additional HFEs or unsafe actions.

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

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

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

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

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

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

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

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

1. Cognitive Reliability and Error Analysis Method (CREAM) (Ref. 2.2.49)
2. Human Error Assessment and Reduction Technique (HEART) (Ref. 2.2.90)/ Nuclear Action Reliability Assessment (NARA) (Ref. 2.2.34)
3. Technique for Human Error Rate Prediction (THERP) with some modifications (Ref. 2.2.83).

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

4. ATHEANA expert elicitation approach (Ref. 2.2.68).

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

**Step 8: Incorporate HFEs into PCSA**—After HFEs are identified, defined, and quantified, they must be reincorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. 2.2.68) provides an overview of the state-of-the-art method for performing this step in PRAs. The term “reincorporated” is used because some HFEs are identified within the fault tree and event tree analysis. All event sequences that contain multiple HFEs are examined for possible dependencies. Figure 4.3-11 shows how the different types of HFEs discussed previously are incorporated into the model based on their temporal phase, which determines where in the model each type of HFE is placed. More detailed discussion of how this is done is provided in Attachment E.

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

#### 4.3.4.3 Classification of HFEs

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

1. The three temporal phases used in PRA modeling:
  - A. Pre-initiator
  - B. Human-induced initiator
  - C. Post-initiator.
2. Error modes:
  - A. Errors of omission
  - B. Errors of commission.
3. Human failure types:
  - A. Slips/lapses
  - B. Mistakes.

4. Informational processing failures:
  - A. Monitoring and detection
  - B. Situation awareness
  - C. Response planning
  - D. Response implementation.

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

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is used for the YMP HRA guidelines is based on the discussion in Chapter 4 of NUREG-1624 (Ref. 2.2.68) and consists of the following elements:

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.
- Situation awareness—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents the operator's understanding of the present situation and their expectations for future conditions and consequences.
- Response planning—This term is defined as the process by which operators decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.
- Response implementation—This term is defined as the activities involved with physically carrying out the actions identified in response planning.

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

### 4.3.5 Fire Analysis

The fire event sequence analysis consists of four parts:

1. **Development of fire ignition frequencies for each location in the operations area.** These are all called fire initiating event frequencies.
2. **Development of the fire severity in terms of both temperature and durations.** This was discussed in Section 4.3.2.
3. **Development of the conditional probability of fire damaging a cask, canister, or waste package target.** This was discussed in Section 4.3.2.
4. **Development of and quantification of fire ESDs and event trees.** Development of the ESDs and event trees is described in the event sequence development analysis (Ref. 2.2.29). Quantification of fire event, event trees is conducted like quantification of other event trees (Sections 4.3, 4.3.1, and 4.3.7).

This section summarizes the method for the fire initiating event analysis performed as a part of the PCSA. The analysis was performed as part of an integrated analysis of internal fires in the surface and subsurface facilities. This section only discusses those aspects of the fire analysis methodology that apply directly to the analysis for Intra-Site Operations and Subsurface Operations. The full fire analysis and detail on the methods and data are documented in Attachment F to this volume. The fire analysis is subject to the boundary conditions described in the following section.

#### 4.3.5.1 Boundary Conditions for Fire Analysis

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

- **Plant Operational State.** Operation initial state conditions are normal with each system operating within its limiting condition for operation restrictions.
- **Number of Fire Events to Occur.** Operations are analyzed to respond to one fire event at a given time. Additional fire events as a result of independent causes or of reignition once a fire is extinguished are not considered.
- **Relationship to Process Buildings.** Fires included in the analysis occur outside of the main process buildings. With regard to the frequency of such fires based on historical fire ignition frequencies from other facilities, the fire frequency across the site is proportional to the number of main process buildings (i.e., for the YMP, the waste handling facilities) on the site. That is, the number of opportunities for fires outside buildings is affected by the number of waste handling facilities being serviced. The number of waste handling facilities for the YMP is six: IHF, RF, WHF, and three CRCFs.

- **Irrelevancy of Industrial Facility Type to Outside Fire Frequency.** The frequency of outside fires at YMP is expected to be similar to those from other industrial facilities. The specific type of facility, the type of construction of the buildings and other features, are not considered relevant to the frequency of outside fires since the ignition sources that exist outside of the buildings are considered to be generic to any industrial facility. This does not extend to the assessment of fire severity, since the type of facility could affect the type and availability of combustibles. Fire severity is addressed in Attachment D.
- **Component Failure Modes.** The failure mode of a SSC affected by a fire is the most severe with respect to consequences. For example, the failure mode for a canister could be the overpressurization of a reduced strength canister.

#### 4.3.5.2 Analysis Method

Nuclear power plant fire risk assessment techniques have limited applicability to the repository surface facilities and operations in the GROA. The general methodological basis of the PCSA fire analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.75). Chemical agent disposal facilities are similar to those in the GROA in that these facilities are handling and disposal facilities for highly hazardous materials. This is a “data based” approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the GROA. To the extent applicable to a non-reactor facility, NUREG/CR-6850, Volumes 1 (Ref. 2.2.42) and 2 (Ref. 2.2.43) are also considered in the development of this analysis method. The method complies with the applicable requirements of *Fire PRA Methodology* (Ref. 2.2.3) that are relevant to non-reactor operations. The three steps in the analysis are summarized below and described in detail in Attachment F, Section F4.

1. **Identification of initiating events.** Outside fire initiating events for the YMP are considered for the potential for a fire to directly affect the waste containers. The fire analysis, therefore, focused on the potential for a fire to directly affect the waste containers. The initiating events for Intra-Site Operations are identified in the event sequence development analysis (Ref. 2.2.29). The steps of this process are detailed below:
  - A. **Identify areas onsite where waste containers can be present**

The processes for the site transporter, cask tractor/cask transfer trailer, and SPM movement of waste containers onsite are evaluated, and the areas where the waste forms traverse or are held pending emplacement handling are identified. Each area where waste containers can be present, even if for only a brief time, is analyzed in Section F5.
  - B. **Correlate the areas with the National Fire Protection Association (NFPA) historical database for outside fires.**

The NFPA historical database identifies the areas outside buildings where fires have occurred. These are grouped into broader categories for use in this study.

C. Define initiating events.

Fire ignition occurrences are identified for each area where a waste container can be present during Intra-Site Operations. The locations of fire initiating events are identified in the MLD (Ref. 2.2.29).

2. **Quantification of fire ignition frequency.** In order to assess the total fire frequency, two pieces of information are required (Ref. 2.2.75): the number of facilities, and the number of fires at and around these facilities. The first piece of data is maintained by the U.S. Census Bureau, which conducts an economic census (Ref. 2.2.86). The second piece of data is tracked by NFPA (Ref. 2.2.1). This approach uses historical data over a 10-year period (1988 to 1997) (Ref. 2.2.86, North American Industry Classification System (NAICS) Codes 324, 325, and 3261). This methodology and data are used to calculate the overall frequency of outside fires per facility-year of operation.
3. **Determine initiating event frequency.** The next step is to determine where these outside fires start, since the initiating events are defined in terms of fires that start in specific outside areas where waste forms reside. One analysis performed by the NFPA provided information for this (Ref. 2.2.1, Section 5). With some interpretation, these data can be used to estimate the fraction of the total fire frequency that should be assigned to the various onsite areas outside the building. By multiplying the appropriate fraction representing areas where waste forms will be times the total frequency of outside fires per facility-year, the frequency is determined for a fire in a particular area where a waste form resides (per facility year).

The frequency is expressed in terms of facility-year, since the number of NFPA fires is divided by the number of NAICS facilities. There is some uncertainty as to what is meant by a “facility” in this context. The NAICS does not make clear whether multiple process buildings can be considered a single facility; although, noting in this context that the purpose of the NAICS is an economic census, it implies that the number of main process buildings (i.e., the throughput of a given site) is more important than the number of sites. Because of this and in order to avoid potentially nonconservative probabilistic results, a boundary condition has been established that each main process building in the GROA constitutes a facility, and that the outside fire frequency pertains to each of them (i.e., each of these buildings generates the necessary conditions to contribute a full measure of potential fire ignitions). The aging pads, buffer areas, and subsurface will not be considered as separate facilities, but rather as support areas for the process buildings (i.e., they are an integral part of a typical facility in that they supply the “raw materials” to the process and take the “product” from the process). In addition, the other BOP support buildings will also not be considered facilities for the purpose of determining the overall frequency of outside fires, for a similar reason. Therefore, the overall frequency of outside fires for the GROA will be the frequency per facility-year, times the number of main process buildings (i.e., number of waste handling facilities), which is six: IHF, WHF, RF, and three CRCFs. Multiplying by 50 yields the frequency over the preclosure period.

### 4.3.5.3 Special Study – Analysis Method for Low-Level Waste Facility Fires

In addition to outside fires, the analysis for Intra-Site Operations also considers fires that affect the Low-Level Waste Facility (LLWF). The methodology used for the analysis of outside fires is not applicable to a fire in this facility. Instead, the fire ignition frequency for the LLWF is adapted from the approach to fire ignition frequencies by building type, which is used for the other surface facilities (Ref. 2.2.84). This methodology provides Equation 19:

$$f_m(A) = c_1 A^r + c_2 A^s \quad (\text{Eq. 19})$$

where

$f_m$  is the fire ignition frequency per  $\text{m}^2\text{-yr}$ ,

A is the floor area (in  $\text{m}^2$ )

$c_1$ ,  $c_2$ ,  $r$ , and  $s$  are coefficients that were determined from historical data observations for different types of facilities. The facility type “warehouse” best suits the LLWF. The coefficients for a warehouse are 3.82, 2.0E-06, -2.08, and -0.05 for  $c_1$ ,  $c_2$ ,  $r$ , and  $s$ , respectively. Multiplying by 50 yields the frequency over the preclosure period.

### 4.3.6 Event Sequence Quantification

#### 4.3.6.1 Overview of Quantification

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

1. The number of demands (sometimes called trials) or the time exposure interval of the operation or activity that gives rise to the event sequence. For example, this could be the number of DPCs in transportation casks anticipated to arrive at the GROA. If applicable, the number of movements for a waste form is included (e.g., the number movements of DPCs in aging overpacks between a waste handling facility and the Aging Facility).
2. The frequency of occurrence per demand or per time interval of the initiating event. For example, this could be the frequency of aging overpack drop per movement. Initiating event frequencies are developed either using fault trees or by direct application of industry-wide data, as explained in Section 4.3.2. Factors one and two are represented in the IETs.
3. The conditional probability of each of the pivotal events of the event sequence, which appear in the associated SRET. These probabilities are the results of a PEFA, fault tree analyses, if applicable (e.g., HVAC in waste handling facilities), and direct



probability input (e.g., moderator introduced). For example, the conditional probability of failure of a canister in an aging overpack given a drop from 3 feet or less is less than 1E-05. Where data does not exist, conditional probabilities can be the result of applied judgment (Section 4.3.10.2).

Fault tree initiating event frequencies calculated in SAPHIRE (or independent frequency data) and point values for conditional probabilities are input directly into the Excel spreadsheet containing the event sequence logic. The event sequence frequency is then estimated by calculating the product of the three factors mentioned above. This methodology can be applied here due to the simplicity of the event sequences and no dependence between pivotal events.

SAPHIRE Version 7.26 (Section 4.2), developed by Idaho National Laboratory, stands for “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations” (Section 4.2). Features of SAPHIRE used to build and quantify fault trees include the following:

- A listing of where a basic event appears, including within cut sets. Conversely, the basic events that are *not* used are known and can be easily removed when it comes time to “clean” the database.
- A context-driven menu system that performs actions (e.g., report cut sets, view importance measures, display graphics) on objects such as fault trees, event trees, and event sequences.

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

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

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

#### 4.3.6.2 Propagation of Uncertainties and Event Sequence Categorization with Uncertainties

The fundamental viewpoint of the PCSA is probabilistic in order to develop information suitable for the risk informed nature of 10 CFR Part 63 (Ref. 2.3.2). Any particular event sequence may or may not occur during any operating time interval, and the quantities of the parameters of the models may not be precisely known. Characterizing uncertainties and propagating these uncertainties through the event tree/fault tree models is an essential element of the PCSA. The PCSA includes both aleatory and epistemic uncertainties. Aleatory uncertainty refers to the inherent variation of a physical process over many similar trials or occurrences. For example, development of a fragility curve to obtain the probability of canister breach after a drop would involve investigating the natural variability of tensile strength of stainless steel. Epistemic uncertainty refers to our state of knowledge about an input parameter or model. Epistemic uncertainty is sometimes called reducible uncertainty because gathering more information can reduce the uncertainty. For example, the calculated uncertainty of a SSC failure rate developed from industry-wide data will be reduced when sufficient GROA specific operational information is included in a Bayesian analysis of the SSC failure rate.

As described in Section 4.3.1, event sequence categorization is performed using the mean value of event sequences emanating from the larger circle in Figure 4.3-4. By the definition of the term, mean values are derived from probability distributions.

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

- A value of  $m$  greater than or equal to one, places the corresponding event sequence into Category 1.
- A value of  $m$  less than one indicates that the corresponding event sequence is not expected to occur before permanent closure. To determine whether the event sequence is Category 2, its probability of occurrence over the preclosure period is compared to 1E-04. A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to  $m$ . The probability,  $P$ , that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution,  $P = 1 - \exp(-m)$ , a value of  $P$  greater than or equal to 1E-04 implies that value of  $m$  is greater than or equal to  $-\ln(1 - P) = m$ , which is numerically equal to 1E-04. Thus, a value of  $m$  greater than or equal to 1E-04, but less than 1, implies the corresponding event sequence is a Category 2 event sequence.
- Event sequences that have a value of  $m$  less than 1E-04 are designated as beyond Category 2.

Using Monte Carlo or Latin Hypercube methods allows probability distributions to be arithmetically treated to obtain the probability distributions of minimal cut sets and the

probability distributions of initiating events. The initiating event frequencies developed from fault trees used Monte Carlo simulation with 10,000 trials and a standard seed so the results could be reproduced. The number of trials for final results was arrived at by increasing the number of trials until the median, mean, and 95th percentile stabilized within the standard Monte Carlo error.

The adequacy of categorization of an event sequence is further investigated if its expected number of occurrences,  $m$ , over the preclosure period is close to a category threshold. If  $m$  is greater than 0.2, but less than 1, the event sequence, which a priori is Category 2, is reevaluated differently to determine if it should be recategorized as Category 1. Similarly, if  $m$  is greater than  $2E-05$ , but less than  $1E-04$ , the event sequence, which a priori is Beyond Category 2, is reevaluated to determine if it should be recategorized as Category 2.

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

If the calculated value of  $m_a$  is less than 1, the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., Category 2. Similarly, if the calculated value of  $m_a$  is less than  $1E-04$ , the alternative distribution confirms that the event sequence category is the same as that predicted by the original determination, i.e., beyond Category 2.

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

Similarly, if the calculated value of  $m_a$  is greater than  $1E-04$ , the alternative distribution indicates that the event sequence is Category 2, instead of beyond Category 2 as calculated in the original determination. In such a case, the conflicting indications are resolved by conservatively assigning the event sequence to Category 2.

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

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

#### **4.3.7.1 Identification of ITS SSCs**

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

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

*“Important to safety*, with reference to structures, systems, and components, means those engineered features of the geologic repository operations area whose function is:

- (1) To provide reasonable assurance that high-level radioactive waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of § 63.111(b)(1) for Category 1 event sequences; or
- (2) To prevent or mitigate Category 2 event sequences that could result in radiological exposures exceeding the values specified at § 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site.”

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

Implementation of the regulatory definition of ITS produced the following specific criteria in the PCSA to classify SSCs. A SSC is classified as ITS if it is relied upon to reduce the frequency of or mitigate the consequences of an event sequence and at least one of the following criteria apply:

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

A SSC is classified as ITS in order to assure safety function availability over the operating lifetime of the repository. The classification process involves the selection of the SSCs in the identified event sequences (including event sequences that involve nuclear criticality) that are

relied upon to perform the identified safety functions such that the preclosure performance objectives of 10 CFR Part 63 (Ref. 2.3.2) are not exceeded. The ITS classification extends only to the attributes of the SSCs involved in providing the ITS function. If one or more components of a system are determined to be ITS, the system is identified as ITS, even though only a portion of the system may actually be relied upon to perform a nuclear safety function. However, the specific safety functions that cause the ITS classification are delineated.

Perturbations from normal operations, human errors in operations, human errors during maintenance (preventive or corrective), and equipment malfunctions may initiate Category 1 or Category 2 event sequences. The SSCs supporting normal operations and not relied upon as described previously for event sequences are identified as non-ITS. In addition, if a SSC (such as permanent shielding) is used solely to reduce normal operating radiation exposure, it is classified as non-ITS.

#### 4.3.7.2 Development of Nuclear Safety Design Bases

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

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

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

1. Mean frequency of SSC failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of failure (e.g., failure to operate or failure to breach), with consideration of uncertainties, less than or equal to the stated criterion value.
2. Mean frequency of seismic event-induced failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of a seismic event-induced failure (e.g., tipover, breach) of less than 1E-04 over the preclosure period, considering the full spectrum of seismic events less severe than that associated with a frequency of 1E-07/yr.
3. High confidence of low mean frequency of failure. It shall be demonstrated by analysis that the ITS SSC will have a high confidence of low mean frequency of failure associated with seismic events of less than or equal to the criterion value. The high confidence of low mean frequency of failure value is a function of uncertainty, expressed as  $\beta_c$ , which is the lognormal standard deviation of the SSC seismic fragility.

4. Preventive maintenance and/or inspection interval. The ITS SSCs shall be maintained or inspected to ensure availability, at intervals not to exceed the criterion value.
5. Mean unavailability over time period. It shall be demonstrated by analysis that the ITS SSCs (e.g., HVAC and emergency electrical power) will have a mean unavailability over a period of a specified number of days, with consideration of uncertainties, of less than the criterion value.

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

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

#### **4.3.7.3 Identification of PSCs**

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

The occurrence of an initiating or pivotal event is usually a combination of human errors and equipment malfunctions. An HRA is performed for the human errors. Those human actions that are relied upon to reduce the frequency of or mitigate the consequence of an event sequence are subject to PSCs. The approach for deriving PSCs from the event sequence analysis is outlined in the following:

1. Use event tree and supporting fault tree models for initiating events and pivotal events to identify HFEs.
2. Identify the types of PSCs necessary to support the HRA analysis for each of the HFEs. For example, provide clarifications about what is to be accomplished, time constraints, use of instrumentation, interlock and permissives that may back-up the human action.
3. Perform an event sequence analysis using screening HRA values. Identify the PSCs that appear to be needed to reduce the probability of or mitigate the severity of event sequences.
4. Work with the design and engineering organizations to add equipment features that will either eliminate the HFE or support crew and operators in the performance of the action. In effect, this entails development of design features that appear instead of a human action or appear in a fault tree under an AND gate with a human action.

5. Quantify event sequences again, identifying HFEs for which a detailed HRA must be performed. The detailed HRA would lead to specific PSCs that are needed to reduce the frequency of event sequences or mitigate their consequences. Additional PSCs are developed from the underlying conditions or parameters of supporting analysis. For example, activity and dose rate measurements are performed to confirm acceptable conditions in the LLWF.

#### 4.3.8 Event Sequence to Dose Relationship

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

1. **Event sequence group identifier.** A unique designation is provided for each event sequence to permit cross-reference between event sequence categorization and consequence and criticality analyses.
2. **End state.** One of the following is provided for each event sequence:
  - A. DE-SHIELD-DEGRADE or DE-SHIELD-LOSS (Direct Exposure). Condition leading to potential exposure due to degradation or LOS provided by the cask, aging overpack, or horizontal aging module (HAM).
  - B. RR-FILTERED (Radionuclide Release, Filtered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., a cask with uncanistered commercial SNF or a canister). However, the availability of the confinement (structural and HVAC with HEPA filtration) provides mitigation of the consequences. Note that this end state is not applicable to Intra-Site Operations.
  - C. RR-UNFILTERED (Radionuclide Release, Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., a cask with uncanistered commercial SNF or a canister) and, if applicable, a breach in the secondary confinement boundary (e.g., no mitigation from HEPA filtration).
  - D. RR-FILTERED-ITC and RR-UNFILTERED-ITC (Radionuclide Release, Important to Criticality, Filtered or Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., a cask with uncanistered commercial SNF or a canister) with or without HEPA filtration (if applicable). In addition, the potential exists for exposing the unconfined waste form to moderator and could result in conditions ITC. This characteristic of the end state is used by both the dose consequence analysts and the criticality analysts. Note that the RR-FILTERED-ITC end state is not applicable to Intra-Site Operations.

- E. ITC (Important to Criticality). This end state is not applicable to Intra-Site Operations because all potential criticality indicators are associated with a radiological release (i.e., end state RR-UNFILTERED-ITC).
3. **General description of the event sequence.** This is a high level description that is explained by the other conditions described above. For example, "... sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from degradation of shielding due to a railcar collision, a railcar derailment, or a drop of an object onto the transportation cask..."
  4. **Material-at-risk.** Identifies and defines the number of each waste form that contributes to the radioactivity or criticality hazard of the end state (e.g., number of TAD canisters, DPCs, HLW canisters, and the like, that are involved in the event sequence).
  5. **Expected number of occurrences.** The expected mean number of occurrences of each designated event sequence over the preclosure period is provided with the associated median and standard deviation.
  6. **The event sequence categorization and basis.** The categorization of the designated event sequence and the basis for the categorization is provided.
  7. **Bounding consequences.** For each Category 1 and Category 2 events sequence, the bounding consequence analysis cross-reference to the bounding event number (from the preclosure consequence analyses) is provided, as applicable.

10 CFR 63.111 (Ref. 2.3.2) requires that the doses associated with Category 1 and Category 2 event sequences meet specific performance objectives. There are no performance objectives for beyond Category 2 event sequences. Dose consequences associated with each Category 1 and Category 2 event sequence are evaluated in preclosure consequence analyses, by comparison, to pre-analyzed release conditions (or dose categories) that are intended to characterize or bound the actual event sequences (Ref. 2.2.30). As such, the results of the event sequence analysis and categorization serve as inputs to the consequence analysis for assignment to dose categories.

#### 4.3.9 Event Sequence to Criticality Relationship

The requirements for compliance with preclosure safety regulations are defined in 10 CFR 63.112 (Ref. 2.3.2). Particularly germane to criticality considerations, is the requirement in 10 CFR 63.112, Paragraph (e) and Subparagraph (e)(6) (Ref. 2.3.2). Paragraph (e) requires an analysis to identify the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. This is a general requirement imposed on all event sequence analyses. Subparagraph (e)(6) specifically notes that the analyses should include consideration of "means to prevent and control criticality." The PCSA criticality analyses are the subject of specialized analyses that are beyond the scope of the event sequence analyses reported in the present calculation. However, the event sequence analyses serve as an input to the PCSA criticality analyses by identifying the event sequences and end states where conditions leading to criticality are in Category 1 or 2. As noted previously, some event sequence end states include the phrase "important to criticality." This indicates that the event sequence has a potential for



introduction of moderator and should be analyzed to determine if reactivity can exceed the Upper Subcriticality Limit (Ref. 2.2.31).

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

- It is bounded (i.e., its analyzed value is greater than or equal to the design limit) or its effect on  $k_{eff}$  is bounded and does not need to be controlled. This is designated as “No” in Table 4.3-1.
- It needs to be controlled if another parameter is not controlled (conditional control). This is designated as “Conditional” in Table 4.3-1.
- It needs to be controlled because it is the primary criticality control parameter. This is designated as “Yes” in Table 4.3-1.

The criticality control parameters analysis, which comprises the background calculations that led to Table 4.3-1, is presented in detail in the *Preclosure Criticality Safety Analysis* (Ref. 2.2.31). Event sequences that impact the criticality control parameters that have been established as needing to be controlled are identified, developed, quantified, and categorized. These event sequences are referred to as event sequences ITC. The following matrix elements, indicating the need for control, are treated in the current event sequence analysis:

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

Table 4.3-1. Criticality Control Parameter Summary

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

NOTE: <sup>a</sup> The *Preclosure Criticality Safety Analysis* (Ref. 2.2.31) considers bounding waste form characteristics. Therefore, there is no potential for a waste form misload.

<sup>b</sup> The *Preclosure Criticality Safety Analysis* (Ref. 2.2.31) considers nine representative DOE SNF types. Because the analysis is for representative types and loading procedures for DOE standardized SNF canisters have not been established yet, consideration of waste form misloads is not appropriate.

<sup>c</sup> Criticality safety design control features are not necessary for HLW canisters because the concentration of fissile isotopes in an HLW canister is too low to have criticality potential.

<sup>d</sup> Moderation is the primary criticality control parameter.

<sup>e</sup> Placing more than four DOE standardized SNF canisters outside the staging racks or a codisposal waste package needs to be controlled.

<sup>f</sup> Needs to be controlled only if moderator is present.

<sup>g</sup> Needs to be controlled only if the soluble boron concentration in the pool and transportation cask/dual purpose canister fill water is less than the minimum required concentration.

<sup>h</sup> Minimum required soluble boron concentration in the pool is 2500 mg/L boron enriched to 90 atom % <sup>10</sup>B.

DOE = U.S. Department of Energy; HLW = high-level radioactive waste; N/A = not applicable; SNF = spent nuclear fuel; WHF = Wet Handling Facility.

Source: *Preclosure Criticality Safety Analysis* (Ref. 2.2.31, Table 6)

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

#### 4.3.10.1 Boundary Conditions

The PCSA is limited to initiating events that constitute a hazard or challenge to a waste form in the GROA. Internal events (such as might occur during waste form handling or movement) and external events (such as seismic or high wind) are included when developing event sequences for the PCSA. However, initiating events that are associated with conditions introduced in SSCs before they reach the site (e.g., drops of casks, canisters, or fuel assemblies during loading at a reactor site, improper drying, closing, or inerting at the reactor site, rail accidents during transport, tornado missile strikes on a transportation cask) or during cask or canister manufacture (i.e., resulting in a reduction of containment strength) are not considered to be within the scope of the PCSA. The anticipation of such defects in SSCs is beyond the current state-of-practice, if

not the state-of-art. Such potential precursors are subject to deterministic regulations (e.g., 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4)) and the associated quality assurance programs. As a result of compliance to such regulations, the SSCs are deemed to pose no undue risk to health and safety. Although the analyses do not address quantitative probabilities, it is clear that conservative design criteria and quality assurance controls result in unlikely exposures to radiation. Other boundary conditions used in the PCSA are listed below.

- **Plant operational state.** Initial state of the facility is normal with each system operating within its vendor prescribed operating conditions.
- **No other simultaneous initiating events.** It is standard practice to not consider the occurrence of other initiating events (human-induced and naturally occurring) during the time span of an event sequence because (a) the probability of two simultaneous initiating events within the time window is small, and (b) each initiating event will cause operations to be terminated, further reducing the conditional probability of the occurrence of a second initiating event, given that the first has occurred.
- **Component failure modes.** The failure mode of a SSC corresponds to that required to make the initiating or pivotal event occur.
- **Use of SSCs that comply with NRC guidance.** Fundamental to the basis for the use of industry-wide reliability parameters within the PCSA, such as failure rates, is the use of SSCs within the GROA that conform to NRC accepted consensus codes and standards, and other regulatory guidance.

#### 4.3.10.2 Use of Engineering Judgment

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

10 CFR Part 63 (Ref. 2.3.2) does not specify analytical methods for demonstrating performance, estimating the reliability of ITS SSCs (whether active or passive), or calculating uncertainty. Instead, the risk-informed and performance-based preclosure performance objectives in 10 CFR Part 63 (Ref. 2.3.2) provide the flexibility to develop a design, and demonstrate that it meets performance objectives for preclosure operations, including the use of well established (discipline-specific) methodologies. As exemplified in the suite of risk-informed regulatory guides developed for 10 CFR Part 50 (Ref. 2.3.1) facilities (e.g., Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis* (Ref. 2.2.73), and “Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision Making: General Guidance” (Ref. 2.2.65, Section 19), such methodologies use deterministic and probabilistic inputs and analysis insights. The range of established techniques in the area of PRA, which is used in the PCSA, often relies on the use

of engineering judgment and expert opinion (e.g., in development of seismic fragilities and HEPs, and in the estimation of uncertainties).

As described in Section 4.3.3, for example, active SSC reliability parameters are developed using a Bayesian approach; and the use of judgment in expressing prior state-of-knowledge is a well-recognized and accepted practice (e.g., *Bayesian Reliability Analysis* (Ref. 2.2.56), “Pitfalls in Risk Calculations” (Ref. 2.2.4), NUREG/CR-6823 (Ref. 2.2.8), and NUREG/CR-2300 (Ref. 2.2.64)).

To provide guidance for compliance to 10 CFR 63.111 and 63.112 (Ref. 2.3.2), the NRC issued HLWRS-ISG-02 (Ref. 2.2.70). This document states that “treatment of uncertainty in reliability estimates may depend on the risk-significance (or reliance) of a canister system in preventing or reducing the likelihood of event sequences.” Furthermore, HLWRS-ISG-02 (Ref. 2.2.70) indicates that reliability estimates for high reliability SSCs may include the use of engineering judgment supported by sufficient technical basis; and empirical reliability analyses of a SSC could include values based on industry experience and judgment (Ref. 2.2.70).

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

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

#### **4.3.10.3 When Empirical Information is not Available**

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

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

1. The conditions associated with the consensus codes and standards and regulatory requirements are conservatively applicable to the GROA.
2. Equivalent quality assurance standards are applied at the GROA.
3. Operating processes are no more severe than those licensed under the aforementioned deterministic regulations.

#### **4.3.10.4 Use of Empirical Reliability Information**

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

#### **4.3.10.5 Use of Qualitative Information When Reliability Information is not Available**

In those cases where historical records of failures to support the PCSA are not available, qualitative information may be used to assign numerical failure probabilities and uncertainty. This approach is consistent with the Bayesian framework used in the PCSA, consistent with HLWRS-ISG-02 (Ref. 2.2.70), and involves the use of judgment in the estimation of reliability or failure probability values and their associated uncertainties. In these cases, the PCSA analyst may use judgment to determine probability and reliability values for components.

The following guidelines are used in the PCSA when it is necessary to use judgment to assess the probability of an event. The analyst selects a median at the point believed to be just as likely that the “true” value will lie above as below. Then, the highest probability value believed possible is conservatively assigned as a 95th percentile or error factor (i.e., the ratio of the 95th percentile to median), rather than a 99th or higher percentile, with justification for the assignments. A lognormal distribution is used because it is appropriate for situations in which the result is a product of multiple uncertain factors or variables. This is consistent with the “A Central Limit Theorem for Latin Hypercube Sampling” (Ref. 2.2.72). The lower bound, as represented by the 5th percentile, is checked to ensure that the distribution developed using the median and 95th percentile does not cause the lower bound to generate values for the variable that are unrealistic compared to the knowledge held by the analyst. In cases for which an upper and lower bound is defensible but no information about a central tendency is available, a uniform distribution between the upper and lower bound is used.

Another way in which risk-informed judgment is applied to obtain an appropriate level of effort in the PCSA, involves a comparison of event sequences. For example, engineering judgment readily indicates that a 30-foot drop of a canister onto an unyielding surface would do more damage to the confinement boundary than a collision of a canister with a wall at a crane speed of 20 feet per minute. A rigorous probabilistic structural analysis of the 30-foot drop is performed, and these results may be conservatively applied to the relatively benign slow speed collision.

## 5. LIST OF ATTACHMENTS

	<b>Number of Pages</b>
Attachment A Event Trees	69
Attachment B System/Pivotal Event Analysis – Fault Trees	96
Attachment C Active Component Reliability Data Analysis	51
Attachment D Passive Equipment Failure Analysis	92
Attachment E Human Reliability Analysis	70
Attachment F Fire Analysis	29
Attachment G Event Sequence Quantification Summary Tables	2
Attachment H Excel Spreadsheet, SAPHIRE Model, and Supporting Files	2 + CD

## 6. BODY OF ANALYSIS

The *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29), which identifies and describes the facilities, equipment, and operations encompassed by Intra-Site Operations and BOP, should be consulted in conjunction with the present analysis for understanding in context.

### 6.0 INITIATING EVENT SCREENING

The NRC's interim staff guidance for its evaluation of the level of information and reliability estimation related to the Yucca Mountain repository, *Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.70, p. 3), states that there are multiple approaches that can be used to estimate the reliability of SSCs that contribute to initiating events or event sequence propagation (i.e., pivotal events), including the use of judgment. 10 CFR 63.102(f) (Ref. 2.3.2) provides that initiating events are to be considered for inclusion in the PCSA for determining event sequences only if they are reasonably based on the characteristics of the geologic setting and the human environment, and are consistent with the precedents adopted for nuclear facilities with comparable or higher risks to workers and the public.

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

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

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

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



## **6.0.1 Boundary Conditions for Consideration of Initiating Events**

### **6.0.1.1 General Statement of Boundary Conditions**

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

### **6.0.1.2 Specific Discussion of Receipt of Properly Dried SNF Canisters**

Under the boundary conditions stated for this analysis, canisters shipped to the repository in transportation casks are received in the intended internally dry conditions. Shipments of SNF received at the repository, whatever their origin, are required to meet the requirements of 10 CFR Part 71 (Ref. 2.3.3). In addition to 10 CFR 71 (Ref. 2.3.3, Section 71.71, (c)(4)), NUREG-1617 (Ref. 2.2.67) provides guidance for the NRC safety reviews of packages used in the transport of SNF under 10 CFR Part 71 (Ref. 2.3.3). The review guidance, NUREG-1617 (Ref. 2.2.67, Section 7.5.1.2), instructs reviewers that, at a minimum, the procedures described in the safety analysis report should ensure that:

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

NUREG-1536 (Ref. 2.2.66, Chapter 8, Section V) refers to an acceptable process to evacuate water from SNF canisters. Following this process results in no more than approximately 0.43 gram-mole (about 8 grams) of water left in the canister when adequate vacuum drying is performed (Ref. 2.2.66, Chapter 8, Section V, Item 1). The following example is cited as providing adequate drying (Ref. 2.2.66, Chapter 8, Section V, Item 1):

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

If the pressure creeps back up to an unacceptable level during the 30-minute evaluation time, or in cases where it is important to control oxidant concentrations or achieve needed process reliability improvements, a further step may be performed as follows (Ref. 2.2.66, Chapter 8, Section V).

The cask is then re-evacuated and re-backfilled with inert gas before final closure. Care should be taken to preserve the purity of the cover gas and, after backfilling, cover gas purity should be verified by sampling.

The procedure described appears to ensure that very little water is left behind. However, the probability of undetected failure when performing the process is not addressed in the deterministic regulation 10 CFR Part 71 Energy: Packaging and Transportation of Radioactive Material (Ref. 2.3.3) or in NUREG-1536 (Ref. 2.2.66). Indeed, there is no after-the-fact water or error detection method in NUREG-1536 or the regulation. Therefore, some unknown number of canisters may arrive in the GROA with more residual water than is expected with proper drying. Because the canisters are welded and are not required to provide for sampling the inside of the canister, nondestructive measurement of the residual water content would be difficult. The following discussion provides reasonable assurance that no significant risks are omitted from the analysis due to adoption of the boundary condition that canisters shipped to the repository in transportation casks are received in the intended internally dry conditions:

1. The YMP accepts, handles, and emplaces TAD canisters in a manner consistent with the specifications laid out in the TAD canister system performance specification (Ref. 2.2.37), which prescribes the use of consensus codes and standards along with design requirements associated with GROA-specific event sequences.
2. **Criticality.** GROA operating processes are similar to those of nuclear power plant sites with respect to the use of cranes, and there are no processes or conditions that would exacerbate adverse effects associated with abnormal amounts of water retention. Event sequences involving drop and breach of a SNF canister are beyond Category 2 as shown in Section 6.8. To receive a license to transport SNF, 10 CFR 71.55 (Ref. 2.3.3) requires the licensee to demonstrate subcriticality given that “the fissile material is in the most reactive credible configuration consistent with the damaged condition of the package and the chemical and physical form of the contents” under the hypothetical accident conditions specified in 10 CFR 71.73 Energy: Packaging and Transportation of Radioactive Material (Ref. 2.3.3). Drop events, which are unlikely to breach the canister, are also unlikely to impart sufficient energy to the fuel to reconfigure it so dramatically that criticality would be possible even if water is present. It is concluded that existing regulations that apply to the canister and transportation cask for transportation to the repository provide reasonable assurance that a criticality event sequence that depends on the presence of water inside the canister and reconfiguration of the fuel would not occur under conditions that could reasonably be achieved during handling at the repository.
3. **Hydrogen explosion or deflagration.** Radiation from SNF can generate radiolytic hydrogen and oxygen gas in a SNF canister if water is inadvertently left in the canister before it is sealed. Given a processing error that leaves enough residual water, the gas concentrations could conceivably reach levels where a deflagration event could occur. However, precautions taken at the generator sites are expected to make receipt of a canister that was improperly dried unlikely. In addition, an ignition source would be required for an explosion or deflagration to occur. High electrical conductivity of the metal canister would dissipate any high voltage electrical discharge (which is unlikely

in any case) and preclude arcing within the canister. Normal handling operations do not subject the canisters to energetic impacts that could cause frictional sparking inside the canister. Therefore, a further unlikely event, such as a canister drop would have to occur to ignite the gas. Considering the combination of unlikely events that must occur, event sequences involving this combination of failures are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.

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

## 6.0.2 Screening of External Initiating Events

### 6.0.2.1 Initial Screening of External Initiating Events

The *External Events Hazards Screening Analysis* (Ref. 2.2.26) identifies potential external initiating events at the repository for the preclosure period and screens a number of them from further evaluation based on severity or frequency considerations. The four questions that constitute the evaluation criteria for external events screening are:

1. Can the external event occur at the repository?
2. Can the external event occur at the repository with a frequency greater than 1E-06/yr, that is, have a 1 in 10,000 chance of occurring in the 100-year preclosure period?
3. Can the external event, severe enough to affect the repository and its operation, occur at the repository with a frequency greater than 1E-06/yr, that is, have a 1 in 10,000 chance of occurring in the 100-year preclosure period?
4. Can a release that results from the external event severe enough to affect the repository and its operations occur with a frequency greater than 1E-06/yr, that is, have a 1 in 10,000 chance of occurring in the 100-year preclosure period?

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

As noted in Table 6.0-1, the potential external initiating event categories that are retained for further evaluation are seismic activity and loss of power. Seismically induced event sequences are developed, categorized, and documented in a separate analysis. Loss of power is analyzed separately for facility impact but is not an initiating event for Intra-Site Operations (Section 6.0.9).

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

External Event Category	Retention Decision. If Not Retained, Basis for Screening.
Seismic activity	YES. Retained for further analysis. <sup>1</sup>
Nonseismic geologic activity	NO. Except for drift degradation, the external events in this category are not applicable to the site or do not occur at a rate that could affect the repository during the preclosure period. The chance of drift degradation severe enough to affect the repository and its operation over the preclosure period is less than 1/10,000.
Volcanic activity	NO. The chance of volcanic activity occurring at the repository over the preclosure period is less than 1/10,000.
High winds / tornadoes	NO. The chance of a high wind or tornado event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
External floods	NO. The chance of a flood event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Lightning	NO. The chance of a lightning event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Loss of power event	YES. Retained for further analysis. Facility event sequence categorization analyses provides disposition. <sup>2</sup>
Loss of cooling capability event	NO. The primary requirements for cooling water at the Yucca Mountain site during the preclosure period are makeup water for the WHF pool and cooling of HVAC chilled water. The chance of a loss of cooling capability occurring at the repository over the preclosure period is less than 1/10,000.
Aircraft crash	NO. The chance of an accidental aircraft crash occurring at the repository over the preclosure period is less than 1/10,000.
Nearby industrial/military facility accidents	NO. The chance of an industrial or military facility accident occurring at the repository over the preclosure period is less than 1/10,000.
Onsite hazardous materials release	NO. The chance of an accident event sequence initiated by the release of onsite hazardous materials at the repository over the preclosure period is less than 1/10,000.
External fires	NO. The chance of an external fire severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Extraterrestrial activity	NO. Extraterrestrial activity is defined as an external event involving objects outside the earth's atmosphere and enters the earth's atmosphere, survive the entry through the earth's atmosphere and strike the surface of the earth. Extraterrestrial activity includes: meteorites, asteroids, comets, and satellites. The chance of an occurrence at the repository over the preclosure period is less than 1/10,000.

NOTE: <sup>1</sup>Seismic events are analyzed separately.

<sup>2</sup>Loss of power events do not affect Intra-Site Operations in a way that threatens a waste container.  
HVAC = heating, ventilation, and air conditioning; WHF = Wet Handling Facility.

Source: Adapted from (Ref. 2.2.26, Sections 6 and 7).

### 6.0.3 Screening of Internal Initiating Events

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

Potential initiating events were qualitatively identified in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29) for quantitative treatment in the present analysis. For completeness, some events that were identified in the event sequence development analysis are extremely unlikely or physically unrealizable and reasonably can be qualitatively screened from further consideration. A qualitative screening argument for certain internal initiating events is developed in the present analysis as documented in Table 6.0-2. The first column of Table 6.0-2 indicates the branch of the IET (where applicable) that pertains to the screened initiating event. Each branch of an IET represents an initiating event or an initiating event group that includes other similar initiating events and corresponds to a small circle on an ESD (Ref. 2.2.29, Attachments F and G). Some of the initiating events that are addressed in Table 6.0-2 were implicitly screened out in the event sequence development analysis, and for that reason there is no applicable event tree. The screening argument for internal flooding is presented in Section 6.0.4. Sections 6.0.4 and 6.0.5 provide detailed screening arguments for internal flooding and diesel fuel oil tank explosions, which are too long for inclusion in Table 6.0-2.

Table 6.0-2. Bases for Screening Internal Initiating Events

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
ISO-ESD05-LLWLIQ (Branch 3)	Impact to a single (liquid) LLW container	Liquid LLW release for this event is not analyzed for categorization because the consequences to a worker for this type of release are a small fraction of the performance objectives. It is classified as an off-normal event in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Appendix IV).
ISO-ESD06-LLW (Branch 3)	Non-fire event involving all LLW containers	Collapse of the LLWF due to a seismic event is analyzed for consequence in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Table 2, Section 6.3.4, and Section 6.8.1), and is bounding. No further analysis for collapse of the LLWF is needed.
ISO-ESD08- LLWLIQ, (Branches 3, 4, and 5)	Structural challenges to a Liquid LLW container or containment boundary during transfer from GROA facilities, resulting in an unfiltered radiological release due to impact or to equipment failure.	Liquid LLW release for this event is not analyzed for categorization, because the consequences to a worker for this type of release are a small fraction of the performance objectives. It is classified as an off normal event in <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Appendix IV)

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
ISO-ESD01-HLW (Branch 4) ISO-ESD01-MCO (Branch 4) ISO-ESD01-DSTD (Branch 4) ISO-ESD01-UCSNF (Branch 4)	Truck trailer collision leading to rollover/drop of transportation cask	PEFA values described in Section 6.3.2.2 and Attachment D, Section D1 do not account for buffer cars and impact limiters, which are always in place for Intra-Site Operations activities. This value is overly conservative, as detailed in Section 6.0.6.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened from further analysis. Section 6.0.4 provides the detailed screening argument.
No applicable event trees	Tipover of site transporter	<p>The site transporter is a crawler-type vehicle with four tank-type treads designed to preclude tipover. The size and weight of a loaded site transporter, along with the low center of gravity, precludes tipover if hit by a general service vehicle, the forces for which would be enveloped by the seismic spectrum described in the sliding/rocking calculation (Ref. 2.2.17). If impacted by another mover (cask tractor, site prime mover, or other site transporter), tipover would still be precluded because all of these vehicles are mechanically speed limited to reduce the frequency of severity of collisions (Ref. 2.2.20, Sections 3.2.1 and 3.2.2).</p> <p>The routes defined in <i>GROA North Portal Site Plan</i> and <i>GROA Aging Pad Site Plan</i> are evenly graded across gentle terrain (Ref. 2.2.28) and (Ref. 2.2.27) and are paved or compacted aggregate. Employing standard construction practices ensures that any culverts required along the transportation paths are barricaded to prevent vehicles from driving off at those points. Therefore, tipover of a site transporter is not analyzed further for categorization.</p>
No applicable event trees	Site transporter, cask tractor, cask transfer trailer collisions at speeds in excess of 2.5 mph	The site transporter, cask tractor, and cask transfer trailer are designed with speed limiters (Ref. 2.2.20, Section 2.2) and (Ref. 2.2.25, Section 3.2.3).
No applicable event trees	SPM collisions at speeds in excess of 9 mph in the GROA	The SPM is used to move waste containers in casks similar to or the same as casks moved by the cask tractor/cask transfer trailer. A design requirement of 9 mph is applied to the SPM (Table 6.9-1). It is reasonable to apply similar design requirements, such as speed limiters, as on other vehicles that are used to transport waste containers in the GROA, in order to reduce the severity of collisions (Ref. 2.2.20); (Ref. 2.2.25); (Ref. 2.2.14); (Ref. 2.2.17); and (Ref. 2.2.15).
No applicable event trees	High-speed collisions	YMP vehicles involved in the movement of waste containers are speed limited to reduce frequency and severity of collisions. Traffic control is also established to limit the speed of vehicles other than waste container transporters or conveyances operating in the vicinity of roads and areas used for waste container transit.

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Cask transfer trailer punctures HTC, HSTC, or HDPC	The ram unit on the cask transfer trailer is designed such that the ram is positioned to preclude puncture of the HTC or HSTC during a collision or seismic event. In addition, the ram is designed to have insufficient force to deform a DPC (Ref. 2.2.25, Table 1); (Ref. 2.2.14); and (Ref. 2.2.15). Therefore, further consideration of this initiating event is not required.
No applicable event trees	Fuel tank explosion involving site transporter, cask tractor, cask transfer trailer, or SPM	Fuel tank design for equipment used to move casks or aging overpacks containing high-level waste shall include a requirement for the tank construction to use a low-temperature melt material. The low-temperature melt material precludes tank explosion as an initiating event. Therefore, fuel tank explosions for these movers are not analyzed further for categorization.
No applicable event trees	Floods affecting areas within the GROA	Flood controls will divert up to 55,000 cubic feet per second. These controls are required to divert a flood capacity of 40,000 cubic feet per second measured at the hydrological concentration point (identified as Collection Point 9 in <i>Yucca Mountain Project Drainage Report and Analysis</i> (Ref. 2.2.24, Table 7-1), which is the external flood event analyzed in the <i>External Events Hazards Screening Analysis</i> (Ref. 2.2.26)). The frequency of exceeding 40,000 cubic feet per second is less than 1E-06 per year (Ref. 2.2.24 and Ref. 2.2.26). Refer also to Table 6.0-1, above.
No applicable event trees	Blocked vents on aging overpack or HAM cause overheating	In NUREG-1864 (Ref. 2.2.11, p. 4-14), the NRC analyzed the maximum canister temperature that would result from blockage of all storage overpack vents. The analysis shows that vent blockage results in a maximum canister temperature that is hundreds of degrees below the temperature at which the canister would fail (canister failure temperature is analyzed in Attachment D, Section D2). The storage overpack and canister configuration analyzed in the NUREG report are very similar to the YMP canister and aging overpack configuration, so these results can be applied in the PCSA. Though the canister would remain well below its failure temperature and failure would be precluded, a conservative failure probability of 1E-06 is used in the PCSA.  Due to design differences, complete blockage of HAM vents is much less likely to occur than in aging overpacks. However, if such a blockage were to occur, the large thermal capacity of the surrounding concrete would result in a similarly low maximum canister temperature and canister failure probability.  Canister overheating that leads to breach due to blocked vents is, therefore, not analyzed further for categorization.
No applicable event trees	Diesel fuel oil tank (Area 70A) or tanker truck explodes	The facility layout is such that the waste handling facilities and the waste container transportation paths are well beyond the estimated stand-off distance for these explosions (Ref. 2.2.28) and (Ref. 2.2.27). Estimated stand-off distances are provided in Table 6.0-5.

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	Moderator intrusion into a transportation cask containing uncanistered CSNF breached due to a thermal challenge	The breach path created due to a thermal challenge would not permit intrusion of moderator for a transportation cask (Section 6.0.7 provides a detailed discussion).
No applicable event trees	Thermal challenge to uncanistered CSNF in a transportation cask results in direct exposure of personnel or unfiltered release of radionuclides	The probability of fuel rod failure (in a transportation cask) at 750°C combined with frequency of a fire event in the buffer area during Intra-Site Operations activities is about 8E-05 (Section 6.0.8 provides a detailed discussion).
No applicable event trees	Loss of power causes equipment failure leading to direct exposure of personnel or unfiltered release of radionuclides	Activities associate with Intra-Site Operations occur outside of waste handling facilities. Failure of AC power to equipment during Intra-Site Operations activities does not result in an initiating event (Section 6.0.9 provides a detailed discussion).

NOTE: Initiator event trees, with branch numbers shown, are provided in Attachment A.

AC = alternating current; °C = degree Celsius; CSNF = commercial spent nuclear fuel; DPC = dual-purpose canister; GROA = geologic repository operations area; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; NRC = U.S. Nuclear Regulatory Commission; NUREG = Nuclear Regulation (U.S. Nuclear Regulatory Commission); PCSA = preclosure safety analysis; PEFA = passive equipment failure analysis; SPM = site prime mover; YMP = Yucca Mountain Project.

Source: Original



#### **6.0.4 Screening of Flooding as an Initiating Event for Intra-Site Operations**

Transportation casks and canisters are not physically susceptible to short-term effects of flood water. Therefore, flood water from sources other than the external events analyzed separately (Ref. 2.2.26) cannot breach a transportation cask or canister. Drains, ordinary housekeeping practices, evaporation, and relatively short handling times ensure that corrosion does not threaten the integrity of the containers over the longer term of the preclosure period.

As indicated in Table 6.0-1, external flooding events that might affect site transportation activities within the GROA and Aging Facility activities are screened from further analysis (Table 6.0-1, “Retention Decisions from External Events Screening Analysis”). No significant source of water exists at the Aging Facility, and water supply line breaks (e.g., damage to a fire hydrant or failure of water main) would not provide a sufficient amount of water or sufficient force to damage a transportation cask. Design and total mass of a transportation cask on conveyance, an aging overpack on a site transporter, or a cask on a cask transfer trailer is sufficient to preclude an initiating event of this type of flooding that would lead to a breach of a cask or canister. (Similarly, internal flooding to the drifts is also screened from further analysis.) Moderator intrusion into canisters resulting from Intra-Site Operations event sequences that might breach a waste container are treated quantitatively, as described in the pivotal event descriptions of Section 6.2.

#### **6.0.5 Screening of Diesel Fuel Oil Storage Tank (Area 70A) and Tanker Truck Explosions**

The following provides an assessment of a potential explosion in diesel fuel oil resupply trucks or in the diesel fuel storage tank (Area 70A), in order to determine if the possible truck routes and the Area 70A tank are situated a safe distance from the waste handling facilities and other SSCs such that no event sequences result from such an explosion. The increased external pressure generated by such an explosion is a function of the amount of explosive material and the distance between the site of the deflagration and the target (i.e., waste container or waste handling facility).

The parameters defined in Table 6.0-3 are used for the purpose of conservatively estimating the hazards associated with a diesel fuel vapor cloud explosion in a diesel fuel oil storage tank in Area 70A or in a tanker truck used for resupplying the tank in Area 70A. These parameters are appropriate to provide a conservative and bounding estimation of the hazards associated with such explosions.

Table 6.0-3. Parameters Used to Estimate Stand-Off Distances for Explosion Involving the Area 70A or a Tanker Truck

Parameter No.	Parameter Description	Applicable Equation No(s).	Input Value
6.0.5-1	A vapor cloud explosion occurs within the vapor space of the diesel storage tank, regardless of the ignition source.  Vapor cloud explosions may occur in unconfined areas, although some degree of congestion is still required. Vapor cloud explosions can only occur in relatively large gas clouds (Ref. 2.2.60, p. 49). An ignition source is required to ignite such a vapor cloud, however, none is specified, because it is evaluated as if ignition is a given event.	—	—
6.0.5-2	The pressure in the vapor space above the tank is approximately atmospheric pressure.  Bulk diesel fuel tanks are commonly vented. Therefore, the vapor mixture in the vapor space above the liquid in the tank will not be pressurized.	Eq. 21	P=101,325 Pa, equivalent to approximately <b>P=14.70 psi</b> (Ref. 2.2.88, p. F-335)
6.0.5-3	The temperature in the vapor space above the liquid in the storage tank is approximately equal to the flash point typical for a low-sulfur diesel fuel blend.  The flash point of a liquid corresponds roughly to the lowest temperature at which the vapor pressure of the liquid is just sufficient to produce a flammable mixture at the lower limit of flammability (Ref. 2.2.33, p. 5-31). For this reason, the flash point was chosen as the temperature of the diesel fuel–air vapor mixture within the tank. This is conservative and bounding.	Eq. 21	T <sub>F</sub> =140°F, equivalent to approximately <b>T<sub>R</sub>=600°R</b> (Ref. 2.2.52, p. 2)
6.0.5-4	The diesel fuel vapor concentration is equal to the UFL for diesel fuel, which is 7.0%.  The UFL and LFL for diesel fuel will vary depending on the concentrations of the components that comprise the grade of the fuel. A typical LFL for a low-sulfur diesel fuel is 0.9%; the UFL for the blend analyzed is 7.0% (Ref. 2.2.52). To provide a bounding quantity of diesel fuel in the diesel fuel–air vapor mixture, the UFL concentration of 7.0% is used.	Eq. 22	<b>0.07</b> (Ref. 2.2.52, p. 2)
6.0.5-5	The space filled by the diesel fuel vapor is equivalent to the tank capacity.  Under normal circumstances, the storage tank and tanker will always have liquid remaining, and a vapor mixture of diesel fuel and air will occupy the tank in the area above the liquid (including the freeboard area above the liquid). In order to conservatively estimate bounding TNT equivalencies for the diesel fuel vapor in the storage tank and in the tanker truck, the vapor mixture for each is calculated as if it occupies the equivalent volume of the liquid capacity.	Eq. 21	120,000 gal equivalent to approximately <b>16,044 ft<sup>3</sup></b> for the Area 70A storage tank (Ref. 2.2.18, p. 1)  10,000 gal, equivalent to approximately <b>1,337 ft<sup>3</sup></b> for the tanker truck

Table 6.0-3. Parameters Used to Estimate Stand-Off Distances for Explosion Involving the Area 70A or a Tanker Truck (Continued)

Parameter No.	Parameter Description	Applicable Equation No(s).	Input Value
6.0.5-6	<p>The molecular weight of diesel fuel is equivalent to that of JP-5 jet fuel.</p> <p>The molecular weight of diesel varies with carbon and hydrogen content. Jet fuel JP-5, which is in the same family of gas oils or fuel oils as diesel, has a similar specific gravity and heat of combustion (0.83 and 43.0 MJ/kg, respectively (Ref. 2.2.77, p. A-36) as compared to a typical blend of diesel fuel (0.83 to 0.86) (Ref. 2.2.52, p. 4) and 44.4 MJ/kg (Ref. 2.2.50, p. 3-6), respectively. The JP-5 molecular weight used to represent diesel fuel oil in the estimation is 170 lb/lb-mol (Ref. 2.2.77, p. A-36)</p>	Eq. 22	<b><i>mw</i> = 170 lb/lb-mol</b>
6.0.5-7	<p>There is sufficient oxygen present in the vapor space to ensure complete combustion of the diesel fuel vapor present.</p> <p>This is conservative and provides for a maximum TNT equivalent value. In reality, imperfect combustion occurs during accidental fires and explosion incidents, mainly due to turbulence, low supply of oxidizer, and other factors that produce free carbon particles (smoke), carbon monoxide, and the like (Ref. 2.2.60, p. 45).</p>	—	—
6.0.5-8	<p>The nominal empirical explosion efficiency, <math>\eta</math>, is 0.03.</p> <p>Estimating the effects of a diesel fuel vapor explosion inside of a bulk storage tank or tanker truck requires the knowledge of the efficiency of the explosion, as shown in Equation 20. The value of the explosion efficiency depends on the method used to determine the contributing mass of fuel (Ref. 2.2.2, p. 165). A value of 0.03 is adequate when the explosion is based on the quantity of fuel present in the vapor cloud, which is the approach followed. The efficiency of the explosion is dependent on the reactivity of the material, with higher reactivity giving a higher efficiency. Highly reactive materials are assigned higher efficiencies: an efficiency of 10% for diethyl ether, 5% for propane, and 15% for acetylene (Ref. 2.2.2, p. 165). Therefore, a nominal efficiency of 3% and a maximized case of 100% appear adequate.</p>	Eq. 20	<b>0.03 (nominal) 1 (maximum)</b>

NOTE: °F = degree Fahrenheit; ft<sup>3</sup> = cubic foot; gal = gallon; lb = pound; lb-mol = pound-mole; LFL = lower flammable limit; MJ = megajoules per kilogram; mw = molecular weight; Pa = Pascal; psi = pounds per square inch; °R = degree Rankine; TNT = trinitrotoluene; UFL = upper flammable limit.

Source: Original

In addition to the parameters identified in Table 6.0-3, the inputs shown in Table 6.0-4 are used to estimate the pressure pulse generated by the combustion of diesel fuel.

Table 6.0-4. Additional Inputs Used for Quantitative Evaluation of a Fuel Tank Explosion

Input	Numerical Value/ Characteristic	Applicable Equation No(s).	Comment
Gas constant	10.73 ft <sup>3</sup> psi °R <sup>-1</sup> lb-mol <sup>-1</sup>	Eq. 21	This value is used to calculate the number of moles of fuel vapor contained in the tank, using the ideal gas law, which is an appropriate approximation of the behavior of gases for the quantitative evaluation provided. (Ref. 2.2.88)
Heat of combustion of TNT	1,943 BTU/lb	Eq. 20	This value is the lower bound of a range of TNT heat combustions given in AIChE ((Ref. 2.2.2), p. 160). By taking the lower value of the range, the vapor cloud in the storage tank has a calculated equivalent TNT mass greater than if a higher value from the range was used, based on the use of this value in Equation 20. The use of this value is conservative.
Heat of combustion of diesel fuel	44.4 MJ/kg (equivalent to 19,089 BTU/lb)	Eq. 20	This value varies depending on the grade of diesel; however, it is typical of those reported in literature. (Ref. 2.2.50, p. 3-6)
Design criteria for transportation cask	20 psi	N/A (used to evaluate stand-off distances)	Transportation casks are designed for the effects of increased external pressure equal to 20 psi (Ref. 2.2.67, Section 2.5.5.4) and (Ref. 2.3.3, Section 71.71, (c)(4)).
Waste handling facility structure design	1 psi	N/A (used to evaluate stand-off distances)	Waste handling facilities are evaluated for distance based on an increased external pressure of 1 psi (Ref. 2.2.74).

NOTE: 1 J = 9.4782E-4 BTU and 1 lb = 0.4536 kg.  
BTU = British Thermal Unit; ft<sup>3</sup> = cubic foot; kg = kilogram; lb = pound; lb-mol = pound-mole; MJ = megajoule; N/A = not applicable; psi = pound per square inch; °R = degree Rankine; TNT = trinitrotoluene.

Source: Original

The term *explosion*, in its most widely accepted sense, means a bursting associated with a loud, sharp noise and an expanding pressure front, varying from a supersonic shock wave to a relatively mild wind (Ref. 2.2.33, p. 4-17). A combustible vapor explodes under a very specific set of conditions. There are two explosive mechanisms that need to be considered when evaluating combustible vapor incidents: detonations and deflagrations. A detonation is a shock reaction where flames travel at supersonic speeds (i.e., faster than sound). Flames travel at subsonic speeds in a deflagration. It is generally recognized that vapor cloud explosions have flames that travel at subsonic speeds and are, therefore, technically classified as deflagrations but are still commonly referred to as explosions (Ref. 2.2.60, p. 48). Therefore, the postulated events in this analysis involve a vapor cloud explosion (deflagration) in Area 70A and in the diesel fuel tanker truck. The following three elements must exist simultaneously in order for a deflagration to occur:

1. A flammable mixture consisting of fuel and oxygen, usually from air, or other oxidant.
2. A means of ignition.
3. An enclosure.

The scenario analyzed includes the ignition of vapors in a tank, regardless of the cause or source of ignition (Table 6.0-3, Parameter 6.0.5-1). There is sufficient oxygen in the air present in the

vapor mixture to act as an oxidizer and completely combust the diesel fuel present such that a bounding trinitrotoluene (TNT)-equivalent value is calculated for the deflagration (Table 6.0-3, Parameter 6.0.5-7).

With proper safety precautions and operating procedures, the occurrence of explosions in the vapor space of fixed-roof storage tanks or tanker trucks are rare events. Explosive mixtures may exist in the vapor space of a tank unless precautions are taken. Any vapor will seek an ignition source, so prevention of ignition cannot be guaranteed (Ref. 2.2.60, pp. 155-156).

The methods applied are based upon *Guidelines for Chemical Process Quantitative Risk Analysis* (Ref. 2.2.2), used to calculate TNT equivalencies and *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44), used to determine the increased external pressure at a given distance. Damages to structures and process equipment of a facility are dependent on the pressure generated by the explosion (Ref. 2.2.2, Tables 2.18a and 2.18b). To calculate the increased external pressure, TNT-equivalency is used. This postulates an equivalency between the flammable material and TNT, factored by an explosion efficiency term. This method is appropriate for this assessment because refined values of the damages caused by the explosion are not required, but rather reasonable estimates.

The following formula (Equation 20) is used to determine the TNT-equivalent values for the 120,000-gal tank (Area 70A) and the 10,000-gal tanker truck (Ref. 2.2.2, pp. 159 and 160):

$$W = \frac{\eta M E_c}{E_{TNT}} \quad (\text{Eq. 20})$$

where

- $W$  = equivalent mass of TNT, in lb
- $\eta$  = empirical explosion efficiency, unitless
- $M$  = mass of hydrocarbon, in lb
- $E_c$  = heat of combustion of flammable gas, in BTU/lb
- $E_{TNT}$  = heat of combustion of TNT, in BTU/lb.

Hydrocarbon materials must first be in a vapor condition before combustion processes can occur. Consequently, the mass,  $M$ , of hydrocarbon is the mass of the diesel fuel in the diesel fuel–air vapor mixture in the storage tank and can be calculated using Equation 22, below. It is conservative to calculate the diesel fuel–air vapor mixture as if it occupies a volume equal to the entire tank capacity, which is 16,044 ft<sup>3</sup> for Area 70A, and 1,337 ft<sup>3</sup> for the tanker truck (Table 6.0-3, Parameter 6.0.5-5). In reality, each tank will always have a quantity of liquid diesel fuel present, with the diesel fuel–air vapor occupying the volume above the liquid, including the tank freeboard volume. However, considering the entire capacity to be available provides for a maximum value of the TNT-equivalent for the deflagration. The quantity,  $M$ , is calculated as a product of the total mass of the vapor mixture, the molecular weight, and the percent concentration.

To obtain the total mass of the diesel fuel–air vapor mixture (in lb-mol), Equation 21 is used. The pressure in the vapor space is evaluated as equivalent to atmospheric pressure, 14.70 psi, because such tanks are typically vented (Table 6.0-3, Parameter 6.0.5-2). The temperature in the vapor space is equivalent to a typical flash point of diesel fuel, 600°R (Table 6.0-3, Parameter 6.0.5-3). Using the stated volume for each container and the ideal gas law (Ref. 2.2.88, p. F-249), the mass of the diesel fuel–air vapor mixture,  $n_{tot}$  is calculated for Area 70A and for the tanker truck as:

$$n_{tot} = \frac{PV}{RT} \quad (\text{Eq. 21})$$

where

- $n_{tot}$  = total mass of the diesel fuel–air vapor mixture, in lb-mole
- $P$  = pressure of diesel fuel–air vapor cloud, in psi
- $V$  = volume of diesel fuel–air vapor cloud, in cubic feet
- $R$  = universal gas constant, in  $\text{ft}^3 \cdot \text{psi} / \text{lb-mole} \cdot \text{R}^\circ$
- $T$  = temperature of diesel fuel–air vapor cloud, in  $\text{R}^\circ$

Therefore, for Area 70A,

$$n_{tot} = \frac{(14.70 \text{ psi})(16,044 \text{ ft}^3)}{(10.73 \text{ ft}^3 \cdot \text{psi} / \text{R}^\circ \cdot \text{lb - mole})(600^\circ \text{R})}$$

$$n_{tot} = 36.6 \text{ lb - mole}$$

and for the tanker truck,

$$n_{tot} = \frac{(14.70 \text{ psi})(1,337 \text{ ft}^3)}{(10.73 \text{ ft}^3 \cdot \text{psi} / \text{R}^\circ \cdot \text{lb - mole})(600^\circ \text{R})}$$

$$n_{tot} = 3.1 \text{ lb - mole}$$

As described in Parameter 6.0.5-4 (Table 6.0-3), the diesel fuel concentration,  $c$ , is equal to the UFL for diesel fuel, which is typically 7.0%. If the concentration of diesel fuel were in the intermediate range between the LFL and UFL, the ignition would be more intense and violent than if the mixture were closer to either the upper or lower limits; however, to maximize the TNT-equivalent values, the upper limit is chosen. The molecular weight of the diesel fuel is approximated to be equivalent to that for JP-5, that is, 170 lb/lb-mol (Table 6.0-3, Parameter 6.0.5-6). Using the mass of the diesel fuel–air vapor mixture ( $n_{tot}$ ) calculated for each tank size, the mass of hydrocarbon,  $M$ , can be calculated using Equation. 22, as follows:

$$M = c n_{tot} mw \quad (\text{Eq. 22})$$

where

- $M$  = mass of diesel fuel in the vapor, in lb
- $c$  = diesel fuel concentration percentage, unitless
- $n_{tot}$  = total mass of the diesel fuel–air vapor mixture, in lb-mole
- $mw$  = molecular weight of the diesel fuel, in lb/lb-mole

Therefore, for Area 70A,

$$M = (0.07)(36.6 \text{ lb – mole})(170 \text{ lb/lb – mole})$$

$$M = 435.5 \text{ lb}$$

and for the tanker truck,

$$M = (0.07)(3.1 \text{ lb – mole})(170 \text{ lb/lb – mole})$$

$$M = 36.9 \text{ lb}$$

Equation 20 can now be used to calculate the TNT-equivalent of a deflagration involving 435.5 lb of diesel fuel in the vapor mixture for Area 70A and a deflagration of 36.9 lb for the tanker truck. The values of the heat of combustion for TNT and diesel fuel are  $E_{TNT} = 1,943 \text{ BTU/lb}$  and  $E_c = 19,089 \text{ BTU/lb}$ , respectively (Table 6.0-4). The value of the explosion efficiency,  $\eta$ , is described in Table 6.0-3, parameter 6.0.5-8, with a nominal value of 3% (0.03) and maximized case of 100% (1.0).

Applying Equation 20 for the nominal case for Area 70A:

$$W = \frac{\eta M E_c}{E_{TNT}}$$

$$W = \frac{(0.03)(435.5 \text{ lb})(19,089 \text{ BTU/lb})}{1,943 \text{ BTU/lb}}$$

$$W = 128.4 \text{ lb}$$

Therefore, for the nominal case ( $\eta = 0.03$ ), the equivalent mass of TNT,  $W$ , is calculated to be 128.4 lb for Area 70A. For the maximized case ( $\eta = 1.0$ ), the value is 4278.6 lb.

Applying Equation 20 for the nominal case for the tanker truck:

$$W = \frac{\eta M E_c}{E_{TNT}}$$

$$W = \frac{(0.03)(36.9 \text{ lb})(19,089 \text{ BTU/lb})}{1,943 \text{ BTU/lb}}$$

$$W = 10.9 \text{ lb}$$

Therefore, for the nominal case ( $\eta = 0.03$ ), the equivalent mass of TNT,  $W$ , is calculated to be 10.9 lb for the tanker truck. For the maximized case ( $\eta = 1.0$ ), the value is 362.5 lb.

The safe distance in regards to the increased external pressure from a postulated explosion is evaluated based on 10 CFR Part 71, Subpart F (Ref. 2.3.3), and Regulatory Guide 1.91, *Evaluations of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plants* (Ref. 2.2.74), NUREG-1617 (Ref. 2.2.67), and *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44, p. 45). For the waste handling facilities and Area 70A, the safe distance is based on a level of peak positive incident overpressure below which no significant damage would be expected. Based on Regulatory Guide 1.91 (Ref. 2.2.74) a pressure level of 1 psi is used to determine a safe distance for the waste handling facilities. For the transportation casks outside of a facility, 20 psi is used to assess the safe distance, based on NUREG-1617 and 10 CFR Part 71 (Ref. 2.2.67 and Ref. 2.3.3).

To calculate the distance in feet from the explosion to a point at which the increased external pressure measures 20 psi and 1 psi for each of the explosion scenarios, the following equation (Equation 23) was used *Handbook of Chemical Hazard Analysis Procedures* (Ref. 2.2.44). The equation is valid for an explosion at ground level at 20°C, ignoring any redirection of the overpressure by structures and terrain. If the explosion occurred up in the air (unconfined in all directions), the distance  $X$  would be reduced by a factor of 1.26.

$$X = W^{1/3} \exp[3.5031 - 0.7241(\ln(P)) + 0.0398(\ln(P))^2] \quad (\text{Eq. 23})$$

where

- $X$  = distance to a given external pressure,  $P$ , in ft
- $W$  = TNT equivalent mass, in lbs
- $P$  = increased external pressure, in psi

Given the increased overpressures of 1 psi and 20 psi, the stand-off distance can be determined. The solver function in Excel was also used with Equation 23 to confirm the distances for each calculated TNT equivalent value. The spreadsheet is included electronically (Attachment H, *Shock wave dissipationRI.xls*). Table 6.0-5 presents the results.



Table 6.0-5. Estimated Stand-Off Distances for Area 70A and a Tanker Resupply Truck

Item Evaluated	Amount of Diesel Fuel Oil	TNT equivalent mass	Distance at which increased external pressure equals 20 psi <sup>a</sup>	Distance at which increased external pressure equals 1 psi <sup>a</sup>
Area 70A tanks	120,000 gal	$W_{\text{nominal}} = 128.4 \text{ lb}$	27 ft	168 ft
		$W_{\text{maximized}} = 4278.6 \text{ lb}$	88 ft	539 ft
Typical tanker truck	10,000 gal	$W_{\text{nominal}} = 10.9 \text{ lb}$	12 ft	74 ft
		$W_{\text{maximized}} = 362.5 \text{ lb}$	39 ft	237 ft

NOTE: <sup>a</sup> Rounded to nearest integer.  
ft = foot; gal = gallon; lb = pound; psi = pound per square inch.

Source: Original

For the waste handling facilities, the nominal Area 70A stand-off distance is 168 ft for 1 psi, and maximized (i.e., calculated  $\eta=1.0$ ), the stand-off distance is 539 ft. The nominal tanker truck stand-off distance is 74 ft for 1 psi, and maximized, the stand-off distance is 237 ft. The current site layout allows considerably more distance between Area 70A and the nearest waste handling facility than the nominal stand-off distance, and at least 200 ft more than the maximized distance (Ref. 2.2.28). Similarly, the roadways that the tanker trucks use to access Area 70A are located well beyond either the nominal or maximized distances to a waste handling facility (Ref. 2.2.28).

The site transportation routes used to move loaded transportation casks in the GROA are the closest to the BOP areas and roadways outside of the security fencing; therefore, transportation casks are at the highest risk for this initiating event. Transportation casks are designed to withstand an increased external pressure of 20 psi, so the nominal stand-off distance for Area 70A is 27 ft, and maximized, the stand-off distance is 88 ft. The nominal tanker truck stand-off distance is 12 ft for 20 psi, and maximized, the stand-off distance is 39 ft. The site transportation routes closest to Area 70A or to the roadways used by tanker trucks to access Area 70A are more than 150 ft inside a security fence and, therefore, well beyond the greatest distance of 88 ft (Ref. 2.2.28).

Therefore, no event sequence involving the waste handling facilities would be expected from a diesel fuel vapor explosion associated with either the 120,000-gal storage tank or a 10,000-gal tanker truck. Explosion of the diesel fuel oil storage tank (Area 70A) or of a tanker resupply truck is not analyzed further for categorization.

### 6.0.6 Conservatism in PEFA Values for Truck Trailer Collision Followed by Rollover/Drop

As summarized in Section 6.3.2.2 and detailed in Attachment D, Section D1, analysis of loaded transportation casks resulted in a passive equipment failure probability of 1E-08 for drops, which did not include or credit the impact limiters. The PSCA incorporated additional conservatism, electing to use 1E-05 for analyzing drops (termed “LLNL, adjusted”). In the waste handling facilities, many activities involving the transportation casks are performed without the impact limiters installed, so this conservatism is reasonable to allow for uncertainty in future cask and canister designs and epistemic uncertainty. However, site transportation activities involving

transportation casks that are moved by the SPM always occur with impact limiters and buffer cars; therefore, a failure probability of 1E-05 for dropping a transportation cask is overly conservative. Thus, the actual calculated failure probability of 1E-08 can be applied appropriately for analyzing drops during site transportation activities that involve a transportation cask with impact limiters installed, while still maintaining conservatism.

### **6.0.7 Probability of Moderator Intrusion for Uncanistered Commercial SNF in Sealed Transportation Casks**

For fires that occur in locations that contain uncanistered commercial SNF sealed within bolted transportation casks, the fire location is floor level. The analysis is performed without the salutary effects of fire suppression (for Intra-Site Operations this means response of firefighters) in order to demonstrate large margins of safety during fire event sequences. Should fire suppression be available, then cask failure would not occur (i.e., it would be orders of magnitude lower in probability). Therefore, if fire suppression water or a flood has occurred before or during the fire, there would be no breach of containment for entry into the cask. (Note that cask seal failure takes approximately one hour during a severe fire to occur and, thus, the breach analysis that ignores fire suppression is quite conservative.) The cask failure mode is from overpressurization and degradation of the seals between the lid and the shell; therefore, the area of the seal provides a small target for fire suppression entry. If the fire brigade responds or other unborated water becomes available after the cask has failed, then as long as the cask is internally pressurized, water cannot enter. Due to the heat source provided by the SNF, in addition to heat generated by the fire, there will always be a higher pressure on the inside of the cask than the atmosphere on the outside of the cask. Moreover, the small area associated with seal failure resists entry of significant amounts of water. There are no water sources other than those used by the fire brigade available during Intra-Site Operations activities.

### **6.0.8 Screening of Release Due to Rupture of Bare Fuel in Transportation Cask Exposed to Fire**

If a transportation cask containing uncanistered commercial SNF is exposed to fire, the contents (fuel rods) could be heated to the point of degradation, allowing release of radionuclides within the sealed transportation cask. In addition, if the fire reaches the top of the transportation cask and causes failure of the lid seals, the radionuclides could be released to the surroundings.

An assessment of the temperature at which SNF rods would fail is summarized in NUREG/CR-6672 (Ref. 2.2.82, Section 7.2.5.2). A critical review of accident conditions indicates that rod rupture is expected to occur at temperatures near 725°C to 750°C. After correcting for differences in burn-up and internal pressure, data in NUREG/CR-6672 (Ref. 2.2.82, Section 7.2.5.2) suggest that SNF rods may fail due to creep rupture at temperatures as low as 700°C or require temperatures as high as 850°C. Because the release of cesium vapors will be greater when rods fail at higher temperatures than lower temperatures, the middle of the range, about 750°C, is taken as the temperature at which rods fail by thermal rupture.

The probability of fuel rod failure at 750°C is 2.7E-04 given exposure to fire (Attachment D, Table D2.1-11). The probability of exposure of a transportation cask containing bare fuel to fire in the Truck or Rail Buffer Areas is 0.3 (Attachment F, Section F5.2.2). The overall probability

that a transportation cask is exposed to a fire sufficient to cause rupture of the fuel rods contained within and release of radionuclides to the surroundings is  $0.3 \times 2.7E-04$ , that is, about  $8E-05$  for Intra-Site Operations.

The analysis includes some extreme conservatisms:

- A view factor of one was used to determine the probability that the fuel rods would heat up to the failure temperature, given exposure of the transportation cask to fire. Not all fires to which a transportation cask could be exposed would be positioned such that such complete exposure to thermal radiation would be possible. For example, some severe fires would be expected to occur at ground level owing to diesel fuel pooling. Transportation casks are elevated on trucks.
- The lid seals are at the top of the transportation cask, which is approximately 15 feet tall. Only a limited fraction of the fires to which a transportation cask could be exposed would be large enough to cause failure of the lid seals even if the lower portion of the cask became hot enough to allow rupture of the fuel rods.

Thus, this event is considered to be beyond Category 2 and is screened from further analysis.

## **6.0.9 Loss of Electrical Power as an Initiating Event for Intra-Site Operations**

Because activities associated with Intra-Site Operations generally occur outside of surface nuclear facilities, the loss of offsite power does not impact Intra-Site Operations with the exception of movers (i.e., site transporter and SPM) that are connected to AC power for operations within the surface nuclear facility. The AC power connection is made (and disconnected) outside of the facility. Intra-Site Operations include transit of the movers between the surface nuclear facility and outside. Therefore, the loss of power to the affected movers (including from a loss of offsite power) was treated as a contributing failure in the analysis as a potential site transporter or SPM collision initiating event.

## **6.1 EVENT TREE ANALYSIS**

The event trees that are quantified in this analysis were developed from ESDs in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29, Attachment F (ESDs) and Attachment G (event trees)). This section describes the modeling of event sequences. The related event trees are discussed and presented in Attachment A.

### **6.1.1 Event Tree Analysis Methods**

#### **6.1.1.1 Linked Event Trees and Fault Trees**

As described in Section 4, the PCSA uses event trees and fault trees to calculate the frequency of occurrence of event sequences. The event tree quantification is supported by FTA (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), active component reliability data (Section 6.3.1 and Attachment C), and PEFA (Section 6.3.2 and Attachment D). The SAPHIRE computer program is used as needed for the fault tree quantification process, and the event

sequences generated from the event trees are quantified using a Microsoft Excel spreadsheet (discussions in Section 4.2 and Section 4.3.1 provide more information).

The YMP preclosure handling uses four types of buildings, as summarized below:

1. The RF accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.
2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program for placement in waste packages destined for emplacement in the repository emplacement drifts.
3. The WHF accepts DPCs and transportation casks containing uncanistered commercial SNF, transfers the SNF to TAD canisters which are destined for the CRCF or the aging pads.
4. The Initial Handling Facility (IHF) accepts SNF canisters from the NNPP and some canisters containing HLW for placement in waste packages destined for emplacement in the repository emplacement drifts.

Preclosure waste handling as modeled in the PCSA also includes Subsurface Operations and Intra-Site Operations. Subsurface Operations involve the TEV, which accepts a waste package in the CRCF or IHF and, by means of rail, transports it and deposits it into the designated location in the emplacement drifts. All other waste form transportation in the GROA, BOP facilities, and the LLWF is evaluated as part of Intra-Site Operations.

Event sequences are developed for each of the four building types, Subsurface Operations, and Intra-Site Operations. Because each type of waste container transported has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container, included and described in the *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29). Event sequences are also developed separately for each major group of waste handling processes during Intra-Site Operations. Therefore, event sequences also distinguish among the various steps in waste handling.

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

1. "OK"
2. Direct Exposure, Degraded Shielding
3. Direct Exposure, LOS
4. Radionuclide Release, Filtered (HVAC) (not applicable to Intra-Site Operations)
5. Radionuclide Release, Unfiltered (HVAC system is not operating)
6. Radionuclide Release, Filtered, Also Important to Criticality (not applicable to Intra-Site Operations)

7. Radionuclide Release, Unfiltered, Also Important to Criticality
8. Important to Criticality (not applicable to the CRCF).

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

Since the reliability model for Intra-Site Operations is less complex than those of the surface processing facilities, event sequences are not modeled completely in SAPHIRE. Instead, the event sequence logic depicted by the event trees is entered into an Excel spreadsheet, with the following data input:

- Event tree logic structure.
- Waste form throughputs and the number of opportunities for initiating the event sequence.
- Initiating event frequencies — In some cases, initiating events are modeled as fault trees, and in those instances, SAPHIRE is used to quantify the initiating event frequencies and uncertainties, with the results input into the spreadsheet.
- Basic event data that provides failure rates for active and passive equipment and for HFEs—The basic event data also includes a probability distribution of uncertainty associated with each basic event. The fault tree models are linked to the basic event library.

Each basic event in the fault tree is characterized by a probability distribution. SAPHIRE's Monte Carlo sampling method is employed to propagate the uncertainties to obtain system failure probability or initiating event frequency mean values and parameters of the underlying probability distribution such as standard deviation. As described in Section 4.3.6, categorization is done on aggregated event sequences, and the resultant probability distributions are also calculated in the Excel spreadsheet. For applicable fault tree models, SAPHIRE accounts for the correlation between analogous basic events sharing the same reliability information, ensuring that the spread of the probability distribution is not underestimated for the event sequences in which these basic events intervene.

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

Event sequences are described and graphically depicted using one or two event trees, depending on whether the ESD considered has a single initiating event or multiple initiating events (represented on the ESD as one or more small circles):

1. **Self-contained event trees.** Self-contained event trees are used when only one initiating event appears in the corresponding ESD (Ref. 2.2.29, Attachment F). An example of a self-contained event tree is ISO-ESD05-LLWDAW, shown in Figure 6.1-1. The feed on the left side of the event tree is the event that represents the frequency of challenge to the successful operation of the process step represented in

the event tree. In the example, the frequency of challenge is equal to the number of low-level waste containers that are handled over the preclosure period. The initiating event is presented next, followed by the pivotal events. By convention, the description of each branching event is stated as a success. The branching under each event heading represents success by an upward branch and failure by a downward branch. If a given pivotal event cannot occur in a given sequence due to a prior pivotal event or is irrelevant to the sequence, it does not appear in the event sequence. Each pathway through a self-contained event tree terminates in an end state. End states that are labeled “OK” mean that the sequence of events does not result in one of the specifically identified undesired outcomes. “OK” may mean that normal operation can continue.

Containers containing DAW	Impact to single container at LLWF	Containment boundary of LLW container remains intact		
LLWDAW	INIT-EVENT	LLW-CONTAINER	#	END-STATE-NAMES
			1	OK
			2	OK
			3	RR-UNFILTERED

ISO-ESD05-LLWDAW - Single Container DAW LLW Operations in the LLWF

2008/01/28 Sheet 17

NOTE: DAW = dry active waste; ESD = event sequence diagram; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility.

Source: Original

Figure 6.1-1. Example of a Self-Contained Event Tree

2. **Separate initiator and SRETs.** Separate event trees for initiating events and system responses are used when more than one initiating event appears in the corresponding ESD. The IET decomposes a group of initiating events into the specific failure events that comprise the group. For example, an IET, ISO-ESD-01, and the corresponding SRET, RESPONSE-TCASK, are shown in Figures 6.1-2 and 6.1-3. In the IET, the

feed on the left side is an event that represents the frequency of challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of transportation casks containing DPCs that are handled over the preclosure period. Unlike the self-contained event tree that has only one defined initiating event, separate initiator and system response event trees contain multiple initiating events. The initiating events for the example (Figure 6.1-2) are railcar derailment, railcar collision, truck trailer collision, and drop of an object on the transportation cask. Since these initiating events have different responses, the IET does not end at end states, but transfers to an SRET. The right side (branches) of the IET represent the initiating event values which, for the Intra-Site Operations, are the parameters of the distribution extracted from independent SAPHIRE fault trees or basic event data and entered into the Excel spreadsheet. If multiple movements need to be accounted for, they are included in the Excel spreadsheet to calculate separately, however, in SAPHIRE models for a surface facility, these movements would be built into an initiating event fault tree.

Figure 6.1-3 provides an example SRET, RESPONSE-TCASK. System response event trees contain only pivotal events. Because the conditional probability of each pivotal event may be specific to the initiating event for each event sequence, the same SRET is quantified as many times as there are initiating events in the IET, using multiple lines in the Excel spreadsheet.

Transportation cask containing DPC	Identify initiating events		
DPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Railcar derailment	2 T => 2	RESPONSE-TCASK
	Railcar collision	3 T => 2	RESPONSE-TCASK
	Truck trailer collision	4 T => 2	RESPONSE-TCASK
	Drop of object	5 T => 2	RESPONSE-TCASK

ISO-ESD01-DPC - Movement of Transportation Cask Containing DPC on Railcar 2008/01/28 Sheet 1

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; RESP = response; TCASK = transportation cask; XFER = transfer.

Source: Original

Figure 6.1-2. Example of an Initiator Event Tree



INIT-EVENT	TRANSCASK	CANISTER	SHIELDING	MODERATOR	#	END-STATE-NAMES
					1	OK
					2	DE-SHIELD-DEGRADE
					3	DE-SHIELD-LOSS
					4	RR-UNFILTERED
					5	RR-UNFILTERED-ITC

RESPONSE-TCASK - Transportation Cask System Response

2008/01/28 Sheet 2

NOTE: DE = direct exposure; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure 6.1-3. Example of a System Response Event Tree

### 6.1.1.3 Summary of the Major Pivotal Events

A self-contained event tree or an SRET may include pivotal events concerning the success or failure of the cask, canister, shielding properties, and moderator intrusion susceptibility. The pivotal events are summarized in Attachment A, Section A3.

The pivotal events applicable to the analysis of Intra-Site Operations do not have associated fault trees because they are used in Excel as point values from the summary of passive event failure probabilities table in Section 6.3. Sections 6.2 and 6.3 provide details about the reliability information developed for this analysis.

### 6.1.2 Waste Form Throughputs

Each IET and self-contained event tree begins with the container throughputs, if applicable, that is, the numbers of casks, aging overpacks, or low-level radioactive waste (LLW) containers to be handled over the preclosure period. The number of containers transported during Intra-Site Operations activities is shown in Table 6.1-1. This number is drawn into the descriptions of specific event trees as needed. With the number of containers as a multiplier in the event tree

and the initiating events specified as a probability per container, the value passed to the system response is the number of occurrences of the initiating event expected over the period of operation. In event sequences for which the given frequency for an initiator is the frequency of occurrence over the preclosure period, such as fire events, the number of waste forms is not included separately.

Table 6.1-1. Waste Form Throughputs over the Preclosure Period

Waste Form Unit	ISO Throughput	Comment
Transportation casks containing a TAD canister	6,978	One canister per cask
Transportation casks containing a dual-purpose canister	346	One canister per cask
Transportation casks containing HLW canisters	2,360	1,860 rail-based transportation casks containing 5 HLW canisters and 500 truck-based transportation casks containing 1 HLW canister
Transportation casks containing DOE standardized canisters	385	5 to 9 canisters per transportation cask
Transportation casks containing MCOs	113	4 canisters per transportation cask
Transportation casks or horizontal shielded transfer casks containing a horizontal DPC	346	These DPCs are sent directly to or come from aging.
Transportation casks containing a naval canister	400	One canister per cask
Transportation cask containing uncanistered CSNF assemblies	3,775	9 BWR or 4 PWR SNF assemblies per cask
Aging overpack containing a TAD canister	8,143	One canister per aging overpack
Aging overpack containing a vertical DPC	346	One canister per aging overpack

NOTE: BWR = boiling water reactor; CSNF = commercial spent nuclear fuel; DOE = Department of Energy; DPC = dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; MCO = multicanister overpack; PWR = pressurized water reactor; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: *Waste Form Throughputs for Preclosure Safety Analysis* (Ref. 2.2.23, Table 4)

### 6.1.3 Guide to Event Trees

Event tree figures are located in Attachment A. Table 6.1-2 contains the crosswalk from each ESD developed in the event sequence development analysis (Ref. 2.2.29, Attachment F) to the associated IET and SRET figure location in Attachment A, Table A5-1.

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

ESD#	ESD Title	Initiator Event Tree Name	Initiator Event Tree Location	System Response Event Tree Name	System Response Event Tree Location
ISO-ESD-01	Event Sequences for Activities Associated with Movement of Transportation Cask during Site Transportation	ISO-ESD01-DPC ISO-ESD01-DSTD ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-MCO ISO-ESD01-NAV ISO-ESD01-TAD ISO-ESD01-UCSNF	Figure A5-2 Figure A5-4 Figure A5-5 Figure A5-6 Figure A5-7 Figure A5-8 Figure A5-9 Figure A5-10	RESPONSE -TCASK	Figure A5-3
ISO-ESD-02	Event Sequences for Activities Associated with Aging Overpack Transit, Placement, and Retrieval	ISO-ESD02-DPC ISO-ESD02-TAD	Figure A5-11 Figure A5-13	RESPONSE -AO	Figure A5-12
ISO-ESD-03	Event Sequences for Activities Associated with the Transporting and Positioning of an HTC or an HSTC	ISO-ESD03-HDPC	Figure A5-14	RESPONSE -HTC	Figure A5-15
ISO-ESD-04	Event Sequences Associated with Impacts during Canister Operations at a Horizontal Aging Module	ISO-ESD04-HDPC	Figure A5-16	RESPONSE -HAM	Figure A5-17
ISO-ESD-05	Event Sequences for Activities Associated with a Single Low-Level Radioactive Waste Container at the Low-Level Waste Facility	ISO-ESD05-LLWDAW ISO-ESD05-LLWLIQ ISO-ESD05-LLWWETnr	Figure A5-18 Figure A5-19 Figure A5-20	N/A	N/A

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

ESD#	ESD Title	Initiator Event Tree Name	Initiator Event Tree Location	System Response Event Tree Name	System Response Event Tree Location
ISO-ESD-06	Event Sequences Associated with Nonfire Events Involving all Low-Level Radioactive Waste Containers at the Low-Level Waste Facility	ISO-ESD06-LLW	Figure A5-21	N/A	N/A
ISO-ESD-07	Event Sequences Associated with Fire Events for All Combustible Low-Level Radioactive Waste at the Low-Level Waste Facility	ISO-ESD07-LLW	Figure A5-22	N/A	N/A
ISO-ESD-08	Event Sequences for Activities Associated with Waste Transfers to the Low-Level Waste Facility	ISO-ESD08-LLWDAW ISO-ESD08-LLWLIQ ISO-ESD08-LLWWETnr ISO-ESD08-LLWWETr	Figure A5-23 Figure A5-25 Figure A5-26 Figure A5-27	RESPONSE -LLW	Figure A5-24
ISO-ESD-09	Event Sequences for Fire Occurring during Site Transportation Activities or at the Aging Facility	ISO-ESD09-DPC ISO-ESD09-DSTD ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-MCO ISO-ESD09-NAV ISO-ESD09-TAD ISO-ESD09-UCSNF	Figure A5-28 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34 Figure A5-35 Figure A5-36	RESPONSE -FIRE	Figure A5-29

NOTE: AO = aging overpack; DAW = dry active low-level radioactive waste; DPC = dual-purpose canister; DSTD = DOE standardized canister; ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations; LLW = low-level radioactive waste; MCO = multiccanister overpack; NAV = naval; nr = nonresin; r = resin; TAD = transportation, aging and disposal (canister); TCASK = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

## 6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS

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

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

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

The fault trees are linked to the event trees via an Excel spreadsheet. Other data inputs to the event tree are either input directly into the spreadsheet representation or are updated through the application of the statistical capabilities of SAPHIRE to generate the required distribution parameters (mean, median, and standard deviation) used to describe the uncertainty associated with the quantified event sequences. The data quantification is usually simple, one or two basic event fault trees, usually having a single top event, an OR gate or AND gate that has the basic events as inputs.

Attachment B, Sections B1 through B3, present all of the system fault trees. These sections describe the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B4 presents the additional fault trees (simple data quantification trees) used in the Intra-Site Operations analysis. These fault trees are self-explanatory, and they are quantified only to develop the appropriate distribution parameters used in the Excel spreadsheet quantification of the event sequences.

A top event occurs when one of the (ITS) success criteria for a given SSC fails to be achieved. At least one success criterion is defined for each system. Multiple success criteria are defined for systems that perform multiple safety functions in the Intra-Site Operations.

Each of the top events for the initiating event fault trees represent the conditional probability that the top event will occur when the system is put into service. That is, the results of the FTA answer a question such as “what is the probability for each canister movement that the site transporter drops the canister?” The expected number of canister drop initiating events during the preclosure period is the product of the number of times a canister is moved by the site transporter during the preclosure operations and the conditional probability of the top event. Such values for the expected number of canister drops are not developed directly, however.

Instead, the IET representation in the Excel spreadsheet links the various fault tree logic models to the canister, or other waste form, and the throughput values to generate the quantified event sequence.

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

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

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

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

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

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

- Physical description
- Operation
- Control system
- System/pivotal event success criteria

- Mission time
- Fault tree results.

## **6.2.2 Summary of Fault Tree Analysis**

### **6.2.2.1 SPM FTA**

The FTA is detailed in Attachment B, Section B1. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### **6.2.2.1.1 Physical Description**

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

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

#### **6.2.2.1.2 Operations**

SPM activities for Intra-Site Operations begin once the railcar or truck trailer carrying a transportation cask arrive onsite at the receipt area. Receipt activities include the placement of temporary protective shielding around the railcar or truck trailer, inspection of the transportation cask, and connection of the railcar or truck trailer to the SPM. Once all receipt activities are completed the SPM with the railcar or truck trailer proceeds to the appropriate facility (CRCF, IHF, RF, or WHF) or, if the facility is not immediately available to receive the cask, to the appropriate buffer area.

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

#### **6.2.2.1.3 Control System**

A simplified schematic of the functional components on the SPMRC/SPMTT is shown in Attachment B, Section B1.

The control system provides features for preventing initiating events:

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

#### **6.2.2.1.4 System/Pivotal Event Success Criteria**

Success criteria for the SPM are the following:

- Prevent collisions which includes:
  - Prevent a runaway situation
  - Respond correctly to operator commands.

Various design features are provided to achieve this success criterion.

#### **6.2.2.1.5 Mission Time**

A nominal one-hour mission time is used to calculate the failure probability for components having a time-based failure rate. Otherwise, failure-on-demand probabilities are used.

For railcar derailment, the probability is based on the distance traveled from the receipt area to any facility 2.0 miles is used for the distance to all facilities, an industry data derailment rate of 1.18E-5 per mile traveled (Attachment C, Table C4-1, DER-FOM).

#### **6.2.2.1.6 Fault Tree Results**

The detailed description in Attachment B, Section B1 documents the application of basic event data, CCFs, and HRA (refer also to Attachment E).

The SPMRC or SPMTT has two credible failure scenarios:

- Collision with site structures, including doors
- SPMRC derailment.

These failure modes may occur with various waste forms that are received in the transportation casks. The site transporter collision with the facility door fault tree model was used to model the collision of the facility door with the SPM.

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



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

Top Event	Mean Probability	Standard Deviation
SPMRC collides with facility structures	4.5E-03	1.3E-02
SPMRC derailment	2.4E-05	2.6E-06
SPMTT collides with facility structures	4.4E-03	1.5E-02

NOTE: SPM = site prime mover; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.

Source: Attachment B, Figures B1.4-1, B1.4-6, B4-2, and Table B4-3

### 6.2.2.2 Site Transporter FTA

The FTA for the site transporter is detailed in Attachment B, Section B2. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### 6.2.2.2.1 Physical Description

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a concrete and steel ventilated aging overpack from a facility vestibule to the aging pads.

The site transporter is a track driven vehicle with four synchronized tracks (two on each side). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not ITS. An integrated diesel powered electric generator provides the energy to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

A rear fork assembly and a pair of support arms are used to lift and lower the cask. The rear forks are inserted in two rectangular slots near the base of aging overpack. Casks are carried in a vertical orientation with the lid at the top. Access to the top of the casks is unobstructed.

A passive restraint system provides stabilization during cask movement. These restraints come into contact with the cask after it has been raised to the desire height. A pin is inserted into each of the three restraint arms to keep the restraint in place, should there be a failure of the electromechanical assembly. The pins also serve as an interlock that prevents movement of a loaded site transporter without the restraints being properly installed.

#### 6.2.2.2.2 Control System

There are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter. All safety interlocks and controls of the site transporter are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No PLC or computer is used to control the machine.

### **6.2.2.2.3 Normal Operations**

Once the aging overpack is securely positioned on the site transporter, movement of the loaded site transporter can begin.

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. At the facility, the operator stops the site transporter outside the facility's entrance vestibule and turns off the diesel generator, and an electric power cable is attached.

Once inside the building, the operator positions the site transporter in the Cask Preparation Room and in the Cask Unloading Rooms

### **6.2.2.2.4 System/Pivotal Event Success Criteria**

Success criteria for the site transporter are the following:

- Prevent a collision of the site transporter with objects, structures, or shield doors which includes
  - Prevent runaway situations
  - Prevent site transporter movements in the wrong direction.

Various design features are provided to achieve these success criteria. The failure to achieve this success criterion defines the top event for a fault tree for the site transporter.

### **6.2.2.2.5 Mission Time**

For quantification of the site transporter fault trees in Attachment B, Section B2, a mission time of one hour per cask transfer is used.

### **6.2.2.2.6 Fault Tree Results**

There are two basic site transporter fault tree developed for the Intra-Site Operations. The scenarios represented and the variations by these fault trees are the following:

1. Site transporter collides with site structures (including facility doors) or other vehicles:
  - A. Importing aging overpack from aging pads to Cask Preparation Room.
  - B. Export aging overpack from Cask Preparation Room to aging pad.
2. Site transporter drops an Aging Overpack.

The results of the analysis are summarized in Table 6.2-2 for the fault trees.

Table 6.2-2. Summary of Top Event Quantification for the Site Transporter

Top Event	Mean Probability	Standard Deviation
Collision	4.8E-03	1.6E-02
Drop	4.0E-08	1.2E-07

Source: Attachment B, Figures B2.4-1, B2.4-6

### 6.2.2.3 Cask Tractor and Cask Transfer Trailer FTA

The FTA for the cask tractor/cask transfer trailer is detailed in Attachment B, Section B3. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### 6.2.2.3.1 Physical Description

The cask tractor is a large, four-wheel drive, diesel tractor designed specifically for pulling the cask transfer trailer. The cask tractor has redundant brakes in addition to having a fail-safe emergency brake. The cask transfer trailer has independently mounted non-driven hydraulic pendular axles with a minimum of four tires per axles that will ensure the cask remains level during transportation across uneven terrain. In addition to the pendular axles, the cask transfer trailer has three other hydraulic systems: (1) stabilizing jacks, (2) cask support skid and positioning system, and (3) hydraulic ram.

#### 6.2.2.3.2 Control System

Operators manually control every operation on the cask tractor/cask transfer trailer. All safety interlocks and controls of the cask tractor and cask transfer trailer are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No PLC or computer is used to control the machine.

#### 6.2.2.3.3 Normal Operations

For normal operations the horizontal cask tractor and trailer are used to transport horizontal casks from facilities to the aging pads. At the aging pads the cask tractor and cask transfer trailer have self-contained rams to insert the horizontal cask into the horizontal aging module (HAM).

#### 6.2.2.3.4 System/Pivotal Event Success Criteria

Success criterion for the cask tractor and cask transfer trailer is the following:

- Prevent a collision of the cask transfer trailer with objects, or structure doors which include:
  - Prevent runaway situations
  - Prevent site transporter movements in the wrong direction
  - Prevent a load drop during lift/lower or transport operations.

Various design features are provided to achieve the success criteria. The failure to achieve this success criterion defines the top event for a fault tree for the cask tractor and cask transfer trailer.

**6.2.2.3.5 Mission Time**

For quantification of the cask transfer trailer fault trees in Attachment B, Section B3, a mission time of two hours per cask transfer is used, except for the failures associated with the facility door closing on the cask transfer trailer for which a mission time of one hour was used.

**6.2.2.3.6 Fault Tree Results**

There is one basic cask tractor and cask transfer trailer fault tree developed for Intra-Site Operations. The scenarios represented and the variations by these fault trees are the following:

1. Cask tractor and cask transfer trailer collision with site structures, vehicles, or facility doors
  - A. Importing horizontal transfer casks from aging pads to Cask Preparation Room.
  - B. Export horizontal transfer casks from Cask Preparation Room to aging pads.

The results of the analysis are summarized in Table 6.2-3 for the fault tree.

Table 6.2-3. Summary of Top Event Quantification for the Cask Tractor and Cask Transfer Trailer

Top Event	Mean Probability	Standard Deviation
Collision	4.7E-3	2.5E-2

Source: Attachment B, Figure B3.4-1

**6.2.2.4 Additional Fault Trees**

Eleven additional fault trees were developed to address events that could impact Intra-Site Operations and are detailed in Attachment B, Section B4. These fault trees are identified in Table 6.2-4. All of these trees are top level trees. The results of quantifying these trees were input directly into the Excel spreadsheet used to quantify Intra-Site event sequences as initiating events. Some provide the link between the top level events in the event trees and the system fault trees described in Attachment B, Sections B1 through B3. This relationship is identified in Table 6.2-4.

Table 6.2-4. Top Level and Linking Fault Trees

Fault Tree	Description	Events considered	System Fault Trees Used as Input
INTRASITE-PMRC-COLLIDE	SPMRC collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMRC-COLLISION (B1.4.1)
INTRASITE-DETRAIL	SPMRC derails during transit from receipt area to facility	SPMRC derailment	None
INTRASITE-PMTT-COLLIDE	SPMTT collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMTT-COLLISION (B1.4.2)
INTRASITE-JIB-CRANE	Drop of heavy load onto TC during receipt processing and transit to facility	Crane drops onto TC	None
INTRASITE-ST-COLLIDE	ST collisions in transport of Aging Overpack from facility to Aging Facility	Collisions during transit or with facility door	INT-2-ST-COLLISION (B2.4)
INTRASITE-HCTT-COLLISION	HCTT collisions in transport of horizontal casks from facility to Aging Facility	HCTT collision during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HCTT-DROP	HCTT drops in transport of horizontal casks from facility to Aging Facility	HCTT drops during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HAM-INSERT	Canister damaged during insertion into HAM	Operator or equipment failure during canister insertion into HAM	None
INTRASITE-HAM-AUX-EQUIPMENT	HAM damaged during canister loading/unloading operations	Impacts from crane operation	None
INTRASITE-HEPA-TRANSFER	Damage to LLW container during transit from WHF to LLWF or offsite	Vehicle collisions during transit	None
INTRASITE-COLL-TRANSFER	Damage to LLW container during transit from WHF to LLWF	Forklift or vehicle collisions during transit	None

NOTE: HAM = horizontal aging module; HCTT = cask tractor/cask transfer trailer (used only for SAPHIRE fault tree codes); LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; ST = site transporter; TC = transportation cask; WHF = Wet Handling Facility.

Source: Original

## 6.3 DATA UTILIZATION

### 6.3.1 Active Component Reliability Data

The fault tree models described in Section 6.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. The active component reliability estimates are developed by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represent the range of the industry-wide information.

### 6.3.1.1 Industry-Wide Reliability Data for Active Components

While data from the facility being studied are the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP is a one-of-a-kind facility, it is necessary to develop the required data from industry-wide data experience of other industries. Industry-wide data sources are documents containing industrial or military experience on component performance. Usually data sources are previous safety/risk analyses and reliability studies performed nationally or internationally, but the data source can also be standards or published handbooks. For the YMP PCSA, an industry-wide database is constructed using a library of industry-wide data sources of reliability data from nuclear power plants, as well as equipment used by the military, chemical processing plants, and other facilities. The sources used are listed in Attachment C, Section C1.2.

The data source scope must be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might be used for electronics data versus mechanical data, so long as the detail and the applicability of the information provided justify its use. In addition, the quality of the data source is considered to be a measure of the source's credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort is made in this analysis to use the highest quality data source available for each active component type and failure mode (TYP-FM).

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the generic source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, is to evaluate the similarity between the YMP operating environment and that represented in each data source to ensure data appropriateness. This evaluation process is described in Attachment C, Section C1.2.

Given the fact that the YMP is a relatively unique facility (although portions are similar to the SNF handling and storage areas of commercial nuclear plants), the data development perspective is to collect as much relevant failure estimate information as possible to cover the spectrum of equipment operational experience. It is reasonable to expect that the YMP equipment would fall within this spectrum (Section 3.2.1). The scope of the sources selected for this data set is therefore deliberately broad to take advantage of the combined experience of many facilities, not a single plant. It is then intended to provide a combined estimate that reflects as best as possible the uncertainty ranges of the individual estimates. This ensures that the data are not skewed towards the possibly atypical behavior of one particular plant, industry or operating environment. The combinatorial process, utilizing Bayes' theorem, is discussed in the following subsection.

Among the active components whose reliability is quantified with industry-wide data are the 200-ton cranes, jib cranes, waste package maneuvering cranes, and the SNF transfer machine (SFTM). Cranes other than mobile/portable (jib) cranes and the SFTM are not used in Intra-Site operations; however they are being discussed in this section for completeness. The rationale for

using such data for these estimates is that a significant amount of crane experience exists within the commercial nuclear power industry and other applications, and this experience can be used to bound the anticipated crane performance at YMP. Furthermore, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants. Crane and SFTM handling incidents that result in a drop are included in the drop probability regardless of cause; they may be caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

Every attempt was made to find more than one data source for each TYP-FM, although multiple sources are not always available for a specific piece of equipment. When data was extracted from several sources in many cases, then combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs were quantified with one data source, 8% with two data sources, 8% with three data sources and 31% with four or more data sources.

### **6.3.1.2 Application of Bayes' Theorem to PCSA Database**

The application of industry-wide data sources introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes' theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in NUREG/CR-6823 (Ref. 2.2.8, Section 8). For the PCSA, the method known as "parametric empirical Bayes" is primarily used. This permits a variety of different sources to be statistically combined and compared, whether the inputs are expressed as the number of failures and exposure time or demands, or as means and lognormal error factors.

A typical application of Bayes' theorem is illustrated as follows. A failure rate for a given component is needed for a fault tree (e.g., a fan motor in the HVAC system). There is no absolute value for the failure rate, but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data to the YMP introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying available data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trials if the failure rate is a certain value. The evidence comprises observations or test

results on the number of failure events that occur over a certain exposure, operational, or test duration.

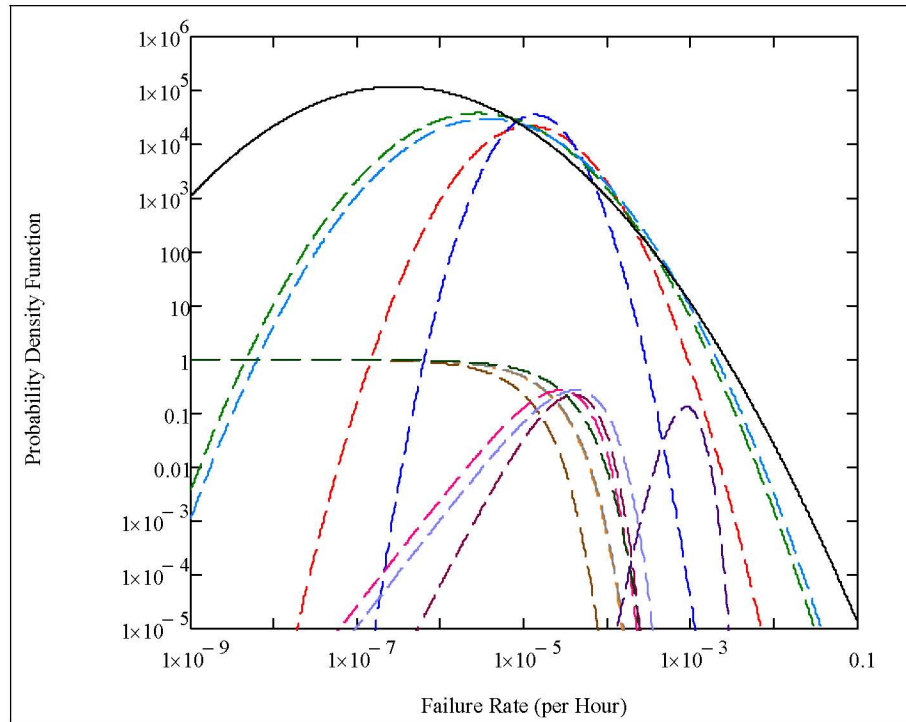
3. Update the probability distribution for the failure rate based on the new body of evidence.

The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The mathematical expression for applying Bayes' theorem to data analysis is described in Attachment C, Section C2.

For the analysis presented herein, MathCAD is used to calculate the population-variability (prior) distributions of active components. As described in Attachment C, Section C2.1, the method of "The Combined Use of Data and Expert Estimates in Population Variability Analysis" (Ref. 2.2.54, pp. 311–321) is used as the basis example for the combinations performed. In this method, the population-variability distribution of the failure rate is approximated by a lognormal distribution whose unknown parameters,  $\nu$  and  $\tau$ , respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating  $\nu$  and  $\tau$  involves calculating the likelihood function associated with the reliability information in each data source. For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate  $x$ , and characterized by its median value and associated error factor. For a data source providing exposure data (given in the form of a number  $n$  of recorded failures over an exposure time  $t$ ), the likelihood function is a Poisson distribution, expressing the probability that  $n$  failures are observed when the expected number of failures is  $x$  times  $t$ .

The maximum likelihood method is used to calculate  $\nu$  and  $\tau$ . This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source because the data sources are independent from each other. It is equivalent and computationally convenient to find the maximum likelihood estimators for  $\nu$  and  $\tau$  by using the sum of the log-likelihood (logarithm of the likelihood) of each data source. As a result, the likelihood functions from the individual data sources and a population-variability PDF for the combination are produced and plotted for comparison, as in the example shown as Figure 6.3-1.





Source: Attachment C, Figure C2.1-1

Figure 6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

If only a single data source is considered applicable to a given TYP-FM combination and if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. However, if the data source does not readily provide a probability distribution, but instead exposure data (i.e., a number of recorded failures over an exposure time for failure rates or over a number of demands for failure probabilities), the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffreys' noninformative prior distribution (i.e., gamma for time-related failure modes, and beta for demand-based failure modes).

Example implementations of the methods used for these cases are provided in Attachment C, Section C2.2.

### 6.3.1.3 Common-Cause Failure Data

Dependent failures are modeled in event tree and fault tree logic models. When possible, potential dependent failures are modeled explicitly via the logic models. For example, failure of the HVAC system is explicitly dependent upon failure in the electrical supply system that is modeled in the fault trees. Similarly, the effects of erroneous calibration or other HFEs can be explicitly included in the system fault tree models and the basic event probabilities considered during the HRA. Otherwise, potential dependencies known as CCFs are included in fault tree

logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate CCF probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. 2.2.46), the Multiple Greek Letter method *Analytical Background and Techniques*. Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780 (Ref. 2.2.58), and the Alpha Factor method (Ref. 2.2.59). In a parametric model, the probability of two or more components failing by a CCF is estimated by use of the equations provided in Section 4.3.3.3.

For the PCSA, CCF rates or probabilities are estimated using the *Alpha Factor Method* (Ref. 2.2.59) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in NUREG/CR-5485 (Ref. 2.2.59) consisted of:

1. Identifying the number of redundant components in each subsystem being reported, (e.g., two, three, or four (termed the CCF group size)).
2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, (i.e., one component at a time, two components at a time, and so on up to failure of all components in a given CCF group).
3. Calculating the alpha factor for a given component type to provide a basis for estimating the probability of CCFs involving two, three, etc., or all components (the equation in Attachment C, Section C3 provides more information).
4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produces prior distributions for the alpha factors. The results are the mean alpha factors and uncertainty bounds, reported in NUREG/CR-5485 (Ref. 2.2.59, Table 5-11) and reproduced in Attachment C, Table C.3-1.

These alpha-factor values are used for failure-on-demand events (e.g., pump fails to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run). For example, for a 2-out-of-2 failure on demand event, the mean alpha factor of 0.047 (shown in the far right column of Table C3-1 associated with  $\alpha_2$ ) was multiplied by the mean failure probability for the appropriate component TYP-FM (from Table C4-1) to yield the CCF probability.

#### **6.3.1.4 Input to SAPHIRE Models**

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data has to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

- .BEA – attributes to assign information to the proper SAPHIRE fields
- .BED – descriptions of the component type name and failure mode
- .BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement to ensure that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the PCSA case was the TYP-FM coding). Examples of descriptions used for the PCSA template data were: clutch failed to operate, relay spurious operation, position sensor fails on demand, and wire rope breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the lognormal error factor, or the shape parameter of the beta or gamma distributions.

Geometric means of the input parameters from the data sources are initially used as screening values for each TYP-FM and are entered into the .BEI file, along with a default error factor of 10. Once the Bayesian combination process is completed for all of the TYP-FM combinations, mean and uncertainty parameter information are entered into the .BEI files, and tested in SAPHIRE before being distributed to the systems analysts.

The template data is used by the fault tree models. The data is imported into SAPHIRE using the MAR-D portion of the SAPHIRE code, then the modify event feature links the template data to each basic event in the fault tree. This permits each active component of the same TYP-FM to mode to utilize the same failure estimate and uncertainty information, based on the results of the industry-wide data investigation and Bayesian combination process.

Attachment C, Section C4, presents a more thorough discussion of the active component reliability data development process, as well as a table of the template data that is imported into SAPHIRE.

### 6.3.1.5 Summary of Active Component Reliability Data in Intra-Site Operations Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the Intra-Site models. Development of this table is discussed in detail in Attachment C, Section C4.

Table 6.3-1. Active Component Reliability Data Summary

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-CRWT-ATB1001-AT-FOH	Screw Actuator Mechanism on Lift Boom #1 Fails	7.54E-05	7.54E-05	

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

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-CRWT-ATB1011-AT-FOH	Screw Actuator Mechanism on Lift Boom #1 Fails	7.54E-05	7.54E-05	
ISO-CRWT-ATB2002-AT-FOH	Screw Actuator Mechanism on Lift Boom #2 Fails	7.54E-05	7.54E-05	
ISO-CRWT-ATB222-AT-FOH	Screw Actuator Mechanism on Lift Boom #2 Fails	7.54E-05	7.54E-05	
ISO-CRWT-ATD0002-AT-FOH	ST D-Axis Electrical Actuator #2 Fails Lift/Lower	7.54E-05	7.54E-05	
ISO-CRWT-ATD001-AT-FOH	ST D-Axis Electrical Actuator #1 Fails Lift/Lower	7.54E-05	7.54E-05	
ISO-CRWT-ATD03-AT-FOH	ST D Axis Electrical Actuator #1 Movement Fails	7.54E-05	7.54E-05	
ISO-CRWT-ATD04-AT-FOH	ST D-Axis Electrical Actuator #2 Movement Fails	7.54E-05	7.54E-05	
ISO-CRWT-ATP002-AT-FOH	ST P-Axis Electrical Failure During Movement	7.54E-05	7.54E-05	
ISO-CRWT-ATR10002-AT-FOH	ST R-Axis Electrical Actuator #1 Fails Movement	7.54E-05	7.54E-05	
ISO-CRWT-BEA#1-BEA-BRK	Boom#1 Fails During Cask Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEA22-BEA-BRK	Boom#2 Fails During Cask Lift	2.40E-08	2.40E-08	
ISO-CRWT-BEAB202-BEA-BRK	Boom#2 Fails During Cask Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEAD003-BEA-BRK	ST D-Axis Actuator Structural Arm #2 Failure Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEAD006-BEA-BRK	ST D-Axis Actuator Structural Arm #1 Failure Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEAP02-BEA-BRK	ST P-Axis Mechanical Failure During Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEAR103-BEA-BRK	ST R-Axis Actuator Structural Arm #1 Failure Movement	2.40E-08	2.40E-08	
ISO-CRWT-BEAR204-BEA-BRK	ST R-Axis Actuator Structural Arm #2 Failure Movement	2.40E-08	2.40E-08	
ISO-CRWT-BRK001--BRK-FOD	Tractor Brake A Fails	1.46E-06		
ISO-CRWT-BRK002--BRK-FOD	Tractor Brake B Fails	1.46E-06		
ISO-CRWT-BRK003--BRK-FOD	Trailer Brakes Fail	1.46E-06		
ISO-CRWT-BRKCCF--BRK-FOD	CCF of Both Tractor Brakes	6.90E-08		1
ISO-CRWT-CBP0000-CBP-OPC	Electrical Power Dist Cable Failure on ST	1.53E-07	9.13E-08	
ISO-CRWT-CON0000-CON-FOH	Electrical Power Dist Connectors Fail on ST	7.10E-05	7.14E-05	1
ISO-CRWT-CTSHC000-CT-SPO	Spurious Command to Raise/Lower AO or STC	2.27E-05	2.27E-05	
ISO-CRWT-DROP11-BEA-BRK	Boom#1 Fails During Cask Lift	2.40E-08	2.40E-08	1

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

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-CRWT-EATR2004-AT-FOH	ST R-Axis electrical Actuator #2 Fails Movement	7.54E-05	7.54E-05	1
ISO-CRWT-ECP0000-ECP-FOH	ST Restraint Arms Position Selector Fails	1.79E-06	1.79E-06	1
ISO-CRWT-ELEC-MOE-FOD	ST Electric Motor Failure	6.00E-05		1
ISO-CRWT-IEL0001-IEL-FOD	Restraint System Interlock Failure	2.75E-05		
ISO-CRWT-LM000011-LC-FOD	ST Lift/Lower Selector Lever Fails	6.25E-04		
ISO-CRWT-LPATH1--ATH-FOH	Pendular Axle Hydraulic 1 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH2--ATH-FOH	Pendular Axle Hydraulic 2 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH3--ATH-FOH	Pendular Axle Hydraulic 3 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH4--ATH-FOH	Pendular Axle Hydraulic 4 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH5--ATH-FOH	Pendular Axle Hydraulic 5 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH6--ATH-FOH	Pendular Axle Hydraulic 6 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH7--ATH-FOH	Pendular Axle Hydraulic 7 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LPATH8--ATH-FOH	Pendular Axle Hydraulic 8 Failure	1.78E-03	8.91E-04	2
ISO-CRWT-LSJATH1-ATH-FOH	Stabilizing Jack 1 Failure	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH2-ATH-FOH	Stabilizing Jack 2 Failure	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH3-ATH-FOH	Actuator (Hydraulic) Failure	8.91E-04	8.91E-04	1
ISO-CRWT-LSJATH4-ATH-FOH	Stabilizing Jack 4 Failure	8.91E-04	8.91E-04	1
ISO-CRWT-LVRD01-LVR-FOH	ST D-Axis Actuator Structural Arm #1 Failure	2.10E-06	2.10E-06	1
ISO-CRWT-LVRD02-LVR-FOH	ST D-Axis Actuator Structural Arm #2 Failure	2.10E-06	2.10E-06	1
ISO-CRWT-PIND004-PIN-BRK	ST D-Axis Actuator Pin #2 Failure Movement	2.12E-09	2.12E-09	1
ISO-CRWT-PIND005-PIN-BRK	ST D-Axis Actuator Pin #1 Failure Movement	2.12E-09	2.12E-09	1
ISO-CRWT-PINP04-PIN-BRK	ST P-Axis Pin failure During Movement	2.12E-09	2.12E-09	1
ISO-CRWT-PINR103-PIN-BRK	ST R-Axis Mechanical Pin #1 Failure During Movement	2.12E-09	2.12E-09	1
ISO-CRWT-PINR202-PIN-BRK	ST R-Axis Mechanical Pin #2 Failure During Movement	2.12E-09	2.12E-09	1
ISO-CRWT-SJKB011-SJK-FOH	Screw Lift on Boom #1 Fails	8.14E-06	8.14E-06	1

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

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-CRWT-SJKB101-SJK-FOH	Screw Lift on Boom #1 Fails	8.14E-06	8.14E-06	1
ISO-CRWT-SJKB202-SJK-FOH	Screw Lift on Boom #2 Fails	8.14E-06	8.14E-06	1
ISO-CRWT-SJKB22-SJK-FOH	Screw Lift on Boom #2 Fails	8.14E-06	8.14E-06	1
ISO-CRWT-ZSD00005-ZS-FOD	ST D-Axis Position Switch Failure Movement	2.93E-04		
ISO-CRWT-ZSD00006-ZS-FOD	ST D-Axis Position Switch Failure Lift/Lower	2.93E-04		
ISO-CRWT-ZSP00003-ZS-FOD	ST P-Axis Position Switch Failure During Movement	2.93E-04		
ISO-CRWT-ZSR00005-ZS-FOD	ST R-Axis Position Switch Failure Movement	2.93E-04		
ISO-HAM-RAM-INSERT	Motor (Hydraulic) Failure	5.39E-04	5.39E-04	1
ISO-HTTCOLLIDE---G65-FOH	Sped Limiter Fails	1.16E-05	1.16E-05	1
ISO-SPMRC-BRP000-BRP-FOD	SPMRC Brake 000 Failure on Demand	5.02E-05		
ISO-SPMRC-BRP001-BRP-FOD	SPMRC Fails to Stop on Loss of Power	5.02E-05		
ISO-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	9.13E-08	9.13E-08	1
ISO-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable - Short Circuit	1.88E-08	1.88E-08	1
ISO-SPMRC-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	1.91E-06	1.91E-06	1
ISO-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	4.00E-06		
ISO-SPMRC--CT001-CT--FOD	On-Board Controller Fails to Respond	4.00E-06		
ISO-SPMRC--CT003-CT--SPO	On-Board Controller Initiates Spurious Signal	2.27E-05	2.27E-05	1
ISO-SPMRC-G65000-G65-FOH	SPMRC Speed Control (Governor) Fails	1.16E-05	1.16E-05	1
ISO-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1.74E-03		
ISO-SPMRC-MOE000-MOE-FSO	SPMRC Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
ISO-SPMRC-SC021--SC--FOH	Speed Controller on SPMRC Pendant Fails	1.28E-04	1.28E-04	1
ISO-SPMRC-SEL021-SEL-FOH	Speed Selector on SPMRC Pendant Fails	4.16E-06	4.16E-06	1
ISO-SPMTT-BRK000-BRP-FOD	Pneumatic Brakes on SPMTT Fail on Demand	5.02E-05		
ISO-SPMTT-BRK001-BRP-FOD	SPMTT Pneumatic Brakes Fail	5.02E-05		
ISO-SPMTT-CBP002-CBP-OPC	SPMTT Power Cable - Open Circuit	1.53E-07	9.13E-08	1

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

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-SPMTT-CBP003-CBP-SHC	Cables (Electrical Power) Short Circuit	3.15E-08	1.88E-08	
ISO-SPMTT-CPL000-CPL-FOH	Truck Trailer Automatic Coupler System Fails	1.91E-06	1.91E-06	1
ISO-SPMTT-CT000-CT-FOD	Controller Mechanical Jamming	4.00E-06		
ISO-SPMTT-CT001-CT-FOD	On-Board Controller Fails to Respond	4.00E-06		
ISO-SPMTT-CT001-CT-SPO	On-Board Controller Spurious Operation	2.27E-05	2.27E-05	1
ISO-SPMTT-CT002-CT-FOH	Controller Failure	6.88E-05	6.88E-05	1
ISO-SPMTT-G65000-G65-FOH	SPMTT Speed Control (Governor) Fails	1.16E-05	1.16E-05	1
ISO-SPMTT-HC001-HC-FOD	Remote Control Transmits Wrong Signal	1.74E-03		
ISO-SPMTT-HC002-HC-SPO	Spurious Signal from Pendant Controller	5.23E-07	5.23E-07	1
ISO-SPMTT-MOE000-MOE-FSO	SPMTT Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
ISO-SPMTT-SC021-SC-FOH	Speed Controller on SPMTT Pendant Fails	1.28E-04	1.28E-04	1
ISO-SPMTT-SEL021-SEL-FOH	Speed Selector on SPMTT Pendant Fails	4.16E-06	4.16E-06	1
ISO-SPMTT-STU001-STU-FOH	SMPTT End Stops Fail	2.11E-04	4.81E-08	4.38E+03
ISO-ST-BRK001-BRK-FOD	ST Fails to Stop on Loss of Power	1.46E-06		
ISO-ST-CBP004-CBP-OPC	ST Power Cable - Open Circuit	9.13E-08	9.13E-08	1
ISO-ST-CBP004-CBP-SHC	ST Power Cable Short Circuit	1.88E-08	1.88E-08	1
ISO-ST-CT000-CT-FOD	ST Primary Stop Switch Fails	4.00E-06		
ISO-ST-CT002-CT-FOH	Direction Controller Fails	6.88E-05	6.88E-05	1
ISO-ST-HC001-HC-FOD	Remote Control Transmits Wrong Signal	1.74E-03		
ISO-ST-HC002-HC-SPO	Spurious Command to Lift/Lower AO or STC	5.23E-07	5.23E-07	1
ISO-ST-MOE0001-MOE-FSO	ST Lock Mode State Fails on Loss of Power	1.35E-08	1.35E-08	1
ISO-ST-MOE000-MOE-FSO	ST Motor (Electric) Fails to Shut Off	1.35E-08	1.35E-08	1
ISO-ST-MOE021-MOE-FSO	Drive System on Primary Propulsion Fails	1.35E-08	1.35E-08	
ISO-ST-SC021-SC-FOH	Speed Controller on ST Pendant Fails	1.28E-04	1.28E-04	
ISO-ST-SC021-SC-SPO	On-Board Controller Initiates Spurious Signal	3.20E-05	3.20E-05	

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

Basic Event Name	Basic Event Description	Basic Event Mean Probability <sup>a</sup>	Mean Failure Rate <sup>a</sup>	Mission Time (Hours)
ISO-ST--SEL021--SEL-FOH	Speed Selector on ST Pendant Fails	4.16E-06	4.16E-06	

NOTE: <sup>a</sup> Although the values in this table are shown to a precision of three significant figures, the values are not known to that level of precision. The values in Attachment C may show fewer significant figures. Such differences are not meaningful in the context of this analysis because the corresponding uncertainties (which are accounted for in the analysis) are much greater than differences due to rounding.

AO = aging overpack; CCF = common-cause failure; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; ST = site transporter.

Source: Attachment C, Section C4.

### 6.3.2 Passive Equipment Failure Analysis

Many event sequences described in Section 6.1 include pivotal events that arise from loss of integrity of a passive component, namely one of the aging overpacks, casks or canisters that contain a radioactive waste form. Such pivotal events involve (1) loss of containment of radioactive material that prevents airborne releases, or (2) LOS effectiveness. Both types of pivotal events may be caused by failure modes caused by either physical impact to the container or by thermal energy transferred to the container. This section summarizes the results of the passive failure analyses detailed in Attachment D that yield the conditional probability of loss of containment or LOS.

#### 6.3.2.1 Probability of Loss of Containment

An overview of the methodology for calculating the probability of failure of passive equipment from drops and impact loads is presented in Section 4.3.2.2. Consistent with *Interim* HLWRS-ISG-02 (Ref. 2.2.70), the methodology essentially consists of comparing the demand upon the equipment to a capacity curve. The probability of failure is the value of the cumulative distribution function for the capacity curve, evaluated at the demand upon the container. More detailed discussion is presented in Attachment D, Section D1. The methodology is applicable to the waste forms associated with Intra-Site activities, including transportation casks, aging overpacks, and canisters. (Note that this does not include LLW containers, because when analyzed for each initiating event, these containers were modeled as if they would always fail.) As described in Section 4.3.2.2, the condition at which a passive component is said to fail depends on the success criteria defined for the component in the operation. Passive components are designed and manufactured to ensure that the success criteria are met in normal operating conditions and with margin, to ensure that the success criteria are also met when subjected to abnormal loads, including those expected during event sequences. The design margins, and in some cases materials, may be dictated by the code and standards applied to a given type of container as characterized by tensile elongation data for impact loads and by strength at temperature data for thermal loads.

As described in Section 4.3.2.2, the probability of a passive failure is often based on consideration of variability (uncertainty) in the applied load, and the variability in the strength



(resistance) of the component. The variability in the physical and thermal loading are derived from the systems analysis that defines the probabilities of physical or thermal loads of a given magnitude in a given event sequence. Such conditions arise from the event sequence analysis described in Section 6.1. For the analysis of the effects of fires on waste containers, probability distributions were developed for both the load and the response. For drops and impacts, however, an event sequence analysis is used to define conservative conditions for the load rather than deal with possible ranges of such parameters. Therefore, the calculation of the probability of passive failures is based on the response or resistance characteristics of the container, given the conservative point value for the drop or impact load defined for a given event sequence.

### 6.3.2.2 Probability of Loss of Containment for Drops and Impacts

Calculation of the probability of failure of the various containers is based on the variability in the strength (resistance) of the container as derived from tests and structural analysis, including FEA, detailed in Attachment D, Section D1. Loss of containment probability analysis has been evaluated for various containers in the studies listed below:

- *Seismic and Structural Container Analysis for the PCSA* (Ref. 2.2.32)
- *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations* (Ref. 2.2.80) and *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository* (Ref. 2.2.81)
- *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert* (Ref. 2.2.21).

All analyses have applied essentially the same methods that include FEA to determine the structural response of the various canisters and casks to drop and impact loads, developing a fragility function for the material used in the respective container, and using the calculated responses (strains) with the fragility function to derive the probability of container breach.

Failure probabilities for drops are summarized in Table 6.3-2. Conservative representations of drop height are defined for operations with each type of container. Sometimes more than one conservative drop height is specified, for example, for normal height crane lifts and two-block height crane lifts. LLNL, in *Seismic and Structural Container Analysis for the PCSA* (Ref. 2.2.32, Section 7) predicts failure probabilities of less than 1.0E-08 for most of the events. If a probability for the event sequence is less than 1E-08, additional conservatism is incorporated into the PCSA by using a failure probability of 1E-05, termed “LLNL, adjusted.” This additional conservatism is added to account for (a) future evolutions of cask and canister designs; and (b) uncertainties such as undetected material defects, undetected manufacturing deviations, and undetected damage associated with handling before the container reaches the repository, which are not included in the tensile elongation data.

LLNL calculates strains by modeling representative casks, aging overpacks and canisters that encompass TAD canisters, naval SNF canisters, and a variety of DPCs with the dynamic finite element code, LS-DYNA (Ref. 2.2.32). For these canisters, only flat-bottom drops are

considered to model transfers by a CTM. This is justified because these canisters fit sufficiently tightly within the CTM and potential dropped canisters are guided by the canister guide sleeve of the CTM to remain in a vertical position.

Probability of failure is conservatively calculated by comparing the peak strain to the cumulative distribution function derived from tensile strain to failure test data. BSC FEA analysis used LS-DYNA to model waste packages. Alloy 22 is not stainless steel, but a nickel based alloy, and the most appropriate metric for probability of failure is a cumulative distribution function over extended toughness fraction (Attachment D, Section D1.4). The probability of failure is calculated using the peak toughness index over the waste package, which is a measure of the alloy's energy absorbing capability.

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

	Drop Height (ft)	Failure Probability	Note
Representative transportation cask <sup>a</sup>	6	1.0E-05	3 degrees from horizontal, LLNL, adjusted, no impact limiters
Aging overpack	3	1.0E-05	LLNL, adjusted
Representative canister	32.5 <sup>b</sup>	1.0E-05	Flat bottomed, LLNL, adjusted

NOTE: <sup>a</sup> Also applies to shielded transfer casks (used for waste forms only inside WHF) and horizontal shielded transfer casks.  
<sup>b</sup> This drop height is greater than the maximum drop height associated with Intra-Site Operations.

LLNL = Lawrence Livermore National Laboratory.

Source: Attachment D, Section D1.

Containment failure probabilities due to other physical impact conditions, equivalent to drops, are listed in Table 6.3-3. These probabilities were modeled by LLNL using FEA, resulting in prediction of failure probabilities of less than 1.0E-08. Again, additional conservatism was incorporated by using a failure probability of 1.0E-05 for most of these events. The side impact event was not adjusted from the LLNL result of < 1.0E-08 because of the very low velocities involved. A comparison of the strains induced by drops and slow speed side impacts, indicates significantly lower strains for the low velocity impacts.

Table 6.3-3. Failure Probabilities Due to Miscellaneous Events

Event	Failure Probability	Note
Derail	1.0E-05	LLNL, adjusted, analogous to 6', 3° from horizontal
Rollover	1.0E-05	LLNL, adjusted, analogous to 6', 3° from horizontal
Drop on	1.0E-05	LLNL, adjusted 10-ton load onto container
Side impact from collision with rigid surface	1.0E-08	Or value for low-speed collision, whichever is greater (Table 6.3-4)

NOTE: LLNL = Lawrence Livermore National Laboratory.

Table 6.3-3. Failure Probabilities Due to Miscellaneous Events (Continued)

Event	Failure Probability	Note
-------	---------------------	------

Source: Attachment D, Section D1.6.

Table 6.3-4 shows failure probabilities for various collision events for various containers as a function of impact speed. For each of the events, the collision speed, whether in miles per hour (mph) or feet per minute (fpm) is converted to feet per second (fps), then to an equivalent drop height in feet. The drop heights are very small compared with the drop heights for the modeled situations summarized in Table 6.3-2. The damage to a container, expressed in terms of strain, is roughly proportional to the impact energy, which is proportional to the drop height, as is readily seen from the following:

Energy from drop =  $mgh \propto Fs$  and  $F \propto mg$ , therefore,  $s \propto h$ , where  $s$  = strain,  $F$  = local force on container from drop,  $m$  = mass of container,  $h$  = drop height, and  $g$  = acceleration due to gravity.

For drop heights other than those for the modeled situations presented in Table 6.3-2, failure probabilities can be estimated by shifting capacity curve to match the conservative failure probabilities listed in Table 6.3-2. The mean failure drop height,  $H_m$ , is found so that the probability of failure,  $P$ , (calculated using Equation 24), is the value listed in Table 6.3-2 for the drop height,  $H_d$ , listed in Table 6.3-2.

$$P = \int_{-\infty}^x N(t) dt \quad \text{and} \quad x = \frac{H_d / H_m - 1}{COV} \quad (\text{Eq. 24})$$

where

- $P$  = Probability of failure for container dropped from height  $H_d$
- $N(t)$  = Standard normal distribution with mean of zero and standard deviation of one
- $t$  = Variable of integration
- $H_d$  = Modeled drop height for which the failure probability has been determined
- $H_m$  = Median failure drop height of the failure drop height distribution such that the failure probability at the modeled drop height,  $H_d$ , is  $P$
- $COV$  = Coefficient of variation, which is the ratio of standard deviation to mean for strain capacity distribution, applied here to stress capacity or true tensile strength

The probabilities of failure for the collision cases listed in Table 6.3-4 are then determined using the above formula with  $H_m$  determined above and with  $H_d$  being the drop height corresponding to the collision speed as listed in Table 6.3-4. The failure probabilities of these events are shown in PEFA Chart.xls included in Attachment H.



Table 6.3-4. Failure Probabilities for Collision Events

Collision Scenario	Speed	Velocity (ft/sec) <sup>a</sup>	Equivalent Drop Height (ft) <sup>b</sup>	Failure Probabilities for Various Container Types				
				Transportation Cask	Canister	Waste Package	MCO	High-Level Radioactive Waste
Railcar	9.0 mph	13.20	2.71	1.00E-08				
Truck trailer	9.0 mph	13.20	2.71	1.00E-08				
Site Transporter	2.5 mph	3.67	0.21		1.00E-08		1.00E-08	1.00E-08

NOTE: <sup>a</sup>. Conversions from the previous column are as follows. From speed in mph: multiply by 5280/3600. From speed in ft / min: divide by 60.

<sup>b</sup>. Calculated as follows based on constant acceleration due to gravity (no air resistance):  $v^2 / (2 \times 32.2 \text{ ft / sec}^2)$ , where v is the velocity in ft / sec. Values are rounded to the nearest hundredth of a ft.

DPC = dual-purpose canister; DSTD = DOE standardized canister; ft = foot; MCO = multicanister overpack; min = minutes; mph = miles per hour; sec = seconds; TAD = transportation, aging, and disposal.

Source: Original

### 6.3.2.3 Probability of Canister Failure in a Fire

In addition to passive equipment failures as a result of structural loads, passive failures can also occur as a result of thermal loads such as exposure to fires or abnormal environmental conditions, for example, loss of HVAC cooling. The PCSA evaluates the probability of loss of containment (breach) due to a fire for several types of waste containers, including: transportation casks containing uncanistered commercial SNF assemblies, and canisters representative of TAD canisters, DPCs, DOE standardized canisters, HLW canisters, and naval SNF canisters.

The methods for analyzing thermally induced passive failures are discussed in Section 4.3.2.2, and detailed in Attachment D. In summary, the probability of failure of a waste container as a result of a fire is evaluated by comparing the demand upon a container (which represents the thermal challenges of the fire vis-à-vis the container), with the capacity of the container (which represents the variability in the temperature at which failure would occur). The demand upon the container is controlled by the fire duration and temperature, because these factors control the amount of energy that the fire could transfer to the container.

In response to a fire, the temperature of the waste container under consideration increases as a function of the fire duration. The maximum temperature is calculated using a heat transfer model that is simplified to allow a probabilistic analysis to be performed that accounts for the variability of key parameters. The model accounts for radiative and convective heat transfers from the fire, and also for the decay heat from the waste form inside a container. The temperature evolution of waste containers is analyzed based on a simplified geometry with a wall thickness that, for the range of waste containers of interest in the PCSA, is representative or conservatively small. Specifically, two characteristic canister wall thicknesses are modeled: 0.5 inches, characteristic of some DPCs and other waste canisters; and 1.0 inches, the anticipated thickness of TAD canisters and naval SNF canisters. The wall thickness of a container is an important parameter that governs both container heating and failure. Other conservative and realistic modeling approaches are introduced in the heat transfer model, as appropriate. For example, fires are conservatively considered to engulf a container, regardless of the fact that a fire at the GROA may simply be in the same room as a container. When handled, TAD canisters, DPCs, DOE standardized canisters, HLW canisters and naval SNF canisters are enclosed within another SSC, for example a transportation cask, the shielded bell of a canister transfer machine, or a waste package. Therefore, a fire does not directly impinge on such canisters. In contrast, the external surface of a transportation cask containing uncanistered commercial SNF may be impinged upon directly by the flames of the fire.

Accounting for the uncertainty of the key parameters of the fires and the heat transfer model, the maximum temperature reached by a waste container, which represents the demand upon the container due to a fire, is characterized with a probability distribution. The distribution is obtained through Monte Carlo simulations.

To determine whether the temperature reached by a waste container is sufficient to cause the container to fail, the fire fragility distribution curve for the container is evaluated. In the PCSA, this curve is expressed as the probability of breach of the container as a function of its temperature. Two failure modes are considered for a container that is subjected to a thermal

challenge: creep-induced failure and limit load failure. Creep, the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load, is possible for long duration fires. Limit load failure corresponds to situations where the load exerted on a material exceeds its structural strength. This failure mode is considered because the strength of a container decreases as its temperature increases. The variability of the key parameters that can lead to a creep-induced failure or limit load failure is modeled with probability distributions. Monte Carlo simulations are then carried out to produce the fire fragility distribution curve for a container.

The probability of a waste container losing its containment function as a result of a fire is calculated by running numerous Monte Carlo simulations in which the temperature reached by the container, sampled from the probability distribution representing the demand on the container, is compared to the sampled failure temperature from the fragility curve. The model counts the simulation result as a failure if the container temperature exceeds the failure temperature. Statistics based upon the number of recorded failures in the total number of simulations are used to estimate the mean of the canister failure probability.

Table 6.3-5 shows the calculated mean and standard deviation for the failure probability of a canister in the following configurations: a canister in a transportation cask, a canister in a waste package, and a canister in a shielded bell.

Table 6.3-5. Summary of Canister Failure Probabilities in Fire

Configuration <sup>a</sup>	Failure Probability	
	Mean	Standard Deviation
Thin-Walled Canister in a Transportation Cask	2.0E-06	1.4E-06
Thick-Walled Canister in a Transportation Cask <sup>b</sup>	1.0E-06	1.0E-06

NOTE: <sup>a</sup> Configurations not addressed in this table include any canister inside an aging overpack. In this configuration, the canister is protected from the fire by the massive concrete overpack. Calculations have shown that the temperatures experienced by the canister in these configurations are well below the canister failure temperature, so that failures for these configurations can be screened. For conservatism, a screening conditional probability of 1E-06 could be used.

<sup>b</sup> Naval SNF canisters are modeled as thick walled. Other canisters are modeled as thin walled.

Source: Attachment D, Table D2.1-9.

Note that no failure probability is provided for a bare canister configuration. The reason for this is that the canister is outside of a cask for only a short time. During that time, the canister is usually inside the shielded bell of the CTM. The preceding analysis addressed a fire outside the shielded bell. When in that configuration, the canister is shielded from the direct effects of the fire. A fire inside the shielded bell, which could directly heat the canister, is not considered to be credible for two reasons. First, the hydraulic fluid used in the CTM equipment is non-flammable and no other combustible material could be present inside the bell to cause a fire. Second, the annular gap between the canister and the bell is only three inches wide, but is approximately 27 feet long. Given this configuration, it is unlikely that there is sufficient inflow of air to sustain a large fire that could heat a significant portion of the canister wall. There may be sufficient inflow to sustain a localized fire, but such a fire would not be adequate to heat the canister to failure.

The canister is also outside of a cask, or shielded bell as it is being moved from a cask into the shielded bell or from the shielded bell into a waste package. The time during which the canister is in this configuration is extremely short, a matter of minutes, so a fire that occurs during this time is extremely unlikely. In addition, because the gap between the top of the cask and ceiling of the transfer cell is generally much shorter than the height of the canister, only a small portion of the canister surface is exposed to the fire. Furthermore, this exposure would only be for the short time that the canister was in motion.

For these reasons, failure of a bare canister was not considered credible and is not explicitly modeled in the PCSA. The bare canister configuration is not applicable to Intra-Site Operations.

#### **6.3.2.4 Probability of Loss of Containment from Heat-up**

In addition to fire-related passive failures, the PCSA considered other passive equipment failures due to abnormal thermal conditions. The thermal event of greatest concern for Intra-Site Operations is loss of cooling on the aging pad (e.g., caused by blockage of the vents of an aging overpack or HAM are blocked for a prolonged period). However, this initiating event has been screened out based on thermal analysis, which determined it is not a challenge to canister containment (Table 6.0-2). Aging overpacks and HAMs are designed to use natural ventilation to move decay heat away from the canister during aging. If all of the vents become blocked for a prolonged period, the process would be impeded. However, each aging overpack and HAM has multiple vents, and each vent opening has a screen to prevent large debris and animal interference from creating blockage. In addition, the aging overpacks and HAMs have instrumentation to monitor canister temperature to determine completion of aging. This instrumentation can also serve to provide a warning if the temperature increases. Lastly, because the instrumentation on each aging overpack and HAM will be checked regularly, it is unlikely that blocked vents will go unnoticed and will be cleared as standard maintenance and housekeeping activities.

#### **6.3.2.5 Probability of Loss/Degradation of Shielding**

Loss or degradation of shielding probabilities are summarized in Table 6.3-6. Some of the items discussed in this section and listed in Table 6.3-6 are not used for Intra-Site Operations, such as the WPTT, but they are included in this section to illustrate the consistency of methodology across facilities and equipment.

Shielding of a waste form that is being transported inside the GROA is accomplished by several types of shielded containers, including: transportation casks, horizontal or vertical shielded transfer casks, aging overpacks, shielded components of a WPTT, and shielded components of a TEV. In addition to a shielding function, sealed transportation casks and horizontal or vertical shielded transfer casks exert a containment function.

A structural challenge may cause shielding degradation or shielding loss. LOS occurs when an SSC fails in a manner that leaves a direct path for radiation to stream, for example as a result of a breach. Degradation of shielding occurs when a shielding SSC is not breached, but its shielding function is degraded. In the PCSA, a shielding degradation probability after a structural challenge is derived for those transportation casks that employ lead for shielding. Finite-element



analyses on the behavior of transportation casks subjected to impacts associated with various collision speeds, reported in *Reexamination of Spent Fuel Shipment Risk Estimates*, NUREG/CR-6672 (Ref. 2.2.82, Section 5.1.4), indicate that lead slumping after an end impact could result in a reduction of shielding; transportation casks without lead are not susceptible to such shielding degradation. This information is used in Attachment D, Section D3, to derive the shielding degradation probability of a transportation cask at drop heights characteristic of crane operations. The distribution is developed for impacts on surfaces made of concrete, which compare to the surfaces onto which drops could occur at the GROA. No impact limiter is relied upon to limit the severity of the impact. Conservatively, the distribution is applied to transportation casks and also shielded transfer casks, regardless of whether or not they use lead for shielding. Thus, for containers that have both a containment and shielding function, the PCSA considers a probability of containment failure (which is considered to result in a concurrent LOS), and also a probability of shielding degradation (which is associated with those structural challenges that are not sufficiently severe to cause loss of containment). Table 6.3-6 displays the resulting shielding degradation probabilities for transportation casks and shielded transfer casks after a structural challenge. Given that there is significant conservatism in the calculation of strain and the uncertainty associated with the fragility (strength), the resulting estimates include uncertainties and are considered conservative

Shielding loss is also considered to potentially affect an aging overpack subjected to a structural challenge, if the waste container inside does not breach. Given the robustness of aging overpacks, a shielding loss after a 3-ft drop height is calculated to have a probability of 5E-06 per aging overpack impact, based upon the judgment that this probability may be conservatively related to but lower than the probability of breach of an unprotected waste container inside the aging overpack (Attachment D, Section D3). If the structural challenge is sufficiently severe to cause the loss of containment (breach) of the waste container inside the aging overpack, the loss of the aging overpack shielding function is considered guaranteed to occur.

A CTM provides shielding with the shield bell, shield skirt, and associated slide gates. Also, the CTM is surrounded by shield walls and doors, which are unaffected by structural challenges resulting from internal random initiating events. Therefore, such challenges leave the shielding function intact. (CTMs are not used for Intra-Site Operations.) The PCSA treats the degradation or loss of shielding of an SSC due to a thermal challenge as described in the following paragraphs.

If the thermal challenge causes the loss of containment (breach) of a canister, the SSC that provides shielding and in which the canister is enclosed is considered to have lost its shielding capability. A transportation cask containing uncanistered commercial SNF is also considered to have lost its shielding if it has lost its containment function.

The shielding structure provided by the CTM is not subjected to drops. Such shields may be subjected to collisions or dropped heavy objects. The analysis detailed in Attachment D, Section D3, indicates there is no challenge to the shielding from these events. Therefore, these components are assigned zero probability in Table 6.3-6.

If the thermal challenge is not sufficiently severe to cause a loss of containment function, it is nevertheless postulated that it will cause shielding loss of the transportation cask, shielded

transfer cask, canister transfer machine, or cask transfer trolley affected by the thermal challenge and in which the waste container is enclosed. This is because the neutron shield on these SSCs is made of a polymer which is not anticipated to withstand a fire without failing. Note, however, that the degradation of gamma shielding of these SSCs is unlikely to be affected by a credible fire. Although credible fires could result in the lead melting in a lead-sandwich transportation cask, there is no way to displace the lead, unless the fire is accompanied by a puncture or rupture of the outer steel wall of the cask. Preliminary calculations were unable to disprove the possibility of hydraulic failure of the steel encasing due to the thermal expansion of molten lead, so loss of gamma shielding for steel-lead-steel transportation casks engulfed in fire is postulated. Conservatively, in the PCSA, transportation casks and shielded transfer casks are postulated to lose their shielding function with a probability of one, regardless of whether or not they use lead for shielding.

Aging overpacks made of concrete are not anticipated to lose their shielding function as a consequence of a fire because the type of concrete used for aging overpacks is not sensitive to spallation. In addition, it is likely that the aging overpacks will have an outer steel liner. For these reasons, a loss of aging overpack shielding in a fire has been screened from consideration in the PCSA

Table 6.3-6. Probabilities of Loss of Shielding

	Probability	Note
Sealed Transportation cask and shielded transfer casks shielding degradation after structural challenge	1.0E-05	Section D, Section D3.4.
Aging overpack shielding loss after structural challenge	5E-06	Section D, Section D3.4.
Shielding loss by fire for waste forms in transportation casks or shielded transfer casks	1	Lead shielding could potential expand and degrade. This probability is conservatively applied to transportation casks that do not use lead for shielding.
Shielding loss by fire for aging overpacks	0	Type of concrete used for aging overpacks is not sensitive to spallation.

Source: Attachment D, Table D3.4-1

### 6.3.2.6 Probability of Other Fire-Related Passive Failures

In addition to the canisters, other passive equipment could fail as a result of a fire. For the PCSA, only failures that would result in a radionuclide release or radiation exposure are considered.

### 6.3.2.7 Application to Event Sequence Models

Table 6.3-7 lists the basic event names for passive failure events used in the event sequence modeling and quantification for Intra-Site Operations. The values are either specifically developed in Attachment D, or are values from bounding events. Probabilities for some events were obtained by extrapolation from developed probabilities as described in this section or in Attachment D. The derivation of all passive failure probabilities is described in Attachment D and shown in PEFA Chart.xls, included in Attachment H.

It is noted that Table 6.3-7 addresses all passive event failures for the various waste form configurations. Table 6.3-8 identifies the specific passive failure basic events used in event sequence modeling and quantification. The probability of each basic event is based on one of the values presented in Tables 6.3-2 through 6.3-7.

Table 6.3-7. Summary of Passive Event Failure Probabilities

	10 T dropped on container	Container vertical drop from normal operating height	Container 30-foot vertical drop	6-foot Horizontal Drop, Rollover	2.5 mph Flat side impact/collision	2.5 mph Localized side impact/collision	9 mph Flat side impact/collision	2.5 mph end-to-end Collision	9 mph end-to-end Collision	Thin-Walled Canister Fire or UCSNF on TT-Cask Fire	Thick-Walled Canister (NAV only) Fire
<b>Loss of Containment</b>											
Canister in Transport Cask	1.E-05	1.E-05	1.E-05	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	2.E-06	1.E-06
Transport Cask with Bare Fuel	1.E-05	1.E-05	1.E-05	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	5.E-02 <sup>1</sup>	6.E-03 <sup>2</sup>
Canister	1.E-05	1.E-05	1.E-05 <sup>3</sup>	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Canister in AO	1.E-05	1.E-05	N/A	1E-08	1.E-08	1.E-08	1.E-08	N/A	N/A	1.E-06	1.E-06
<b>Loss of Shielding</b>											
Transport Cask	1.E-05	1.E-05	—	1.E-05	1.E-08	1.E-08	1.E-08	1.E-08	1.E-08	~ 1	~ 1
Aging Overpack	1.E-05	5.E-06	N/A	N/A	1.E-05	1.E-05	1.E-05	1.E-05	1.E-05	~ 0	~ 0

NOTE: <sup>1</sup> Truck cask

<sup>2</sup> Rail cask

<sup>3</sup> Ram impact or vertical drop (used 30-ft canister drop, but actual height is 6 ft); ram strength by design not to puncture, therefore less than force of 30-ft drop)

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

Source: Attachment D

Table 6.3-8. Passive Failure Basic Events used in Intra-Site Operations Event Sequence Analysis

Basic Event ID	Basic Event Description	Basic Event Value
CANISTER_AO_DROP	Canister in aging overpack fails due to drop	1E-05
CANISTER_AO_IMPACT	Canister in aging overpack fails due to impact	1E-08
CANISTER_HAM_IMPACT	HAM fails due to impact	1E-08
CANISTER_HAM_OPS	Canister fails due to impact	1E-05
CANISTER1	Canister inside a transportation cask fails due to derailment, collision, or impact event (that is, when canister failure is included as part of transportation cask failure)	1
CONTAINER_LLW	LLW container fails	1
MODERATOR_SOP	Presence of moderator during nonfire event sequences	0
SHIELD_AO_DROP	Aging overpack shielding loss due to drop	5E-06
SHIELD_AO_IMPACT	Aging overpack shielding loss due to impact	1E-05
SHIELD_HAM_IMPACT	HAM shielding loss due to impact	1E-05
SHIELD_TCASK_COL	Transportation cask shielding loss due to a collision event	1E-08
SHIELD_TCASK_DROP	Transportation cask shielding loss due to drop event	1E-05
SHIELD_TCASK_DROPON	Transportation cask shielding loss due to an object dropping on the cask	1E-05
TCASK_COLLIDE_RC	Transportation cask on railcar fails due to collision	1E-08
TCASK_COLLIDE_TT	Transportation cask with impact limiters on truck trailer fails due to collision, resulting in drop/rollover (see note)	1E-08
TCASK_DERAIL	Transportation cask fails due to derailment	1E-05
TCASK_DROPON	Transportation cask fails due to object impact	1E-05
TCASK_DROPON_UCSNF	Transportation cask containing UCSNF fails due to object impact	1E-05
TCASK_HTC_DROP	HTC or HSTC fails due to drop	1E-05
TCASK_HTC_IMPACT	HTC or HSTC fails due to collision/impact	1E-08
THERMAL		
FIRE_CANISTER_AO	Canister inside an aging overpack/HAM fails due to thermal challenge	1E-06
FIRE_CANISTER_TC	Canister inside a transportation cask fails due to thermal challenge	2E-06
FIRE_CANISTER_TC_NAV	Naval canister inside a transportation cask fails due to thermal challenge	1E-06
FIRE_MODERATOR	Presence of moderator during fire event sequences	1
FIRE_MODERATOR_NA	Moderator ability to reach contents in a fire	0
FIRE_SHIELD_AO	Aging overpack shielding loss due to fire	0
FIRE_SHIELD_TCASK	Transportation cask shielding loss due to fire	1
FIRE_TCASK_UCSNF	Transportation cask containing UCSNF fails due to fire	5E-02

NOTE: Refer to Attachment D, Section D2, provides a detailed discussion of PEFA.  
HAM = horizontal aging module; HSTC = horizontal shielded transfer cask; HTC = transportation cask that is never upended; LLW = low-level radioactive waste; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

### 6.3.3 Miscellaneous Data

Table 6.3-9 identifies the frequencies associated with fires evaluated for Intra-Site operations. Data that are not defined as Active Component Reliability Data (Section 6.3.1) or Passive Equipment Failure Data (Section 6.3.2), but are used in the reliability analysis for this facility are listed in Table 6.3-10.

Table 6.3-9. Fire Analysis Frequencies

Initiating Event	Mean frequency (per 50 years)
Fire Threatens a Waste Form During Onsite Transport	9E-07 fires/operation
Fire Threatens a Waste Form in Buffer Area	0.3 fires
Fire Threatens a Waste Form on Aging Pad	0.6 fires
Fire Threatens LLW in the LLWF	4.1E-01 fires
Large Fire Threatens LLW in the LLWF	6.8E-02 fires

NOTE: LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility.

Source: Attachment F, Table F5.3-1 and Table F6-1.

Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
CONTAINER_LLW	LLW container fails	1	To be conservative, initiating events involving LLW containers are modeled as if the container always fails.	N/A
MODERATOR_SOP	Presence of moderator during nonfire event sequences	0	There is no other moderator source outside of the waste handling facilities. Moderator is only present for Intra-Site Operations during fire events in which a fire brigade attempts to extinguish the fire with water.	N/A
FIRE_MODERATOR	Presence of moderator during fire event sequences	1	Moderator is only present for Intra-Site Operations during fire events in which a fire brigade attempts to extinguish the fire with water. To be conservative, the fire initiating events are modeled as if the fire brigade always responds and always uses sufficient water to act as a moderator.	N/A
FIRE_MODERATOR_NA	Used for waste forms for which moderator is not a concern during fire events (i.e., HLW and UCSNF)	0	Criticality safety design control features are not necessary for HLW canisters because the concentration of fissile isotopes in an HLW canister is too low to have criticality potential (Ref. 2.2.31, Table 6).  As described in Section 6.0.7, moderator cannot reach cask contents for the UCSNF waste form during fire events.	<i>Preclosure Criticality Safety Analysis</i> (Ref. 2.2.31, Table 6), and Section 6.0.7
DPC_RC	Number of transportation casks containing DPCs on railcars	346	This basic event represents the number of transportation casks containing DPCs estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
HDPC_RC	Number of transportation casks containing HDPCs on railcars	346	This basic event represents the number of transportation casks containing HDPCs estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
HLW_RC	Number of transportation casks containing HLW on railcars	1,860	This basic event represents the number of transportation casks containing HLW estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)

Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
NAV_RC	Number of transportation casks containing naval canisters on railcars	400	This basic event represents the number of transportation casks containing naval canisters estimated to arrive on railcars over the preclosure period.	(Ref. 2.2.23)
MCO_RC	Number of transportation casks containing MCOs on railcars	113	This basic event represents the number of transportation casks containing MCOs estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
DSTD_RC	Number of transportation casks containing DOE standardized canisters on railcars	385	This basic event represents the number of transportation casks containing DOE standardized canisters estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
TAD_RC	Number of transportation casks containing TAD canisters on railcars	6,978	This basic event represents the number of transportation casks containing TAD canisters estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
UCSNF_RC	Number of transportation casks containing uncanistered commercial spent nuclear fuel on railcars	0	This basic event represents the number of transportation casks containing uncanistered commercial spent nuclear fuel estimated to arrive on railcars over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
DPC_TT	Number of transportation casks containing DPCs on truck trailers	0	This basic event represents the number of transportation casks containing DPCs estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
HDPC_TT	Number of transportation casks containing HDPCs on truck trailers	0	This basic event represents the number of transportation casks containing HDPCs estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)



Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
HLW_TT	Number of transportation casks containing HLW on truck trailers	500	This basic event represents the number of transportation casks containing HLW estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
NAV_TT	Number of transportation casks containing naval canisters on truck trailers	0	This basic event represents the number of transportation casks containing naval canisters estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
MCO_TT	Number of transportation casks containing MCOs on truck trailers	113	This basic event represents the number of transportation casks containing MCOs estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
DSTD_TT	Number of transportation casks containing DOE standardized canisters on truck trailers	385	This basic event represents the number of transportation casks containing DOE standardized canisters estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
TAD_TT	Number of transportation casks containing TAD canisters on truck trailers	0	This basic event represents the number of transportation casks containing TAD canisters estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis, and engineering judgment. That is, TADs will not arrive on truck trailers because fully loaded TADs are too heavy to allow transport on truck trailers. If the rail system is not fully operational when the repository is opened, it is logical that, if necessary, other truck casks (or truck cask/canister systems) would be used. Therefore, it is not necessary to analyze TADs on truck trailers.	(Ref. 2.2.23) and engineering judgment
UCSNF_TT	Number of transportation casks containing uncanistered commercial spent nuclear fuel on truck trailers	3,775	This basic event represents the number of transportation casks containing uncanistered commercial spent nuclear fuel estimated to arrive on truck trailers over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)

Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
DPC_AO	Number of DPCs aged in an aging overpack at the Aging Facility	346	This basic event represents the estimated number of aging overpacks containing DPCs to be sent to the Aging Facility over the preclosure period for thermal management. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
TAD_AO	Number of TAD canisters aged in an aging overpack at the Aging Facility	8,143	This basic event represents the estimated number of aging overpacks containing TAD canisters to be sent to the Aging Facility over the preclosure period for thermal management. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
HDPC_HAM	Number of HDPCs aged in a HAM at the Aging Facility	346	This basic event represents the estimated number of HTCs containing HDPCs to be sent to the Aging Facility for thermal management in HAMs over the preclosure period. The value for this basic event is obtained from the throughput analysis.	(Ref. 2.2.23)
DAW_HEPAs_WHF_ITS_STAGE1_ONLY	Number of DAW HEPAs (WHF ITS STAGE 1 only)	1,800	For dose calculations, these HEPA filters are the only DAW that are anticipated to have significant levels of contaminants; "1,800" is based on <i>Shielding Requirements and Dose Rate Calculations for WHF and LLWF</i> (Ref. 2.2.22, Section 3.1.9), which estimated 30 filters are changed every 10 months (to maintain contamination levels at or below Class B for LLW), over the 50-year preclosure period. In addition, it is conservatively estimated that each HEPA filter will be containerized and moved to the LLWF individually.	(Ref. 2.2.22, Section 3.1.9)
WET_SOLID_RESIN_XFRS	Number of HICs containing WET-res (from WHF resin beds)	150	Sluicing each resin bed once per year (3 beds total), results in 150 high-integrity containers (HICs) over the preclosure period. This is conservative, because the WHF could opt to do a maintenance shutdown of the facility and sluice all three resin beds into one HIC. This would result in a minimum number of HICs, that is, 50 HICs over the preclosure period.	(Ref. 2.2.22, Sections 3.1.6 and 3.1.8)

Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
WET_SOLID_NONR ESIN_XFR	WET-nr (WHF pool filters)	150	Operational plan for storing and moving pool filters: Filters from WHF PWTS will be stored in WHF in a HIC. It is estimated that 520 filters will be generated annually, and each HIC holds up to 200 filters. This results in 3 HICs per year, and each filled HIC will be moved to the LLWF (or directly offsite) on a flatbed trailer (lowboy or equivalent). Over the 50-yr preclosure period, this results in 150 HICs.	(Ref. 2.2.85)
Boundary to CRCF3 (080)	Distance between the GROA boundary and the furthest waste handling facility (CRCF3 (080))	2	Manually measured on scale drawing the travel distance (miles) between the GROA boundary and the furthest waste handling facility (CRCF-3). Rounded to one significant figure.	(Ref. 2.2.28)
Furthest Aging Pad to CRCF3 (080)	Distance between CRCF3 (080) and the furthest aging pad (17P)	2	Manually measured on scale drawing the travel distance (miles) between CRCF3 (080) and the furthest aging pad (17P). Rounded to one significant figure.	(Ref. 2.2.27)
No. Moves Each Transportation Cask – ESD-01	Number of times a transportation cask on a railcar or a transportation cask on a truck trailer travels between the site boundary and a facility	1	The TC/RC or TC/TT is only moved once between the site boundary and the facility: upon receipt of the TC, it is moved to a facility where the TC is removed from the RC or TT.	(Ref. 2.2.29)
No. Moves via ST – ESD-02	Number of times an aging overpack travels between a surface handling facility and the Aging Facility (via the site transporter)	2	The aging overpack is moved twice - once from a handling facility to the Aging Facility for thermal management, and once from the Aging Facility to a handling facility when aging is complete.	(Ref. 2.2.29)
No. Moves via Cask Tractor/Cask Transfer Trailer – ESD-03	Number of times an HTC or HSTC containing an HDPC travels between a surface handling facility and the Aging Facility (via the cask tractor/cask transfer trailer)	2	The HDPC is moved twice (in either an HTC or an HSTC) – once to the Aging Facility for thermal management, and once to a handling facility when aging is complete.	(Ref. 2.2.29)
No. Moves via Cask Transfer Trailer – ESD-04	Number of times an HDPC is inserted into or retrieved from a HAM (cask transfer trailer operations)	2	The HDPC is moved twice – once to insert the canister into the HAM for aging, and once to retrieve it for handling at the WHF.	(Ref. 2.2.29)
No. Moves – per LLW container; ESD-05	The average number of movements within the LLWF for a given LLW container	3	Engineering judgment, based on general knowledge of warehouse movements involving typical equipment such as forklifts.	N/A

Table 6.3-10. Miscellaneous Data Used in the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	Reference(s)
No. Transfers per LLW container ESD-08	The overall number of transfer movements for each LLW container (i.e., from the generating facility to either the LLWF or offsite)	1	Engineering judgment, based on general knowledge of warehouse movements involving typical equipment such as forklifts.	N/A

NOTE: CRCF = Canister Receipt and Closure Facility; DAW = dry active waste; DOE = Department of Energy; DPC = dual-purpose canister; ESD = event sequence diagram; GROA = geologic repository operations area; HAM = horizontal aging module; HEPA = high-efficiency particulate air filter; HLW = high-level radioactive waste; HDPC = horizontal dual-purpose canister; HIC = high-integrity container; HSTC = horizontal shielded transfer cask; HTC = horizontal transportation cask that is not upended; ITS = important to safety; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; MCO = multicanister overpack; PWTS = pool water treatment system; RC = railcar; ST = site transporter; TAD = transportation, aging, and disposal; TT = truck trailer; UCSNF = uncanistered commercial spent nuclear fuel; WHF = Wet Handling Facility.

Source: Original (further information provided in "References" column)

## 6.4 HUMAN RELIABILITY ANALYSIS

The PCSA has emphasized HRA because the waste handling processes include substantial interactions between equipment and operating personnel. If there are human interactions that are typically associated with the operation, test, calibration, or maintenance of a certain type of SSC (e.g., drops from a crane when using slings), and this SSC has been treated using industry-wide data, per Attachment C, then HFEs may be implicit in the reliability data. The analyst is tasked with determining whether that is the case. Otherwise, the analyst includes explicit identification, qualitative modeling, and quantification of HFEs, as described in this section. The methodology applied is provided in Section 4.3.4, and the detailed description of the HRA is presented in Attachment E.

### 6.4.1 HRA Scope

The scope of the HRA is established in order to focus the analysis on the issues pertinent to the goals of the overall PCSA. Thus, the scope is as follows:

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers. Such scenarios may include the need for mitigation of radionuclides, such as provided by the confinement HVAC system in a waste handling facility.
2. Pursuant to the above, the following types of HFEs are excluded:
  - A. HFEs resulting in standard industrial injuries (e.g., falls)
  - B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount
  - C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.
3. The identification of HFEs is restricted to those areas of the facility that handle waste forms, and only during the times that waste forms are being handled (e.g., HFEs are not identified for the site transportation of empty aging overpacks).
4. The exception to #3 is that system-level HFEs are considered for support systems when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.
5. Post-initiator recovery actions (as defined in Attachment E, Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.
6. In accordance with the boundary conditions of the PCSA discussed in Section 4.3.10.1, initiating events associated with conditions introduced in SSCs before they reach the site are not, by definition of 10 CFR 63.2 (Ref. 2.3.2) within the scope of the PCSA nor, by extension, within the scope of the HRA.

## 6.4.2 Base Case Scenarios

The first step in this analysis is to describe Intra-Site Operations in sufficient detail such that the human reliability analysts can identify specific deviations that would lead to a radiation release, a direct exposure, or a criticality event.

Intra-Site Operations cover the following four high-level operational activities:

1. Site transportation of SNF and HLW
2. Aging activities, including transit between the waste handling facilities and the Aging Facility, and thermal aging of TAD canisters and DPCs
3. LLWF operations
4. BOP facilities that directly or indirectly establish or support the repository infrastructure and operating services systems.

The base case scenario represents a realistic description of expected facility, equipment, and operator behavior for the selected operation. These scenarios are created from discussions between the human reliability analysts, other PCSA analysts, and personnel from engineering and operations. In addition to a detailed description of the operation itself, these base case scenarios include a brief description of the initial conditions and relevant equipment features (e.g., interlocks).

## 6.4.3 Identification of Human Failure Events

There are many possible human errors that could occur at YMP, the effects of which might be significant to safety. Human errors, based upon the three temporal phases used in PRA modeling, are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs
- Post-initiator HFEs<sup>1</sup>:
  - Non-recovery
  - Recovery.

Each of these types of HFEs is defined in Attachment E, Section E5.1.1.1. The PCSA model was developed and quantified with pre-initiator and human-induced initiator HFEs included in

---

<sup>1</sup> Terminology common to nuclear power plants refers to post-initiator non-recovery events as Type C events and recovery events as Type CR events.

the model. The safety philosophy of waste handling operations is that an operator need not take any action after an initiating event, and there are no actions identified that could exacerbate the consequences of an initiating event. This stems from the definitions and modeling of initiating events and subsequent pivotal events as described in Section 6.1 and Attachment A. All initiating events are proximal causes of either radionuclide release or direct exposure to personnel. With respect to the latter, personnel evacuation was not considered in reducing the frequency of direct exposure, but personnel action could cause an initiating event. With respect to the former, pivotal events address containment integrity, confinement availability, shielding integrity, and moderator availability that have no post-initiator human interactions. Containment and shielding integrity are associated only with the physical robustness of the waste containers. For waste handling facilities, confinement availability is associated with a continuously operating HVAC and the status of equipment confinement doors. Human interactions for HVAC are pre-initiator. Human actions for shielding are associated the initiator phase. Recovery post-initiator HFEs were not identified and not relied upon to reduce event sequence frequency. Thus, the focus of the HRA task is to support the other PCSA tasks to identify these two HFE phases.

### **Pre-Initiator HFEs**

Pre-initiator HFEs are identified by the system analysts when modeling fault trees during the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human CCF.

### **Human-Induced Initiator HFEs**

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the facility and the SSCs in order to appropriately model the human interface. This iterative process began with the HAZOP evaluation, the MLD and event sequence development, and the event tree and fault tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the model. Included in this process is an extensive information collection process where industry data for potential vulnerabilities and HFE scenarios are reviewed. The following sources were examined:

- “Summary Tables.” *Large Truck Crash Causation Study*. (Ref. 2.2.38)
- “Speeding Counts...on All Roads!” (Ref. 2.2.39)
- *Traffic Safety Facts 2002: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System* (Ref. 2.2.40)
- *Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report* (Ref. 2.2.9)

- *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 – 2002*, NUREG-1774 (Ref. 2.2.53)
- Control of Heavy Loads at Nuclear Power Plants, NUREG-0612 (Ref. 2.2.63)
- *Naval Facilities Engineering Command (NAVFAC) Internet Web Site*, Navy Crane Center. The database includes the following information:
  - Naval Crane Center Quarterly Reports (“Crane Corner”) 2001 through 2007
  - Naval Crane Center Fiscal Year 2006 Crane Safety Reports (covers fiscal year 2001 through 2006)
  - Naval Crane Center Fiscal Year 2006 Audit Report
- *DOE Occurrence Reporting and Processing System (ORPS) Internet Web Site*, Operational Experience Summaries (2002 through 2007)
- Institute of Nuclear Power Operations database, which contains the following information:
  - Licensee event reports
  - Equipment Performance and Information Exchange System
- Nuclear Plant Reliability Data System.
- *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)* (Ref. 2.2.10)
- All SCIENTECH/Licensing Information Service data on independent SNF storage installation events (1994 through 2007) and Dry Storage Information Forum (New Orleans, LA, May 2-3, 2001). This database includes the following information:
  - Inspection reports
  - Trip reports
  - Correspondence

HFEs identified include both errors of omission and errors of commission.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., PSFs). This combination of conditions and human factor concerns then becomes the EFC for a specific HFE. Additions and refinements to these initial EFCs are made during the preliminary and detailed analyses.



#### 6.4.4 Preliminary Analysis

A preliminary analysis is performed to allow HRA resources for the detailed analyses to be focused on only the most risk-significant HFEs. The preliminary analysis includes verification of the validity of HFEs included in the initial PCSA model, assignment of conservative HEPs to all HFEs and verification of those probabilities. The actual quantification of preliminary values is a six-step process that is described in detail in Appendix E.III of Attachment E. Once the preliminary probabilities are assigned, the PCSA model is quantified (initial quantification) to determine which HFEs require a detailed quantification. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, an aggregated event sequence is Category 1 or Category 2 according to 10 CFR 63.111 (Ref. 2.3.2) performance objectives.

In cases where HFEs are completely mitigated by hardware (i.e., interlocks), the HFE is generally assigned a value of 1.0 unless otherwise noted, and the hardware is modeled explicitly in the fault tree.

HFE probabilities produced in this HRA are mean values; uncertainties are accounted for by applying an error factor to the mean value of the overall HFE, according to the guidelines presented in Section E3.4 of Attachment E.

#### 6.4.5 Detailed Analysis

Once preliminary values have been assigned, the model is run and HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, that sequence is Category 1 or Category 2. A dominant sequence is one that does not meet the performance objectives according to 10 CFR 63.111 (Ref. 2.3.2). The objective of a detailed analysis is to develop a more realistic HRA and identify design features to be added that will provide compliance with the aforementioned regulation. Many of the ITS features in Section 6.9 were identified during the HRA. The preliminary values were sufficient to demonstrate compliance with the performance objectives of 10 CFR 63.111; therefore no detailed analyses were performed for this HRA.

#### 6.4.6 Human Failure Event Probabilities used in Intra-Site Operations Event Sequences Analysis

The results of the HRA are the HFE probabilities used in the event tree and fault tree quantification process, which are listed in Table 6.4-1.

Table 6.4-1. Human Failure Event Probability Summary

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
ISO-OPSI-COMP-DROP-HFI-NOD	Operator drops object onto transportation cask	1	N/A <sup>a</sup>	N/A	Historic Data

Table 6.4-1. Human Failure Event Probability Summary (Continued)

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
ISO-HEPA-XFER-L-FORKLIFT	Operator punctures drum of LLW with forklift	5	N/A <sup>a</sup>	N/A	Historic Data
ISO-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HCTT in the facility	3	3E-03	5	Preliminary
ISO-OPHTINTCOL01-HFI-NOD	Operator causes collision of HCTT due to cask tractor overspeed	3	1	N/A	Preliminary
ISO-OP-HAMIMPACT-HFI-NOD	Operator causes HAM impact with crane	4	3E-03	5	Preliminary
ISO-OP-HAMINSERT-HFI-NOD	Operator misaligns transport and HAM opening	4	1E-03	5	Preliminary
ISO-OPRCOLLIDE1-HFI-NOD	Operator causes SPM/railcar collision in the facility	1	3E-03	5	Preliminary
ISO-OPRCINTCOL01-HFI-NOD	Operator initiates PMRC runaway	1	1	N/A	Preliminary
ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes site transporter collision in the facility	2	3E-03	5	Preliminary
ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes SPM/truck trailer collision in the facility	1	3E-03	5	Preliminary
ISO-OPTTINTCOL01-HFI-NOD	Operator initiates truck trailer runaway	1	1	N/A	Preliminary
ISO-PMRC-DERAIL-PER-MILE	PMRC derailment	1	N/A <sup>a</sup>	N/A	Historic Data
ISO-VEH-COLISION-COL-RAT	Collision of RC, TT, ST or HCTT with SSC during transport across the GROA	8	7E-07	10	Historic Data

NOTE: <sup>a</sup> Historical data was used to produce a probability of crane drops; this historical data is not included as part of the HRA, but is addressed in Attachment C.

ESD = event sequence diagram; GROA = geologic repository operations area; HAM = horizontal aging module; HCTT = cask tractor and cask transfer trailer; HFE = human failure event; LLW = low-level radioactive waste; N/A = not applicable; PMRC = prime mover railcar; RC = railcar; SPM = site prime mover; SSC = structure, system, or component; ST = site transporter; TT = truck trailer.

Source: Attachment E, Table E7-1.

## **6.5 FIRE INITIATING EVENTS**

Attachment F of this document describes the work scope, definitions and terms, method, and results for the fire analysis performed as part of the PCSA. The internal events of the PCSA are evaluated with respect to the fire initiating events and modified as necessary to address fire-induced failure that lead to exposures. The list of fire-induced failures included in the model, are evaluated as to fire vulnerability, and fragility analyses are conducted as needed (Section 6.3.2 and Attachment D, Section D2).

Fire initiating event frequencies have been calculated for each initiating event for Intra-Site operations. Section F5 of Attachment F details the analysis performed to determine the frequencies, using the methodology described in Section F4 of Attachment F.

### **6.5.1 Input to Initiating Events**

Frequency of vehicle fire per operation and the number of movements of waste forms on site are the values that contribute to calculating initiating event frequencies for on-site transportation of waste form. Locations where waste forms may be placed for short periods of time during on-site receipt or long periods of time for on-site storage (i.e., aging) while awaiting processing are the inputs to calculating initiating event frequencies for waste forms outside buildings that are not in active transport. An uncertainty distribution is applied to the ignition frequency, and contributes to the resulting distribution for fire initiating event frequencies. The uncertainty distribution is determined by using a team judgment process.

In addition, the floor area of the LLW building is the value that contributes to calculating the initiating event frequency for a fire in that building. An uncertainty distribution is applied to the ignition frequency based on the uncertainty in the historically observed fire information that serves as the basis for the building fire model.

### **6.5.2 Initiating Event Frequencies**

The results of the fire initiating event analysis are the fire initiating event frequencies and their associated distributions, as presented in Table 6.5-1. The frequencies represent the probability, over the length of the pre-closure surface operation period, that a fire will threaten the stated waste container. Calculations performed to obtain the initiating event frequencies are detailed in Section F5.2 of Attachment F.

Uncertainty distributions are utilized in the contribution to initiating event frequency calculations to account for the statistical uncertainty in the data. Uncertainty distributions utilized for this analysis are lognormal distributions.

Table 6.5-1. Fire Initiating Event Frequency Distributions

Initiating Event	Mean frequency (per 50 years)	Error Factor	Distribution
Fire Threatens a Waste Form During Onsite Transport	9 E-07 fires/operation	15	lognormal
Fire Threatens a Waste Form in Buffer Area	0.3 fires	15	lognormal
Fire Threatens a Waste Form on Aging Pad	0.6 fires	15	lognormal
Fire Threatens LLW in the LLWF	4.1E-01 fires	2.0	lognormal
Large Fire Threatens LLW in the LLWF	6.8E-02 fires	2.0	lognormal

NOTE: LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility.

Source: Attachment F, Tables F5.3-1 and F6-1.

## 6.6 NOT USED

## 6.7 EVENT SEQUENCE FREQUENCY RESULTS

This section provides the results of the event sequence quantification as produced from the Excel spreadsheet and the SAPHIRE (Ref. 2.2.76) FTA. Quantification of an event sequence consists of calculating its number of occurrences over the preclosure period by combining the frequency of a single initiating event with the conditional probabilities of pivotal events that comprise the sequence. The quantification results are presented as an expression of the mean and median number of occurrences of each event sequence over the preclosure period, and the standard deviation as a measure of uncertainty. Section 6.8 describes the process for aggregation of similar event sequences to permit categorization as Category 1, Category 2, or beyond Category 2 event sequences.

This section presents a summary of how the quantification is performed for Intra-Site Operations using a combination of Excel (for quantification) and SAPHIRE (to produce probability and uncertainty values for the calculation), as described in Section 4.3). The results presented in this section, in Attachment G, and in Section 6.8 include a summary of all event sequences that are quantified, a list of off-normal events not analyzed for categorization, and a table summarizing the results of the final (grouped) quantification.

### 6.7.1 Process for Event Sequence Quantification

Internal event sequences that are based on the event trees presented in Section 6.1 and fault trees presented in Section 6.2 are quantified using Excel and SAPHIRE. The event sequence quantification methodology is presented in Section 4.3.1.1 (using SAPHIRE with Excel) and Section 4.3.6 (general). An event sequence frequency is the product of several factors, as follows (with examples):

- *Number of times the operation or activity that gives rise to the event sequence is performed over the preclosure period:* An example of this value would be the total number of transfers of a waste form between waste handling facilities over the preclosure period.
- *Probability of occurrence of the initiating event for the event sequence considered:* Continuing with the previous example, this could be the probability of collision involving a mover carrying the waste form between waste handling facilities. The initiating event probability is entered into Excel as parameters of the distribution (mean, median, and standard deviation), which are either produced from a fault tree in SAPHIRE or are based on a basic event value (data).
- *Conditional probability of each of the pivotal events of the event sequence (shown graphically in the SRET for each ESD):* For Intra-Site Operations, the pivotal events represent a passive failure, for example, cask/canister breach.

As illustrated in Section 4.3.1.1, uncertainties in input parameters such as throughput rates, equipment failure rates, passive failure probabilities, and HFEs used to calculate basic event

probabilities are propagated through the fault trees used and the event sequence logic to quantify the uncertainty in the event sequence quantification.

### **6.7.2 Event Sequence Quantification Summary**

Table G-1 in Attachment G presents the results of the event sequence quantifications. Table G-1 summarizes the results of the quantification and lists the following elements: (1) event tree from which the sequence is generated, (2) event sequence designator (ID), (3) initiating event description, (4) event sequence logic, (5) event sequence end state, (6) event sequence mean value, (7) event sequence median value, and (8) event sequence standard deviation (i.e., the uncertainty). As an example, Table 6.7-1 below presents an excerpt from Table G-1, showing ISO-ESD-01 event sequence quantifications for DPC waste forms only.

Table 6.7-1. Example Event Sequence Quantification Summary Table

Event Tree	Se- quence	Description	Logic	End State	Calc'd Mean	Calc'd Median	Calc'd Std. Deviation
ISO-ESD01-DPC	3-2	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from degradation of shielding due to a railcar collision. In this sequence the transportation cask remains intact, and the shielding fails.	INTRASITE_SPMRC_COLLIDE, /TCASK_COLLIDE_RC, SHIELD_TCASK_COL	DED	1.E-08	7.E-09	7.E-08
ISO-ESD01-DPC	3-3	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from loss of shielding due to a railcar collision. In this sequence the transportation cask fails, and the canister remains intact.	INTRASITE_SPMRC_COLLIDE, TCASK_COLLIDE_RC, /CANISTER1	DEL	0.E+00	0.E+00	0.E+00
ISO-ESD01-DPC	3-4	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release from cask/canister breach due to a railcar collision. In this sequence the transportation cask and the canister fail, but moderator is prevented from entering the canister.	INTRASITE_SPMRC_COLLIDE, TCASK_COLLIDE_RC, CANISTER1, /MODERATOR_SOP	RRU	1.E-08	7.E-09	7.E-08
ISO-ESD01-DPC	3-5	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release important to criticality from cask/canister breach due to a railcar collision. In this sequence the transportation cask and the canister fail, and moderator is not prevented from entering the canister.	INTRASITE_SPMRC_COLLIDE, TCASK_COLLIDE_RC, CANISTER1, MODERATOR_SOP	RUC	0.E+00	0.E+00	0.E+00
ISO-ESD01-DPC	2-2	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from degradation of shielding due to a railcar derailment. In this sequence the transportation cask remains intact, and the shielding fails.	INTRASITE_DERAIL, /TCASK_DERAIL, SHIELD_TCASK_DROP	DED	7.E-08	7.E-08	1.E-08

Table 6.7-1. Example Event Sequence Quantification Summary Table (Continued)

Event Tree	Se- quence	Description	Logic	End State	Calc'd Mean	Calc'd Median	Calc'd Std. Deviation
ISO-ESD01-DPC	2-3	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from loss of shielding due to a railcar derailment. In this sequence the transportation cask fails, and the canister remains intact.	INTRASITE_DERAIL, TCASK_DERAIL, /CANISTER1	DEL	0.E+00	0.E+00	0.E+00
ISO-ESD01-DPC	2-4	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release from cask/canister breach due to a railcar derailment. In this sequence the transportation cask and the canister fail, but moderator is prevented from entering the canister.	INTRASITE_DERAIL, TCASK_DERAIL, CANISTER1, /MODERATOR_SOP	RRU	7.E-08	7.E-08	1.E-08
ISO-ESD01-DPC	2-5	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release important to criticality from cask/canister breach due to a railcar derailment. In this sequence the transportation cask and the canister fail, and moderator is not prevented from entering the canister.	INTRASITE_DERAIL, TCASK_DERAIL, CANISTER1, MODERATOR_SOP	RUC	0.E+00	0.E+00	0.E+00
ISO-ESD01-DPC	4-2	N/A - No DPCs will be transported by TT		N/A			
ISO-ESD01-DPC	4-3	N/A - No DPCs will be transported by TT		N/A			
ISO-ESD01-DPC	4-4	N/A - No DPCs will be transported by TT		N/A			
ISO-ESD01-DPC	4-5	N/A - No DPCs will be transported by TT		N/A			
ISO-ESD01-DPC	5-2	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from degradation of shielding due to an object dropped onto the transportation cask. In this sequence the transportation cask remains intact, and the shielding fails.	INTRASITE_JIB_CRANE, /TCASK_DROPON, SHIELD_TCASK_DROPON	DED	1.E-07	7.E-08	7.E-08



Table 6.7-1. Example Event Sequence Quantification Summary Table (Continued)

Event Tree	Se- quence	Description	Logic	End State	Calc'd Mean	Calc'd Median	Calc'd Std. Deviation
ISO-ESD01-DPC	5-3	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in a direct exposure from loss of shielding due to an object dropped onto the transportation cask. In this sequence the transportation cask fails, and the canister remains intact.	INTRASITE_JIB_CRANE, TCASK_DROPON, /CANISTER1	DEL	0.E+00	0.E+00	0.E+00
ISO-ESD01-DPC	5-4	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release from cask/canister breach due to an object dropped onto the transportation cask. In this sequence the transportation cask and the canister fail, but moderator is prevented from entering the canister.	INTRASITE_JIB_CRANE, TCASK_DROPON, CANISTER1, /MODERATOR_SOP	RRU	1.E-07	7.E-08	7.E-08
ISO-ESD01-DPC	5-5	This sequence represents a structural challenge to a DPC inside a transportation cask resulting in an unfiltered radiological release important to criticality from cask/canister breach due to an object dropped onto the transportation cask. In this sequence the transportation cask and the canister fail, and moderator is not prevented from entering the canister.	INTRASITE_JIB_CRANE, TCASK_DROPON, CANISTER1, MODERATOR_SOP	RUC	0.E+00	0.E+00	0.E+00
ISO-...	<i>Refer to Attachment G, Table G-1 for the complete table of event sequence quantifications.</i>						

NOTE: DPC = dual-purpose canister, N/A = not applicable; TT = truck trailer.

Source: Original

## 6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION

An aggregation process is applied prior to a categorization of event sequences, as described in Section 4.3.1. It is appropriate for purposes of categorization to add the frequencies of event sequences derived from an ESD that elicit the same combination of failure and success of pivotal events and that have the same end state. This is termed final event sequence quantification (Section 6.8.1), and the results give the final frequency of occurrence. Using the final frequency of occurrence, the event sequences are categorized according to the definition of Category 1 and Category 2 event sequences given in 10 CFR 63.2 (Ref. 2.3.2). Dose consequences for Category 1 and Category 2 event sequences are subject to the performance objectives of 10 CFR 63.111 (Ref. 2.3.2), and are evaluated in *Preclosure Consequence Analyses* (Ref. 2.2.30). Event sequences with a frequency of occurrence less than one chance in 10,000 of occurring before closure of the repository are designated as beyond Category 2 event sequences and are not analyzed for dose consequences.

Rather than calculate dose consequences for each Category 2 event sequence identified in the categorization process, dose consequences are performed for a set of bounding events that encompass the end states and material at risk for event sequences. Therefore, dose consequences are determined for a representative set of postulated Category 2 event sequences, identified in Table 6.8-1 (Ref. 2.2.30, Table 2). Because all waste containers types and configurations that are applicable to the repository are included in Table 6.8-1, some of the bounding event sequences do not apply to this analysis (e.g., 2-06, “Uncanistered commercial SNF in pool”). Once event sequence categorization is complete, Category 2 event sequences are cross referenced with the bounding event number given in Table 6.8-1, thus assuring that Category 2 event sequences have been evaluated for dose consequences and compared to the 10 CFR 63.111 performance objectives.

Table 6.8-1. Bounding Category 2 Event Sequences

Bounding Event Number	Affected Waste Form	Description of End State	Material At Risk
2-01	LLWF inventory and HEPA filters	Seismic event resulting in LLWF collapse and failure of HEPA filters and ductwork in other facilities.	HEPA filters LLWF inventory
2-02	HLW canister in transportation cask	Breach of sealed HLW canisters in a sealed transportation cask	5 HLW canisters
2-03	HLW canister	Breach of sealed HLW canisters in an unsealed waste package	5 HLW canisters
2-04	HLW canister	Breach of sealed HLW canister during transfer (one drops onto another)	2 HLW canisters
2-05	Uncanistered commercial SNF in transportation cask	Breach of uncanistered commercial SNF in a sealed truck transportation cask in air	4 PWR or 9 BWR commercial SNF
2-06	Uncanistered commercial SNF in pool	Breach of uncanistered commercial SNF in an unsealed truck transportation cask in pool	4 PWR or 9 BWR commercial SNF

Table 6.8-1. Bounding Category 2 Event Sequences (Continued)

Bounding Event Number	Affected Waste Form	Description of End State	Material At Risk
2-07	DPC in air	Breach of a sealed DPC in air	36 PWR or 74 BWR commercial SNF
2-08	DPC in pool	Breach of commercial SNF in unsealed DPC in pool	36 PWR or 74 BWR commercial SNF
2-09	TAD canister in air	Breach of a sealed TAD canister in air within facility	21 PWR or 44 BWR commercial SNF
2-10	TAD canister in pool	Breach of commercial SNF in unsealed TAD canister in pool	21 PWR or 44 BWR commercial SNF
2-11	Uncanistered commercial SNF	Breach of uncanistered commercial SNF assembly in pool (one drops onto another)	2 PWR or 2 BWR commercial SNF
2-12	Uncanistered commercial SNF	Breach of uncanistered commercial SNF in pool	1 PWR or 1 BWR commercial SNF
2-13	Combustible and noncombustible LLW	Fire involving LLWF inventory	Combustible and noncombustible inventory
2-14	Uncanistered commercial SNF in truck transportation cask	Breach of a sealed truck transportation cask due to a fire	4 PWR or 9 BWR commercial SNF
<p>NOTE: BWR = boiling water reactor; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; HLW = high-level radioactive waste; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; PWR = pressurized water reactor; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal canister.</p> <p>Source: <i>Preclosure Consequence Analyses</i> (Ref. 2.2.30, Table 2).</p>			

### 6.8.1 Event Sequence Grouping and Final Quantification

Event sequences are modeled to represent the GROA operations and SSCs. Accordingly, an event sequence is unique to a given operational activity in a given operational area, which is depicted in an ESD. When more than one initiating event shares the same ESD and, thus, elicits the same pivotal events and the same end states, it may be necessary to quantify the event sequence for each initiating event individually because the conditional probabilities of the pivotal events depend on the specific initiating event. In such cases, the frequencies of event sequences from the same ESD, with the same path through the event tree and with the same end state, are added together, thus comprising an event sequence grouping.

For example, an ESD may show event sequences that could occur during movement of a canister in an aging overpack via site transporter between a surface facility and the Aging Facility. More than one initiating event, such as a drop or collision, may share the same ESD, and, therefore, elicit the same pivotal events and end states; however, it may give rise to event sequences that are quantified for each initiating event because the conditional probabilities of their pivotal events depend on the specific initiating event.

By contrast, some ESDs indicate a single initiating event. Such initiating events may be composites of several individual initiating events, but because the conditional probabilities of pivotal events and the end states are the same for each of the constituents, the initiators are grouped before the event sequence quantification. In the PCSA, this grouping is performed for a given waste container configuration at the ESD level. The waste container configurations considered are listed below.

- Naval SNF canister in a transportation cask.
- HLW canister in a transportation cask.
- DOE standardized canister, containing DOE-owned SNF in a transportation cask.
- Multicanister overpack in a transportation cask.
- TAD canister in a transportation cask or in an aging overpack.
- DPC in a transportation cask or in an aging overpack.
- Horizontal DPC in a transportation cask (a transportation cask that is never upended or a horizontal shielded transfer cask) or in a HAM.
- Uncanistered commercial SNF in a transportation cask.
- LLW, including dry active waste, wet-solid LLW (evaluated separately as resin or non-resin), and liquid LLW.

In Excel, the grouping of event sequences is carried out by calculating the combined mean, median, and standard deviation of the event sequence lines that end in the same end state for each waste form in an ESD. The event sequence frequencies from this step comprise the final event sequence quantification, used for categorization.

An illustration of the grouping of event sequences is described in the following. The potential structural challenges to a given canister during its transfer by the site transporter to the Aging Facility are due to drops and collisions. The event sequences involving the aging overpack are quantified separately twice, once for each initiating event. After an initiating event occurs, the event sequences that elicit the same system response and lead to the same end state, that is, those event sequences that follow the same path on the SRET, are grouped together for purposes of categorization. Thus, the two individual event sequences initiated by a drop or collision that eventually result in a specific end state, such as an unfiltered radionuclide release, are grouped together for the purposes of categorization as a single aggregated event sequence with a unique name termed the “event sequence group ID”. Since there are three different end states that can lead to exposure of personnel to radiation (i.e., result in an end state other than “OK”), there are three aggregated event sequences involving the TAD canister in an aging overpack, each having a unique name. The frequency of each of these aggregated event sequences represents the sum of frequencies of the two individual event sequences.

The uncertainties in the grouped event sequences are generated as described in Section 4.3.1.1.

## 6.8.2 Event Sequence Categorization

Based on the resultant frequency of occurrence, the event sequences are categorized as Category 1 or Category 2, per the definitions in 10 CFR 63.2 (Ref. 2.3.2), or as beyond Category 2. The categorization is done on the basis of the expected number of occurrences of each event sequence during the preclosure period. For purposes of this discussion, the expected number of occurrences of a given event sequence over the preclosure period is represented by the quantity  $m$ .

Some event sequences are not directly dependent on the duration of the preclosure period. For example, the expected number of occurrences of drops of an aging overpack containing a TAD canister during transportation operations over the preclosure period is essentially controlled by the number of TAD canisters and the number of movements of these canisters in aging overpacks. The duration of the preclosure period is not directly relevant for this event sequence, but it is implicitly built into the operations. In contrast, for other event sequences, time is a direct input. For example, fire-induced event sequences are evaluated over a period of time. Fire-induced event sequences for Intra-Site Operations are evaluated over a period of 50 years, because the surface facilities are expected to operate for no longer than 50 years (*Basis of Design for the TAD Canister-Based Repository Design Concept* (Ref. 2.2.16, Section 2.2.2.7)).

Using the parameter  $m$  for a given event sequence, categorization is performed using the screening criteria specified in 10 CFR 63.2 (Ref. 2.3.2), as follows:

- Event sequences that are expected to occur one or more times before permanent closure of the GROA are referred to as Category 1 event sequences (Ref. 2.3.2). Thus, a value of  $m$  greater than or equal to one means the event sequence is a Category 1 event sequence.
- Event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences (Ref. 2.3.2). Thus, a value of  $m$  less than one but greater than or equal to 1E-04, means the event sequence is a Category 2 event sequence.
- A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to  $m$ . The probability,  $P$ , that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution,  $P = 1 - e^{-m}$  (Ref. 2.2.8, p. A-3) a value of  $P$  greater than or equal to 1E-04 implies the value of  $m$  is greater than or equal to  $-\ln(1 - P) = -\ln(1 - 1E-04)$ , which is numerically equal to 1E-04. Thus, a value of  $m$  greater than or equal to 1E-04, but less than one, implies the corresponding event sequence is a Category 2 event sequence.
- Event sequences that have a value of  $m$  less than 1E-04 are designated as beyond Category 2.

An uncertainty analysis is performed on  $m$  to determine the main characteristics of its associated probability distribution, specifically the mean, 50th percentile (i.e., the median), and the standard deviation.

### 6.8.3 Final Event Sequence Quantification Summary

Initially, the results of the event sequence quantification process are reported in a single table of all event sequences (Attachment G, Table G-1) generated from the model presented in Attachment H. Following the final categorization, the event sequences for the respective Category 2 (Table 6.8-3) and beyond Category 2 (Attachment G, Table G-3) are tabulated separately. There are no Category 1 (Table 6.8-2) events for Intra-Site Operations. Other sorting may be performed, for example, event sequences that have end states ITC are tabulated separately (Attachment G, Table G-4). The format of the table headings and content are essentially the same for Tables 6.8-2, 6.8-3, G-2, G-3, and G-4, as follows:

1. Event Sequence Group ID – manually assigned in Excel.
2. End State – from ESD development.
3. Description (of the event sequence) – narrative that describes the initiating event(s) and identifies the pivotal events that are involved for the sequence.
4. Material-At-Risk – describes the type of waste form involved and the amount of material (e.g., an event involving one transportation cask containing HLW would involve 5 HLW canisters, which represents the material-at-risk).
5. Mean (event sequence frequency) – number of occurrences over the preclosure period.
6. Median (event sequence frequency) – number of occurrences over the preclosure period.
7. Standard Deviation (of the event sequence frequency) – the calculated standard deviation.
8. Event Sequence Category – declaration of Category 1, Category 2, or beyond Category 2.
9. Basis for Categorization – the foundation for categorization declaration (e.g., categorization by mean value or from sensitivity study (using an error factor) for near threshold means, as described in Section 4.3.6.2)
10. Consequence analysis (applies to Tables 6.8-2 and 6.8-3 only) – cross-reference to the bounding event number in the dose consequence analysis (Table 6.8-1 and (Ref. 2.2.30), Appendices IV and V, Table 2, and Section 7).

An additional table (Table 6.8-4) is included for events that were identified during ESD development (Ref. 2.2.29) but were not analyzed for categorization. Separate analyses identified

these events as off-normal because the consequences to a worker for this type of release are a small fraction of the performance objectives (Ref. 2.2.30).

Table 6.8-2. Category 1 Final Event Sequences Summary

Event Sequence Group ID	End State	Description	Material-At-Risk	Mean	Median	Std Dev	Event Seq. Cat.	Basis for Categorization	Consequence Analysis
None	—	—	—	—	—	—	—	—	—

NOTE: ID = identification.

Source: Original



Table 6.8-3. Category 2 Final Event Sequences Summary

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO09-TAD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a TAD canister inside a transportation cask or aging overpack, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	1 TAD canister	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>
ISO09-HLW-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to an HLW canister inside a transportation cask, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	5 HLW canisters	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>
ISO09-NAV-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a naval SNF canister inside a transportation cask, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	1 naval SNF canister	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO09-DSTD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a DOE standardized canister inside a transportation cask, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	9 DOE standardized canisters	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>
ISO09-DPC-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a DPC inside a transportation cask or aging overpack, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	1 DPC	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>
ISO09-HDPC-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a horizontal DPC inside a transportation cask, a horizontal aging module, or a horizontal STC, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	1 DPC	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO09-MCO-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to an MCO inside a transportation cask, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	4 MCOs	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e,a</sup>
ISO09-UCSNF-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a transportation cask with uncanistered SNF assemblies, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the transportation cask containment function remains intact, and the shielding fails.	1 transportation cask with uncanistered SNF assemblies	3.E-01	8.E-02	1.E+00	Category 2	Mean of distribution for number of occurrences of event sequence near a category threshold. Categorization confirmed by alternative distribution	N/A <sup>e</sup>
ISO07-LLW-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a thermal challenge to the inventory of LLW present in the LLW Facility, due to a fire at that facility, resulting in an unfiltered radionuclide release. In this sequence, the combustible LLW forms present in the facility burn.	inventory of LLW at the LLW Facility	7.E-02	6.E-02	3.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	2-13

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO05-DAW-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a container with a HEPA filter from the WHF, during processing operations at the LLW Facility, resulting in an unfiltered radionuclide release. In this sequence, the container fails.	1 container with HEPA filter from the WHF	6.E-02	2.E-02	2.E-01	Category 2	Mean of distribution for number of occurrences of event sequence	2-01
ISO09-UCSNF-SEQ3-RRU	Unfiltered radionuclide release	This event sequence represents a thermal challenge to a transportation cask with uncanistered SNF assemblies, due to a fire, resulting in an unfiltered radionuclide release. In this sequence, the transportation cask fails, and a moderator is excluded from entering the cask.	1 transportation cask with uncanistered SNF assemblies	2.E-02	4.E-03	6.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	2-14
ISO05-WETnr-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a container with wet-solid waste (pool filter) from the WHF, during processing operations at the LLW Facility, resulting in an unfiltered radionuclide release. In this sequence, the container fails.	1 container with pool filter from the WHF	5.E-03	2.E-03	1.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	2-01

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO08-DAW-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a container with a HEPA filter from the WHF, during transfer to the LLW Facility, resulting in an unfiltered radionuclide release. In this sequence, the container fails.	1 container with HEPA filter from the WHF	2.E-03	6.E-04	5.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-01
ISO08-WETnr-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a container with wet-solid waste (pool filter) from the WHF, during transfer to the LLW Facility, resulting in an unfiltered radionuclide release. In this sequence, the container fails.	1 container with pool filter from the WHF	2.E-03	7.E-04	3.E-03	Category 2	Mean of distribution for number of occurrences of event sequence	2-01
ISO02-TAD-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a structural challenge to a TAD canister inside an aging overpack, during transit to or from the Aging facility, resulting in a direct exposure from loss of shielding. In this sequence, the canister remains intact, and the shielding fails.	1 TAD canister	8.E-04	8.E-04	2.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	N/A <sup>e</sup>

Table 6.8-3. Category 2 Final Event Sequences Summary (Continued)

Event Sequence Group ID <sup>a</sup>	End State	Description	Material-At-Risk <sup>b</sup>	Mean <sup>c</sup>	Median <sup>c</sup>	Std Dev <sup>c</sup>	Event Seq. Cat.	Basis for Categorization	Consequence Analysis <sup>d</sup>
ISO01-UCSNF-SEQ2-DED	Direct exposure, degradation of shielding	This event sequence represents a structural challenge to a transportation cask with uncanistered SNF assemblies, during intra-site movement, resulting in a direct exposure from degradation of shielding. In this sequence, the transportation cask containment function remains intact, and the shielding fails.	1 transportation cask with uncanistered SNF assemblies	2.E-04	6.E-05	4.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	N/A <sup>e</sup>
ISO08-WETR-SEQ2-RRU	Unfiltered radionuclide release	This event sequence represents a structural challenge to a container with wet-solid resin from the WHF, during transfer to the LLW Facility, resulting in an unfiltered radionuclide release. In this sequence, the container fails.	1 container with wet-solid resin from the WHF	2.E-04	5.E-05	5.E-04	Category 2	Mean of distribution for number of occurrences of event sequence	2-01

NOTE: <sup>a</sup> The expected number of occurrences, over the preclosure period, of event sequences involving MCOs may not lead to an acceptable categorization with regard to 10 CFR 63.111 (Ref. 2.3.2) performance objectives. Therefore, further investigation of these event sequences may be needed. As a consequence, the categorization of event sequences involving MCOs is considered to be preliminary and no bounding event number for consequence analyses is provided.

<sup>b</sup> The material at risk is, as relevant, based upon the nominal capacity of the waste container involved in the event sequence under consideration, or accounts for the specific operation covered by the event sequence.

<sup>c</sup> The mean, median, and standard deviation displayed are for the number of occurrences, over the preclosure period, of the event sequence under consideration.

<sup>d</sup> The bounding event number provided in this column identifies the bounding Category 2 event sequence identified in Table 6.8-1 from the *Preclosure Consequence Analyses* (Ref. 2.2.30, Table 2) that results in dose consequences that bound the event sequence under consideration.

<sup>e</sup> Because of the large distances to the locations of the offsite receptors, dose to members of the public from direct radiation after a Category 2 event sequence is reduced by more than 13 orders of magnitude to insignificant levels (Ref. 2.2.19).

DOE = U.S. Department of Energy; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; HLW = high-level radioactive waste; ID = identification; LLW = Low Level Waste; MCO = multicanister overpack; N/A = not applicable; SNF = spent nuclear fuel; STC = shielded transfer cask; TAD = transportation, aging, and disposal; WHF = Wet Handling Facility.

Source: Original

Table 6.8-4. Off-Normal Events Not Analyzed for Categorization

Event Sequence Group ID or Description	End State	Description	Material-At-Risk	Basis
<b>ISO-ESD-05</b>				
ISO05-DAW-SEQ2-RRU	RR-UNFILTERED	This sequence represents a structural challenge to a DAW LLW container containing DAW (other than stage 1 ITS HEPA filters generated by the WHF), during handling operations at the LLW Facility, resulting in an unfiltered radiological release in the LLWF. In this sequence the container fails.	DAW LLW (55-gal drum)	Off-normal event (Ref. 2.2.30, Appendix V)  Except for stage 1 ITS HEPA filters generated by the WHF, DAW LLW release for this event is not analyzed for categorization, because the consequences to a worker for this type of release are a small fraction of the performance objectives.
ISO05-LIQ-SEQ2-RRU	RR-UNFILTERED	This sequence represents a structural challenge to a liquid LLW processing component, during processing operations at the LLW Facility, resulting in an unfiltered radiological release.	Liquid LLW tank contents	Off-normal event (Ref. 2.2.30, Appendix IV)  Liquid LLW release for this event is not analyzed for categorization, because the consequences to a worker for this type of release are a small fraction of the performance objectives.
<b>ISO-ESD-08</b>				
ISO08-LIQ-SEQ2-RRU	RR-UNFILTERED	This sequence represents a structural challenge to a liquid LLW processing component during transfer to the LLW Facility, resulting in an unfiltered radiological release. In this sequence the container fails.	Liquid LLW tank contents	Off-normal event (Ref. 2.2.30, Appendix IV)  Liquid LLW release for this event is not analyzed for categorization, because the consequences to a worker for this type of release are a small fraction of the performance objectives.

NOTE: <sup>1</sup> Except for the Wet Handling Facilities, liquid LLW is moved from generating facilities to the tanks at the LLWF in HICs.

DAW = dry active (low-level radioactive) waste; ESD = event sequence diagram; HEPA = high-efficiency particulate air; HIC = high-integrity container; ID = identification; ISO = Intra-Site Operations; ITS = important to safety; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; WHF = Wet Handling Facility.

Source: Original

## **6.9 IMPORTANT TO SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS AND PROCEDURAL SAFETY CONTROL REQUIREMENTS**

The results of the PCSA are used to define design bases for repository SSCs to prevent or mitigate event sequences that could lead to the release of radioactive material and/or result in radiological exposure of workers or the public. Potential releases of radioactive material are minimized to ensure resulting worker and public exposures to radiation are below the limits established by 10 CFR 63.111 (Ref. 2.3.2). This strategy requires using prevention features in the repository design wherever reasonable. This strategy is implemented by performing the PCSA as an integral part of the design process in a manner consistent with a performance-based, risk-informed philosophy. This integral design approach ensures the ITS design features and operational controls are selected in a manner that ensures safety while minimizing design and operational complexity through the use of proven technology. Using this strategy, design rules are developed to provide guidance on the safety classification of SSCs. The following information is developed in order to implement this strategy:

- Essential safety functions needed to ensure worker and public safety.
- SSCs relied upon to ensure essential safety functions.
- Design criteria that will ensure that the essential safety functions will be performed with a high degree of reliability and margin of safety.
- Administrative and PSCs that, in conjunction with the repository design ensure operations are conducted within the limits of the PCSA.

Section 6.9.1 identifies ITS SSCs, and Section 6.9.2 identifies the PSCs.

### **6.9.1 Important to Safety Structures, Systems, and Components**

Table 6.9-1 contains the nuclear safety design bases for the Intra-Site Operations and BOP ITS SSCs. The first three columns identify the ITS system or facility, the subsystem or function, and the component. The fourth column identifies the safety function relied upon in the event sequence analysis. The fifth column provides the characteristics of the safety function (i.e. controlling parameter or value) that is demonstrated to occur or exist in the design. The sixth column provides an example event sequence in which the safety function and the characteristic is relied upon. The seventh column provides the source (e.g., usually a fault tree) for the controlling parameter or value.



Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Aging Facility (AP)	Aging Handling/ Aging Overpack	Horizontal Aging Module (HAM) (170-HAC0-ENCL-00001)	Protect against <sup>b</sup> direct exposure to personnel	1. The mean conditional probability of loss of HAM gamma shielding due to an impact or collision shall be less than or equal to $1 \times 10^{-5}$ per impact.	ISO-ESD04-HDPC (Seq. 3-2)	SHIELD_HAM_IMPACT Table 6.3-7
	Aging Handling/ Cask Transfer	Cask Tractor (for use with the Cask Transfer Trailer) (170-HAT0-HEQ-00001)	Limit speed	2. The speed of the cask tractor shall be limited to 2.5 mph.	ISO-ESD03-HDPC (Seq. 2-4)	TCASK_HTC_IMPACT Table 6.3-7
			Preclude fuel tank explosion	3. The cask tractor fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0
		Cask Transfer Trailer (for use with Transportation Casks and Horizontal Shielded Transfer Casks) (PWR DPC: [170-HAT0-TRLY-00001]) (BWR DPC: [170-HAT0-TRLY-00002])	Limit speed	4. The speed of the cask transfer trailer shall be limited to 2.5 mph.	ISO-ESD03-HDPC (Seq. 2-4)	TCASK_HTC_IMPACT Table 6.3-7
			Preclude fuel tank explosion	5. The cask transfer trailer fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0
			Reduce severity of a drop	6. The cask transfer trailer shall preclude dropping a cask from a height greater than 6 feet measured from the equipment base.	ISO-ESD03-HDPC (Seq. 3-4)	TCASK_HTC_DROP Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Aging Facility (AP) (continued)	Aging Handling/ Cask Transfer (continued)	Cask Transfer Trailer (for use with Transportation Casks and Horizontal Shielded Transfer Casks)  (PWR DPC: [170-HAT0-TRLY-00001])  (BWR DPC: [170-HAT0-TRLY-00002])  (continued)	Preclude puncture of a cask	7. The cask transfer trailer shall preclude puncture of a cask due to collision.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0
			Preclude puncture of a canister	8. The cask transfer trailer shall preclude puncture of a canister by the hydraulic ram.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0
		Site Transporter (170-HAT0-MEQ-00001)	Limit speed	9. The speed of the site transporter shall be limited to 2.5 mph.	ISO-ESD02-TAD (Seq. 2-3)	CANISTER_AO_IMPACT Table 6.3-7
			Preclude fuel tank explosion	10. The site transporter fuel tank shall preclude fuel tank explosions.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0
			Reduce severity of a drop	11. The site transporter shall preclude a vertical drop of an aging overpack from a height greater than 3 ft measured from the equipment base.	ISO-ESD02-TAD (Seq. 3-3)	CANISTER_AO_DROP Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Aging Facility (AP) (continued)	Aging Handling/ Cask Transfer (continued)	Horizontal Shielded Transfer Cask (HSTC) (170-HAC0-HEQ-00001)	Provide containment	12. The mean conditional probability of breach of a canister in a sealed HSTC on a cask transfer trailer resulting from a drop shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD03-HDPC (Seq. 3-4)	TCASK_HTC_DROP Table 6.3-7
				13. The mean probability of breach of a canister in an HSTC on a cask transfer trailer resulting from a drop of a load onto the HSTC shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD04-HDPC (Seq. 2-3)	CANISTER_HAM_OPS Table 6.3-7
				14. The mean conditional probability of breach of a canister in a sealed HSTC on a cask transfer trailer resulting from a side impact or collision shall be less than or equal to $1 \times 10^{-8}$ per impact.	ISO-ESD03-HDPC (Seq. 2-4)	TCASK_HTC_IMPACT Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Aging Facility (AP) (continued)	Aging Handling/ Aging Overpack	Aging Overpack (TAD: [170-HAC0-ENCL-00003])  (Vertical DPC: [170-HAC0-ENCL-00002])	Protect against <sup>b</sup> direct exposure to personnel	15. The mean conditional probability of loss of shielding of the aging overpack resulting from an impact or collision shall be less than or equal to $1 \times 10^{-5}$ per impact.	ISO-ESD02-TAD (Seq. 2-2)	SHIELD_AO_IMPACT Table 6.3-7
				16. The mean conditional probability of loss of shielding of the aging overpack resulting from a drop shall be less than or equal to $5 \times 10^{-6}$ per drop.	ISO-ESD02-TAD (Seq. 3-2)	SHIELD_AO_DROP Table 6.3-7
DOE and Commercial Waste Package System (DS)	Canistered Spent Nuclear Fuel	Dual-Purpose Canister (DPC) Transportation, Aging, and Disposal (TAD) Canister  (Both Analyzed as a Representative Canister)	Provide containment	17. The mean conditional probability of breach of a canister within an aging overpack following a drop shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD02-TAD (Seq. 3-3)	CANISTER_AO_DROP Table 6.3-7
				18. The mean conditional probability of breach of a canister within an aging overpack resulting from a side impact or collision shall be less than or equal to $1 \times 10^{-8}$ per event.	ISO-ESD02-TAD (Seq. 2-3)	CANISTER_AO_IMPACT Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
DOE and Commercial Waste Package System (DS) (Continued)	Canistered Spent Nuclear Fuel (Continued)	Dual-Purpose Canister (DPC) Transportation, Aging, and Disposal (TAD) Canister (Both Analyzed as a Representative Canister) (Continued)	Provide containment (Continued)	19. The mean conditional probability of breach of a canister in a HAM resulting from a collision or side impact shall be less than or equal to $1 \times 10^{-8}$ per event.	ISO-ESD04-HDPC (Seq. 3-3)	CANISTER_HAM_IMPACT Table 6.3-7
				20. The mean conditional probability of breach of a canister resulting from a drop of a load onto a HAM shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD04-HDPC (Seq. 2-3)	CANISTER_HAM_OPS Table 6.3-7
				21. The mean conditional probability of breach of a canister contained within a cask resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $2 \times 10^{-6}$ per fire event.	ISO-ESD09-TAD (Seq. 2-4)	FIRE_CANISTER_TC Table 6.3-7
				22. The mean conditional probability of breach of a canister located within a HAM resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $1 \times 10^{-6}$ per fire event.	ISO-ESD09-HDPC (Seq. 5-4)	FIRE_CANISTER_AO Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
DOE and Commercial Waste Package System (DS) (Continued)	Canistered Spent Nuclear Fuel (Continued)	Dual-Purpose Canister (DPC) Transportation, Aging, and Disposal (TAD) Canister (Both Analyzed as a Representative Canister) (Continued)	Provide containment (Continued)	23. The mean conditional probability of breach of a canister contained within an aging overpack resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $1 \times 10^{-6}$ per fire event.	ISO-ESD09-TAD (Seq. 5-4)	FIRE_CANISTER_AO Table 6.3-7
		DOE Standardized Canister	Provide containment	24. The mean conditional probability of breach of a DOE standardized canister contained within a cask resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $2 \times 10^{-6}$ per fire event.	ISO-ESD09-DSTD (Seq. 2-4)	FIRE_CANISTER_TC Table 6.3-7
	HLW Canister	Provide containment	25. The mean conditional probability of breach of a HLW canister contained within a cask resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $2 \times 10^{-6}$ per fire event.	ISO-ESD09-HLW (Seq. 2-3)	FIRE_CANISTER_TC Table 6.3-7	

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Naval SNF Waste Package System (DN)	Naval SNF	Naval SNF Canister (Analyzed as a Representative Canister)	Provide containment	26. The mean conditional probability of breach of a canister contained within a cask resulting from the spectrum of fires <sup>c</sup> shall be less than or equal to $1 \times 10^{-6}$ per fire event.	ISO-ESD09-NAV (Seq. 2-4)	FIRE_CANISTER_TC_NAV Table 6.3-7
Mechanical Handling System (H)	Cask Handling	Transportation Cask (Analyzed as a Representative Cask)	Provide containment	27. The mean conditional probability of breach of a canister in a sealed cask on a railcar, truck trailer, or cask transfer trailer resulting from a drop shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD01-TAD (Seq. 2-4)	TCASK_DERAIL Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				28. The mean probability of breach of a canister in a sealed cask on a railcar, truck trailer, or cask transfer trailer resulting from a drop of a load onto the cask shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD01-TAD (Seq. 5-4)	TCASK_DROPON Table 6.3-7
				29. The mean conditional probability of breach of a canister in a sealed cask on a railcar, truck trailer, or cask transfer trailer resulting from a side impact or collision shall be less than or equal to $1 \times 10^{-8}$ per impact.	ISO-ESD01-TAD (Seq. 3-4)	TCASK_COLLIDE_RC Table 6.3-7



Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System (H) (Continued)	Cask Handling (Continued)	Transportation Cask (Analyzed as a Representative Cask) (Continued)	Provide containment (Continued)	30. The mean conditional probability of breach of a sealed cask containing uncanistered commercial spent nuclear fuel on a truck trailer resulting from a collision followed by a rollover/drop shall be less than or equal to $1 \times 10^{-8}$ per drop.	ISO-ESD01-UCSNF (Seq. 4-4)	TCASK_COLLIDE_TT Section 6.0.6
				31. The mean conditional probability of breach of a sealed cask containing uncanistered commercial spent nuclear fuel resulting from a drop of a load onto the cask shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD01-UCSNF (Seq. 5-4)	TCASK_DROPON_UCSNF Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System (H) (Continued)	Cask Handling (Continued)	Transportation Cask (Analyzed as a Representative Cask) (Continued)	Protect against <sup>b</sup> direct exposure to personnel	32. The mean conditional probability of loss of gamma shielding of a cask resulting from a drop shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD01-TAD (Seq. 2-2)	SHIELD_TCASK_DROP Table 6.3-7
				33. The mean conditional probability of loss of gamma shielding of a cask resulting from a collision or side impact shall be less than or equal to $1 \times 10^{-8}$ per impact.	ISO-ESD01-TAD (Seq. 3-2)	SHIELD_TCASK_COL Table 6.3-7
				34. The mean conditional probability of loss of gamma shielding of a cask resulting from a drop of a load onto it shall be less than or equal to $1 \times 10^{-5}$ per drop.	ISO-ESD01-TAD (Seq. 5-2)	SHIELD_TCASK_DROPON Table 6.3-7
		Site Prime Mover	Limit speed	35. The speed of the site prime mover shall be limited to 9 mph.	ISO-ESD01-TAD (Seq. 2-4)	TCASK_DERAIL Table 6.3-7

Table 6.9-1. Preclosure Nuclear Safety Design Bases for Intra-Site Operations ITS SSCs (Continued)

System or Facility (System Code)	Subsystem or Function (as Applicable) <sup>c</sup>	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
Mechanical Handling System (H) (Continued)	Cask Handling (Continued)	Site Prime Mover	Preclude fuel tank explosion	36. The fuel tank of a site prime mover that enters a facility shall preclude fuel tank explosions.	Initiating event does not require further analysis <sup>a</sup>	Section 6.0

NOTE: <sup>a</sup> Design requirement is applied to reduce the frequency of any event sequence that could result in damage to a waste container to the beyond Category 2 frequency range.

<sup>b</sup> 'Protect against' in this table means either 'reduce the probability of' or 'reduce the frequency of'.

<sup>c</sup> The term "spectrum of fires" refers to the variations in the intensity and duration of the fire that are considered along with conditions that control the rate of heat transfer to the container (Attachment D, Figures D2.1-4 and D2.1-5).

DOE = U.S. Department of Energy; DPC = dual-purpose canister; ft = feet; HAM = horizontal aging module; HLW = high level waste; HSTC = horizontal shielded transfer cask; ITS = important to safety; mph = miles per hour; SNF = spent nuclear fuel; SSCs = structures, systems, and components; TAD = transportation, aging, and disposal (canister).

Source: Original

## 6.9.2 Procedural Safety Controls

PSCs are the controls that are relied upon to limit or prevent potential event sequences or mitigate the consequences. For this analysis, all PSCs were derived to reduce the initiating event sequence to an acceptable level.

Table 6.9-2 lists the PSCs that are required to support the event sequence analysis and categorization. If applicable, the event sequence column identifies a representative event sequence that relies upon the PSC.

Table 6.9-2. Summary of Procedural Safety Controls for Intra-Site Operations

Item	Procedural Safety Controls	Basis for Selection	Final Event Sequence ID References
1	The amount of time that a waste form container spends in each process area or in a given process operation, including total residence time in a facility, is periodically compared against the average exposure times used in the PCSA. Additionally, component failures per demand and component failures per time period are compared against the PCSA. Significant deviations will be analyzed for risk significance.	PCSA uses exposure/residence times and reliability data to calculate the probability of an initiating event, or the probability of seismic induced failures that lead to an event sequence. This control ensures that the average exposure times and reliability data are maintained consistent with those analyzed in the PCSA.	Applies to all event sequence and fault tree quantification that uses data from Attachment C. Also applies to fire analysis per Section 4.3 and Attachment E.

NOTE: PCSA = preclosure safety analysis.

Source: Original

## 7. RESULTS AND CONCLUSIONS

This analysis and its predecessor the event sequence development analysis (Ref. 2.2.29), are part of the PCSA for the GROA that supports the license application. In combination, these documents identify, evaluate, quantify, and categorize event sequences for the GROA facilities and operations. They are part of a collection of analysis reports that encompass all waste handling activities and facilities of the GROA from initial operations to the end of the preclosure period. PRA techniques derived from both nuclear power plant and aerospace methods are used to perform the analyses to comply with the risk-informed aspects of 10 CFR Part 63, Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada (Ref. 2.3.2, Sections 63.111 and 63.112) and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report*. NUREG-1804 (Ref. 2.2.69). The identification and development of the event sequences is limited to those that might lead to direct exposure of workers or onsite members of the public; radiological releases that may affect the public or workers (onsite and offsite); and criticality.

The analysis results, largely obtained in sequential steps, are discussed and presented in the logical progression through Section 6 of this document, but are not reiterated here. Instead, only key points are highlighted. For the ungrouped event sequence results and the complete grouped event sequence summaries, it is necessary to provide electronic files due to the large size of hard copy versions (Attachments G and H). In addition, the SAPHIRE files and Excel spreadsheet that represent the model for this analysis, are not well represented in paper form. Therefore, these outputs are also provided electronically (Attachment H). Table 7-1 identifies a set of summary results with general descriptions and the location within this analysis for each result provided.

Table 7-1. Key to Results

Result	Description	Cross Reference
Grouping of event sequences	Grouping of event sequences and description of event sequence groups	Table G-1
Quantification of event sequences	Calculation of probability distributions for the numbers of occurrences of internal event sequence groups over the preclosure period	Table G-2
Categorization of event sequences	Assignment of frequency categories Category 1, Category 2, or beyond Category 2 to internal event sequence groups based on mean numbers of occurrences	Table 6.8-2 Table 6.8-3 Table G-3
Designation of SSCs as ITS	Identification of SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1
Statement of nuclear safety design bases	Determination of nuclear safety design bases for SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1

Table 7-1. Key to Results (Continued)

Result	Description	Cross Reference
Statement of procedural safety controls	Determination of procedural safety controls that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-2

NOTE: ITS = important to safety; SSCs = structures, systems, and components.

Source: Original

### Summary of Event Sequences

The analysis concludes that there are no Category 1 event sequences and 17 Category 2 event sequences. Table 7-2 gives the number of Category 2 event sequences by end state for each waste form.

Table 7-2. Summary of Category 2 End States

End State <sup>a</sup>	Description	Waste Forms									
		DPC	HDPC	HLW	Naval	MCO	DSTD	TAD	UCSNF	LLW	
DE-SHIELD-DEGRADE	Direct exposure due to degradation of shielding	—	—	—	—	—	—	—	—	1	—
DE-SHIELD-LOSS	Direct exposure due to loss of shielding	1	1	1	1	1	1	2	1	—	—
RR-UNFILTERED	Radionuclide release, unfiltered	—	—	—	—	—	—	—	—	1	6
RR-UNFILTERED-ITC	Radionuclide release, unfiltered, also important to criticality	—	—	—	—	—	—	—	—	—	—
ITC	Important to criticality	—	—	—	—	—	—	—	—	—	—

NOTE: <sup>a</sup> The end states “radionuclide release, filtered” and “radionuclide release, filtered, also important to criticality” do not apply to Intra-Site Operations, because there is no applicable HVAC for confinement.

DPC = dual-purpose canister; DSTD = DOE standardized canister; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; MCO = multicanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered spent nuclear fuel.

Source: Original

### Summary of Conservatism

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

1. Fire frequency and damage analyses are performed without relying on fire suppression. This increases the calculated frequency of large fires and also increases the duration and peak temperature of fires, thereby significantly increasing the calculated probability of waste container failure. However, for applicable waste containers, fire events are evaluated as if moderator can be present to ensure any initiating events that could result in Category 1 or Category 2 for radiological release also ITC are inspected closely.
2. In the PEFA for thermal and fire scenarios, conservatism is built into the boundary conditions, which considers the fire as occurring next to the waste containers instead of only a fraction of the fire occurrence being near the waste containers. A fire closer to the target will lead to a higher target failure probability than a fire located further away. By considering all fires to be next to the waste containers, the thermal PEFA yields higher waste container failure probabilities than is likely.
3. For event sequences in which a cask containing a canister is subjected to a drop, slapdown, or load dropped onto it, the calculated containment failure probability pertains to the canister inside without regard to the integrity of the cask. That is, cask containment is not relied upon to mitigate dose or reduce probability of containment failure.
4. The structural PEFA uses a conservative failure probability of 1E-5, whereas the actual PEFA assessment indicates values of less than 1E-8 failure probabilities. This conservatism provides event sequence quantification results orders of magnitude higher than what they would be if the actual PEFA assessment values were used.
5. The event sequence development for shielding degradation of transportation casks caused by an impact event, considers all casks as if they contained lead gamma shielding that could slump. However, not all transportation casks received at the GROA will be leaded casks. Because non-leaded casks are not affected by this degraded shielding condition, the introduction of this conservatism increases the event sequence quantification value.
6. The structural analyses for drops and collisions of canisters or casks model a rigid, unyielding surface as the target.
7. The structural analysis for drops of loads onto casks or canisters uses a rigid unyielding surface for the dropped load.
8. The probabilities of event sequences involving drops of casks and canisters represent a drop height of up to 40 feet for casks and 45 feet for bare canisters. This is much higher than the normal operational lift height but is applied for all lower height drop events. This is conservative because using probabilities for the lower drop heights when applicable would result in less structural challenge to casks and canisters.
9. Transportation casks are generally analyzed without impact limiters.

10. The speed limitation of 9 mph for SPMs and 2.5 mph for site transporters and cask tractors/cask transfer trailers is set to ensure no damage to casks and canisters. The probability of damage at such speeds is calculated to be less than 1E-08 per impact. Speeds could be considerably larger without changing the category of event sequences.
11. The HRA screening values used for HFEs are typically one or more orders of magnitude higher than values that would be obtained through a detailed analysis.
12. Categorization of event sequences is based on the highest category after application of a conservative adjustment (described in Section 4.3) to account for additional uncertainty in the calculated uncertainties.
13. The throughput analysis (Ref. 2.2.23), in some cases, is based on doubling or tripling the probable available quantity of waste containers to account for the uncertainty in the partitioning of these waste containers (e.g., of the total of 346 DPCs arriving at the GROA, the throughput analysis considers that 346 DPCs are transferred from vertical transportation casks and another 346 DPCs are transferred from horizontal transportation casks). By including this conservatism in the analysis, the event sequence quantification results are higher than they are likely to be.
14. The PEFA values used for drops, collisions, and impacts involving transportation casks moved outside of handling facilities do not account for the use of buffer cars. This conservatism results in a higher probability of failure than is likely.
15. The probability of failure associated with the structural analysis of casks and canisters owing to mechanical impact loads is conservatively based on the maximum effective plastic strain of any brick (i.e., finite element mesh) in the modeled structure rather than relying on evidence of through the wall cracking.
16. Event sequences involving the HAMs are quantified using passive equipment failure values for aging overpacks. This is conservative because HAM design and configuration are more robust than an aging overpack when evaluated for structural challenge.
17. LLW containers are modeled as if they would fail given any initiating event.
18. All railcar derailment and truck trailer collision events are analyzed as if every event resulted in a rollover leading to a drop of the transportation cask. It is very unlikely that every low speed derailment or collision would result in a drop.



**ATTACHMENT A**  
**EVENT TREES**

---

## CONTENTS

	<b>Page</b>
A1 INTRODUCTION .....	A-7
A2    READER'S GUIDE TO THE EVENT TREE DESCRIPTIONS .....	A-7
A3    SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES .....	A-7
A4 EVENT TREE DESCRIPTIONS .....	A-8
A4.1  EVENT TREES FOR ISO-ESD-01 .....	A-8
A4.2  EVENT TREES FOR ISO-ESD-02 .....	A-14
A4.3  EVENT TREES FOR ISO-ESD-03 .....	A-17
A4.4  EVENT TREES FOR ISO-ESD-04 .....	A-19
A4.5  EVENT TREES FOR ISO-ESD-05 .....	A-21
A4.6  EVENT TREES FOR ISO-ESD-06 .....	A-23
A4.7  EVENT TREES FOR ISO-ESD-07 .....	A-23
A4.8  EVENT TREES FOR ISO-ESD-08 .....	A-24
A4.9  EVENT TREES FOR ISO-ESD-09 .....	A-27
A5 EVENT TREES .....	A-32

**FIGURES**

	<b>Page</b>
A5-1. Example IET Showing Navigation Aids.....	A-32
A5-2. IET for ISO-ESD-01 – DPC – Movement of Transportation Cask Containing DPC on Railcar .....	A-35
A5-3. System-Response Event Tree for ISO-ESD-01 – RESPONSE-TCASK – Transportation Cask System Response.....	A-36
A5-4. IET for ISO-ESD-01 – DSTD – Movement of Transportation Cask Containing DOE Standardized Canister on Railcar or Truck Trailer.....	A-37
A5-5. IET for ISO-ESD-01 – HDPC – Movement of HTC (Transportation Cask) Containing HDPC on Railcar.....	A-38
A5-6. IET for ISO-ESD-01 – HLW – Movement of Transportation Cask Containing HLW Canister(s) on Railcar or Truck Trailer.....	A-39
A5-7. IET for ISO-ESD-01 – MCO – Movement of Transportation Cask Containing DOE MCO on Railcar or Truck Trailer.....	A-40
A5-8. IET for ISO-ESD-01 – NAV – Movement of Transportation Cask Containing Naval Canister on Railcar.....	A-41
A5-9. IET for ISO-ESD-01 – TAD – Movement of Transportation Cask Containing TAD Canister on Railcar or Truck Trailer.....	A-42
A5-10. IET for ISO-ESD-01 – UCSNF – Movement of Transportation Cask Containing UCSNF on Railcar or Truck Trailer.....	A-43
A5-11. IET for ISO-ESD-02 – DPC – Movement of Aging Overpack Containing DPC on Site Transporter To/From Aging Facility .....	A-44
A5-12. System-Response Event Tree for ISO-ESD-02 – RESPONSE-AO – Aging Overpack System Response.....	A-45
A5-13. IET for ISO-ESD-02 – TAD – Movement of Aging Overpack Containing TAD Canister on Site Transporter To/From Aging Facility.....	A-46
A5-14. IET for ISO-ESD-03 – HDPC– Movement of HTC or HSTC Containing HDPC on Cask Transfer Trailer To/From Aging Facility .....	A-47
A5-15. System-Response Event Tree for ISO-ESD-03 –RESPONSE-HTC – HTC/HSTC System Response .....	A-48
A5-16. IET for ISO-ESD-04 – HDPC– Canister Insertion or Retrieval Operations at a HAM .....	A-49
A5-17. System-Response Event Tree for ISO-ESD-04 – RESPONSE-HAM – HAM System Response .....	A-50
A5-18. Event Tree for ISO-ESD-05-LLWDAW –Single Container DAW LLW Operations in LLWF .....	A-51

A5-19.	Event Tree for ISO-ESD-05-LLWLIQ –Single Container Liquid LLW Operations in the LLWF .....	A-52
A5-20.	Event Tree for ISO-ESD-05-LLWWETnr –Single Container Wet-Solid (Non-Resin) LLW Operations in LLWF .....	A-53
A5-21.	Event Tree for ISO-ESD-06-LLW –Non-Fire Events Involving all LLW Containers in the LLWF .....	A-54
A5-22.	Event Tree for ISO-ESD-07-LLW – Fire Events Involving all Combustible LLW in Containers in the LLWF.....	A-55
A5-23.	IET for ISO-ESD-08-LLWDAW – Transfer of DAW LLW between Generating Facility and LLWF or GROA Boundary .....	A-56
A5-24.	System-Response Event Tree for ISO-ESD-08 – RESPONSE-LLW – LLW Transfers-System Response .....	A-57
A5-25.	IET for ISO-ESD-08-LLWLIQ – Transfer of Liquid LLW between Generating Facility and LLWF or GROA Boundary .....	A-58
A5-26.	IET for ISO-ESD-08-LLWWETnr – Transfer of Wet-Solid (Non-Resin) LLW between Generating Facility and LLWF or GROA Boundary .....	A-59
A5-27.	IET for ISO-ESD-08-LLWWETr – Transfer of Wet-Solid (Resin) LLW between Generating Facility and LLWF or GROA Boundary .....	A-60
A5-28.	IET for ISO-ESD-09 – DPC – Fire Affecting DPC during Transportation or Aging Activities .....	A-61
A5-29.	System-Response Event Tree for ISO-ESD-09 – RESPONSE-FIRE – Transportation and Aging Activities Fire System Response .....	A-62
A5-30.	IET for ISO-ESD-09 – DSTD – Fire Affecting DOE Standardized Canister (DSTD) during Transportation Activities.....	A-63
A5-31.	IET for ISO-ESD-09 – HDPC – Fire Affecting HDPC during Transportation or Aging Activities.....	A-64
A5-32.	IET for ISO-ESD-09 – HLW – Fire Affecting HLW Canister(s) during Transportation Activities .....	A-65
A5-33.	IET for ISO-ESD-09 – MCO – Fire Affecting DOE MCO during Transportation Activities .....	A-66
A5-34.	IET for ISO-ESD-09 – NAV – Fire Affecting Naval Canister during Transportation Activities .....	A-67
A5-35.	IET for ISO-ESD-09 – TAD – Fire Affecting TAD Canister during Transportation or Aging Activities.....	A-68
A5-36.	IET for ISO-ESD-09 – UCSNF – Fire Affecting UCSNF in a Transportation Cask during Transportation Activities .....	A-69

**TABLES**

	<b>Page</b>
A4.1-1. Summary of Event Trees for ISO-ESD-01 .....	A-9
A4.1-2. Initiating Event Assignments for ISO-ESD-01.....	A-10
A4.1-3. Basic Event Associated with the TRANSCASK Pivotal Events of ISO-ESD-01 .....	A-11
A4.1-4. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-01 ....	A-12
A4.1-5. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-01 ....	A-13
A4.1-6. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-01 .....	A-14
A4.2-1. Summary of Event Trees for ISO-ESD-02 .....	A-15
A4.2-2. Initiating Event Assignments for ISO-ESD-02.....	A-15
A4.2-3. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-02 ....	A-16
A4.2-4. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-02 ....	A-16
A4.2-5. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-02 .....	A-16
A4.3-1. Summary of Event Trees for ISO-ESD-03 .....	A-17
A4.3-2. Initiating Event Assignments for ISO-ESD-03.....	A-17
A4.3-3. Basic Event Associated with the TRANSCASK Pivotal Events of ISO-ESD-03 .....	A-18
A4.3-4. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-03 ....	A-18
A4.3-5. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-03 ....	A-18
A4.3-6. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-03 .....	A-19
A4.4-1. Summary of Event Trees for ISO-ESD-03 .....	A-19
A4.4-2. Initiating Event Assignments for ISO-ESD-04.....	A-20
A4.4-3. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-04 ....	A-20
A4.4-4. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-04 ....	A-20
A4.4-5. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-04 .....	A-21
A4.5-1. Summary of Event Trees for ISO-ESD-05 .....	A-21
A4.5-2. Initiating Event Assignments for ISO-ESD-05.....	A-22
A4.5-3. Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-05 .....	A-22

---

A4.7-1.	Summary of Event Trees for ISO-ESD-07 .....	A-23
A4.7-2.	Initiating Event Assignments for ISO-ESD-07.....	A-23
A4.7-3.	Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-07 .....	A-24
A4.8-1.	Summary of Event Trees for ISO-ESD-08 .....	A-24
A4.8-2.	Initiating Event Assignments for ISO-ESD-08.....	A-26
A4.8-3.	Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-08 .....	A-26
A4.9-1.	Summary of Event Trees for ISO-ESD-09 .....	A-27
A4.9-2.	Initiating Event Assignments for ISO-ESD-09.....	A-28
A4.9-3.	Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-09 ....	A-29
A4.9-4.	Basic Events Associated with the SHIELDING Pivotal Events of ISO-ESD-09...	A-30
A4.9-5.	Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-09 .....	A-31
A5-1.	Correspondence between ESDs and Event Trees .....	A-33

## ATTACHMENT A EVENT TREES

### A1 INTRODUCTION

This attachment presents event trees that are derived from the ESDs in Attachment F of *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. 2.2.29). All IETs and SRETs are located at the end of this attachment. Refer to Table A5-1 for the figure locations of specific event and response trees. The event trees are presented in ESD order. For example, the event trees associated with ISO-ESD-01 appear first, and those associated with ISO-ESD-02 appear after that, and so on. Then the first IET associated with the ESD appears first and the SRET(s) are placed immediately following the first IET followed by the remaining IETs for that ESD. For example, the first IET (ISO-ESD01-DPC) is the first event tree figure. The SRET (RESPONSE-TCASK) follows, and the remaining IETs for that ESD follow the SRET. The same ordering is done for each ESD group in turn.

### A2 READER'S GUIDE TO THE EVENT TREE DESCRIPTIONS

The following sections are organized by ESD. The event trees that correspond to each ESD are presented as follows:

1. The event trees for each waste container type are briefly described and listed (initiator and SRETs or self-contained event trees, as applicable).
2. The initiating events are described and listed. The listing is provided as a table that includes the assignments of fault trees or basic events to the initiating events. The goal of the initiating event table is to provide a link to the underlying system fault tree (Section 6.2 and Attachment B) or basic event (Section 6.3 and Attachment C). Note that the initiating event frequencies are defined on a per-unit-handled basis. Thus, when the initiating event frequencies are multiplied by the number of units handled over the preclosure period, the result is an initiating event frequency over the preclosure period.
3. The SRET that corresponds to the IET or the system response for a self-contained event tree is covered as follows. Each pivotal event used in an event tree is listed in the event tree description section and summarized in Section A3. Each pivotal event is accompanied by a table that provides the association between the name given to the pivotal event in the event tree and the associated system fault tree or basic event. The goal of the pivotal event table is to provide a link to the underlying fault tree (Section 6.2) or basic event (Section 6.3).

### A3 SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES

A self-contained event tree or a SRET may include pivotal events of following types:

**TRANSCASK.** This pivotal event represents the success or failure of the transportation cask to contain radioactive material after a structural challenge caused by the initiating event. The failure of this pivotal event leads to the loss of the cask's containment function. The failure

probability for this pivotal event is determined by PEFA and is given in Table 6.3-4 in Section 6.3.2.2. In accordance with a simplifying approximation, the same failure probability is used for all casks for the various initiating events.

**CANISTER.** This pivotal event represents the success or failure of the canister to contain radioactive material after the structural challenge caused by the initiating event. Failure of a containment pivotal event means that a release could occur if the canister containment barrier is breached (along with the cask or waste package containment, as applicable). In accordance with a simplifying approximation, the conditional probability of canister breach given cask breach is taken to be 1. Note that this does not apply to uncanistered commercial SNF, for which no canister failure probability is applied.

**SHIELDING.** Failure of a shielding pivotal event means that a direct exposure could occur. Casks, some canisters, aging overpacks, and HAMS include integral shielding that could be pierced or degraded in some impact events. Thus, this pivotal event represents the success or failure of the shielding function after the impact caused by the initiating event. Failure of shielding in this instance refers to an unspecified degree of shielding degradation due to the impact.

**MODERATOR.** This pivotal event represents the conditional probability of introducing liquid moderator (e.g., water) into a breached canister, given that a breached canister is present. Failure of a moderator pivotal event results in an end state that may be susceptible to nuclear criticality. The opportunity for criticality also depends on other pivotal events (e.g., loss of containment, which may allow liquid moderator into a breached canister) and physical properties of the waste form. For Intra-Site Operations, the only opportunity to introduce a moderator is if a fire brigade responds to a fire. All other events have no moderator presence. In addition, DOE HLW is not affected by the presence of a moderator source, and uncanistered commercial SNF in a transportation cask challenged by fire does not permit moderator entry, as described in Section 6.0; therefore, the conditional probability for moderator entry for HLW and uncanistered commercial SNF is always entered in the Excel spreadsheet as “0.00E+0”.

**LLW CONTAINER.** This pivotal event represents the success or failure of a LLW container to contain radioactive material after a structural challenge caused by the initiating event. Failure of a containment pivotal event means that a release could occur if the containment barrier is breached.

## **A4 EVENT TREE DESCRIPTIONS**

### **A4.1 EVENT TREES FOR ISO-ESD-01**

ISO-ESD-01 covers event sequences associated with receipt of a truck trailer or railcar carrying a transportation cask (Ref. 2.2.29, Figure F-1). This ESD covers eight waste form types in transportation casks. Corresponding to each type is an IET (Table A4.1-1). The IETs transfer to the same SRET.



Table A4.1-1. Summary of Event Trees for ISO-ESD-01

Waste Form Unit	Associated Event Trees	Number of Units
Transportation cask containing DPC	Initiator: ISO-ESD01-DPC Response: RESPONSE-TCASK	346
Transportation cask containing HDPC	Initiator: ISO-ESD01-HDPC Response: RESPONSE-TCASK	346
Transportation cask containing HLW canisters	Initiator: ISO-ESD01-HLW Response: RESPONSE-TCASK	2,360
Transportation cask containing NAV canister	Initiator: ISO-ESD01-NAV Response: RESPONSE-TCASK	400
Transportation cask containing MCOs	Initiator: ISO-ESD01-MCO Response: RESPONSE-TCASK	113
Transportation cask containing DSTDs	Initiator: ISO-ESD01-DSTD Response: RESPONSE-TCASK	385
Transportation cask containing a TAD canister	Initiator: ISO-ESD01-TAD Response: RESPONSE-TCASK	6,978
Transportation cask containing UCSNF	Initiator: ISO-ESD01-UCSNF Response: RESPONSE-TCASK	3,775

NOTE: DOE = Department of Energy; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval canister; MCO = multicanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.23, Table 4)

#### A4.1.1 Initiating Events for ISO-ESD-01

The following initiating events are associated with ISO-ESD-01. The assignments made for quantification of these initiating events are indicated in Table A4.1-2.

**Railcar Derailment**—This initiating event accounts for the potential impact to the transportation cask on a railcar due to a derailment. It is conservatively analyzed as if every derailment results in a rollover followed by a drop. Note also that uncanistered commercial SNF arrives only on trucker trailers, therefore, derailment event sequences are not quantified for uncanistered commercial SNF.

**Railcar or Truck Trailer Collision**—These initiating events cover the potential impact to a transportation cask on either a railcar conveyance or a truck trailer conveyance due to a collision. Truck trailer collisions are conservatively analyzed as if every collision results in a rollover followed by a drop. Note that truck trailer collision event sequences are not quantified for waste form types that are not transported on truck trailer conveyances (i.e., DPCs, HDPCs, TAD canisters, and naval canisters), and railcar collisions are not evaluated for uncanistered commercial SNF, which comes in only on truck trailers.

**Drop of Object onto Transportation Cask**—This initiating event accounts for the potential impact to the transportation cask on the conveyance due to an object dropped onto the cask.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Railcar derailment	ISO-ESD01-DPC ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-NAV ISO-ESD01-MCO ISO-ESD01-DSTD ISO-ESD01-TAD ISO-ESD01-UCSNF	INTRASITE_DERAIL
Railcar collision	ISO-ESD01-DPC ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-NAV ISO-ESD01-MCO ISO-ESD01-DSTD ISO-ESD01-TAD ISO-ESD01-UCSNF	INTRASITE_SPMRC_COLLIDE
Truck trailer collision	ISO-ESD01-DPC ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-NAV ISO-ESD01-MCO ISO-ESD01-DSTD ISO-ESD01-TAD ISO-ESD01-UCSNF	INTRASITE_SPMTT_COLLIDE
Drop of object onto transportation cask	ISO-ESD01-DPC ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-NAV ISO-ESD01-MCO ISO-ESD01-DSTD ISO-ESD01-TAD ISO-ESD01-UCSNF	INTRASITE_JIB_CRANE

NOTE: DOE = Department of Energy; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval canister; MCO = multicanister overpack; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

### A4.1.2 System-Response Event Tree RESPONSE-TCASK

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

**TRANSCASK.** Table A4.1-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.1-3. Basic Event Associated with the TRANSCASK Pivotal Events of ISO-ESD-01

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD01-DPC	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-HDPC	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-HLW	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_SPMTT_COLLIDE	TCASK_COLLIDE_TT
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-NAV	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-MCO	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_SPMTT_COLLIDE	TCASK_COLLIDE_TT
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-DSTD	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_SPMTT_COLLIDE	TCASK_COLLIDE_TT
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-TAD	INTRASITE_SPMRC_COLLIDE	TCASK_COLLIDE_RC
	INTRASITE_DERAILED	TCASK_DERAILED
	INTRASITE_JIB_CRANE	TCASK_DROPON
ISO-ESD01-UCSNF	INTRASITE_SPMTT_COLLIDE	TCASK_COLLIDE_TT
	INTRASITE_JIB_CRANE	TCASK_DROPON

NOTE: DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval canister; MCO = multiccanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

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

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD01-DPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	CANISTER1
ISO-ESD01-HDPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-HLW	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	
ISO-ESD01-NAV	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-MCO	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE	
	INTRASITE_JIB_CRANE	
ISO-ESD01-DSTD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	
ISO-ESD01-TAD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-UCSNF	INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	

NOTE: DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; N/A = not applicable; NAV = naval canister; MCO = multicanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

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

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD01-DPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-HDPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-HLW	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-NAV	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-MCO	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-DSTD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL	SHIELD_TCASK_COL SHIELD_TCASK_DROP
	INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-TAD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	SHIELD_TCASK_COL SHIELD_TCASK_DROP SHIELD_TCASK_DROPON
ISO-ESD01-UCSNF	INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	SHIELD_TCASK_DROP SHIELD_TCASK_DROPON

NOTE: DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval canister; MCO = multiccanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

**MODERATOR.** Table A4.1-6 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD01-DPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	MODERATOR_SOP
ISO-ESD01-HDPC	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-HLW	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	
ISO-ESD01-NAV	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-MCO	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	
ISO-ESD01-DSTD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	
ISO-ESD01-TAD	INTRASITE_SPMRC_COLLIDE INTRASITE_DERAIL INTRASITE_JIB_CRANE	
ISO-ESD01-UCSNF	INTRASITE_SPMTT_COLLIDE INTRASITE_JIB_CRANE	

NOTE: DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval canister; MCO = multiccanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

#### A4.2 EVENT TREES FOR ISO-ESD-02

ISO-ESD-02 covers event sequences associated with a site transporter carrying a DPC or TAD canister in an aging overpack (Ref. 2.2.29, Figure F-2). IETs and a SRET represent the ESD (Table A4.2-1).

Table A4.2-1. Summary of Event Trees for ISO-ESD-02

Waste Form Unit	Associated Event Trees	Number of Units
Aging overpack containing a DPC	Initiator: ISO-ESD02-DPC Response: RESPONSE-AO	346
Aging overpack holding a TAD canister	Initiator: ISO-ESD02-TAD Response: RESPONSE-AO	8,143

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; TAD = transportation, aging, and disposal.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.23, Table 4)

#### A4.2.1 Initiating Events for ISO-ESD-02

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

**Site Transporter Collision**—This initiating event accounts for the potential impact to the canister in an aging overpack due to a collision involving the site transporter. The probability of collision per canister moved is modeled as a fault tree as described in Attachment B. The initiating event is specified as a probability of collision per canister movement.

**Site Transporter Drops Aging Overpack**—This initiating event accounts for the potential impact to the canister in an aging overpack due to a drop during transport via the site transporter. The probability of drop per canister moved is modeled as a fault tree as described in Attachment B. The initiating event is specified as a probability of drop per canister movement.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Site transporter collision	ISO-ESD02-DPC	INTRASITE_ST_COLLIDE
	ISO-ESD02-TAD	INTRASITE_ST_AO_DROP
Site transporter drops aging overpack	ISO-ESD02-DPC	INTRASITE_ST_COLLIDE
	ISO-ESD02-TAD	INTRASITE_ST_AO_DROP

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; ST = site transporter; TAD = transportation, aging, and disposal.

Source: Original

#### A4.2.2 System-Response Event Tree RESPONSE-AO

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

**CANISTER.** Table A4.2-3 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-3. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-02

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD02-DPC	INTRASITE_ST_COLLIDE	CANISTER_AO_IMPACT
	INTRASITE_ST_AO_DROP	CANISTER_AO_DROP
ISO-ESD02-TAD	INTRASITE_ST_COLLIDE	CANISTER_AO_IMPACT
	INTRASITE_ST_AO_DROP	CANISTER_AO_DROP

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; ST = site transporter; TAD = transportation, aging, and disposal.

Source: Original

**SHIELDING.** Table A4.2-4 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.2-4. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-02

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD02-DPC	INTRASITE_ST_COLLIDE	SHIELD_AO_IMPACT
	INTRASITE_ST_AO_DROP	SHIELD_AO_DROP
ISO-ESD02-TAD	INTRASITE_ST_COLLIDE	SHIELD_AO_IMPACT
	INTRASITE_ST_AO_DROP	SHIELD_AO_DROP

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; ST = site transporter; TAD = transportation, aging, and disposal.

Source: Original

**MODERATOR.** Table A4.2-5 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

Table A4.2-5. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-02

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD02-DPC	INTRASITE_ST_COLLIDE	MODERATOR_SOP
	INTRASITE_ST_DROP	
ISO-ESD02-TAD	INTRASITE_ST_COLLIDE	
	INTRASITE_ST_DROP	

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; ISO = Intra-Site Operations; ST = site transporter; TAD = transportation, aging, and disposal.

Source: Original



### A4.3 EVENT TREES FOR ISO-ESD-03

ISO-ESD-03 covers event sequences associated with a cask tractor/cask transfer trailer moving an HDPC in an HTC or HSTC (Ref. 2.2.29, Figure F-3). An IET and a SRET represent the ESD (Table A4.3-1).

Table A4.3-1. Summary of Event Trees for ISO-ESD-03

Waste Form Unit	Associated Event Trees	Number of Units
HTC or HSTC containing HDPC	Initiator: ISO-ESD03-HDPC Response: RESPONSE-HTC	346

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.23, Table 4)

#### A4.3.1 Initiating Events for ISO-ESD-03

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

**Impact to HTC or HSTC**—This initiating event accounts for the potential impact to the HTC or HSTC during movement to or from the Aging Facility. The initiating event is specified as a probability of impact per cask (movement).

**Cask Tractor/Cask Transfer Trailer drops an HTC or HSTC**—This initiating event accounts for the potential drop of the HTC or HSTC during movement to or from the Aging Facility. The initiating event is specified as a probability of drop per cask.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Impact to HTC or HSTC	ISO-ESD03-HDPC	INTRASITE_HCTT_COLLISION
Cask tractor/cask transfer trailer drops an HTC or HSTC	ISO-ESD03-HDPC	INTRASITE_HCTT_DROP

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations.

Source: Original

#### A4.3.2 System-Response Event Tree RESPONSE-HTC

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

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

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD03-HDPC	INTRASITE_HCTT_COLLISION	TCASK_HTC_IMPACT
	INTRASITE_HCTT_DROP	TCASK_HTC_DROP

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations.

Source: Original

**CANISTER.** Table A4.3-4 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD03-HDPC	INTRASITE_HCTT_COLLISION	CANISTER1
	INTRASITE_HCTT_DROP	

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

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

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD03-HDPC	INTRASITE_HCTT_COLLISION	SHIELD_TCASK_COL
	INTRASITE_HCTT_DROP	SHIELD_TCASK_DROP

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

**MODERATOR.** Table A4.3-6 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD03-HDPC	INTRASITE_HCTT_COLLISION INTRASITE_HCTT_DROP	MODERATOR_SOP

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

#### A4.4 EVENT TREES FOR ISO-ESD-04

ISO-ESD-04 covers event sequences during canister insertion and retrieval operations at the HAM (Ref. 2.2.29, Figure F-4). This ESD covers one type of waste form. An IET and a SRET represent the ESD (Table A4.4-1).

Table A4.4-1. Summary of Event Trees for ISO-ESD-03

Waste Form Unit	Associated Event Trees	Number of Units
HDPC in an HTC/HSTC or HAM	Initiator: ISO-ESD04-HDPC Response: RESPONSE-HAM	346

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations.

Source: *Waste Form Throughputs for Preclosure Safety Analysis*, (Ref. 2.2.23, Table 4)

##### A4.4.1 Initiating Events for ISO-ESD-04

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

**Impact during insertion and retrieval**—This initiating event accounts for the potential impact to the HTC/HSTC, canister, or HAM during canister insertion or retrieval operations at the HAM. The initiating event is specified as a probability of an impact per waste container. It is conservatively modeled to include an unlikely drop of the canister.

**Impact involving auxiliary equipment**—This initiating event accounts for potential impact to or drop of a heavy object onto the HAM caused by auxiliary equipment present at the Aging Facility. The initiating event is specified as a probability of an impact per waste container.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Impact during insertion and retrieval	ISO-ESD04-HDPC	INTRASITE_HAM_INSERT
Impact involving auxiliary equipment	ISO-ESD04-HDPC	INTRASITE_HAM_AUX_EQUIP

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

#### A4.4.2 System-Response Event Tree RESPONSE-HTC

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

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

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD04-HDPC	INTRASITE_HAM_INSERT	CANISTER_HAM_OPS
	INTRASITE_HAM_AUX_EQUIP	CANISTER_HAM_IMPACT

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

**SHIELDING.** Table A4.4-4 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

Table A4.4-4. Basic Event Associated with the SHIELDING Pivotal Events of ISO-ESD-04

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD04-HDPC	INTRASITE_HAM_INSERT	SHIELD_HAM_IMPACT
	INTRASITE_HAM_AUX_EQUIP	

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

**MODERATOR.** Table A4.4-5 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD04-HDPC	INTRASITE_HAM_INSERT INTRASITE_HAM_AUX_EQUIP	MODERATOR_SOP

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; ISO = Intra-Site Operations.

Source: Original

#### A4.5 EVENT TREES FOR ISO-ESD-05

ISO-ESD-05 covers event sequences for activities associated with LLW containers in the LLWF (Ref. 2.2.29, Figure F-5). A single initiating event, “Impact to a single LLW container”, is associated with ISO-ESD-05. Because there is only one initiating event, the event trees are self contained (Table A4.5-1).

Table A4.5-1. Summary of Event Trees for ISO-ESD-05

Waste Form Units	Associated Event Trees	Number of Units
LLW container containing DAW	Initiator: ISO-ESD05-LLWDAW Response: N/A	1,800 <sup>a</sup>
LLW container containing liquid LLW	Initiator: ISO-ESD05-LLWLIQ Response: N/A	N/A <sup>c</sup>
LLW container containing wet-solid LLW	Initiator: ISO-ESD05-LLWWETnr Response: N/A	150 <sup>b</sup>

NOTE: <sup>a</sup> For dose calculations, these HEPA filters are the only DAW that are anticipated to have significant levels of contaminants; “1,800” is based on *Shielding Requirements and Dose Rate Calculations for WHF and LLW* (Ref. 2.2.22, Section 3.1.9), in which it is assumed and rationalized 30 filters are changed every 10 months (to maintain contamination levels at or below Class B for LLW), over the 50-year preclosure period. In addition, each HEPA filter will be containerized and moved to the LLWF individually.

<sup>b</sup> WHF pool filters are most common source of wet-solid (non-resin) LLW and are most likely to have the worst contaminant types and levels, due to repackaging of PWR and BWR material (Ref. 2.2.13) and (Ref. 2.2.22). An estimated 520 pool filters will be produced annually (Ref. 2.2.85), which will be placed in HICs (approximately 200 per HIC). This results in 3 HICs per year, or 150 HICs over the 50-year preclosure period.

<sup>c</sup> Liquid LLW release is classified as an off-normal event, since the consequences to a worker are a small fraction of the performance objectives (Ref. 2.2.30, Appendix IV). Liquid LLW events are not evaluated further in this document.

BWR = boiling water reactor; DAW = dry active low-level radioactive waste; ESD = event sequence diagram; HEPA = high-efficiency particulate air; HIC = high-integrity canister; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; N/A = not applicable; nr = non-resin; PWR = pressurized water reactor; WHF = Wet Handling Facility.

Source: *Shielding Requirements and Dose Rate Calculations for WHF and LLW* (Ref. 2.2.22); *Low-Level Waste Management Plan* (Ref. 2.2.13); “Reference Information for Processing of Spent Pool Water Treatment System, Spent Clean-up Filters, and Spent Resin Generated in the Wet Handling Facility” (Ref. 2.2.85); *Preclosure Consequence Analyses* (Ref. 2.2.30).

### A4.5.1 Initiating Events for ISO-ESD-05

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

**Impact to a single LLW container**—This initiating event accounts for a collision that breaches a LLW container in the LLWF. The probability of impact per container moved is based on a basic event involving forklifts.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Impact a single LLW container	ISO-ESD05-LLWDAW	ISO_ESD05_Forklift_LLW_Impact
	ISO-ESD05-LLWLIQ	
	ISO-ESD05-LLWWETnr	

NOTE: DAW = dry active low-level radioactive waste; ESD = event sequence diagram; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; nr = non-resin.

Source: Original

### A4.5.2 Pivotal Events

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

**LLW CONTAINER.** Table A4.5-3 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

Table A4.5-3. Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-05

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD05-LLWDAW ISO-ESD05-LLWLIQ ISO-ESD05-LLWWETnr	ISO_ESD05_Forklift_LLW_Impact	CONTAINER_LLW

NOTE: DAW = dry active low-level radioactive waste; ESD = event sequence diagram; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; nr = non-resin.

Source: Original

#### A4.6 EVENT TREES FOR ISO-ESD-06

ISO-ESD-06 covers event sequences for non-fire events involving all LLW containers in the LLWF (Ref. 2.2.29, Figure F-6). A single initiating event, “Non-fire event involving all LLW containers”, is associated with ISO-ESD-06. To involve (i.e., to possibly breach) all containers in the LLWF without fire necessitates a collapse of the LLWF. Collapse of the LLWF due to a seismic event is analyzed for consequence in *Preclosure Consequence Analyses* (Ref. 2.2.30, Table 2, Section 6.3.4, and Section 6.8.1) and is bounding. No further analysis for collapse of the LLWF is needed.

#### A4.7 EVENT TREES FOR ISO-ESD-07

ISO-ESD-07 covers event sequences associated with a large fire at the LLWF involving all combustible LLW. This ESD applies to the full inventory LLW. A single initiating event, “Fire event involving all combustible LLW”, is associated with ISO-ESD-07. Because there is only one initiating event, the event tree is self-contained (Table A4.7-1).

Table A4.7-1. Summary of Event Trees for ISO-ESD-07

Waste Form Units	Associated Event Trees	Number of Units	Number of Occurrences over the Preclosure Period
LLW containers containing combustible LLW	Initiator: ISO-ESD07-LLW Response: N/A	(all)	1

NOTE: ESD = event sequence diagram; ISO = Intra-Site Operations; LLW = low-level radioactive waste; N/A = not applicable.

Source: Attachment F

##### A4.7.1 Initiating Events for ISO-ESD-07

ISO-ESD-07 covers event sequences for fire involving all LLW containers in the LLWF (Ref. 2.2.29, Figure F-7). A single initiating event, “Fire event involving all combustible LLW”, is associated with ISO-ESD-07. Table A4.7-2 summarizes the event trees for ISO-ESD-07. The probability of occurrence over the preclosure period is discussed in Section 6.5 and Attachment F.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Fire event involving all combustible LLW in containers	ISO-ESD07-LLW	ISO_ESD07_Ignition_Freq_LLW

NOTE: ESD = event sequence diagram; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; N/A = not applicable.

Source: Original

### A4.7.2 Pivotal Events

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

**LLW CONTAINER.** Table A4.7-3 indicates the basic event that is associated with this pivotal event for each initiating event. (It is the same for all waste form types and all initiating events shown.)

Table A4.7-3. Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-07

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD07-LLW	ISO_ESD07_Ignition_Freq_LLW	CONTAINER_LLW

NOTE: ESD = event sequence diagram; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; N/A = not applicable.

Source: Original

### A4.8 EVENT TREES FOR ISO-ESD-08

ISO-ESD-08 covers event sequences associated with transfers of LLW within the GROA boundary (Ref. 2.2.29, Figure F-8). This ESD covers all LLW forms, and corresponding to each type is an IET (Table A4.8-1). The IETs transfer to the same SRET.

Table A4.8-1. Summary of Event Trees for ISO-ESD-08

Waste Form Units	Associated Event Trees	Number of Units
LLW container containing DAW	Initiator: ISO-ESD08-LLWDAW Response: RESPONSE-LLW	1,800 <sup>a</sup>
LLW container containing wet-solid LLW (resin from WHF only)	Initiator: ISO-ESD08-LLWWETr Response: RESPONSE-LLW	150 <sup>b</sup>
LLW container containing wet-solid LLW (non-resin)	Initiator: ISO-ESD08-LLWWETnr Response: RESPONSE-LLW	150 <sup>c</sup>
LLW container containing liquid LLW	Initiator: ISO-ESD08-LLWLIQ Response: RESPONSE-LLW	N/A <sup>d</sup>



Waste Form Units	Associated Event Trees	Number of Units
------------------	------------------------	-----------------

NOTE: <sup>a</sup> For dose calculations, these HEPA filters are the only DAW that are anticipated to have significant levels of contaminants; "1,800" is based on *Shielding Requirements and Dose Rate Calculations for WHF and LLW* (Ref. 2.2.22, Section 3.1.9), in which it is assumed and rationalized 30 filters are changed every 10 months (to maintain contamination levels at or below Class B for LLW), over the 50-year preclosure period. In addition, each HEPA filter will be containerized and moved to the LLWF individually.

<sup>b</sup> Sluicing each resin bed once per year (3 beds total), results in 150 high-integrity containers (HICs) over the preclosure period (Ref. 2.2.22, Section 3.1.8). This is conservative, because the WHF could opt to do a maintenance shutdown of the facility and sluice all three resin beds into one HIC. This would result in a minimum number of HICs, that is, 50 HICs over the preclosure period.

<sup>c</sup> WHF pool filters are most common source of wet-solid (non-resin) LLW and are most likely to have the worst contaminant types and levels, due to repackaging of PWR and BWR material (Ref. 2.2.13) and (Ref. 2.2.22). An estimated 520 pool filters will be produced annually (Ref. 2.2.85), which will be placed in HICs (approximately 200 per HIC). This results in 3 HICs per year, or 150 HICs over the 50-year preclosure period.

<sup>d</sup> Liquid LLW release is classified as an off-normal event, since the consequences to a worker are a small fraction of the performance objectives (Ref. 2.2.30, Appendix IV). Liquid LLW events are not evaluated further in this document.

BWR = boiling water reactor; DAW = dry active low-level radioactive waste; ESD = event sequence diagram; HEPA = high-efficiency particulate air; HIC = high-integrity canister; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; N/A = not applicable; PWR = pressurized water reactor; WHF = Wet Handling Facility.

Source: *Shielding Requirements and Dose Rate Calculations for WHF and LLW* (Ref. 2.2.22); *Low-Level Waste Management Plan* (Ref. 2.2.13); "Reference Information for Processing of Spent Pool Water Treatment System, Spent Clean-up Filters, and Spent Resin Generated in the Wet Handling Facility" (Ref. 2.2.85); *Preclosure Consequence Analyses* (Ref. 2.2.30)

#### A4.8.1 Initiating Events for ISO-ESD-08

The assignments made for quantification of these initiating events are indicated in Table A4.8-2. The initiating events are specified as frequency of occurrence per container movement.

**Impacts involving dry active LLW**—This initiating event accounts for potential structural challenge to a dry active LLW container that occurs during transfer from the generating facility.

**Equipment failure or collision involving wet-solid LLW (spent resin)**—This initiating event accounts for potential structural challenges to a wet-solid LLW container (i.e., a truck- or trailer-mounted HIC) containing spent resin that occurs during transfer of the HIC from the WHF.

**Equipment failure involving non-resin wet-solid LLW**—This initiating event accounts for potential structural challenge to a wet-solid LLW container containing wet-solid LLW (particularly filters from WHF pool water treatment system contained in a HIC) that occurs during transfer from the generating facility.

**Initiating events involving liquid LLW container transfers**—This is an amalgamation of initiating events that account for potential structural challenges to liquid LLW containers (or containment boundaries) that occur during transfer operations. It includes initiating events for impacts, loss of containment, and equipment failures. Note that release of liquid LLW is classified as an off-normal event because the consequences to a worker are a small fraction of the performance objectives (Ref. 2.2.30, Appendix IV). Therefore, liquid LLW events are not evaluated further for categorization.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Impacts involving dry active LLW	ISO-ESD08-LLWDAW	ISO_ESD08_INTRASITE_HEPA_TRANSFER
Equipment failure or collision involving wet-solid LLW (resin)	ISO-ESD08-LLWWETr	ISO_ESD08_INTRASITE_HEPA_TRANSFER_Wet_resin
Equipment failure involving liquid LLW (nonWHF-generated) and non-resin wet-solid LLW	ISO-ESD08-LLWWETnr	ISO_ESD08_INTRASITE_COLL_TRANSFER_Wet_nr
Initiating events involving liquid LLW container transfers	ISO-ESD08-LLWLIQ	N/A <sup>1</sup>

NOTE: <sup>1</sup>Liquid LLW release is classified as an off-normal event, since the consequences to a worker are a small fraction of the performance objectives (Ref. 2.2.30, Appendix IV). Liquid LLW events are not evaluated further in this document.

DAW = dry active low-level radioactive waste; ESD = event sequence diagram; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; N/A = not applicable.

Source: Original

#### A4.8.2 System-Response Event Tree RESPONSE-LLW

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

**LLW CONTAINER.** Table A4.8-3 indicates the basic event or fault tree associated with this pivotal event for each initiating event.

Table A4.8-3. Basic Events Associated with the LLW CONTAINER Pivotal Events of ISO-ESD-08

Initiator Event Tree	Initiating Event Name	Associated Basic Event or Fault Tree
ISO-ESD08-LLWDAW	ISO_ESD08_INTRASITE_HEPA_TRANSFER	CONTAINER_LLW
ISO-ESD08-LLWWETr	ISO_ESD08_INTRASITE_HEPA_TRANSFER_Wet_resin	
ISO-ESD08-LLWWETnr	ISO_ESD08_INTRASITE_COLL_TRANSFER_Wet_nr	
ISO-ESD08-LLWLIQ	N/A <sup>1</sup>	N/A <sup>1</sup>

NOTE: <sup>1</sup>Liquid LLW release is classified as an off-normal event, since the consequences to a worker are a small fraction of the performance objectives (Ref. 2.2.30, Appendix IV). Liquid LLW events are not evaluated further in this document.

DAW = dry active low-level radioactive waste; ESD = event sequence diagram; HEPA = high efficiency particulate air; ISO = Intra-Site Operations; LIQ = liquid; LLW = low-level radioactive waste; N/A = not applicable.

Source: Original

## A4.9 EVENT TREES FOR ISO-ESD-09

ISO-ESD-09 covers event sequences associated with fires during transportation and Aging Facility activities (Ref. 2.2.29, Figure F-9). This ESD covers all waste form types (Table A4.9-1). Corresponding to each canister type is an IET (Table A4.9-1). The IETs transfer to the same SRET.

Table A4.9-1. Summary of Event Trees for ISO-ESD-09

Waste Form Unit	Associated Event Trees	Number of Units
DPC in transportation cask or aging overpack	Initiator: ISO-ESD09-DPC Response: RESPONSE-FIRE	346
HDPC in HTC or HSTC or HAM	Initiator: ISO-ESD09-HDPC Response: RESPONSE-FIRE	346
HLW canisters in transportation cask	Initiator: ISO-ESD09-HLW Response: RESPONSE-FIRE	2,360
Naval canister in transportation cask	Initiator: ISO-ESD09-NAV Response: RESPONSE-FIRE	400
MCOs in transportation casks	Initiator: ISO-ESD09-MCO Response: RESPONSE-FIRE	113
DSTDs in transportation casks	Initiator: ISO-ESD09-DSTD Response: RESPONSE-FIRE	385
TAD canister in transportation cask or aging overpack	Initiator: ISO-ESD09-TAD Response: RESPONSE-FIRE	8,143
UCSNF in a transportation cask	Initiator: ISO-ESD09-UCSNF Response: RESPONSE-FIRE	3,775

NOTE: DOE = Department of Energy; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations; NAV = naval; MCO = multiccanister overpack; TAD = transportation, aging, and disposal; UCSNF = uncanistered commercial spent nuclear fuel.

Source: *Waste Form Throughputs for Preclosure Safety Analysis* (Ref. 2.2.23, Table 4)

### A4.9.1 Initiating Events for ISO-ESD-09

The following initiating events are associated with ISO-ESD-09. The assignments made for quantification of these initiating events are indicated in Table A4.9-2. The initiating events are specified as frequency of occurrence per waste form type (for movement activities) or over the preclosure period (for holding or aging activities).

**Fire affects transportation cask during staging in buffer area**—This initiating event covers potential thermal challenge to a waste container on a railcar or truck trailer, as applicable, due to fire during staging in a buffer area.

**Fire affects transportation cask during movement between GROA boundary and either buffer area or a handling facility**—This initiating event covers potential thermal challenge to a waste container on a railcar or truck trailer due to fire during movement between the GROA boundary and either a buffer area or a surface facility.

**Fire affects aging overpack, HTC, or HSTC during movement among facilities or to/from Aging Facility**—This initiating event covers the potential thermal challenge to a waste container due to fire during movement between a surface facility and the Aging Facility.

**Fire at Aging Facility**—This initiating event covers the potential thermal challenge to a waste container due to fire during aging at the Aging Facility.

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

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Fire affects transportation cask during staging in buffer area	ISO-ESD09-DPC ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-NAV ISO-ESD09-MCO ISO-ESD09-DSTD ISO-ESD09-TAD ISO-ESD09-UCSNF	ISO_ESD09_Fires_TC_Buffer
Fire affects transportation cask during movement between GROA boundary and either buffer area or a handling facility	ISO-ESD09-DPC ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-NAV ISO-ESD09-MCO ISO-ESD09-DSTD ISO-ESD09-TAD ISO-ESD09-UCSNF	ISO_ESD09_Fires_TC_Movement
Fire affects aging overpack, HTC, or HSTC during movement among facilities or to/from Aging Facility	ISO-ESD09-DPC ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-NAV ISO-ESD09-MCO ISO-ESD09-DSTD ISO-ESD09-TAD ISO-ESD09-UCSNF	ISO_ESD09_Fires_AF_Movement

Table A4.9-2. Initiating Event Assignments for ISO-ESD-09 (Continued)

Initiating Event Description	Initiator Event Tree	Initiating Event Data Source (Fault Tree or Basic Event Name from Spreadsheet)
Fire at Aging Facility	ISO-ESD09-DPC ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-NAV ISO-ESD09-MCO ISO-ESD09-DSTD ISO-ESD09-TAD ISO-ESD09-UCSNF	ISO_ESD09_Fires_AF_Aging

NOTE: AF = Aging Facility; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; GROA = geologic repository operations area; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations; NAV = naval; MCO = multicanister overpack; TAD = transportation, aging, and disposal; TC = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

### A4.9.2 System-Response Event Tree RESPONSE-FIRE

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

**CANISTER.** Table A4.9-3 indicates the fault trees or basic events that are associated with this pivotal event for each initiating event.

Table A4.9-3. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-09

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD09-DPC	ISO_ESD09_Fires_TC_Buffer	FIRE_CANISTER_TC
	ISO_ESD09_Fires_TC_Movement	
	ISO_ESD09_Fires_AF_Movement	FIRE_CANISTER_AO
	ISO_ESD09_Fires_AF_Aging	
ISO-ESD09-HDPC	ISO_ESD09_Fires_TC_Buffer	FIRE_CANISTER_TC
	ISO_ESD09_Fires_TC_Movement	
	ISO_ESD09_Fires_AF_Movement	FIRE_CANISTER_AO
	ISO_ESD09_Fires_AF_Aging	
ISO-ESD09-HLW	ISO_ESD09_Fires_TC_Buffer	FIRE_CANISTER_TC
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-NAV	ISO_ESD09_Fires_TC_Buffer	FIRE_CANISTER_TC_NAV
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-MCO	ISO_ESD09_Fires_TC_Buffer	FIRE_CANISTER_TC

Table A4.9-3. Basic Events Associated with the CANISTER Pivotal Events of ISO-ESD-09 (Continued)

Initiator Event Tree	Initiating Event Name	Associated Basic Event
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-DSTD	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_CANISTER_TC
ISO-ESD09-TAD	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement ISO_ESD09_Fires_AF_Movement ISO_ESD09_Fires_AF_Aging	FIRE_CANISTER_TC  FIRE_CANISTER_AO
ISO-ESD09-UCSNF	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_TCASK_UCSNF

NOTE: AF = Aging Facility; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval; MCO = multicanister overpack; TAD = transportation, aging, and disposal; TC = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

**SHIELDING.** Table A4.9-4 indicates the basic event that is associated with this pivotal event for each initiating event.

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

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD09-DPC	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
	ISO_ESD09_Fires_AF_Movement	FIRE_SHIELD_AO
	ISO_ESD09_Fires_AF_Aging	
ISO-ESD09-HDPC	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
	ISO_ESD09_Fires_AF_Movement	FIRE_SHIELD_AO
	ISO_ESD09_Fires_AF_Aging	
ISO-ESD09-HLW	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-NAV	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-MCO	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-DSTD	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
ISO-ESD09-TAD	ISO_ESD09_Fires_TC_Buffer	FIRE_SHIELD_TCASK
	ISO_ESD09_Fires_TC_Movement	
	ISO_ESD09_Fires_AF_Movement	FIRE_SHIELD_AO

Table A4.9-4. Basic Events Associated with the SHIELDING Pivotal Events of ISO-ESD-09 (Continued)

Initiator Event Tree	Initiating Event Name	Associated Basic Event
	ISO_ESD09_Fires_AF_Aging	
ISO-ESD09-UCSNF	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_SHIELD_TCASK

NOTE: AF = Aging Facility; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval; MCO = multiccanister overpack; TAD = transportation, aging, and disposal; TC = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

**MODERATOR.** Table A4.9-5 indicates the basic event that is associated with this pivotal event for each initiating event.

Table A4.9-5. Basic Event Associated with the MODERATOR Pivotal Events of ISO-ESD-09

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD09-DPC	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement ISO_ESD09_Fires_AF_Movement ISO_ESD09_Fires_AF_Aging	FIRE_MODERATOR
ISO-ESD09-HDPC	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement ISO_ESD09_Fires_AF_Movement ISO_ESD09_Fires_AF_Aging	FIRE_MODERATOR
ISO-ESD09-HLW	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_MODERATOR_NA
ISO-ESD09-NAV	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_MODERATOR
ISO-ESD09-MCO	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_MODERATOR
ISO-ESD09-DSTD	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_MODERATOR
ISO-ESD09-TAD	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement ISO_ESD09_Fires_AF_Movement ISO_ESD09_Fires_AF_Aging	FIRE_MODERATOR

Table A4.9-5. Basic Events Associated with MODERATOR Pivotal Events of ISO-ESD-09 (Continued)

Initiator Event Tree	Initiating Event Name	Associated Basic Event
ISO-ESD09-UCSNF	ISO_ESD09_Fires_TC_Buffer ISO_ESD09_Fires_TC_Movement	FIRE_MODERATOR_NA

NOTE: AF = Aging Facility; DPC = dual-purpose canister; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; ISO = Intra-Site Operations; NAV = naval; MCO = multicatcher overpack; TAD = transportation, aging, and disposal; TC = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

### A5 EVENT TREES

The following figures provide a graphic representation, developed in SAPHIRE, of the event sequence structure. Navigation from an IET to the corresponding system response tree is shown in the rightmost two columns on the IETs as shown in Figure A5-1. The numbers under the “#” symbol may be used by the reader to refer to a particular branch of an event tree, but it is not used elsewhere in this analysis.

Transportation cask containing waste form	Identify initiating events		
#_WASTEFORMS	INIT_EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Deraiment of railcar w/ waste form	2 T => 2	RESPONSE-SAMPLE
	Collision of railcar w/ waste form	3 T => 2	RESPONSE-SAMPLE
	Collision of truck trailer w/ waste form	4 T => 2	RESPONSE-SAMPLE
	Drop of object onto waste form	5 T => 2	RESPONSE-SAMPLE

Indicates system response event tree

Indicates system response event tree's sheet number

Sheet number

TWF-ESD01-WASTEFORM - Movement of Transportation Cask Containing Waste Form on Conveyance

2008/01/07 Sheet 1

Source: Original

Figure A5-1. Example IET Showing Navigation Aids



Table A5-1. Correspondence between ESDs and Event Trees

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
ISO-ESD-01	Event Sequences for Activities Associated with Movement of Transportation Cask during Site Transportation	ISO-ESD01-DPC ISO-ESD01-DSTD ISO-ESD01-HDPC ISO-ESD01-HLW ISO-ESD01-MCO ISO-ESD01-NAV ISO-ESD01-TAD ISO-ESD01-UCSNF	Figure A5-2 Figure A5-4 Figure A5-5 Figure A5-6 Figure A5-7 Figure A5-8 Figure A5-9 Figure A5-10	RESPONSE-TCASK	Figure A5-3
ISO-ESD-02	Event Sequences for Activities Associated with Aging Overpack Transit, Placement, and Retrieval	ISO-ESD02-DPC ISO-ESD02-TAD	Figure A5-11 Figure A5-13	RESPONSE-AO	Figure A5-12
ISO-ESD-03	Event Sequences for Activities Associated with the Transporting and Positioning of an HTC or an HSTC	ISO-ESD03-HDPC	Figure A5-14	RESPONSE-HTC	Figure A5-15
ISO-ESD-04	Event Sequences Associated with Impacts during Canister Operations at a Horizontal Aging Module	ISO-ESD04-HDPC	Figure A5-16	RESPONSE-HAM	Figure A5-17
ISO-ESD-05	Event Sequences for Activities Associated with a Single Low-Level Radioactive Waste Container at the Low-Level Waste Facility	ISO-ESD05-LLWDAW ISO-ESD05-LLWLIQ ISO-ESD05-LLWWETnr	Figure A5-18 Figure A5-19 Figure A5-20	N/A	N/A
ISO-ESD-06	Event Sequences Associated with Nonfire Events Involving all Low-Level Radioactive Waste Containers at the Low-Level Waste Facility	ISO-ESD06-LLW	Figure A5-21	N/A	N/A

Table A5-1. Correspondence between Event Trees and ESDs (Continued)

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
ISO-ESD-07	Event Sequences Associated with Fire Events for All Combustible Low-Level Radioactive Waste in the Low-Level Waste Facility	ISO-ESD07-LLW	Figure A5-22	N/A	N/A
ISO-ESD-08	Event Sequences for Activities Associated with Waste Transfers to the Low-Level Waste Facility	ISO-ESD08-LLWDAW ISO-ESD08-LLWLIQ ISO-ESD08-LLWWETnr ISO-ESD08-LLWWETr	Figure A5-23 Figure A5-25 Figure A5-26 Figure A5-27	RESPONSE-LLW	Figure A5-24
ISO-ESD-09	Event Sequences for Fire Occurring during Site Transportation Activities or at the Aging Facility	ISO-ESD09-DPC ISO-ESD09-DSTD ISO-ESD09-HDPC ISO-ESD09-HLW ISO-ESD09-MCO ISO-ESD09-NAV ISO-ESD09-TAD ISO-ESD09-UCSNF	Figure A5-28 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34 Figure A5-35 Figure A5-36	RESPONSE-FIRE	Figure A5-29

NOTE: AO = aging overpack; DAW = dry active low-level radioactive waste; DPC = dual-purpose canister; DSTD = DOE standardized canister; ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; MCO = multiccanister overpack; NAV = naval; nr = nonresin; r = resin; TAD = transportation, aging and disposal; TCASK = transportation cask; UCSNF = uncanistered commercial spent nuclear fuel.

Source: Original

Transportation cask containing DPC	Identify initiating events			
DPC	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	Railcar derailment	2	T => 2	RESPONSE-TCASK
	Railcar collision	3	T => 2	RESPONSE-TCASK
	Truck trailer collision	4	T => 2	RESPONSE-TCASK
	Drop of object	5	T => 2	RESPONSE-TCASK

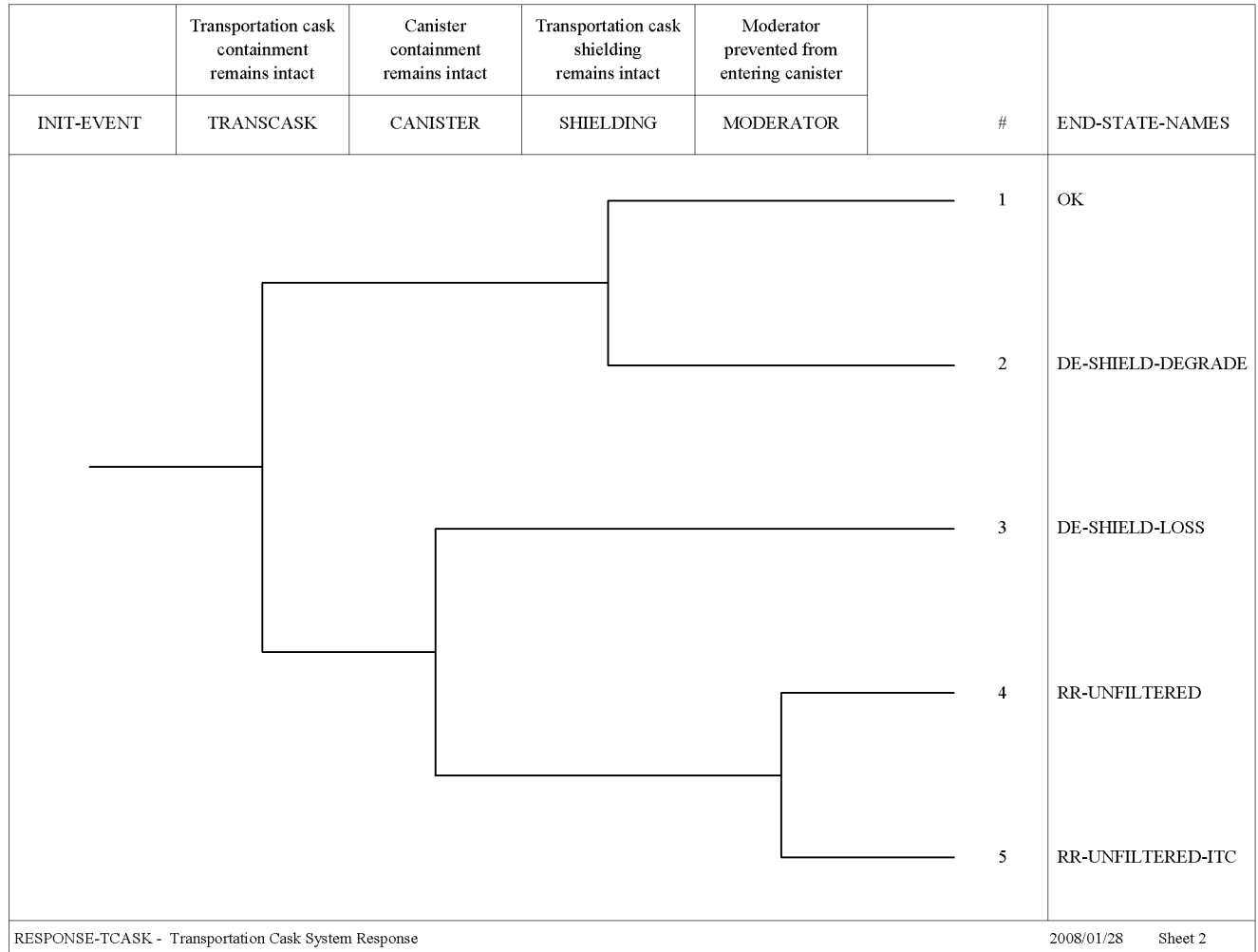
ISO-ESD01-DPC - Movement of Transportation Cask Containing DPC on Railcar

2008/01/28 Sheet 1

NOTE: DPC = dual-purpose canister; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; T = transfer; TCASK = transportation cask; XFER = transfer.

Source: Original

Figure A5-2. IET for ISO-ESD-01 – DPC – Movement of Transportation Cask Containing DPC on Railcar



NOTE: DE = direct exposure; ESD = event sequence diagram; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RR = radionuclide release; TC = transportation cask; TCASK = transportation cask; TRANSCASK = transportation cask.

Source: Original

Figure A5-3. System-Response Event Tree for ISO-ESD-01 – RESPONSE-TCASK – Transportation Cask System Response

Transportation cask containing DOE standardized canister	Identify initiating events		
DSTD	INIT-EVENT	#	XFER-TO-RESP-TREE
	Railcar derailment	1	OK
	Railcar collision	2 T => 2	RESPONSE-TCASK
	Truck trailer collision	3 T => 2	RESPONSE-TCASK
	Drop of object	4 T => 2	RESPONSE-TCASK
		5 T => 2	RESPONSE-TCASK

ISO-ESD01-DSTD - Movement of Transportation Cask Containing DOE Standardized Canister (DSTD) on Railcar or Truck Trailer 2008/01/28 Sheet 3

NOTE: DSTD = Department of Energy standardized canister; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; ST = site transporter; T = transfer; TCASK = transportation cask; TT = transportation cask; XFER = transfer.

Source: Original

Figure A5-4. IET for ISO-ESD-01 – DSTD – Movement of Transportation Cask Containing DOE Standardized Canister on Railcar or Truck Trailer

HTC containing HDPC	Identify initiating events		
HDPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Railcar derailment	2	T => 2
	Railcar collision	3	T => 2
	Truck trailer collision	4	T => 2
	Drop of object	5	T => 2

ISO-ESD01-HDPC - Movement of HTC (Transportation Cask) Containing HDPC on Railcar

2008/01/28 Sheet 4

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; TCASK = transportation cask; T = transfer.

Source: Original

Figure A5-5. IET for ISO-ESD-01 – HDPC – Movement of HTC (Transportation Cask) Containing HDPC on Railcar

Transportation cask containing HLW canister(s)	Identify initiating events		
HLW	INIT-EVENT	#	XFER-TO-RESP-TREE
	Railcar derailment	1	OK
	Railcar collision	2	T => 2 RESPONSE-TCASK
	Truck trailer collision	3	T => 2 RESPONSE-TCASK
	Drop of object	4	T => 2 RESPONSE-TCASK
		5	T => 2 RESPONSE-TCASK

ISO-ESD01-HLW - Movement of Transportation Cask Containing HLW Canister(s) on Railcar or Truck Trailer

2008/01/28 Sheet 5

NOTE: ESD = event sequence diagram; HLW = high-level radioactive waste; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; T = transfer; TCASK = transportation cask; TT = truck trailer; XFER = transfer.

Source: Original

Figure A5-6. IET for ISO-ESD-01 – HLW – Movement of Transportation Cask Containing HLW Canister(s) on Railcar or Truck Trailer

Transportation cask containing DOE MCO	Identify initiating events		
MCO	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Railcar derailment	2	T => 2
	Railcar collision	3	T => 2
	Truck trailer collision	4	T => 2
	Drop of object	5	T => 2

ISO-ESD01-MCO - Movement of Transportation Cask Containing DOE MCO on Railcar or Truck Trailer

2008/01/28 Sheet 6

NOTE: ESD = event sequence diagram; MCO = multicanister overpack; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; T = transfer; TCASK = transportation cask; TT = truck trailer; XFER = transfer.

Source: Original

Figure A5-7. IET for ISO-ESD-01 – MCO – Movement of Transportation Cask Containing DOE MCO on Railcar or Truck Trailer



Transportation cask containing naval canister	Identify initiating events				
NAV	INIT-EVENT	#	XFER-TO-RESP-TREE		
		1	OK		
		Railcar derailment	2	T => 2	RESPONSE-TCASK
		Railcar collision	3	T => 2	RESPONSE-TCASK
		Truck trailer collision	4	T => 2	RESPONSE-TCASK
		Drop of object	5	T => 2	RESPONSE-TCASK
ISO-ESD01-NAV - Movement of Transportation Cask Containing Naval Canister on Railcar		2008/01/28	Sheet 7		

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; NAV = naval; RESP = response; TCASK = transportation cask; XFER = transfer.

Source: Original

Figure A5-8. IET for ISO-ESD-01 – NAV – Movement of Transportation Cask Containing Naval Canister on Railcar

Transportation cask containing TAD canister	Identify initiating events		
TAD	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Railcar derailment	2	T => 2 RESPONSE-TCASK
	Railcar collision	3	T => 2 RESPONSE-TCASK
	Truck trailer collision	4	T => 2 RESPONSE-TCASK
	Drop of object	5	T => 2 RESPONSE-TCASK
ISO-ESD01-TAD - Movement of Transportation Cask Containing TAD Canister on Railcar or Truck Trailer		2008/01/28	Sheet 8

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; T = transfer; TAD = transportation, aging, and disposal; TCASK = transportation cask; TT = truck trailer; XFER = transfer.

Source: Original

Figure A5-9. IET for ISO-ESD-01 – TAD – Movement of Transportation Cask Containing TAD Canister on Railcar or Truck Trailer

Transportation cask containing UCSNF	Identify initiating events		
UCSNF	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Railcar derailment	2	T => 2
	Railcar collision	3	T => 2
	Truck trailer collision	4	T => 2
	Drop of object	5	T => 2
ISO-ESD01-UCSNF - Movement of Transportation Cask Containing UCSNF on Railcar or Truck Trailer		2008/01/28	Sheet 9

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RC = railcar; RESP = response; T = transportation cask; TCASK = transportation cask; TT = truck trailer; UCSNF = uncanistered commercial spent nuclear fuel; XFER = transfer.

Source: Original

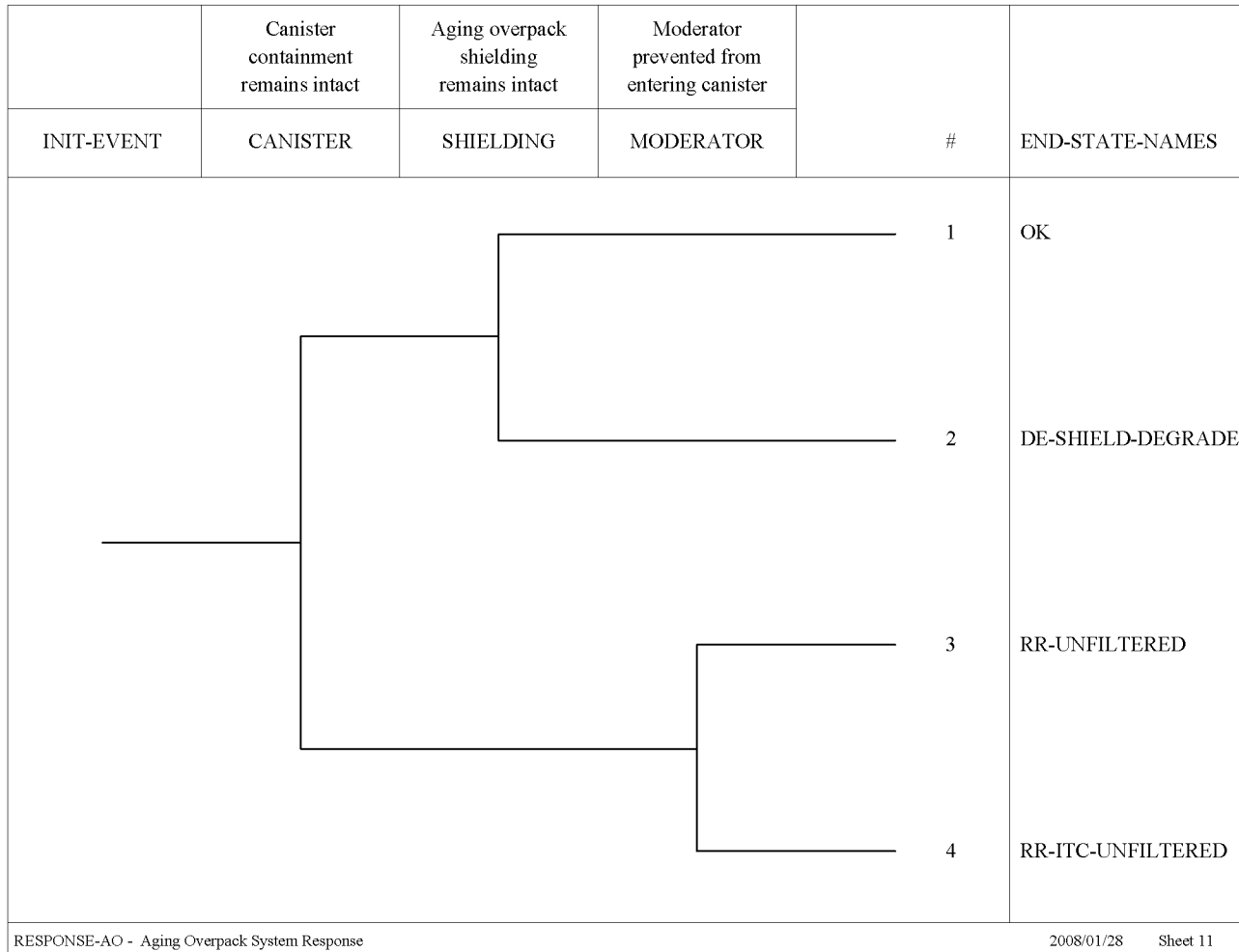
Figure A5-10. IET for ISO-ESD-01 – UCSNF – Movement of Transportation Cask Containing UCSNF on Railcar or Truck Trailer

Aging overpack containing DPC	Identify initiating events		
DPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
		2	T => 11 RESPONSE-AO
		3	T => 11 RESPONSE-AO
ISO-ESD02-DPC - Movement of Aging Overpack Containing DPC on Site Transporter To/From Aging Facility		2008/01/28	Sheet 10

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; ST = site transporter; T = transfer; XFER = transfer.

Source: Original

Figure A5-11. IET for ISO-ESD-02 – DPC – Movement of Aging Overpack Containing DPC on Site Transporter To/From Aging Facility



NOTE: AO = aging overpack; DE = direct exposure; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-12. System-Response Event Tree for ISO-ESD-02 – RESPONSE-AO – Aging Overpack System Response

Aging overpack containing TAD canister	Identify initiating events		
TAD	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
		2	T => 11
		3	T => 11
ISO-ESD02-TAD - Movement of Aging Overpack Containing TAD Canister on Site Transporter To/From Aging Facility		2008/01/28	Sheet 12

NOTE: AO = aging overpack; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; ST = site transporter; T= transfer; TAD = transportation, aging, and disposal; XFER = transfer.

Source: Original

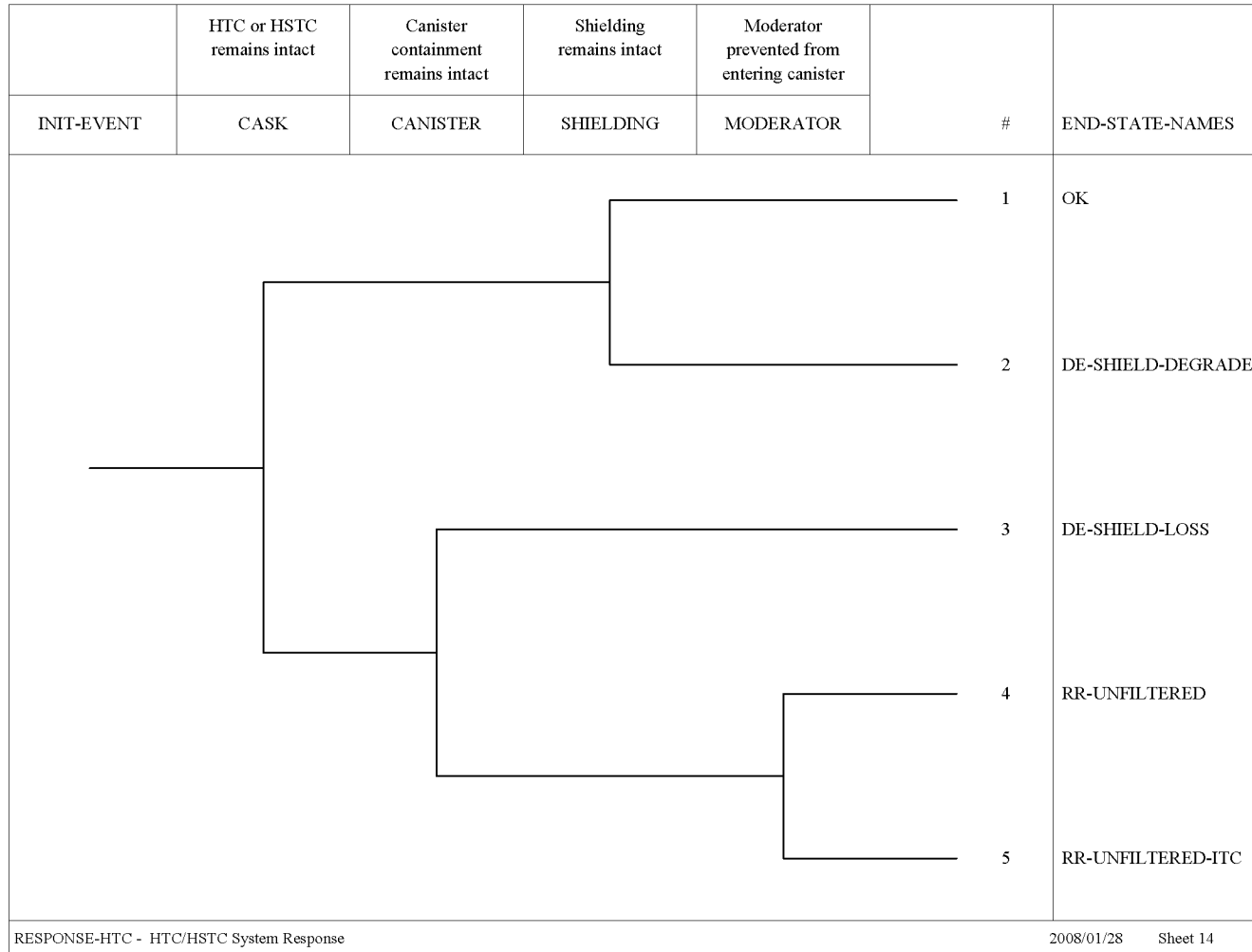
Figure A5-13. IET for ISO-ESD-02 – TAD – Movement of Aging Overpack Containing TAD Canister on Site Transporter To/From Aging Facility

HTC or HSTC containing HDPC	Identify initiating events		
HDPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
		2	T => 14 RESPONSE-HTC
		3	T => 14 RESPONSE-HTC
ISO-ESD03-HDPC - Movement of HTC or HSTC Containing HDPC on Cask Transfer Trailer To/From Aging Facility		2008/01/28	Sheet 13

NOTE: ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; T= transportation cask; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-14. IET for ISO-ESD-03 – HDPC– Movement of HTC or HSTC Containing HDPC on Cask Transfer Trailer To/From Aging Facility



NOTE: DE = direct exposure; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-15. System-Response Event Tree for ISO-ESD-03 –RESPONSE-HTC – HTC/HSTC System Response



HTC, HSTC or HAM containing HDPC	Identify initiating events		
HDPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Impact during insertion or retrieval	2	T => 16 RESPONSE-HAM
	Impact involving auxiliary equip.	3	T => 16 RESPONSE-HAM

ISO-ESD04-HDPC - Canister Insertion or Retrieval Operations at a HAM

2008/01/28 Sheet 15

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; XFER = transfer.

Source: Original

Figure A5-16. IET for ISO-ESD-04 – HDPC– Canister Insertion or Retrieval Operations at a HAM

Identify initiating events	Canister containment remains intact	Cask or HAM shielding remains intact	Moderator prevented from entering canister	#	END-STATE-NAMES
INIT-EVENT	CANISTER	SHIELDING	MODERATOR		
				1	OK
				2	DE-SHIELD-DEGRADE
				3	RR-UNFILTERED
				4	RR-ITC-UNFILTERED
RESPONSE-HAM - HAM System Response				2008/01/28	Sheet 16

NOTE: DE = direct exposure; ESD = event sequence diagram; HAM = horizontal aging module; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-17. System-Response Event Tree for ISO-ESD-04 – RESPONSE-HAM – HAM System Response

Containers containing DAW	Impact to single container at LLWF	Containment boundary of LLW container remains intact		END-STATE-NAMES
LLWDAW	INIT-EVENT	LLW-CONTAINER	#	
			1	OK
			2	OK
			3	RR-UNFILTERED
ISO-ESD05-LLWDAW - Single Container DAW LLW Operations in the LLWF			2008/01/28	Sheet 17

NOTE: DAW = dry active LLW; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RR = radionuclide release.

Source: Original

Figure A5-18. Event Tree for ISO-ESD-05-LLWDAW –Single Container DAW LLW Operations in LLWF

Containers with Liquid LLW	Impact to single container at LLWF	Containment boundary of LLW container remains intact	#	END-STATE-NAMES
LLWLIQ	INIT-EVENT	LLW-CONTAINER		
			1	OK
			2	OK
			3	RR-UNFILTERED
ISO-ESD05-LLWLIQ - Single Container Liquid LLW Operations in the LLWF			2008/01/28	Sheet 18

NOTE: ESD = event sequence diagram; INIT-EVENT = initiating event; IET = initiator event tree; ISO = Intra-Site Operations; LIQ = Liquid LLW; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RR = radionuclide release.

Source: Original

Figure A5-19. Event Tree for ISO-ESD-05-LLWLIQ –Single Container Liquid LLW Operations in the LLWF

Containers with Wet-Solid (non-resin) LLW	Impact to single container at LLWF	Containment boundary of LLW container remains intact		END-STATE-NAMES
LLWWETNR	INIT-EVENT	LLW-CONTAINER	#	
			1	OK
			2	OK
			3	RR-UNFILTERED
ISO-ESD05-LLWWETNR - Single Container Wet-Solid (Non-Resin) LLW Operations in the LLWF			2008/01/28	Sheet 19

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RR = radionuclide release; WETnr = wet-solid LLW (non-resin).

Source: Original

Figure A5-20. Event Tree for ISO-ESD-05-LLWWETnr –Single Container Wet-Solid (Non-Resin) LLW Operations in LLWF

Containers containing LLW	Non-fire event involving all LLW containers	Containment boundaries of all LLW containers remain intact	#	END-STATE-NAMES
LLW	INIT-EVENT	LLW-CONTAINERS-ALL		
			1	OK
			2	OK
			3	RR-UNFILTERED

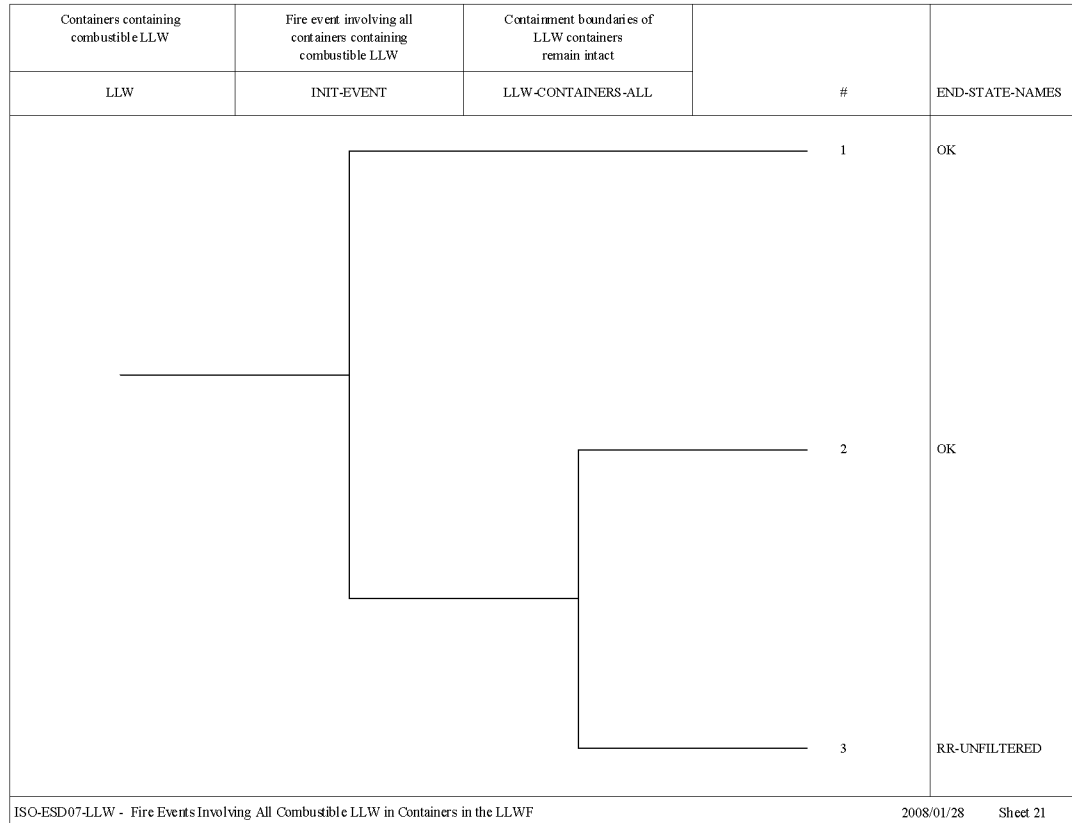
ISO-ESD06-LLW - Non-Fire Events Involving all LLW Containers in the LLWF

2008/01/28 Sheet 20

NOTE: ESD = event sequence diagram; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RR = radionuclide release.

Source: Original

Figure A5-21. Event Tree for ISO-ESD-06-LLW –Non-Fire Events Involving all LLW Containers in the LLWF



2008/01/28

NOTE: ESD = event sequence diagram; ISO = Intra-Site Operations; INIT-EVENT = initiating event; LLW = low-level radioactive waste; RR = radionuclide release.

Source: Original

Figure A5-22. Event Tree for ISO-ESD-07-LLW – Fire Events Involving all Combustible LLW in Containers in the LLWF

Containers with dry active LLW	Identify initiating events			
LLWDAW	INIT-EVENT		#	XFER-TO-RESP-TREE
			1	OK
	Equip. failure/collision affecting wet-solid LLW		2	T => 23
	Impact affecting dry active or liquid LLW		3	T => 23
	Loss of containment boundary		4	T => 23
	Equip. failure affecting liquid LLW or non-resin wet-solid LLW		5	T => 23

ISO-ESD08-LLWDAW - Transfer of DAW LLW between Generating Facility and LLWF or GROA Boundary 2008/01/28 Sheet 22

NOTE: DAW = dry active low-level radioactive waste; ESD = event sequence diagram; IET = initiator event tree; GROA = geologic repository operations area; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RESP = response; T= transfer; XFER = transfer.

Source: Original

Figure A5-23. IET for ISO-ESD-08-LLWDAW – Transfer of DAW LLW between Generating Facility and LLWF or GROA Boundary



	Containment boundary of LLW container remains intact		
INIT-EVENT	CONTAIN	#	END-STATE-NAMES
		1	OK
		2	RR-UNFILTERED
RESPONSE-LLW - LLW Transfer System Response		2008/01/28 Sheet 23	

NOTE: ESD = event sequence diagram; ISO = Intra-Site Operations; INIT-EVENT = initiating event; LLW = low-level radioactive waste; RR = radionuclide release.

Source: Original

Figure A5-24. System-Response Event Tree for ISO-ESD-08 – RESPONSE-LLW – LLW Transfers-System Response

Containers with Liquid LLW	Identify initiating events			
LLWLIQ	INIT-EVENT		#	XFER-TO-RESP-TREE
			1	OK
	Equip. failure/collision affecting wet-solid LLW		2	T => 23
	Impact affecting dry active or liquid LLW		3	T => 23
	Loss of containment boundary		4	T => 23
	Equip. failure affecting liquid LLW or non-resin wet-solid LLW		5	T => 23
ISO-ESD08-LLWLIQ - Transfer of Liquid LLW between Generating Facility and LLWF or GROA Boundary				2008/01/28 Sheet 24

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; GROA = geologic repository operations area; ISO = Intra-Site Operations; LIQ = Liquid LLW; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; RESP = response; T= transfer; XFER = transfer.

Source: Original

Figure A5-25. IET for ISO-ESD-08-LLWLIQ – Transfer of Liquid LLW between Generating Facility and LLWF or GROA Boundary

Containers with Wet-Solid (Non-Resin) LLW	Identify initiating events			
LLWWETNR	INIT-EVENT		#	XFER-TO-RESP-TREE
			1	OK
	Equip. failure/collision affecting wet-solid LLW		2	T => 23 RESPONSE-LLW
	Impact affecting dry active or liquid LLW		3	T => 23 RESPONSE-LLW
	Loss of containment boundary		4	T => 23 RESPONSE-LLW
	Equip. failure affecting liquid LLW or non-resin wet-solid LLW		5	T => 23 RESPONSE-LLW
ISO-ESD08-LLWWETNR - Transfer of Wet-Solid (Non-Resin) LLW between Generating Facility and LLWF or GROA Boundary				
			2008/01/28	Sheet 25

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; RESP = response; T= transfer; XFER = transfer.

Source: Original

Figure A5-26. IET for ISO-ESD-08-LLWWETnr – Transfer of Wet-Solid (Non-Resin) LLW between Generating Facility and LLWF or GROA Boundary

Containers with Wet-Solid (Resin) LLW	Identify initiating events			
LLWWETR	INIT-EVENT		#	XFER-TO-RESP-TREE
			1	OK
	Equip. failure/collision affecting wet-solid LLW		2	T => 23 RESPONSE-LLW
	Impact affecting dry active or liquid LLW		3	T => 23 RESPONSE-LLW
	Loss of containment boundary		4	T => 23 RESPONSE-LLW
	Equip. failure affecting liquid LLW or non-resin wet-solid LLW		5	T => 23 RESPONSE-LLW

ISO-ESD08-LLWWETR - Transfer of Wet-Solid (Resin) LLW between Generating Facility and LLWF or GROA Boundary

2008/01/28 Sheet 26

NOTE: ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; LLW = low-level radioactive waste; RESP = response; T= transfer; XFER = transfer.

Source: Original

Figure A5-27. IET for ISO-ESD-08-LLWWETR – Transfer of Wet-Solid (Resin) LLW between Generating Facility and LLWF or GROA Boundary

Transportation cask or aging overpack containing DPC	Identify initiating events		
DPC	INIT-EVENT	#	XFER-TO-RESP-TREE
	Fire affects TC during staging	1	OK
	Fire affects TC during movement	2	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	3	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	4	T => 28 RESPONSE-FIRE
		5	T => 28 RESPONSE-FIRE

ISO-ESD09-DPC - Fire Affecting DPC during Transportation or Aging Activities

2008/01/28 Sheet 27

NOTE: AO = aging overpack; DPC = dual-purpose canister; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RESP = response; ST = site transportation; T= transfer; TC = transportation cask; TFER = transfer.

Source: Original

Figure A5-28. IET for ISO-ESD-09 – DPC – Fire Affecting DPC during Transportation or Aging Activities

	Canister containment remains intact	Shielding remains intact	Moderator prevented from entering canister		
INIT-EVENT	CANISTER	SHIELDING	MODERATOR	#	END-STATE-NAMES
				1	OK
				2	DE-SHIELD-DEGRADE
				3	RR-UNFILTERED
				4	RR-UNFILTERED-ITC
RESPONSE-FIRE - Transportation and Aging Activities Fire System Response					2008/01/28 Sheet 28

NOTE: ESD = event sequence diagram; INIT-EVENT = initiating event; ISO = Intra-Site Operations; ITC = important to criticality; RR = radionuclide release.

Source: Original

Figure A5-29. System-Response Event Tree for ISO-ESD-09 – RESPONSE-FIRE – Transportation and Aging Activities Fire System Response

Transportation cask containing DOE standardized canister	Identify initiating events		
DSTD	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-DSTD - Fire Affecting DOE Standardized Canister (DSTD) during Transportation Activities 2008/01/28 Sheet 29

NOTE: AO = aging overpack; DSTD = Department of Energy standardized canister; ESD = event sequence diagram; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; RESP = response; ST = site transportation; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-30. IET for ISO-ESD-09 – DSTD – Fire Affecting DOE Standardized Canister during Transportation Activities

HTC, HSTC or HAM containing HDPC	Identify initiating events		
HDPC	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-HDPC - Fire Affecting HDPC during Transportation or Aging Activities 2008/01/28 Sheet 30

NOTE: AO = aging overpack; ESD = event sequence diagram; HDPC = horizontal dual-purpose canister; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-31. IET for ISO-ESD-09 – HDPC – Fire Affecting HDPC during Transportation or Aging Activities



Transportation cask containing HLW canister(s)	Identify initiating events		
HLW	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-HLW - Fire Affecting HLW Canister(s) during Transportation Activities

2008/01/28 Sheet 31

NOTE: AO = aging overpack; ESD = event sequence diagram; IET = initiator event tree; ISO = Intra-Site Operations; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; INIT-EVENT = initiating event; RESP = response; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-32. IET for ISO-ESD-09 – HLW – Fire Affecting HLW Canister(s) during Transportation Activities

Transportation cask containing DOE MCO	Identify initiating events		
MCO	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-MCO - Fire Affecting DOE MCO during Transportation Activities

2008/01/28 Sheet 32

NOTE: AO = aging overpack; ESD = event sequence diagram; IET = initiator event tree; ISO = Intra-Site Operations; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; INIT-EVENT = initiating event; MCO = multicaster overpack; RESP = response; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-33. IET for ISO-ESD-09 – MCO – Fire Affecting DOE MCO during Transportation Activities

Transportation cask containing naval canister	Identify initiating events		
NAV	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-NAV - Fire Affecting Naval Canister during Transportation Activities

2008/01/28 Sheet 33

NOTE: AO = aging overpack; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT = initiating event; ISO = Intra-Site Operations; NAV = naval; RESP = response; T = transfer; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-34. IET for ISO-ESD-09 – NAV – Fire Affecting Naval Canister during Transportation Activities

Transportation cask or aging overpack containing TAD canister	Identify initiating events		
TAD	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
		2	T => 28 RESPONSE-FIRE
		3	T => 28 RESPONSE-FIRE
		4	T => 28 RESPONSE-FIRE
		5	T => 28 RESPONSE-FIRE
ISO-ESD09-TAD - Fire Affecting TAD Canister during Transportation or Aging Activities		2008/01/28 Sheet 34	

NOTE: AO = aging overpack; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; T= transfer; TAD = transportation, aging, and disposal; TC = transportation cask; XFER = transfer.

Source: Original

Figure A5-35. IET for ISO-ESD-09 – TAD – Fire Affecting TAD Canister during Transportation or Aging Activities

Transportation cask containing UCSNF	Identify initiating events		
UCSNF	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	Fire affects TC during staging	2	T => 28 RESPONSE-FIRE
	Fire affects TC during movement	3	T => 28 RESPONSE-FIRE
	Fire affects AO, HTC, or HSTC during movement	4	T => 28 RESPONSE-FIRE
	Fire at Aging Facility	5	T => 28 RESPONSE-FIRE

ISO-ESD09-UCSNF - Fire Affecting UCSNF in a Transportation Cask during Transportation Activities

2008/01/28 Sheet 35

NOTE: AO = aging overpack; ESD = event sequence diagram; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; IET = initiator event tree; INIT-EVENT = initiating event; ISO = Intra-Site Operations; RESP = response; T= transfer; TC = transportation cask; UCSNF = uncanistered spent nuclear fuel; XFER = transfer.

Source: Original

Figure A5-36. IET for ISO-ESD-09 – UCSNF – Fire Affecting UCSNF in a Transportation Cask during Transportation Activities

**ATTACHMENT B**  
**SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES**

## CONTENTS

	<b>Page</b>
B1 SITE PRIME MOVER ANALYSIS – FAULT TREES.....	B1-8
B1.1 REFERENCES .....	B1-8
B1.2 SITE PRIME MOVER DESCRIPTION .....	B1-8
B1.3 SYSTEM DESCRIPTION.....	B1-9
B1.4 DEPENDENCIES AND INTERACTIONS ANALYSIS .....	B1-12
B1.5 SITE PRIME MOVER RELATED FAILURE SCENARIOS .....	B1-12
B2 SITE TRANSPORTER - FAULT TREE ANALYSIS.....	B2-1
B2.1 REFERENCES .....	B2-1
B2.2 SITE TRANSPORTER DESCRIPTION.....	B2-1
B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS .....	B2-9
B2.4 SITE TRANSPORTER FAILURE SCENARIOS .....	B2-9
B3 CASK TRACTOR AND CASK TRANSFER TRAILER FAULT TREE ANALYSIS.....	B3-1
B3.1 REFERENCES .....	B3-1
B3.2 CASK TRACTOR AND CASK TRANSFER TRAILER DESCRIPTION..	B3-1
B3.3 DEPENDENCE AND INTERACTIONS ANALYSIS.....	B3-2
B3.4 CASK TRACTOR AND CASK TRANSFER TRAILER FAILURE SCENARIOS .....	B3-3
B4 ADDITIONAL FAULT TREES.....	B4-1

**FIGURES**

	<b>Page</b>
B1.3-1. Site Prime Mover Simplified Schematic Intra-Site and In-Facility .....	B1-10
B1.5-1. Uncertainty Results of the INT-1-SPMRC-COLLISION Fault Tree .....	B1-17
B1.5-2. Cut Set Generation Results for the INT-1-SPMRC-COLLISION Fault Tree .....	B1-17
B1.5-3. INT-1-SPMRC-COLLISION Sheet 1 of 3 .....	B1-19
B1.5-4. INT-1-SPMRC-COLLISION Sheet 2 of 3 .....	B1-20
B1.5-5. INT-1-SPMRC-COLLISION Sheet 3 of 3 .....	B1-21
B1.5-6. Uncertainty Results of the SPMTT Collision Fault Tree .....	B1-25
B1.5-7. Cut Set Generation Results for the SPMTT Collision Fault Tree .....	B1-26
B1.5-8. INT-1-SPMTT-COLLISION Sheet 1 of 3 .....	B1-28
B1.5-9. INT-1-SPMTT-COLLISION Sheet 2 of 3 .....	B1-29
B1.5-10. INT-1-SPMTT-COLLISION Sheet 3 of 3 .....	B1-30
B2.2-1 Site Transporter .....	B2-3
B2.2-2. Simplified Block Diagram of the Site Transporter Subsystems .....	B2-4
B2.4-1. Uncertainty Results Site Transporter Collision .....	B2-12
B2.4-2. Cut Set Generation Results .....	B2-13
B2.4-3. INT-2-ST-COLLISION -Site Transporter Collision Sheet 1 of 3 .....	B2-15
B2.4-4. INT-2-ST-COLLISION Site Transporter Collision Sheet 2 of 3 .....	B2-16
B2.4-5. INT-2-ST-COLLISION Site Transporter Collision Sheet 3 of 3 .....	B2-17
B2.4-6. Uncertainty Results for Site Transporter Load Drop during Lift/Movement Fault Tree .....	B2-23
B2.4-7. Cut Set Generation Results for Site Transporter Load Drop during Lift/Movement Fault Tree .....	B2-23
B2.4-8. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 1 of 12 .....	B2-27
B2.4-9. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 2 of 12 .....	B2-28
B2.4-10. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 3 of 12 .....	B2-29
B2.4-11. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 4 of 12 .....	B2-30
B2.4-12. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 5 of 12 .....	B2-31



**FIGURES (Continued)**

	<b>Page</b>
B2.4-13. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 6 of 12.....	B2-32
B2.4-14. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 7 of 12.....	B2-33
B2.4-15. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 8 of 12.....	B2-34
B2.4-16. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 9 of 12.....	B2-35
B2.4-17. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 10 of 12.....	B2-36
B2.4-18. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 11 of 12.....	B2-37
B2.4-19. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 12 of 12.....	B2-38
B3.4-1. Uncertainty Results for the Cask Tractor and Cask Transfer Trailer Collision Fault Tree INT-HCTT-COLLISION.....	B3-6
B3.4-2. Cut Set Generation Results for Cask Tractor and Cask Transfer Trailer Collision Fault Tree INT-HCT-COLLISION.....	B3-7
B3.4-3. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION) Sheet 1 of 5.....	B3-10
B3.4-4. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION) Sheet 2 of 5.....	B3-11
B3.4-5. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION) Sheet 3 of 5.....	B3-12
B3.4-6. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION) Sheet 4 of 5.....	B3-13
B3.4-7. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION) Sheet 5 of 5.....	B3-14
B4-1. Fault Tree for INTRASITE-PMRC-COLLIDE.....	B4-4
B4-2. Fault Tree for INTRASITE-DERAIL.....	B4-5
B4-3. Fault Tree for INTRASITE-PMTT-COLLIDE.....	B4-6
B4-4. Fault Tree for INTRASITE-JIB-CRANE.....	B4-7
B4-5. Fault Tree for INTRASITE-ST-COLLIDE.....	B4-8
B4-6. Fault Tree for INTRASITE-HCTT-COLLISION.....	B4-9

**FIGURES (Continued)**

	<b>Page</b>
B4-7. Fault Tree for INTRASITE-HCTT-DROP .....	B4-10
B4-8. Fault Tree for INTRASITE-HAM-INSERT .....	B4-11
B4-9. Fault Tree for INTRASITE-HAM-AUX-EQUIPMENT .....	B4-12
B4-10. Fault Tree for INTRASITE-HEPA-TRANSFER .....	B4-13
B4-11. Fault Tree for INTRASITE-COLL-TRANSFER .....	B4-14

**TABLES**

	<b>Page</b>
B1.4-1	Dependencies and Interactions Analysis .....B1-12
B1.5-1.	Basic Event Probability for SPMRC Collision.....B1-15
B1.5-2.	Cut Sets for INT-1-SPMRC-COLLISION .....B1-18
B1.5-3.	Basic Event Probability for SPMTT Collision .....B1-23
B1.5-4.	Cut Sets for SPMTT Collision.....B1-26
B2.2-1.	Site Transporter Remote or Pendant Controls .....B2-6
B2.3-1.	Dependencies and Interactions Analysis .....B2-9
B2.4-1.	Basic Event Probability for INT-2-ST-COLLISION .....B2-11
B2.4-2.	Cut Sets for the Site Transporter Collision in Facility.....B2-14
B2.4-3.	Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree.....B2-20
B2.4-4.	Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree.....B2-24
B3.3-1.	Dependencies and Interactions Analysis .....B3-2
B3.4-1.	Basic Event Probabilities for Collision of the Cask Tractor and Cask Transfer Trailer, INT-HCTT-COLLISION.....B3-4
B3.4-2.	Cut Sets for Collision of Cask Tractor and Cask Transfer Trailer (INT-HCTT- COLLISION) .....B3-7
B4-1.	Top Level and Linking Fault Trees .....B4-1
B4-2.	Basic Events for Additional Fault Trees.....B4-2
B4-3.	Resulting Distribution Parameters Used in Quantification Spreadsheet .....B4-3

## ACRONYMS AND ABBREVIATIONS

### Acronyms

AC	alternating current
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
DPC	dual-purpose canister
DSTD	U.S. Department of Energy standardized canister
FRA	Federal Railroad Administration
HAM	horizontal aging module
HLW	high-level radioactive waste
HSTC	horizontal shielded transfer cask
IHF	Initial Handling Facility
MCO	multicanister overpack
RF	Receipt Facility
SNF	spent nuclear fuel
SPM	site prime mover
SPMRC	site prime mover railcar
SPMTT	site prime mover truck trailer
STC	shielded transfer cask
WHF	Wet Handling Facility

### Abbreviations

HP	horsepower
Hz	hertz
in	inch
kW	kilowatt
mi/hr	miles per hour
rpm	rotations per minute
V	volt

## **ATTACHMENT B**

### **SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES**

This attachment describes the fault trees developed for Intra-Site Operations. The fault trees are described in relation to each of the major systems or equipment involved in operations, with subsections providing a physical description and brief operational description of the system or equipment. In addition, the specific functions that the system performs to prevent or mitigate initiating events and the conditions required for that function to be successful are also described, together with the system dependencies and interactions. Fault trees and basic events are identified as well.

#### **B1 SITE PRIME MOVER ANALYSIS – FAULT TREES**

##### **B1.1 REFERENCES**

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

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

##### **Design Inputs**

- B1.1.1 \*AAR S-2043. 2003. *Performance Specification for Trains Used to Carry High-Level Radioactive Material*. Washington, D.C.: Association of American Railroads. TIC: 257585.

##### **Design Constraints**

- B1.1.2 49 CFR 571. Transportation: Federal Motor Vehicle Safety Standards. Internet accessible.
- B1.1.3 Motor Vehicle Safety. 49 U.S.C. 301. Internet accessible.

#### **B1.2 SITE PRIME MOVER DESCRIPTION**

##### **B1.2.1 Overview**

The site prime mover (SPM) is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs during Intra-Site Operations and within the Canister Receipt and Closure Facility (CRCF), the Wet Handling Facility (WHF), the Initial Handling Facility (IHF) and the Receipt Facility (RF).

Movement of the SPM railcar (SPMRC) or SPM truck trailer (SPMTT) within the facilities is limited to the Entry Vestibule and the Cask Preparation Area.

Transportation casks arriving at the facilities can contain:

- Dual-purpose canisters (DPCs)
- Horizontal DPCs
- Multicanister overpacks (MCOs)
- U.S. Department of Energy standardized canisters (DSTDs)
- Transportation, aging, and disposal canisters
- Navy spent nuclear fuel (SNF)
- High-level radioactive waste (HLW)
- Uncanistered commercial SNF canisters.

### **B1.3 SYSTEM DESCRIPTION**

#### **B1.3.1 Site Prime Mover**

The SPM is a commercially available vehicle that has the capability of moving both railcars and truck trailers loaded with transportation casks. Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations.

The driving and braking power comes directly from the road tires as they are in contact with the rails. Weight sharing between the flanged rail and regular road wheels is automatically varied to achieve the required power transmission needs. More weight can be distributed on the rail wheels when moving, or more on the road wheels when braking, accelerating, and negotiating inclines. The SPM has speed limiters that set the maximum speed of the vehicle to less than 9.0 mi/hr.

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

The SPM is equipped with both an automatic wagon coupling system for railcars and a fifth wheel coupling device for truck trailers. In addition, the SPM is equipped with the following: high-performance compressors, a priority filling system, an electronic regulating valve with filling speed adjustments, and a 100-gallon diesel fuel tank.

##### **B1.3.1.1 Railcars**

Railcars used for movement of transportation casks shall be designed in accordance with Federal Railroad Administration (FRA) requirements under authority delegated by the Secretary of Transportation. The FRA administers a safety program that oversees the movement of nuclear shipments throughout the national rail transportation system. Performance standards are addressed in the Association of American Railroads *Performance Specification for Trains Used to Carry High-Level Radioactive Material, Standard S-2043* (Ref. B1.1.1).

### B1.3.1.2 Truck Trailers

The U.S. Department of Transportation has the primary responsibility for regulating the safe transport of radioactive materials in the United States. It sets the standards for packaging, transporting, and handling radioactive materials, including labeling, shipping papers, loading, and unloading requirements.

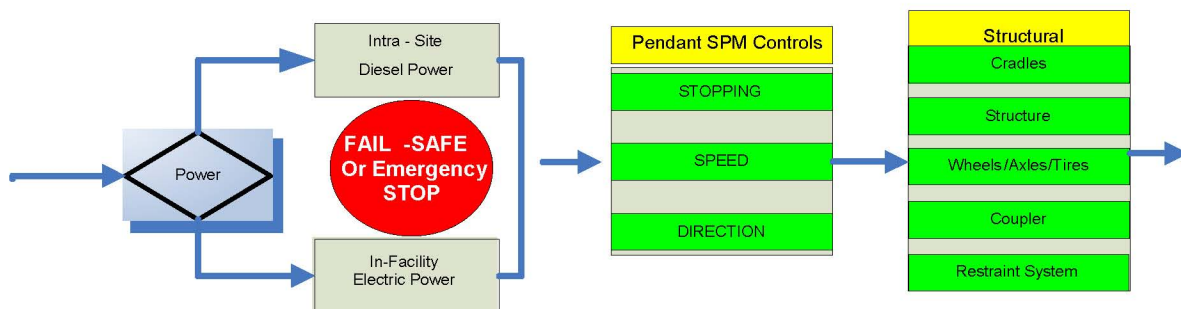
Trailers used for the movement of transportation casks are designed in accordance with the National Highway Traffic Safety Administration requirements as authorized by Title 49, U.S.C.301, Standards and Compliance, Section 30111: Standards (Ref. B1.1.3). The requirements are delineated in 49 CFR 571 (Ref. B1.1.2).

### B1.3.1.3 Subsystems

The SPMRC and SPMTT systems are composed of four subsystems:

1. Power plant—A diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all Intra-Site Operations. For operations conducted inside facilities, the SPM is connected to facility 480V, 3-phase, and 60-Hertz power.
2. Vehicle controls—During Intra-Site Operations, the operator controls the SPM at the operator’s console inside the SPM. For all operations inside of facilities, the operator controls the SPM with either a remote (wireless) controller or through a pendant connected to the vehicle.
3. Structural—Structural subsystems include restraints for securing the transportation casks to the railcar/truck trailer, automatic coupler hardware, cradles for supporting the transportation cask, and wheels/tires and axles.
4. Brakes—For the railcar, the brakes comply with FRA requirements; for the truck trailer the braking system complies with 49 CFR 571 (Ref. B1.1.2).

A simplified schematic of the functional components on the SPMRC/SPMTT is shown in Figure B1.3-1.



Source: Original

Figure B1.3-1. Site Prime Mover Simplified Schematic Intra-Site and In-Facility

## **B1.3.2 Operations**

### **B1.3.2.1 Normal Operations**

Intra-Site SPM operations begin once the railcar/truck trailer carrying a transportation cask arrives onsite at the receipt area. Receipt activities include the placement of temporary protective shielding around the railcar/truck trailer, inspection of the transportation cask, and connection of the railcar/truck trailer to the SPM. Once all receipt activities are completed the SPM with the railcar/truck trailer proceeds to the appropriate facility (CRCE, IHF, RF, or WHF).

In-facility SPM operations begin when the SPM has positioned the railcar/truck trailer outside the entry vestibule at the facility such that the railcar/truck trailer is pushed into the facility. The SPM diesel engine is shut down and the outer and inner vestibule doors are opened. Facility power is connected to the SPM for all operations inside the facility.<sup>1</sup>

The operator connects the pendant controller or uses a remote (wireless) controller to move the railcar/truck trailer into the vestibule. Once inside, the outer vestibule door is closed. The Cask Preparation Area Vestibule door is then opened and the SPM moves the railcar/truck trailer into position in the Cask Preparation Area. Once in position, the SPM is disconnected from the railcar/truck trailer and returns to the inner vestibule area. The Cask Preparation Area Vestibule door is then closed. The inner and outer vestibule doors can then be opened and the SPM exits the facility. Once outside, the SPM is shut down and the facility power is removed and the inner and outer vestibule doors are closed.

### **B1.3.2.2 Site Prime Mover Off-Normal Operations**

In the event of loss of power, the SPM is designed to stop, retain control of the railcar/truck trailer, and enter a locked mode. Upon the restoration of power the SPM stays in the locked mode until operator action is taken to return to normal operations.

### **B1.3.2.3 Site Prime Mover Testing and Maintenance**

Testing and maintenance of the SPM is done on a periodic basis and does not affect the normal operations of the SPM. Testing and/or maintenance are not performed on a SPM when it is coupled with a railcar/truck trailer. A SPM that has malfunctioned or has a warning light lit on the SPM is deemed unserviceable and turned in for maintenance. Unserviceable vehicles are not be used.

If an unserviceable state is identified during movement, the SPM is immediately placed in a safe state (as quickly as possible) and recovery actions for the SPM are invoked.

---

<sup>1</sup> The SPM is never operated inside a facility using the diesel engine.



## B1.4 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B1.4-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B1.4-1 Dependencies and Interactions Analysis

Systems, Structures, & Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Structural	Material failure Coupler Wheels/tires/axle	—	—	—	—
Brakes	Material failure	—	—	Failure to engage (set)	—
Power plant	Governor fails Safe state on	—	—	Failure to stop	—
Remote control	Spurious commands	—	—	Improper command	Collide with end stops

Source: Original

## B1.5 SITE PRIME MOVER RELATED FAILURE SCENARIOS

There are two basic SPM fault trees developed for Intra-Site Operations. The top events for these fault trees are:

- SPMRC collision while entering facility (INT-1-SPMRC-COLLISION)
  - SPMRC with DPC collides with facility structures
  - SPMRC with a horizontal DPC collides with facility structures
  - SPMRC with MCO collides with facility structures
  - SPMRC with DSTD collides with facility structures
  - SPMRC with transportation, aging, and disposal canister collides with facility structures
  - SPMRC with Navy SNF collides with facility structures
  - SPMRC with HLW collides with facility structures

- SPMRC with uncanistered commercial SNF collides with facility structures.
- SPMTT collision while entering facility (INT-1-SPMTT-COLLISION)
  - SPMTT with MCO collides with facility structures
  - SPMTT with DSTD collides with facility structures
  - SPMTT with uncanistered commercial SNF collides with facility structures
  - SPMTT with HLW collides with facility structures.

### **B1.5.1 SPMRC Collision While Entering Facility (INT-1-SPMRC-COLLISION)**

#### **B1.5.1.1 Description**

Collision can occur as a result of human error or hardware failures. Hardware failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

#### **B1.5.1.2 Success Criteria**

The success criteria for preventing a collision include safety design features incorporated in the SPM for hardware failures, and the SPM operator maintains situational awareness and proper control of the movement of the SPM. To avoid collisions, the SPM must stop when commanded, be prevented from entering a runaway situation, or respond correctly to a SPM movement command.

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

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a governor on the diesel engine for outside facility movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

#### **B1.5.1.3 Design Features and Requirements**

##### **Requirements**

- Since the dominant contributor to a SPMRC collision in the facility is human error, no priority is given to either the remote or the pendant controllers.
- The SPM is operated on electrical power when inside the building.

- The SPM is disconnected from the railcar at the preparation area and moved out of the building before cask preparation activities begin.

### **Design Features**

- The SPM has two off-equipment control devices that have complete control over the SPMRC.
- Drive system contains both a governor and a transmission constraint which limits the maximum speed of the SPM to 9.0 mi/hr.
- There are no common-cause failures (CCFs) identified for the SPMRC.

### **System Configuration and Operating Conditions**

#### **Requirements**

- Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a “deadman switch.”
- On the loss of alternating current (AC) power derived from the facility (CRCF, RF, IHF, or WHF), the SPM immediately enters the lock mode state. The lock mode state is reversible without specific operator action.

#### **Design Features and Inputs**

Stopping the SPM is accomplished by pushing the “stop” button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source immediately responds by removing power from the propulsion system on the SPM.

#### **Testing and Maintenance**

##### **Requirements**

There shall be no maintenance or testing permitted on an SPM loaded with a transportation cask.

##### **Design Feature**

None

#### **B1.5.1.4 Fault Tree Model**

The fault tree model for “SPMRC Collision” while entering facility, “INT-1-SPMRC-COLLISION,” accounts for both human error and/or SPMRC hardware problems that could result in a collision. Figure B1.5-1 contains the uncertainty results obtained from running the fault tree for INT-1-SPMRC-COLLISION. Figure B1.5-2 provides the cut set generation results

for the INT-1-SPMRC-COLLISION fault tree. Figures B1.5-3 through B1.5-5 show the fault trees as modeled.

The fault trees for collisions involving the SPMRC and SPMTT are functionally identical. The fault tree for the SPMTT is discussed in the next section.

The fault tree for the top event is a collision of the SPMRC as shown in Figure B1.5-3 through B1.5-5. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop or exceeding a safe speed. Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

### B1.5.1.5 Basic Event Data

Table B1.5-1 contains a list of basic events used in the SPMRC collision fault tree. The mission time has been set at one hour which allows sufficient time to move the SPMRC from the receipt area to the individual facilities (CRCF, IHF, RF, or WHF).

Table B1.5-1. Basic Event Probability for SPMRC Collision

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-OPRCCOLLIDE1-HFI-NOD	Operator causes collision	1	3.000E-03	3.000E-03	0.000E+00	0.000E+00
ISO-OPRCINTCOL01-HFI-NOD	Operator initiates runaway	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
ISO-PWR-LOSS	Loss of site power	1	4.100E-06	4.100E-06	0.000E+00	0.000E+00
ISO-SPMRC--CT001-CT--FOD	On-board controller fails to respond	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	3	2.270E-05	0.000E+00	2.270E-05	1.000E+00
ISO-SPMRC-BRP000-BRP-FOD	SPMRC brake 000 failure on demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC – open circuit	3	9.130E-08	0.000E+00	9.130E-08	1.000E+00
ISO-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	3	1.880E-08	0.000E+00	1.880E-08	1.000E+00
ISO-SPMRC-CPL000-CPL-FOH	Railcar automatic coupler system fails	3	1.910E-06	0.000E+00	1.910E-06	1.000E+00
ISO-SPMRC-CT000--CT--	SPMRC primary	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00

Table B1.5-1. Basic Event Probability for SPMRC Collision (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
FOD	stop switch fails					
ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	3	1.160E-05	0.000E+00	1.160E-05	1.000E+00
ISO-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1	1.740E-03	1.740E-03	0.000E+00	0.000E+00
ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00
ISO-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	3	1.280E-04	0.000E+00	1.280E-04	1.000E+00
ISO-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	3	4.160E-06	0.000E+00	4.160E-06	1.000E+00

NOTE: <sup>a</sup> 1 is direct input probability; and 3 is lambda and mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability; SPMRC = site prime mover railcar.

Source: Original

### B1.5.1.5.1 Human Failure Events

Two human errors have been identified for this fault tree.

- Operator causes collision (INT-OPRCCOLLIDE1-HFI-NOD) is assigned a screening value of 3E-03.
- Operator initiates runaway (INT-OPRCINTCOL01-HFI-NOD) is assigned a screening value of 1.0.

### B1.5.1.5.2 Common-Cause Failures

There are no CCFs.

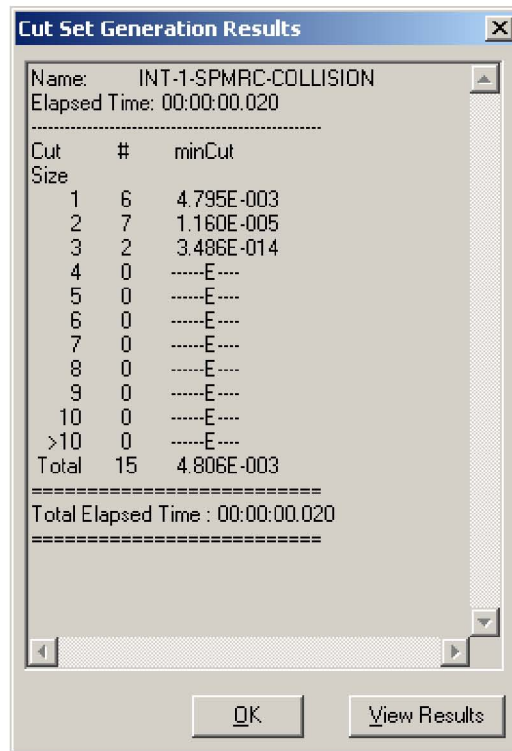
### B1.5.1.6 Uncertainty and Cut Set Generation Results

As stated, figure B1.5-1 contains the uncertainty results obtained from running the fault tree for INT-1-SPMRC-COLLISION. Figure B1.5-2 provides the cut set generation results for the INT-1-SPMRC-COLLISION fault tree.



Source: Original

Figure B1.5-1. Uncertainty Results of the INT-1-SPMRC-COLLISION Fault Tree



Source: Original

Figure B1.5-2. Cut Set Generation Results for the INT-1-SPMRC-COLLISION Fault Tree

**B1.5.1.7 Cutsets**

Table B1.5-2 contains the cut sets for INT-1-SPMRC-COLLISION.

Table B1.5-2. Cut Sets for INT-1-SPMRC-COLLISION

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
62.42	62.42	3.000E-03	ISO-OPRCCOLLIDE1-HFI-NOD	Operator causes collision	3.000E-03
98.62	36.20	1.740E-03	ISO-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1.740E-03
99.66	1.04	5.020E-05	ISO-SPMRC-BRP000-BRP-FOD	SPMRC brake 000 failure on demand	5.020E-05
99.90	0.24	1.160E-05	ISO-OPRCINTCOL01-HFI-NOD	Operator initiates runaway	1.000E+00
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E-05
99.98	0.08	4.000E-06	ISO-SPMRC--CT001-CT--FOD	On-board controller fails to respond	4.000E-06
100.00	0.08	4.000E-06	ISO-SPMRC-CT000--CT--FOD	SPMRC primary stop switch fails	4.000E-06
100.00	0.04	1.910E-06	ISO-SPMRC-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	1.910E-06
100.00	0.00	2.058E-10	ISO-PWR-LOSS	Loss of site power	4.100E-06
			ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E-05
100.00	0.00	4.583E-12	ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E-05
			ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	9.130E-08
100.00	0.00	9.438E-13	ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E-05
			ISO-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	1.880E-08
100.00	0.00	5.535E-14	ISO-PWR-LOSS	Loss of site power	4.100E-06
			ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	1.350E-08
100.00	0.00	3.370E-14	ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	2.270E-05
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E-05
			ISO-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	1.280E-04
100.00	0.00	1.233E-15	ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	9.130E-08
			ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	1.350E-08
100.00	0.00	1.095E-15	ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	2.270E-05
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E-05

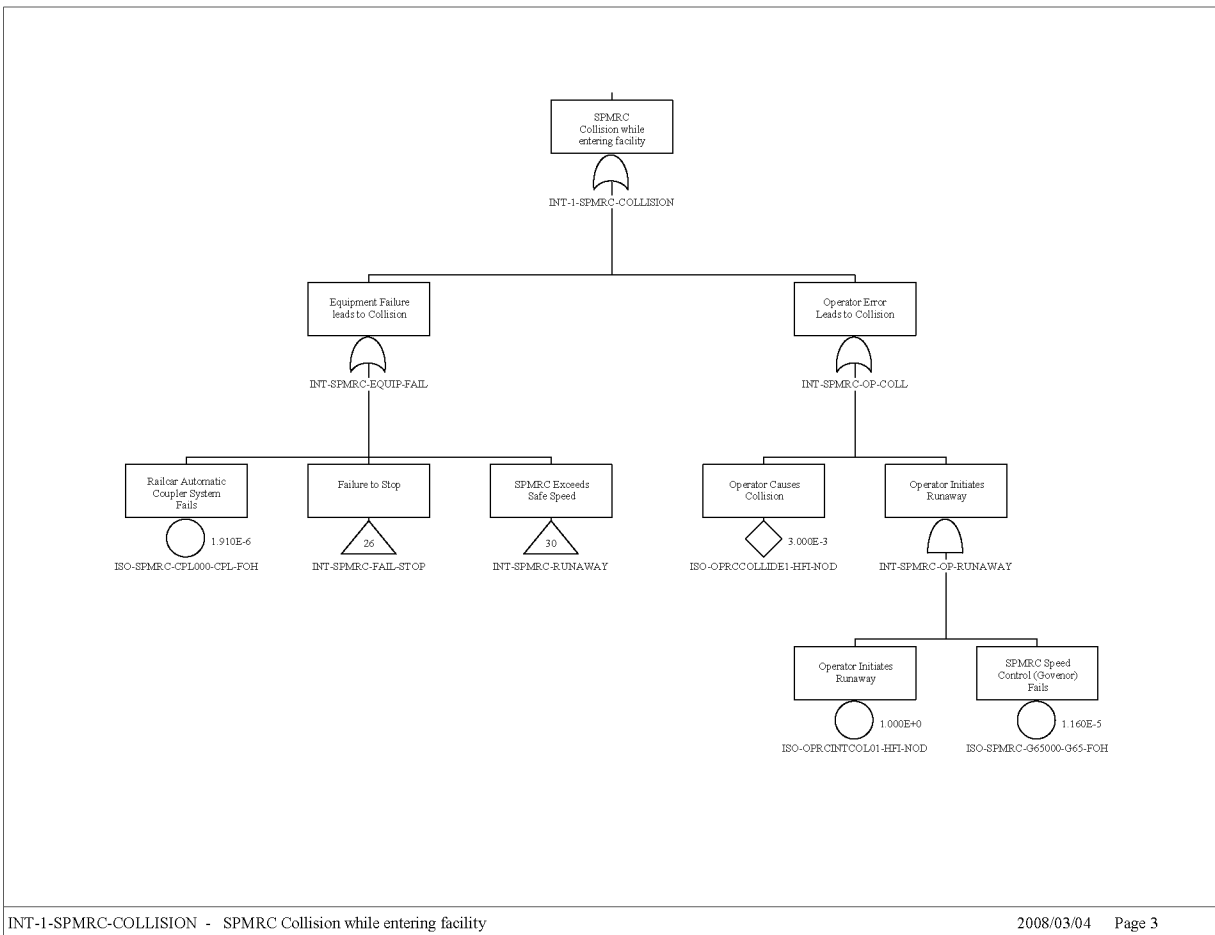
Table B1.5-2. Cut Sets for INT-1-SPMRC-COLLISION (Continued)

% Total	% Cut Set	Probability/Frequency	Basic Event	Description	Event Probability
			ISO-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	4.160E-06

NOTE: Prob. = probability; SPMRC = site prime mover railcar.

Source: Original

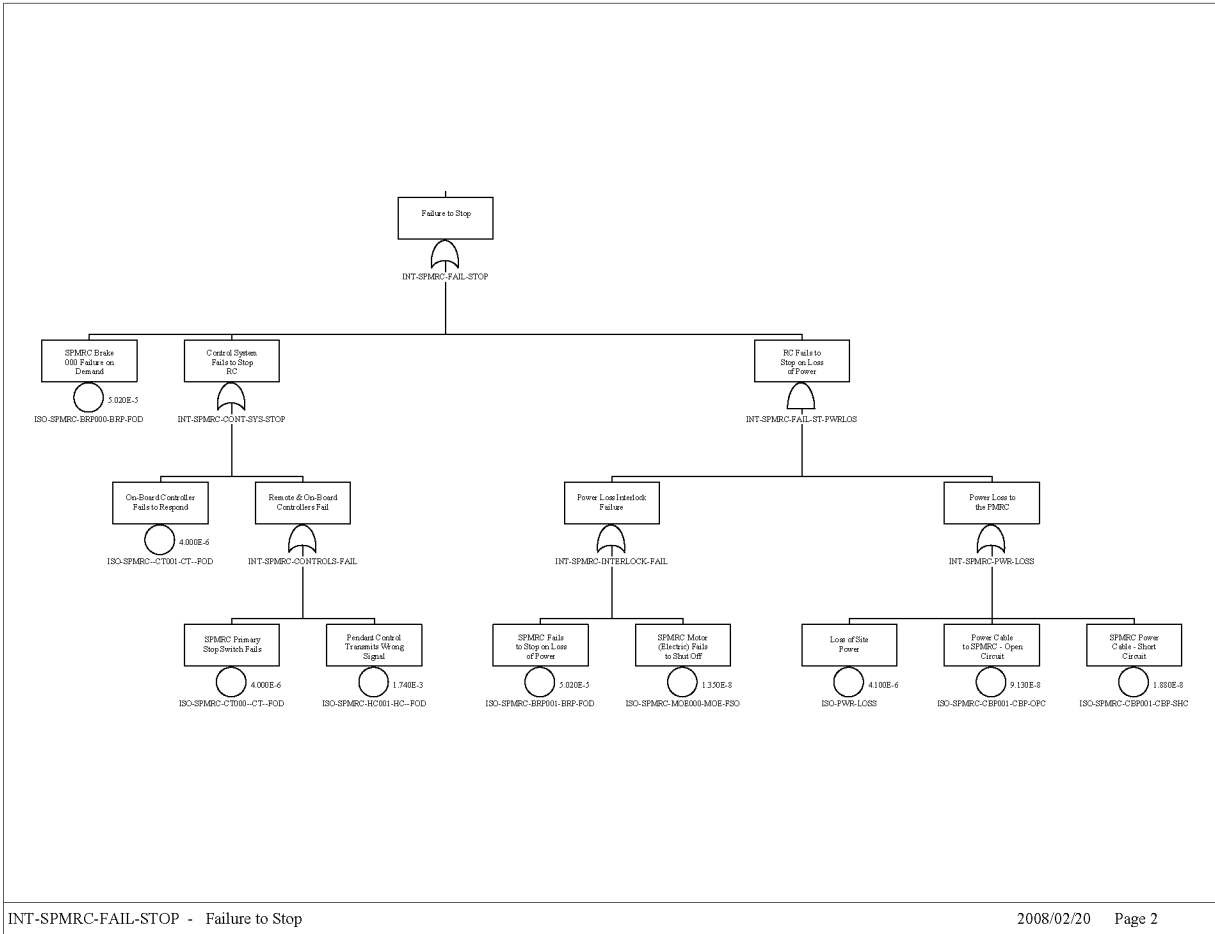
**B1.5.1.8 Fault Trees**



Source: Original

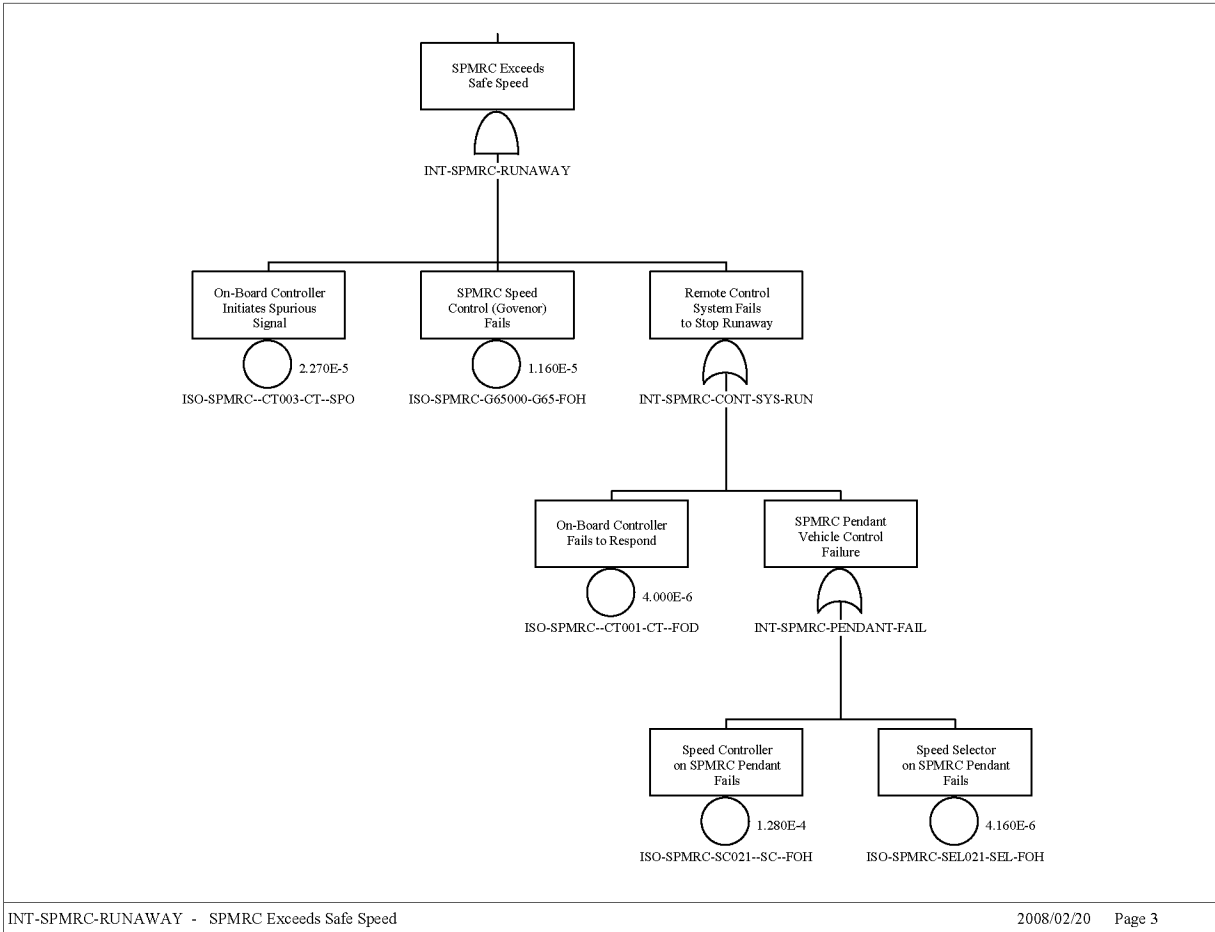
Figure B1.5-3. INT-1-SPMRC-COLLISION Sheet 1 of 3





Source: Original

Figure B1.5-4. INT-1-SPMRC-COLLISION Sheet 2 of 3



Source: Original

Figure B1.5-5. INT-1-SPMRC-COLLISION Sheet 3 of 3

## B1.5.2 SPMTT Collision Entering Facility (INT-1-SPMTT-COLLISION)

### B1.5.2.1 Description

Collision can occur as a result of human error or hardware failures. Hardware failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

The fault tree for collisions involving the SPMRC and SPMTT are functionally identical. The fault tree for the SPMRC was discussed in the previous section.

### B1.5.2.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the SPM for hardware failures, and the SPM operator maintains situational awareness and proper control of the movement of the SPM. To avoid collisions, the SPM must stop when commanded,

be prevented from entering a runaway situation, or respond correctly to a SPM movement command.

The SPM is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the SPM by either commanding a “stop” from the start/stop button or by releasing the palm switch which initiates an emergency stop. At anytime there is a loss of power detected, the SPM performs a controlled stop. Once stopped, the SPM stops all movement and enters into “lock mode” safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM. The SPM remains in this fail safe mode until power is returned and restarted by the operator.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a governor on the diesel engine for outside movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mi/hr. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

### **B1.5.2.3 Design Features and Requirements**

#### **Requirements**

- Since the dominant contributor to SPMTT collision in the facility is human error, no priority is given to either the remote or the pendant controllers.
- The SPM is operated on electrical power when inside the building.
- The SPM is disconnected from the railcar at the preparation area and moved out of the building before cask preparation activities begin.

#### **Design Features**

- The SPM has two off-equipment control devices that have complete control over the SPMTT.
- Drive system contains both a governor and a transmission constraint which limits the maximum speed of the SPM to 9.0 mi/hr.
- There are no CCFs identified for the SPMTT.

### **System Configuration and Operating Conditions**

#### **Requirements**

- Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a “deadman switch.”

- On the loss of AC power derived from the facility, the SPM immediately enters the lock mode state. The lock mode state is not be reversible without specific operator action.

### Design Features and Inputs

Stopping the SPM is accomplished by pushing the “stop” button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source, is to immediately respond by removing power from the propulsion system.

### Testing and Maintenance

#### Requirements

There is no maintenance or testing permitted on a SPM loaded with a transportation cask.

#### Design Feature

None.

#### B1.5.2.4 Fault Tree Model

The fault tree model for “SPM Collision” accounts for both human error and/or SPMTT hardware problems that could result in a collision.

The top event is a collision of the SPMTT and the fault trees are shown in Figure B1.5-8, B1.5-9, and B1.5-10. This collision may occur due to a human error coupled with the failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop or exceeding a safe speed. Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

#### B1.5.2.5 Basic Event Data

Table B1.5-3 contains a list of basic events used in the SPMTT collision fault trees. The mission time has been set at one hour which is conservative because it will not require more than one hour to disconnect the SPM from the railcar and remove it from the facility.

Table B1.5-3. Basic Event Probability for SPMTT Collision

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes collision of TT	1	3.000E-03	3.000E-03	0.000E+00	0.000E+00
ISO-OPTTINTCOL01-HFI-NOD	Operator initiates runaway	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
ISO-PWR-LOSS-2	Loss of power	1	4.100E-06	4.100E-06	0.000E+00	0.000E+00
ISO-SPMTT--CT001-CT-FOD	On-board controller fails to respond	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00

Table B1.5-3. Basic Event Probability for SPMTT Collision (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-SPMTT--CT001-CT-SPO	On-board controller spurious operation	3	2.270E-05	0.000E+00	2.270E-05	1.000E+00
ISO-SPMTT-BRK000-BRP-FOD	Pneumatic brakes on SPMTT fail on demand	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	1	5.020E-05	5.020E-05	0.000E+00	0.000E+00
ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	3	9.130E-08	0.000E+00	9.130E-08	1.000E+00
ISO-SPMTT-CBP003-CBP-SHC	Cables (electrical power) short circuit	3	1.880E-08	0.000E+00	1.880E-08	0.000E+00
ISO-SPMTT-CPL000-CPL-FOH	Truck trailer automatic coupler system fails	3	1.910E-06	0.000E+00	1.910E-06	1.000E+00
ISO-SPMTT-CT000--CT-FOD	Controller mechanical jamming	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
ISO-SPMTT-CT002--CT-FOH	Controller failure	3	6.880E-05	0.000E+00	6.880E-05	1.000E+00
ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	3	1.160E-05	0.000E+00	1.160E-05	1.000E+00
ISO-SPMTT-HC001-HC-FOD	Remote control transmits wrong signal	1	1.740E-03	1.740E-03	0.000E+00	0.000E+00
ISO-SPMTT-HC002--HC--SPO	Spurious signal from pendant controller	3	5.230E-07	0.000E+00	5.230E-07	1.000E+00
ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00
ISO-SPMTT-SC021--SC-FOH	Speed controller on SPMTT pendant fails	3	1.280E-04	0.000E+00	1.280E-04	1.000E+00
ISO-SPMTT-SEL021-SEL-FOH	Speed selector on SPMTT pendant fails	3	4.160E-06	0.000E+00	4.160E-06	1.000E+00
ISO-SPMTT-STU001-STU-FOH	SPMTT end stops fail	3	2.107E-04	0.000E+00	4.810E-08	4.380E+03

NOTE: <sup>a</sup> 1 is direct input probability; and 3 is lambda and mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability; SPMTT = site prime mover truck trailer; TT= truck trailer.

Source: Original

### B1.5.2.5.1 Human Failure Events

Two human errors have been identified for this fault tree.

1. Operator causes collision (060-OPTTCOLLIDE1-HFI-NOD) is assigned a screening value of  $5E-03$ .
2. Operator initiates runaway (060-OPTTINTCOL01-HFI-NOD) is assigned a screening value of 1.0.

**B1.5.2.5.2 Common-Cause Failures**

There are no CCFs.

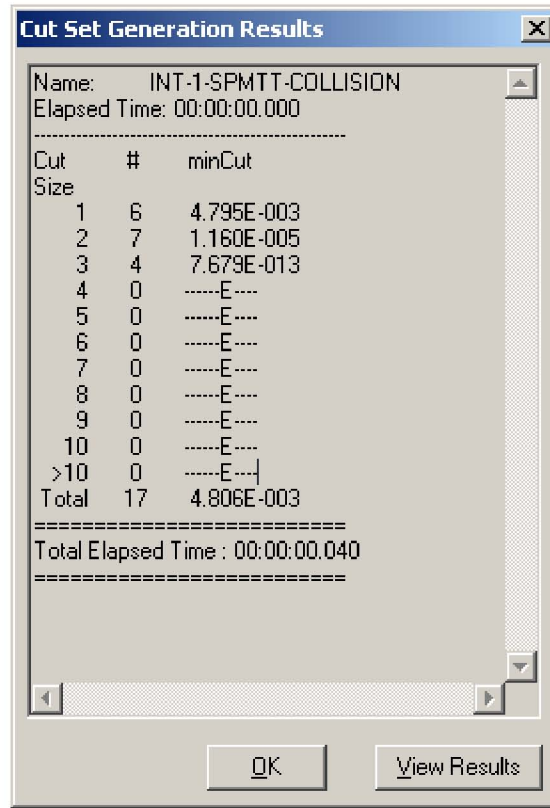
**B1.5.2.6 Uncertainty and Cut Set Generation Results**

Figure B1.5-6 contains the uncertainty results obtained from running the fault tree for SPMTT collision. Figure B1.5-7 provides the cut set generation results for the SPMTT collision fault tree.

Uncertainty Results			
Name	INT-1-SPMTT-COLLISION		
Random Seed	1234	Events	19
Sample Size	10000	Cut Sets	17
Point estimate	4.806E-003		
Mean Value	4.374E-003		
5th Percentile Value	5.420E-004		
Median Value	2.353E-003		
95th Percentile Value	1.296E-002		
Minimum Sample Value	1.056E-004		
Maximum Sample Value	9.548E-001		
Standard Deviation	1.453E-002		
Skewness	4.078E+001		
Kurtosis	2.306E+003		
Elapsed Time	00:00:00.940		
<input type="button" value="OK"/>			

Source: Original

Figure B1.5-6. Uncertainty Results of the SPMTT Collision Fault Tree



Source: Original

Figure B1.5-7. Cut Set Generation Results for the SPMTT Collision Fault Tree

### B1.5.2.7 Cut Sets

Table B1.5-4 contains the cut sets for SPMTT collision.

Table B1.5-4. Cut Sets for SPMTT Collision

% Total	% Cutset	Probability/Frequency	Basic Event	Description	Event Probability
62.42	62.42	3.000E-03	ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes collision of TT	3.000E-03
98.62	36.20	1.740E-03	ISO-SPMTT-HC001-HC--FOD	Remote control transmits wrong signal	1.740E-03
99.66	1.04	5.020E-05	ISO-SPMTT-BRK000-BRP-FOD	Pneumatic brakes on SPMTT fail on demand	5.020E-05
99.90	0.24	1.160E-05	ISO-OPTTINTCOL01-HFI-NOD	Operator initiates runaway	1.000E+00
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E-05
99.98	0.08	4.000E-06	ISO-SPMTT--CT001-CT--FOD	On-board controller fails to respond	4.000E-06
100.00	0.08	4.000E-06	ISO-SPMTT-CT000--CT--FOD	Controller mechanical jamming	4.000E-06

Table B1.5-4. Cut Sets for SPMTT Collision (Continued)

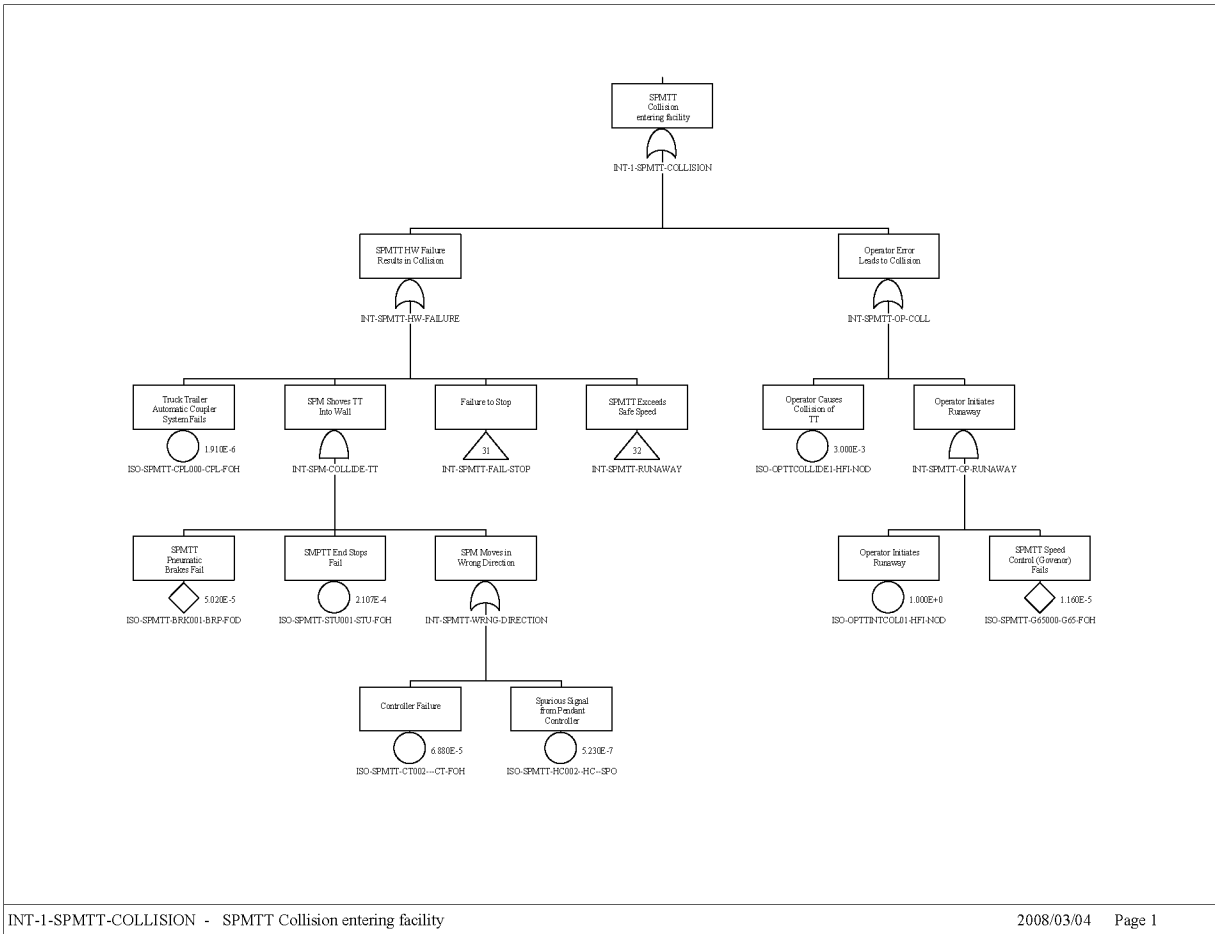
% Total	% Cutset	Probability/ Frequency	Basic Event	Description	Event Probability
100.00	0.04	1.910E-06	ISO-SPMTT-CPL000-CPL-FOH	Truck trailer automatic coupler system fails	1.910E-06
100.00	0.00	2.058E-10	ISO-PWR-LOSS-2	Loss of power	4.100E-06
			ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E-05
100.00	0.00	4.583E-12	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E-05
			ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	9.130E-08
100.00	0.00	9.438E-13	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E-05
			ISO-SPMTT-CBP003-CBP-SHC	Cables (electrical power) short circuit	1.880E-08
100.00	0.00	7.275E-13	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E-05
			ISO-SPMTT-CT002--CT-FOH	Controller failure	6.880E-05
			ISO-SPMTT-STU001-STU-FOH	SMPTT end stops fail	2.107E-04
100.00	0.00	5.535E-14	ISO-PWR-LOSS-2	Loss of power	4.100E-06
			ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	1.350E-08
100.00	0.00	3.370E-14	ISO-SPMTT--CT001-CT--SPO	On-board controller spurious operation	2.270E-05
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E-05
			ISO-SPMTT-SC021--SC--FOH	Speed controller on SPMTT pendant fails	1.280E-04
100.00	0.00	5.531E-15	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E-05
			ISO-SPMTT-HC002--HC--SPO	Spurious signal from pendant controller	5.230E-07
			ISO-SPMTT-STU001-STU-FOH	SMPTT end stops fail	2.107E-04
100.00	0.00	1.233E-15	ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	9.130E-08
			ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	1.350E-08
100.00	0.00	1.095E-15	ISO-SPMTT--CT001-CT--SPO	On-board controller spurious operation	2.270E-05
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E-05
			ISO-SPMTT-SEL021-SEL-FOH	Speed selector on SPMTT pendant fails	4.160E-06

NOTE: SPMTT = site prime mover tractor and trailer; TT = truck trailer.

Source: Original



**B1.5.2.8 Fault Trees**

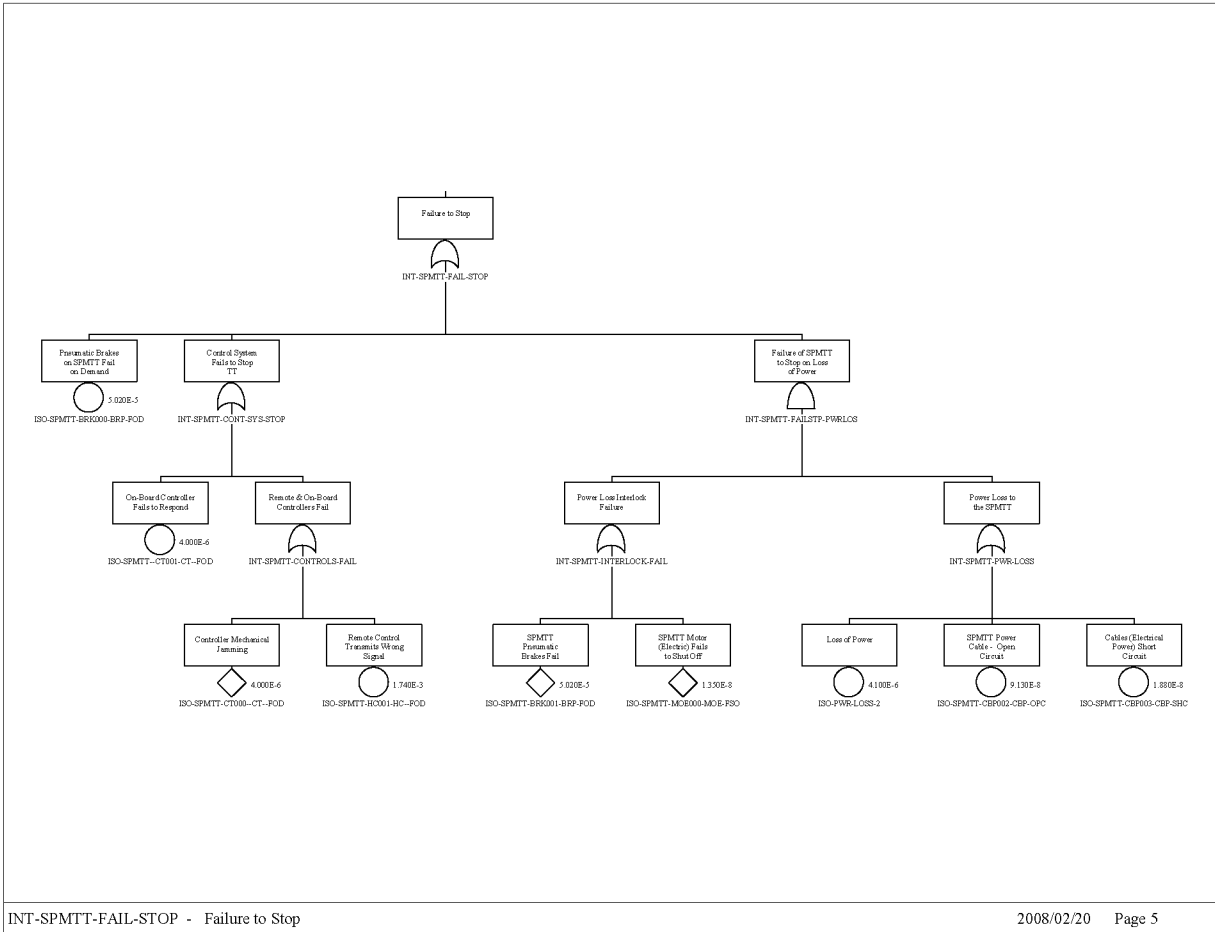


INT-1-SPMTT-COLLISION - SPMTT Collision entering facility

2008/03/04 Page 1

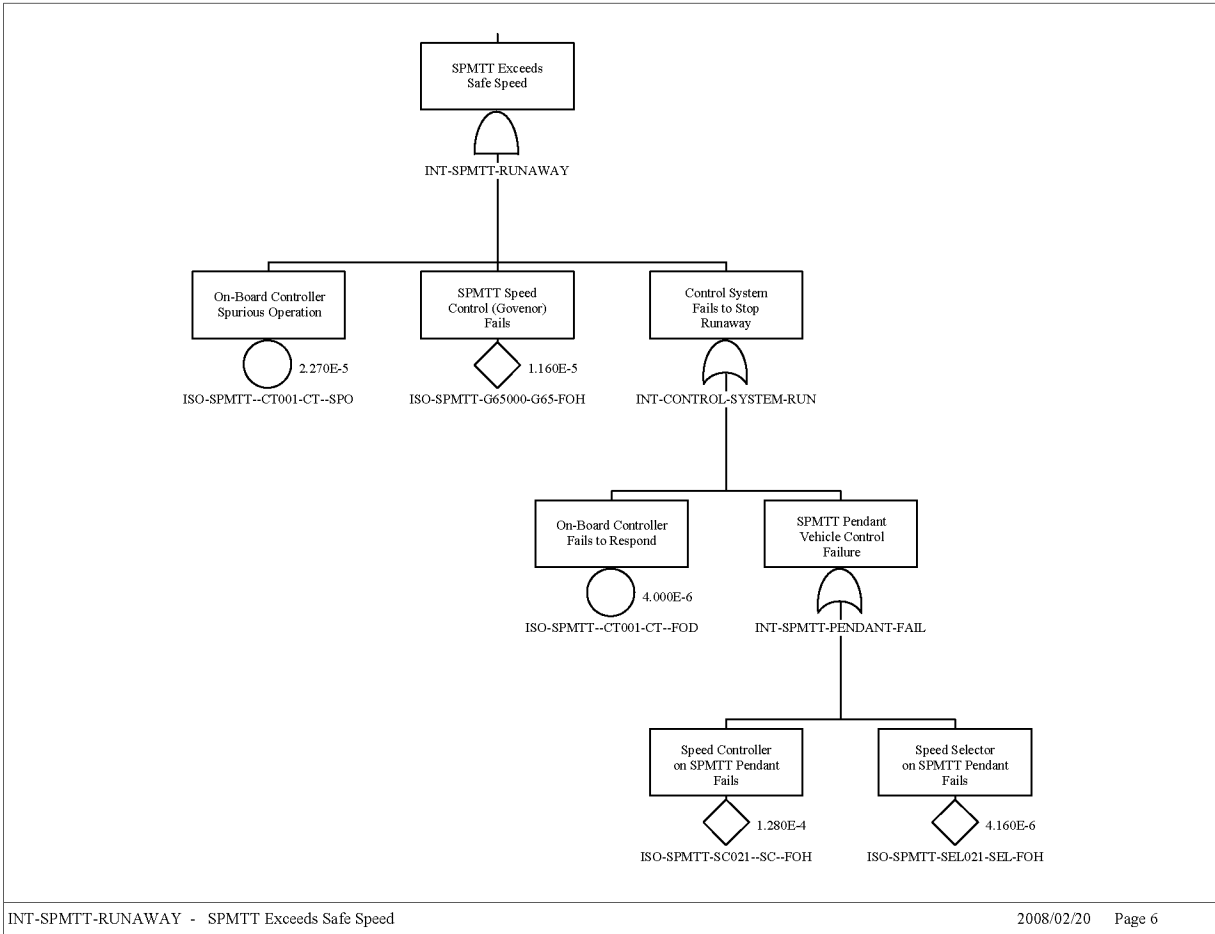
Source: Original

Figure B1.5-8. INT-1-SPMTT-COLLISION Sheet 1 of 3



Source: Original

Figure B1.5-9. INT-1-SPMTT-COLLISION Sheet 2 of 3



Source: Original

Figure B1.5-10. INT-1-SPMTT-COLLISION Sheet 3 of 3

## **B2 SITE TRANSPORTER - FAULT TREE ANALYSIS**

### **B2.1 REFERENCES**

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

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

#### **Design Inputs**

- B2.1.1 BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report – Site Transporter*. 170-30R-HAT0-00100-000-Rev 000. Las Vegas Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.
- B2.1.2 BSC 2007. *Exhibit D, Statement of Work for Mechanical Handling Equipment Design*. 000-3SW-MGR0-00100-000 REV 003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.200770904.0031.
- B2.1.3 Morris Material Handling 2007. *P&ID Site Transporter*. V0-CY05-QHC4-00459-00049-001 Rev. 004. Oak Creek, Wisconsin: Morris Material Handling. ACC:ENG.20071022.0012.

### **B2.2 SITE TRANSPORTER DESCRIPTION**

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a cylindrical concrete and steel ventilated aging overpack or, for the Wet Handling Facility, a cylindrical-steel shielded transfer cask (STC). The site transporter is used for Intra-Site Operations and within the CRCF, the WHF, and the RF<sup>2</sup>.

Movement of the the site transporter within a facility is limited to a facility's entrance vestibule, cask preparation area, and the cask unloading rooms.

#### **B2.2.1 Overview**

The interface between the site transporter and the aging overpack is via two parallel rectangular lift slots that pass through the containers near their lower ends. Orientation of the aging

---

<sup>2</sup> Variations in the use of the site transporter for Intra-Site Operations, WHF and the RF are addressed in their respective volumes.

overpack is such that the axis of the aging overpack is vertical with the lid at the top. Access to the top of the aging overpack is unobstructed..

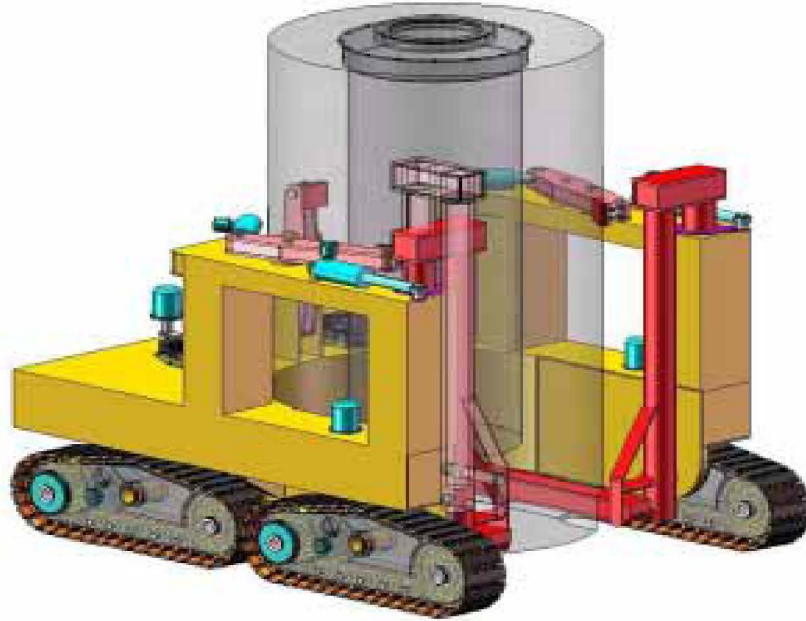
An integrated, diesel powered, electric generator provides electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable (or remote control) from the facility main electrical supply. See *Mechanical Handling Design Report – Site Transporter* (Ref. B2.1.1, Section 2.1).

The site transporter is a track driven vehicle with four synchronized tracks (two on each side of the site transporter). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not important to safety.

A rear fork assembly consists of a pair of arms that extend to the front of the site transporter. These forks move up and down for the purpose of raising, lowering, and supporting the aging overpack during movement. A pair of support arms is located at the front of the site transporter which is moved into position around the forks to provide support and assistance during the lifting and lowering of the aging overpack.

A passive restraint system provides stability during aging overpack movement. There are two mechanisms that control aging overpack movement on the pitch and roll axis. These restraints are not engaged until the aging overpack has been raised to the desired height. Once engaged, three pins are inserted, one in each restraint arm that keep the restraints in place should there be a failure of the electromechanical assembly used to position and secure the restraint device. Properly installed, they also serve as interlocks that prevent movement of a loaded site transporter.

Control of the site transporter is provided by a wireless remote control or a wired pendant. Although these devices only provide a subset of the controls and indicators that are available on the control console located on the site transporter, they contain all the necessary controls and indicators to perform and monitor the operation state of the site transporter during normal operations. The site transporter is shown in Figure B2.2-1.



Source: (Ref. B2.1.1)

Figure B2.2-1 Site Transporter

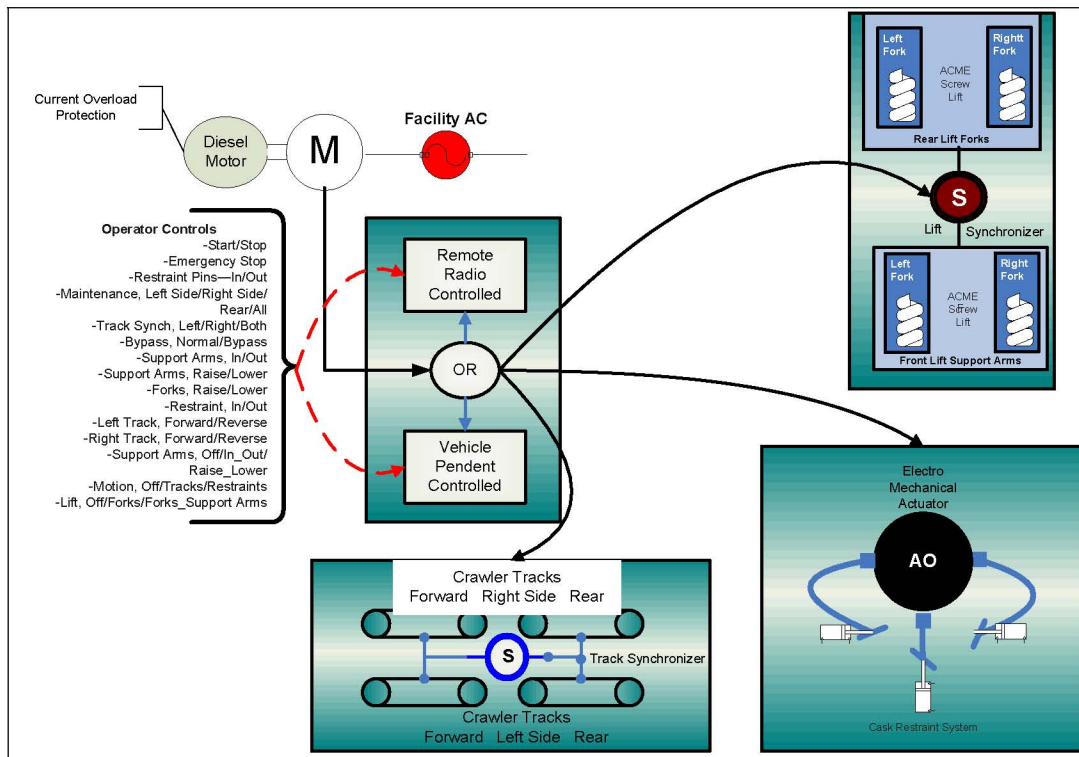
The site transporter system is composed of six subsystems (Ref. B2.1.1):

1. Crawler Tracks Subsystem—Four crawlers, two on each side of the site transporter, are used to move the vehicle. These crawlers use tracks with chamfered flat steel plates mounted to double-grouser shoes on a continuous chain.
2. Power Plant Subsystem—A diesel engine, generator, and diesel fuel tank are enclosed in the back of the site transporter. During Intra-Site Operations, the diesel engine drives the generator, which provides the required 480 V AC/3-phase/60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480 V AC/3-phase/60 Hz power is supplied to operate the vehicle.
3. Rear Lift Fork Subsystem—The site transporter contains a pair of arms that extend forward from the site transporter through slots in the aging overpack. The lift/lower drive system utilizes an ACME type nut that changes the elevation of the fork as the screw lift mechanism turns through the ACME nut. A lift synchronizer controls the lift/lower operation.
4. Lift Support Arms Subsystem—Two support arms with electromechanical actuators are located on the front of the site transporter. These support arms are rotated 90 degrees to provide support and stabilization for the lift forks during lifting/lowering/moving operations. ACME nuts are used on these arms and synchronized with the lift forks during lifting/lowering/moving.

5. Restraint Subsystem—A two axis restraint system is incorporated to stabilize the cask during site transporter movement. The restraints are emplaced/retracted with electromechanical actuators. These restraints, when positioned against the aging overpack are secured with a locking pin. The three locking pins serve as an interlock and must be properly installed before the site transporter can be moved.
6. Vehicle Controls Subsystem—There are two modes of control provided on the site transporter. Operators can control every operation on the site transporter with either a remote (wireless) controller or through a pendant connected to the site transporter.

Note: In addition to the six subsystems identified above, Ref. B2.1.1 also includes a description of the site transporter “car body.” Events associated with car body failure are screened from this analysis based on the results of the stress analysis contained in this reference.

A simplified block diagram of the functional subsystems on the site transporter is shown in Figure B2.2-2.



NOTE: AC = alternating current; AO = aging overpack; M = motor; S = synchronizer.

Source: Original

Figure B2.2-2. Simplified Block Diagram of the Site Transporter Subsystems

### B2.2.1.1 Site Transporter Crawler Tracks Subsystem Description

The site transporter moves by four tracks mounted on the crawler frames with two on each side of the vehicle to increase stability when traversing terrain that includes sudden changes in

elevation such as a drainage trough or curb. The site transporter is designed to negotiate roadways with a 5% grade and up to a 2% cross-slope (*Exhibit D, Statement of Work for Mechanical Handling Equipment Design*, (Ref. B2.1.2). Special pads are included on the tracks to reduce the wear and tear on concrete or roadways.

Each track is driven by its own electric motor (50 HP at 900 rpm) through its own gear reduction and final chain drive reduction. During forward operations, motors on both sides of the machine drive are synchronized. During turns the outside tracks are driven faster and for very sharp turns the tracks are counter-rotated to turn the site transporter about its own vertical centerline ((Ref. B2.1.1), Section 2.1.2).

#### **B2.2.1.2 Power Plant Subsystem Description**

The power plant subsystem supplies the site transporter with 480 V AC, 3-phase power at 60 Hz. Because of the risk of contamination from their various fluids, there are no storage batteries or capacitors in the system. The generator is size approximately 110% more than the highest power requirement for the vehicle.

The 150 kW generator is sized for seven hours of continuous operation with a fuel tank containing 99 gallons of diesel fuel (*Mechanical Handling Design Report – Site Transporter* ((Ref. B2.1.1), Section 2.2.3). The fuel tank capacity is sized to minimize the amount of fuel taken inside the facilities, but sufficient to transport a loaded aging overpack three miles and return to the site transporter’s point of origin without refueling ((Ref. B2.1.2) , Section 7.2.2-2).

When entering a building the generator is shut down and a power source from the building is plugged into the site transporter’s integral receptacle to allow the site transporter to operate inside the building without a source of combustion.

The motor drive system and current overload protection system prevents the site transporter from exceeding 2.5 mi/hr ((Ref. B2.1.1), Section 3.2.1).

#### **B2.2.1.3 Rear Lift Forks Subsystem Description**

The rear forks are only capable of moving up or down. Each fork is driven by its own gear reduction and 16 HP, 900 rpm electric motor. The output of the drive is a rotating ACME type screw which, as it turns inside the rear fork lift tube, drives an ACME nut that raises or lowers the fork. The height of the rear lift fork is controlled by limit switches as well as being mechanically unable to lift an aging overpack height more than 12 in. above the floor/ground ((Ref. B2.1.1), Sections 2.1.4 and 2).

#### **B2.2.1.4 Lift Support Arms Subsystem Description**

The front support arms have constrained movement which consists of a clockwise/counterclockwise rotation and up and down movement. The right and left assemblies are mirror images of one another and move as a synchronous pair, although they are each driven by their own gear reduction and 20 HP, 900 rpm electric motor ((Ref. B2.1.1), Section 2.1.5).



The operator positions the lift support arms around the lifting forks. After the site transporter has been positioned properly around the aging overpack, the rear forks are raised to contact the bottom of the aging overpack’s lifting slots. Limit and position switches ensure the lift support arms are in the correct position. Additional limit switches prevent the support arms from exceeding the 12-in. lift.

**B2.2.1.5 Restraints Subsystem Description**

When the load on the site transporter is ready to be lifted, the three arms of the restraint system are activated and moved to a location “near” the aging overpack. This location is determined by a combination of operator observation and integral limit switches.

After the aging overpack has been raised to the specified transportation height, the restraint arms are engaged and locked to hold the aging overpack in place during movement. The arms are moved by linear electromechanical actuators. In addition, a locking pin is utilized to take extreme loads as well as serve as an interlock device. The three restraint arms must be properly pinned before the interlock allows the site transporter to be moved ((Ref. B2.1.3), Sheet 1 of 3).

**B2.2.1.6 Vehicle Controls Subsystem Description**

The site transporter can be operated in two modes: a remote (wireless) control and an operator controlled pendant ((Ref. B2.1.1), Section 2.1.7). Both of these devices have the same capability. Table B2.2-1 contains a list of controls that are available on the controller and the corresponding activation device ((Ref. B2.1.3), Sheet 3 of 3).

Table B2.2-1. Site Transporter Remote or Pendant Controls

Site Transporter Operation	Activation Device on Controller
Start/stop	Pushbutton
Emergency stop	Palm button
Restraint pin—engage(in)/disengage (out)	Selector switch
Maintenance—left side/right side/rear/all	Keyed selector switch
Track synch—left/right/both	Selector switch
Bypass—normal/bypass	Keyed selector switch
Support arms—in/out	Induction pushbutton
Support arms—raise/lower	Induction pushbutton
Forks—raise/lower	Induction pushbutton
Restraint—in/out	Induction pushbutton
Left track—forward/reverse	Induction pushbutton
Right track—forward/reverse	Induction pushbutton
Support arms—off/in-out/raise-lower	Selector switch
Motion—off/tracks/restraints	Selector switch
Lift—off/forks/forks support arms	Selector switch

Source: Original

All safety interlocks and controls of the site transporter are hard wired between the specific relays, drives, circuit breakers, and other electrical equipment. No programmable logic controller or computer is used to control the machine.

### **B2.2.2 Normal Operations**

Once the lift has been completed, the operator performs the final positioning of the upper restraint arms and inserts a pin in each arm. When the pins are properly installed, the site transporter can move.

The operator trails behind the site transporter during movement using the remote control to drive the site transporter to the desired location. Once the site transporter arrives at the facility, the operator stops the vehicle outside the Entry Vestibule and turns off the diesel generator. An electrical umbilical cable is manually retrieved from inside the building and attached to the site transporter. The site transporter is never operated inside a facility on diesel power.

Once inside the building, the operator positions the site transporter in the appropriate room associated with aging overpack loading or unloading activities. Before work is performed on the aging overpack, the site transporter operator removes the pins from the restraint arms and disengages them from the aging overpack. The movement interlock is engaged when the pins are removed. The operator then lowers the aging overpack to the floor. The procedure is reversed when it is necessary to move the site transporter again inside the facility. Once inside the appropriate room, the pins are removed, the restraints are disengaged, the aging overpack is lowered to the floor, and the umbilical cable is removed.

The operations used to move an unloaded aging overpack are identical but not considered in this analysis.

### **B2.2.3 Site Transporter Off-Normal Operations**

There are four off-normal conditions that could occur during the movement of an aging overpack. When any of these occur, the operator response encompasses only those actions to return the aging overpack to a safe state. The off-normal conditions include the following:

- Loss of power while lowering the forks
- Loss of power while rotating the lift support arms
- On-board generator failing to operate
- Track belt failing.

In the event of a loss of power, the site transporter is designed to stop, retain its load, and enter a locked mode. Upon the restoration of power the site transporter stays in the locked mode until operator action is taken ((Ref. B2.1.2), Section 7.2.3-5).

### **B2.2.4 Site Transporter Testing and Maintenance**

Testing and maintenance of the site transporter is done on a periodic basis and does not affect the normal operations of the site transporter. Testing and/or maintenance are not performed on a site transporter loaded with an aging overpack or an STC. A site transporter that has malfunctioned

or has a warning light lit on the site transporter is deemed unserviceable and turned in for maintenance. Unserviceable vehicles are not used.

If an unserviceable state is identified during a lift/lower or movement activity, the site transporter is immediately placed in a safe state (as quickly as possible) and recovery actions for the site transporter are invoked.

### **B2.2.5 Site Transporter System Requirements and Design Features**

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals can not be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cable disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

#### **Requirements**

Two means of stopping the site transporter are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that is the equivalent of a dead man switch.

On the loss of AC power derived from the facility, the site transporter performs a controlled stop. Once stopped the site transporter enters the “lock mode,” safe state. The “lock mode,” safe state is not reversible without specific operator action.

There is no testing or maintenance permitted on a site transporter loaded with an aging overpack.

Since the dominant contributor to site transporter collision in the facility is human error, no priority is given to either the remote or the pendant controllers.

#### **Design Features**

Stopping the site transporter is accomplished by pushing the “stop” button on the remote or pendant controller. The site transporter, upon receiving a stop command from either control source immediately responds by removing power from the propulsion system.

The site transporter is only able to perform one function at any time. It can lift an aging overpack or it can move it, but it can not perform both functions at the same time. This feature is accomplished by interlock and by power limitations inherent in the sizing of the power plant that ensures a limited amount of power for each of the electromechanical devices and drive system.

### B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B2.3-1 with the following dependencies:

1. Functional dependence
2. Environmental dependence
3. Spatial dependence
4. Human dependence
5. Failures based on external events.

Table B2.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environ- mental	Spatial	Human	External Events
Lift booms	Material failure - ACME screw/nut	—	—	—	—
Lift support arms	Material failure - ACME screw/nut	—	—	—	—
Restraint arms	Material failure - lock pin failure	—	—	—	—
Power plant	Current overload protection fails - safe state on	—	—	Failure to stop Failure to remove power cable	—
Remote control	Spurious commands	—	—	Improper command	Collide with crane rigging
Tracks	Material failure	—	—	Failure to stop	—

Source: Original

### B2.4 SITE TRANSPORTER FAILURE SCENARIOS

There are two basic site transporter fault trees developed for Intra-Site Operations. The top events for these fault trees and the variations are as follows:

1. Site transporter collision entering/leaving facility (INT-2-ST-COLLISION).
2. Site transporter drops load during lift/lower (INTRASITE-ST-AO-DROP).

Tipover of the site transporter was also considered, but is screened out as an initiating event (Table 6.0-2).

## **B2.4.1 Site Transporter Collision (INT-2-ST-COLLISION)**

### **B2.4.1.1 Description**

Collisions can occur as a result of human error or hardware failures (human error events are uniquely identified but all have the same screening value of  $3E-3$ ). Hardware failures leading to a collision consist of the site transporter fails to stop when commanded, the site transporter exceeds a safe speed, or the site transporter moves in the wrong direction.

### **B2.4.1.2 Success Criteria**

The success criteria for preventing a collision include safety design features incorporated in the site transporter for hardware failures, and the site transporter operator maintains situational awareness and proper control of the movement of the site transporter. To avoid collisions, the site transporter must stop when commanded, be prevented from entering a runaway situation, or respond correctly to a site transporter movement command.

The site transporter is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the site transporter by either commanding a “stop” from the start/stop button or by releasing the palm switch which initiates an emergency stop. At anytime there is a loss of power detected, the site transporter immediately stops all movement and enters into “lock mode” safe state. The site transporter remains in this locked mode until power is returned and the operator restarts the site transporter.

Runaway situations on the site transporter are prevented by mechanical constraints. The maximum speed of the site transporter is limited by motor current overload protection ((Ref. B2.1.1), Section 3.2.1). The site transporter motor speed and gearing prevents the site transporter from exceeding 2.5 mi/hr.

The prevention of site transporter movements in the wrong direction is prevented by the limitation of the power plant that prevents simultaneous operations.

### **B2.4.1.3 Design Features and Features**

#### **Requirements**

The site transporter has two off-equipment control devices that have complete control over the site transporter.

#### **Features**

Drive system consists of an electric motor and a transmission constraint which limits the maximum speed of the site transporter to 2.5 mi/hr.

### B2.4.1.4 Fault Tree Model

The fault tree model for a site transporter collision entering/leaving facility (INT-2-ST-COLLISION) accounts for the both human error and/or site transporter hardware problems that could result in a collision.

The fault tree considers mechanical failures that fail to stop the site transporter, events that could cause the site transporter to exceed safe speed, and events that could cause the site transporter to move in the wrong direction.

### B2.4.1.5 Basic Event Data

Tables B2.4-1 lists the basic events used in the INT-2-ST-COLLISION fault tree.

Table B2.4-1. Basic Event Probability for INT-2-ST-COLLISION

Name	Description	Calc. Type <sup>a</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-LOSP-4	Failure of offsite power	1	4.100E-06	4.100E-06	0.000E+00	0.000E+00
ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes collision	1	3.000E-03	3.000E-03	0.000E+00	0.000E+00
ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	3	9.130E-08	0.000E+00	9.130E-08	1.000E+00
ISO-ST---CBP004-CBP--SHC	ST power cable short circuit	3	1.880E-08	0.000E+00	1.880E-08	1.000E+00
ISO-ST---CT000---CT-FOD	ST primary stop switch fails	1	4.000E-06	4.000E-06	0.000E+00	0.000E+00
ISO-ST---CT002---CT-FOH	Direction controller fails	3	6.880E-05	0.000E+00	6.880E-05	1.000E+00
ISO-ST---HC001--HC-FOD	Remote control transmits wrong signal	1	1.740E-03	1.740E-03	0.000E+00	0.000E+00
ISO-ST---HC002---HC--SPO	Spurious command to lift/lower AO or STC	3	5.230E-07	0.000E+00	5.230E-07	1.000E+00
ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00
ISO-ST---MOE021--MOE-FSO	Drive system on primary propulsion fails	3	1.350E-08	0.000E+00	1.350E-08	0.000E+00
ISO-ST---SC021---SC-FOH	Speed controller on ST pendant fails	3	1.280E-04	0.000E+00	1.280E-04	0.000E+00
ISO-ST---SC021---SC-SPO	On-board controller initiates spurious signal	3	3.200E-05	0.000E+00	3.200E-05	0.000E+00
ISO-ST---SEL021--SEL-FOH	Speed selector on ST pendant fails	3	4.160E-06	0.000E+00	4.160E-06	0.000E+00

NOTE: <sup>a</sup> 1 is direct input probability; and 3 is lambda and mission time.

AO = aging overpack; Calc. = calculation; ST = site transporter; STC = shielded transfer cask (used in WHF).

Source: Original

### B2.4.1.5.1 Human Failure Events

There is one human event (ISO-OPSTCOLLIDE2-HFI-NOD) in the collision trees for the site transporter and accounts for the site transporter operator causing the collision. This human error is set at the screening value of  $3E-03$ .

### B2.4.1.5.2 Common-Cause Failures

There are no CCF events identified for the site transporter collision events.

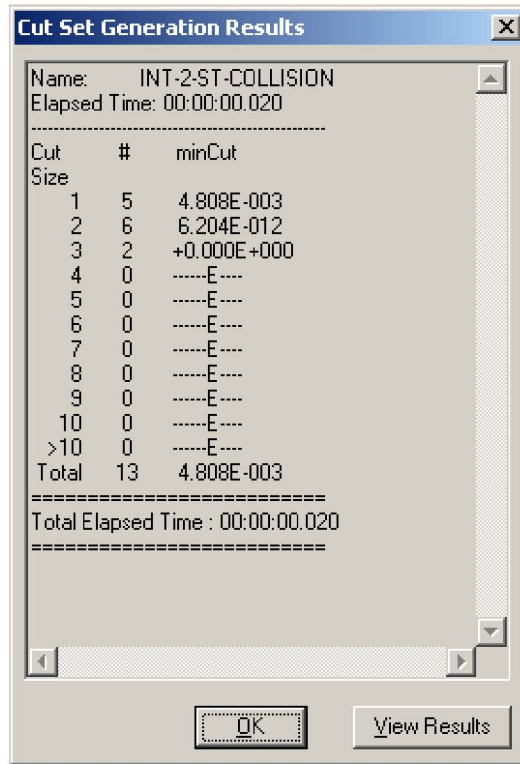
### B2.4.1.6 Uncertainty and Cut Set Generation

Figures B2.4-1 and B2.4-2 contain the uncertainty and the cut set generation results for a site transporter collision.

Uncertainty Results			
Name	INT-2-ST-COLLISION		
Random Seed	1234	Events	14
Sample Size	10000	Cut Sets	13
Point estimate	4.808E-003		
Mean Value	4.579E-003		
5th Percentile Value	5.253E-004		
Median Value	2.360E-003		
95th Percentile Value	1.214E-002		
Minimum Sample Value	9.461E-005		
Maximum Sample Value	8.614E-001		
Standard Deviation	1.595E-002		
Skewness	2.732E+001		
Kurtosis	1.090E+003		
Elapsed Time	00:00:00.890		
<input type="button" value="OK"/>			

Source: Original

Figure B2.4-1. Uncertainty Results Site Transporter Collision



Source: Original

Figure B2.4-2. Cut Set Generation Results



### B2.4.1.7 Cut Sets

Table B2.4-2 provides the cut sets developed for the site transporter collision fault tree.

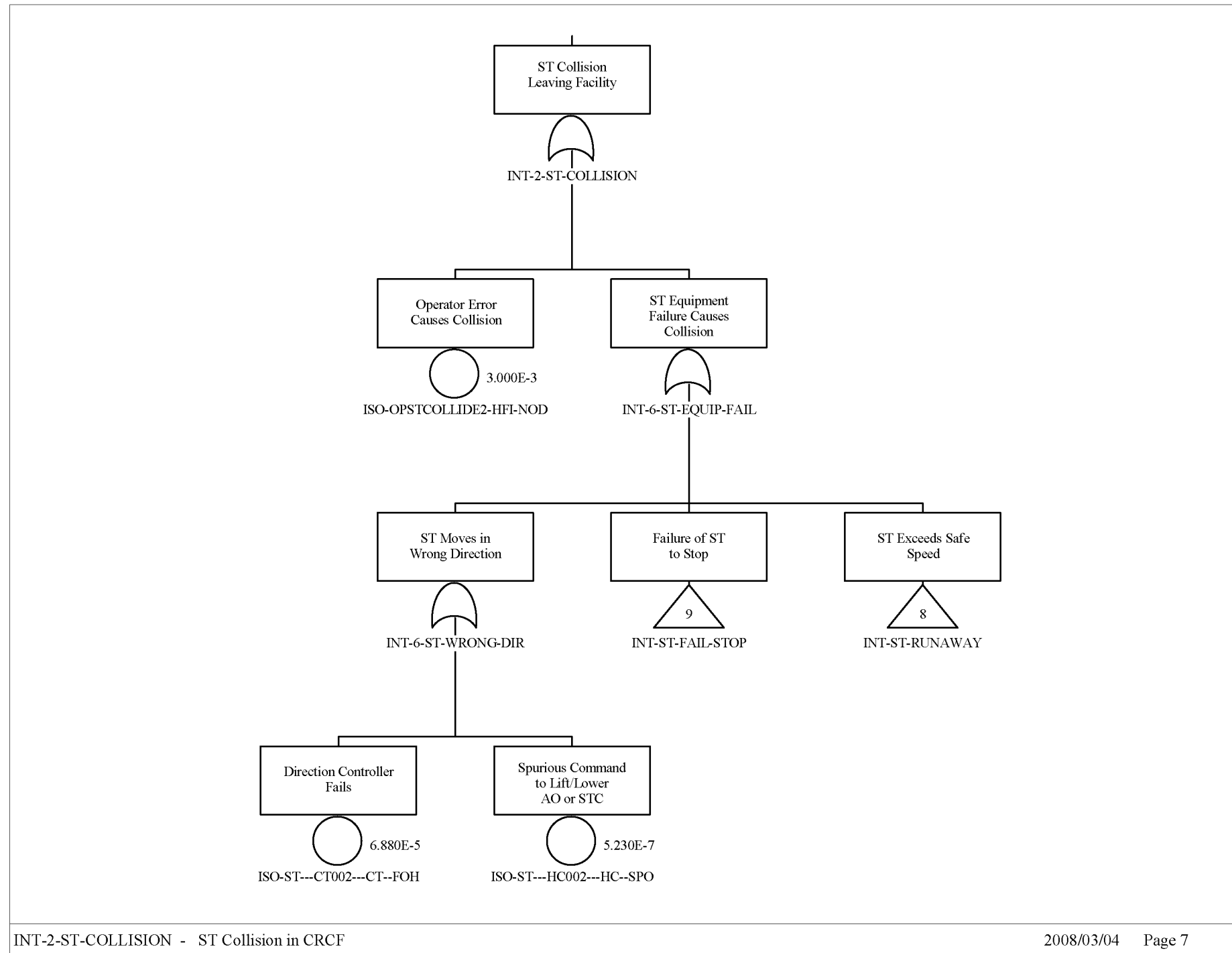
Table B2.4-2. Cut Sets for the Site Transporter Collision in Facility

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
62.40	62.40	3.000E-03	ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes collision	3.000E-03
98.59	36.19	1.740E-03	ISO-ST---HC001--HC--FOD	Remote control transmits wrong signal	1.740E-03
100.00	1.43	6.880E-05	ISO-ST---CT002---CT--FOH	Direction controller fails	6.880E-05
100.00	0.08	4.000E-06	ISO-ST---CT000---CT--FOD	ST primary stop switch fails	4.000E-06
100.00	0.01	5.230E-07	ISO-ST---HC002---HC--SPO	Spurious command to lift/lower AO or STC	5.230E-07
100.00	0.00	5.986E-12	ISO-LOSP-4	Failure of offsite power	4.100E-06
			ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-06
100.00	0.00	1.333E-13	ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-06
			ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E-08
100.00	0.00	5.535E-14	ISO-LOSP-4	Failure of off site power	4.100E-06
			ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	1.350E-08
100.00	0.00	2.745E-14	ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E-06
			ISO-ST---CBP004-CBP--SHC	ST power cable short circuit	1.880E-08
100.00	0.00	1.233E-15	ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E-08
			ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	1.350E-08

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask (used in WHF)

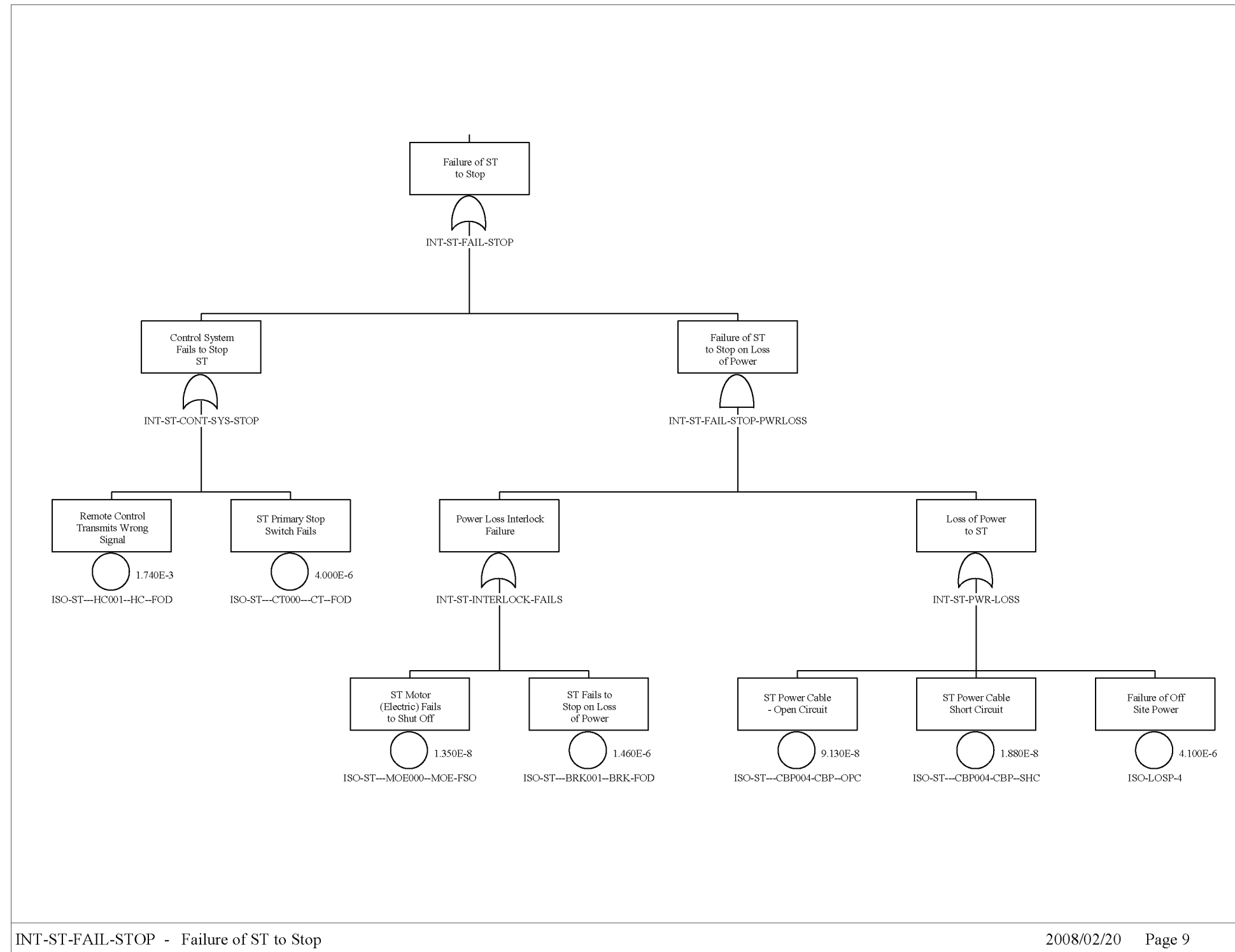
Source: Original

### B2.4.1.8 Fault Tree



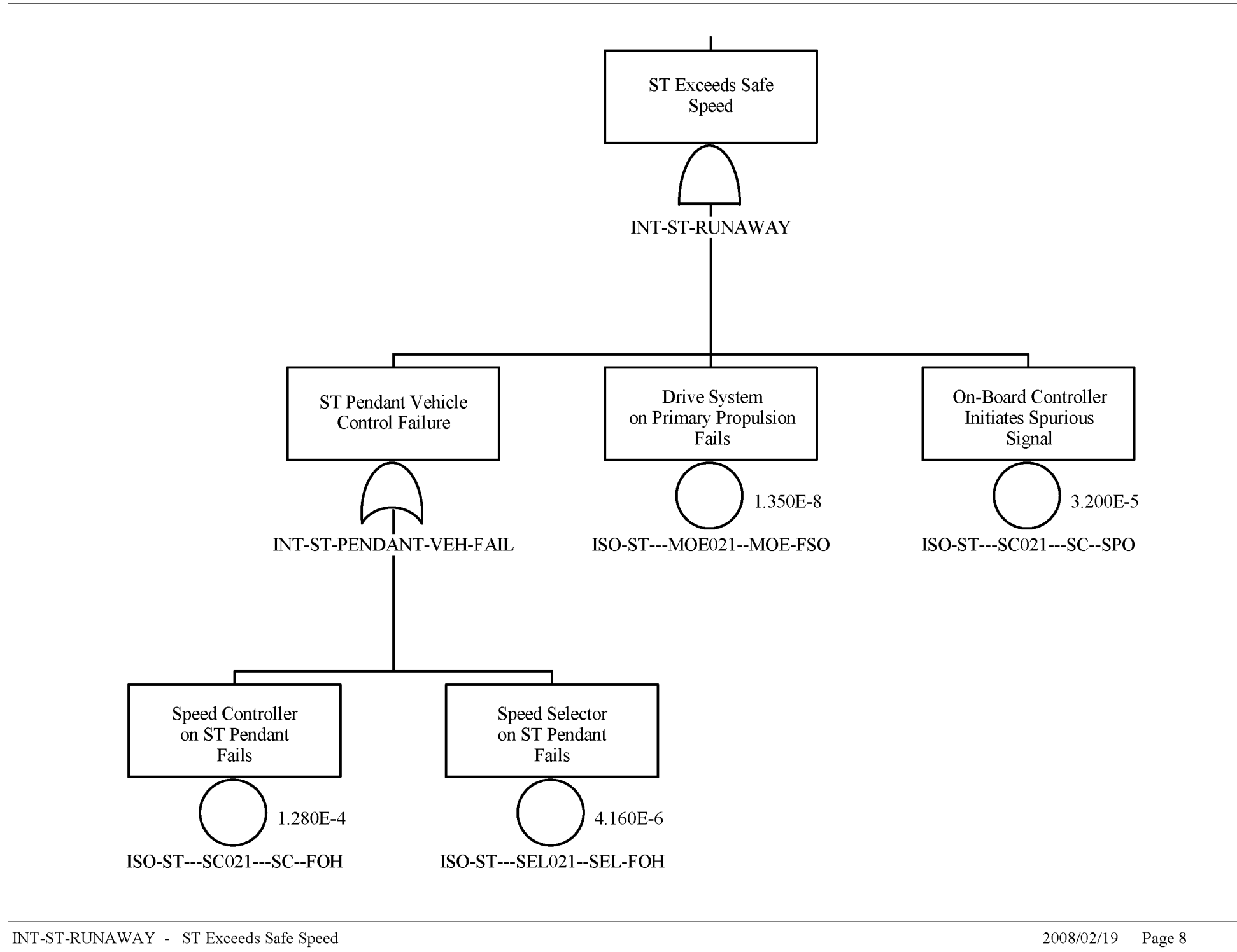
Source: Original

Figure B2.4-3. INT-2-ST-COLLISION -Site  
Transporter Collision Sheet  
1 of 3



Source: Original

Figure B2.4-4. INT-2-ST-COLLISION Site  
Transporter Collision Sheet  
2 of 3



Source: Original

Figure B2.4-5. INT-2-ST-COLLISION Site Transporter Collision Sheet 3 of 3

## **B2.4.2 Site Transporter Load Drop during Lift and Movement (INTRASITE-ST-AO-DROP)**

### **B2.4.2.1 Description**

The site transporter conducts lift/lowering and movement operations at the aging pads and inside the facilities. Since the site transporter is only capable of performing one operation at a time, it is not possible to move an aging overpack while it is being lifted/lowered. For activities associated with lifting the aging overpack, there are four distinct failure modes. Those associated with electrical failures, site transporter controller failures, mechanical failures during lifting/lowering, and mechanical failures during movement.

### **B2.4.2.2 Success Criteria**

The potential for a load drop exists when there is a loss of site transporter power, a mechanical failure of the lift/lowering devices, aging overpack restraint device failure during movement, or a failure of the site transporter control system during these operations.

If there is a failure of the electrical system during lifting/lower or movement, the ACME screw/nuts prevent the rear forks and the lift support arms from moving.

The ACME devices also serve to prevent a load drop when there is a lift boom failure. There are four of these devices. One on each of the rear forks and one on each of the lift support arms.

The aging overpack restraint system is engaged after the lift has been accomplished and released prior to performing a lowering operation. These devices restrict the movement of the aging overpack during transport. There are three of these restraints that prevent/restrict movement in the roll-pitch-axis. Pins are used in these devices that prevent the release of the restraint in the advent of an electromechanical failure that controls the position of these devices.

There is an interlock built-in to the restraint system. Movement of the site transporter is prevented until the three pins in the restraint system have been properly installed. These pins also preclude an inadvertent release of the restraint system since they have to be physically removed by the operator before the restraints can be released.

The receipt of inadvertent command signals is also prevented in that the site transporter can only perform one operation at a time due to the limitations in the power plant.

### **B2.4.2.3 Design Requirements and Features**

#### **Requirements**

On the loss or removal of AC power derived from the facility, the site transporter performs a controlled stop. Once stopped the site transporter enters the “lock mode,” safe state. The “lock mode,” safe state is not reversible without specific operator action.

## Features

There are no electrical storage devices in the design of the site transporter. When the facility AC power cable is removed, the site transporter is incapable of movement.

Two operators have the capability of stopping any operation performed by the site transporter when it is inside a facility.

### B2.4.2.4 Fault Tree Model

The fault tree model for site transporter drop load during lift and movement addresses:

- Electrical failures, including motor and distribution events and the failure to enter a “lock mode,” safe state.
- A load drop during the lifting or lowering of the aging overpack, which includes mechanical failure of the lifting booms and restraint/lifting arms.
- Failure of the aging overpack restraint subsystem during the lift/lowering/moving of the site transporter.
- Failure of the site transporter control subsystem.

NOTE: The fault tree defines the movement of the aging overpack in a three axis system as:

1. A roll movement side-to-side as the “R-axis.”
2. A pitch movement front-to-back as the “P-axis.”
3. An up or down movement as the “D-axis.”

### B2.4.2.5 Basic Events

Table B2.4-3 lists the basic events used in the “Site Transporter Load Drop during Lift and Movement” (INTRASITE-ST-AO-DROP) fault tree.

Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree

Name	Description	Calc Type <sup>b</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATB222-AT--FOH	Screw actuator mechanism on lift boom #2 fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATD03-AT--FOH	ST D-axis electrical actuator #1 movement fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATD04-AT--FOH	ST D-axis electrical actuator #2 movement fails	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATP002-AT--FOH	ST P-axis electrical failure during movement	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-ATR10002-AT-FOH	ST R-axis electrical actuator #1 fails movement	3	7.540E-05	0.000E+00	7.540E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-BEA#1-BEA-BRK	Boom #1 fails during cask movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEA22-BEA-BRK	Boom #2 fails during cask lift	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEAD003-BEA-BRK	ST D-axis actuator structural arm #2 failure movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEAD006-BEA-BRK	ST D-axis actuator structural arm #1 failure movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEAP02-BEA-BRK	ST P-Axis mechanical failure during movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-BEAR103-BEA-BRK	ST R-axis actuator structural arm #1 failure movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>

Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree (Continued)

Name	Description	Calc Type <sup>b</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-BEAR204-BEA-BRK	ST R-axis actuator structural arm #2 failure movement	3	2.400E-08	0.000E+00	2.400E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-CBP0000-CBP-OPC	Electrical power dist cable failure on ST	3	1.530E-07	0.000E+00	9.130E-08	0.000E+00 <sup>a</sup>
ISO-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	3	7.100E-05	0.000E+00	7.140E-05	1.000E+00
ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	3	2.270E-05	0.000E+00	2.270E-05	0.000E+00 <sup>a</sup>
ISO-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	3	2.400E-08	0.000E+00	2.400E-08	1.000E+00
ISO-CRWT-EATR2004-AT-FOH	ST R-axis electrical actuator #2 fails movement	3	7.540E-05	0.000E+00	7.540E-05	1.000E+00
ISO-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	3	1.790E-06	0.000E+00	1.790E-06	1.000E+00
ISO-CRWT-ELEC-MOE-FOD	ST electric motor failure	1	6.000E-05	6.000E-05	0.000E+00	1.000E+00
ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00 <sup>a</sup>
ISO-CRWT-LM000011-LC-FOD	ST lift/lower selector lever fails	1	6.250E-04	6.250E-04	0.000E+00	0.000E+00 <sup>a</sup>
ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	3	2.100E-06	0.000E+00	2.100E-06	1.000E+00
ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	3	2.100E-06	0.000E+00	2.100E-06	1.000E+00
ISO-CRWT-PIND004-PIN-BRK	ST D-axis actuator pin #2 failure movement	3	2.120E-09	0.000E+00	2.120E-09	1.000E+00
ISO-CRWT-PIND005-PIN-BRK	ST D-axis actuator pin #1 failure movement	3	2.120E-09	0.000E+00	2.120E-09	1.000E+00
ISO-CRWT-PINP04-PIN-BRK	ST P-axis pin failure during movement	3	2.120E-09	0.000E+00	2.120E-09	1.000E+00
ISO-CRWT-PINR103-PIN-BRK	ST R-axis mechanical pin #1 failure during movement	3	2.120E-09	0.000E+00	2.120E-09	1.000E+00
ISO-CRWT-PINR202-PIN-BRK	ST R-axis mechanical pin #2 failure during movement	3	2.120E-09	0.000E+00	2.120E-09	1.000E+00
ISO-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	3	8.140E-06	0.000E+00	8.140E-06	1.000E+00
ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	3	8.140E-06	0.000E+00	8.140E-06	1.000E+00
ISO-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	3	8.140E-06	0.000E+00	8.140E-06	1.000E+00



Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree (Continued)

Name	Description	Calc Type <sup>b</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	3	8.140E-06	0.000E+00	8.140E-06	1.000E+00
ISO-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00 <sup>a</sup>
ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00 <sup>a</sup>
ISO-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00 <sup>a</sup>
ISO-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	1	2.930E-04	2.930E-04	0.000E+00	0.000E+00 <sup>a</sup>
ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	3	1.350E-08	0.000E+00	1.350E-08	1.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

<sup>b</sup> 1 is direct input probability; and 3 is lambda and mission time..

AO = aging overpack; Calc. = calculation; ST = site transporter; STC = shielded transfer cask (used in WHF).

Source: Original

#### B2.4.2.5.1 Human Failure Events

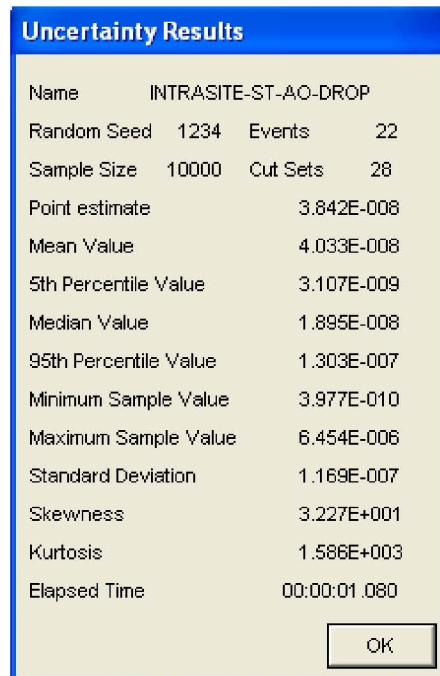
There are no human error events incorporated in the tree.

#### B2.4.2.5.2 Common-cause Failures

There are no CCFs identified in this fault tree.

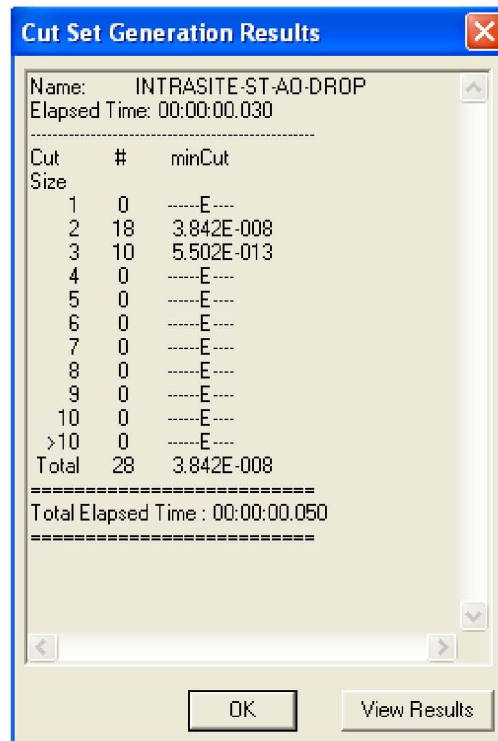
#### B2.4.2.6 Uncertainty and Cut Set Generation

Figures B2.4-6 and B2.4-7 contain the uncertainty and the cut set generation results for “Site Transporter Load Drop during Lift and Movement” fault tree using a cutoff probability of 1E-15.



Source: Original

Figure B2.4-6. Uncertainty Results for Site Transporter Load Drop during Lift/Movement Fault Tree



Source: Original

Figure B2.4-7. Cut Set Generation Results for Site Transporter Load Drop during Lift/Movement Fault Tree

**B2.4.2.7 Cut Sets**

Table B2.4-4 contains the top 25 cut sets for “Site Transporter Load Drop during Lift/Movement” (INTRASITE-ST-AO-DROP) fault tree.

Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree

<b>% Total</b>	<b>Cut Set %</b>	<b>Probability/ Frequency</b>	<b>Basic Event</b>	<b>Description</b>	<b>Probability</b>
36.92	36.92	1.419E-08	ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E-05
			ISO-CRWT-LM000011-LC-FOD	ST lift/lower selector lever fails	6.250E-04
57.89	20.97	8.057E-09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-05
			ISO-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	2.930E-04
78.86	20.97	8.057E-09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-05
			ISO-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	2.930E-04
99.83	20.97	8.057E-09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E-05
			ISO-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	2.930E-04
99.94	0.11	4.063E-11	ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E-05
			ISO-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	1.790E-06
99.96	0.02	7.032E-12	ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E-08
			ISO-CRWT-ZSD00006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-04
99.98	0.02	7.032E-12	ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E-08
			ISO-CRWT-ZSD00006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-04
99.98	0.00	1.810E-12	ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E-05
			ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E-08
99.98	0.00	1.810E-12	ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E-05
			ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E-08
99.98	0.00	1.810E-12	ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E-05
			ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E-08
99.98	0.00	1.810E-12	ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E-05

Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree (Continued)

% Total	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
			ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E-08
99.98	0.00	9.639E-13	ISO-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	7.140E-05
			ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E-08
99.98	0.00	8.100E-13	ISO-CRWT-ELEC-MOE-FOD	ST electric motor failure	6.000E-05
			ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E-08
99.98	0.00	1.798E-13	ISO-CRWT-ATB1001-AT-FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E-06
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-04
99.98	0.00	1.798E-13	ISO-CRWT-ATB2002-AT-FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E-06
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E-04
99.98	0.00	5.040E-14	ISO-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E-08
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E-06
99.98	0.00	5.040E-14	ISO-CRWT-BEA22-BEA-BRK	Boom #2 fails during cask lift	2.400E-08
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E-06
99.98	0.00	5.040E-14	ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E-08
			ISO-CRWT-LVRD01-LVR-FOH	ST D-Axis actuator structural arm #1 failure	2.100E-06
99.98	0.00	5.040E-14	ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E-08
			ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	2.100E-06
99.98	0.00	4.627E-14	ISO-CRWT-ATB1001-AT-FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-05
			ISO-CRWT-ATD001-AT-FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E-05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E-06
99.98	0.00	4.627E-14	ISO-CRWT-ATB1001-AT-FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-05

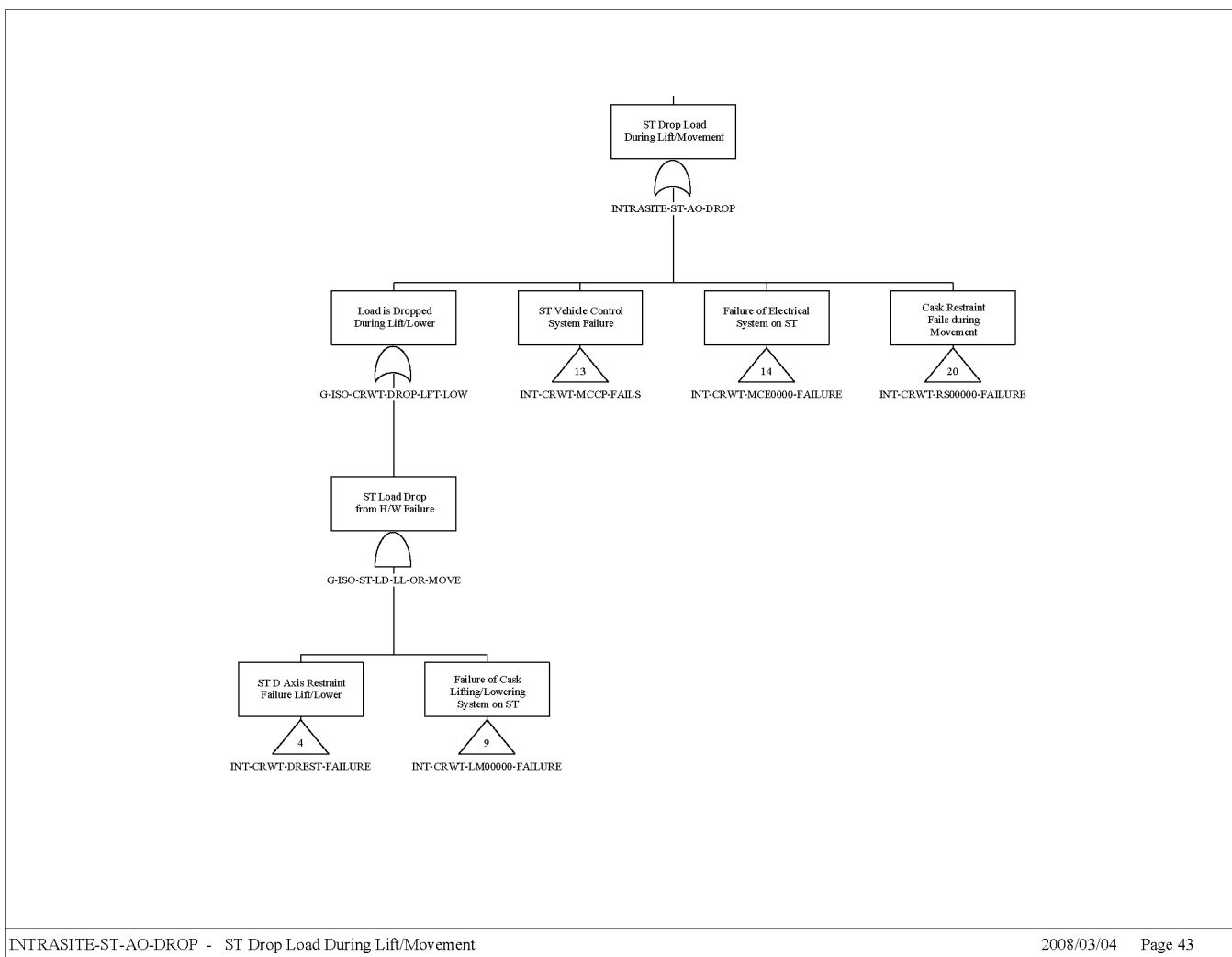
Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree (Continued)

% Total	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
			ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E-05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E-06
99.98	0.00	4.627E-14	ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-05
			ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E-05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E-06
99.98	0.00	4.627E-14	ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E-05
			ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E-05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E-06
99.98	0.00	1.289E-15	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-05
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E-06
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E-06
99.98	0.00	1.289E-15	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E-05
			ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	2.100E-06
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E-06

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask (used in WHF).

Source: Original

### B2.4.2.8 Fault Trees

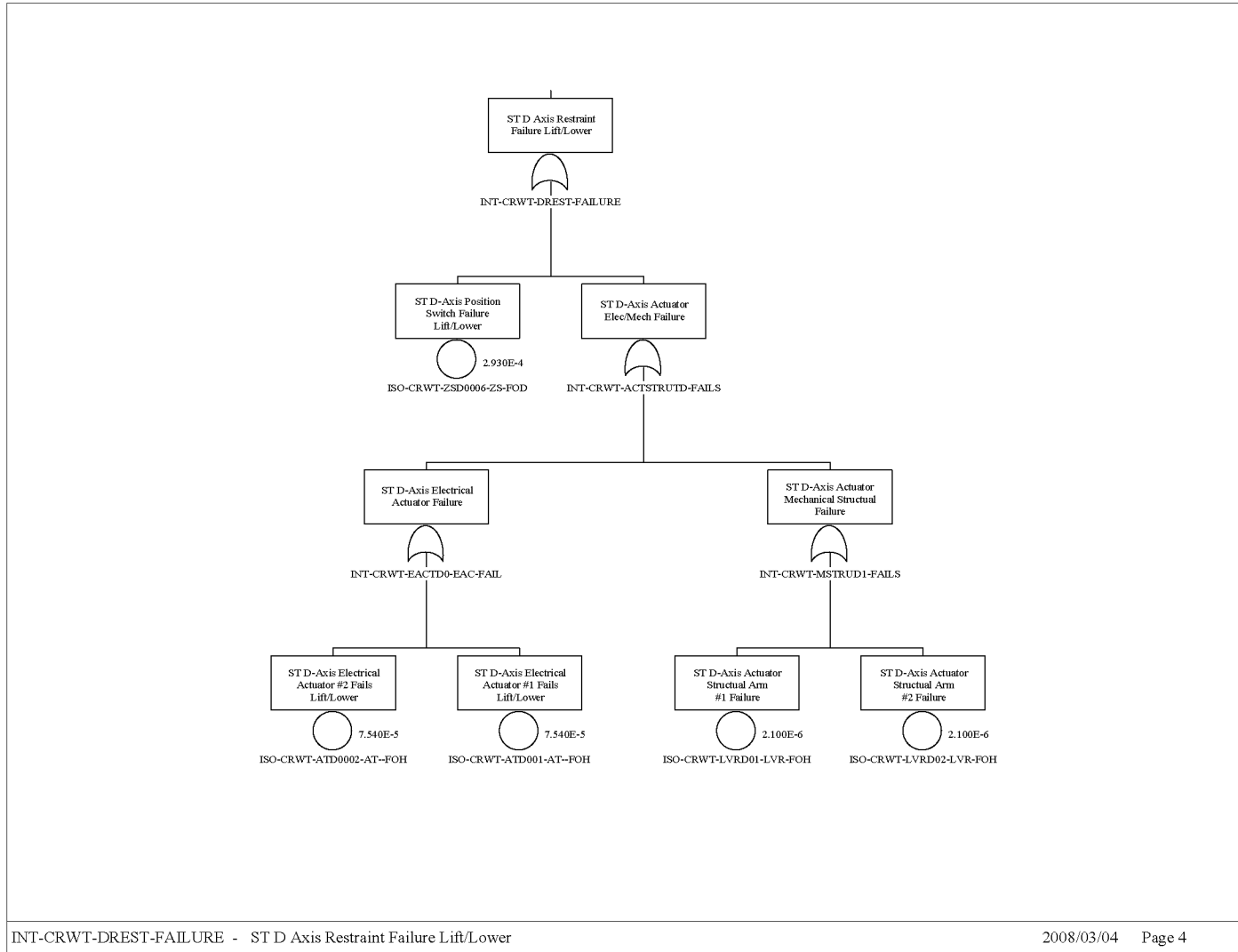


B2-27

Source: Original

Figure B2.4-8. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 1 of 12

March 2008

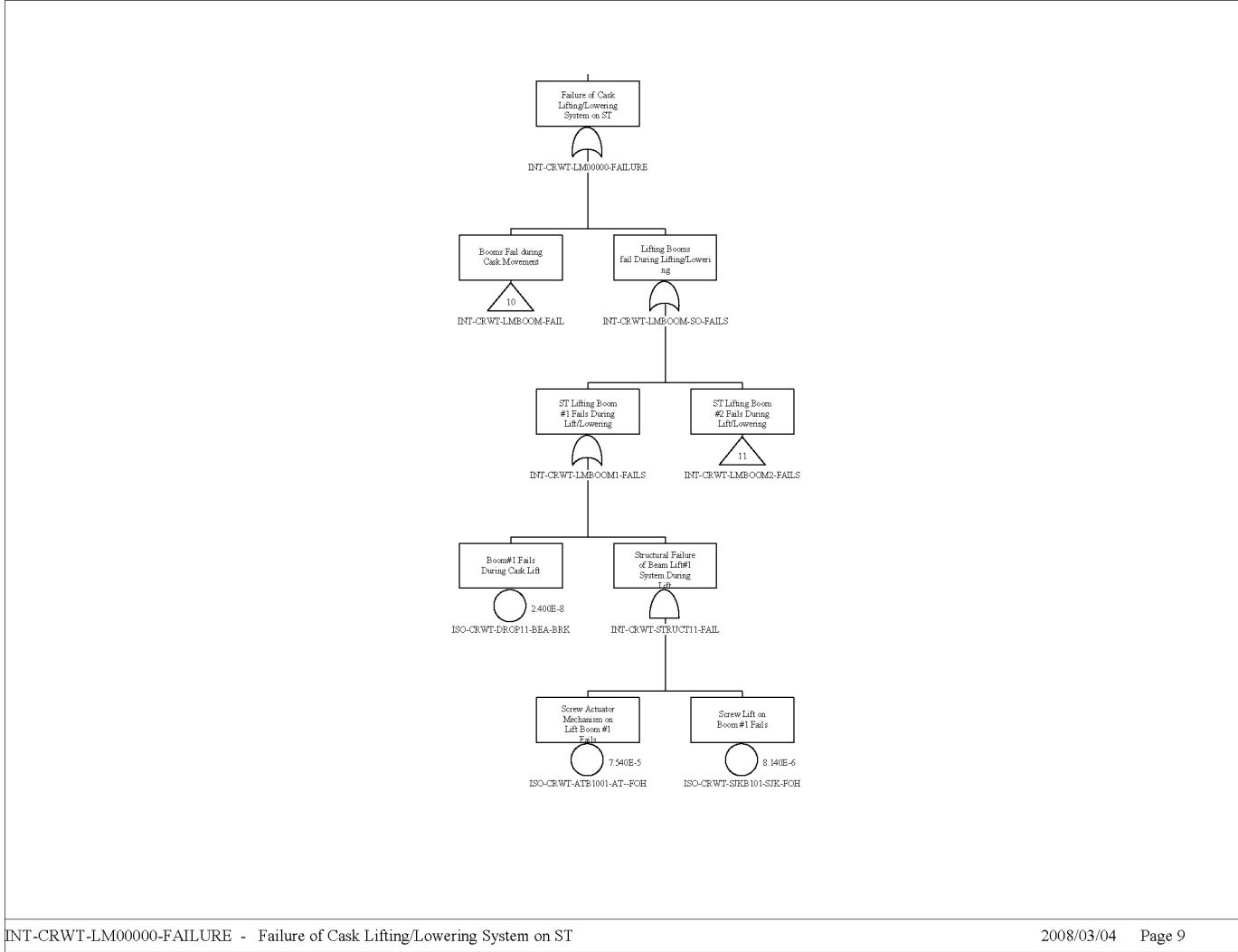


B2-28

March 2008

Source: Original

Figure B2.4-9. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 2 of 12



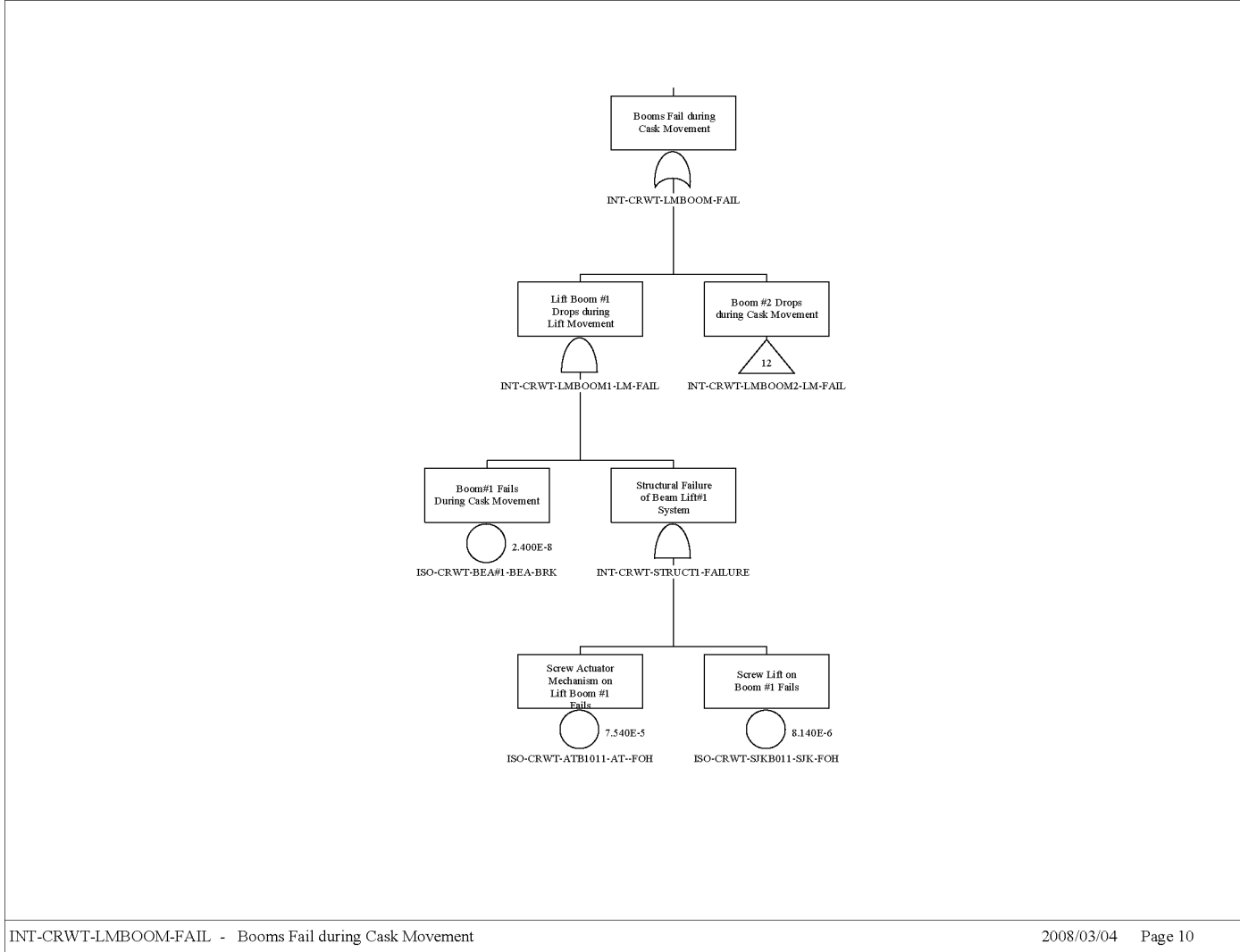
B2-29

Source: Original

Figure B2.4-10. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 3 of 12

March 2008



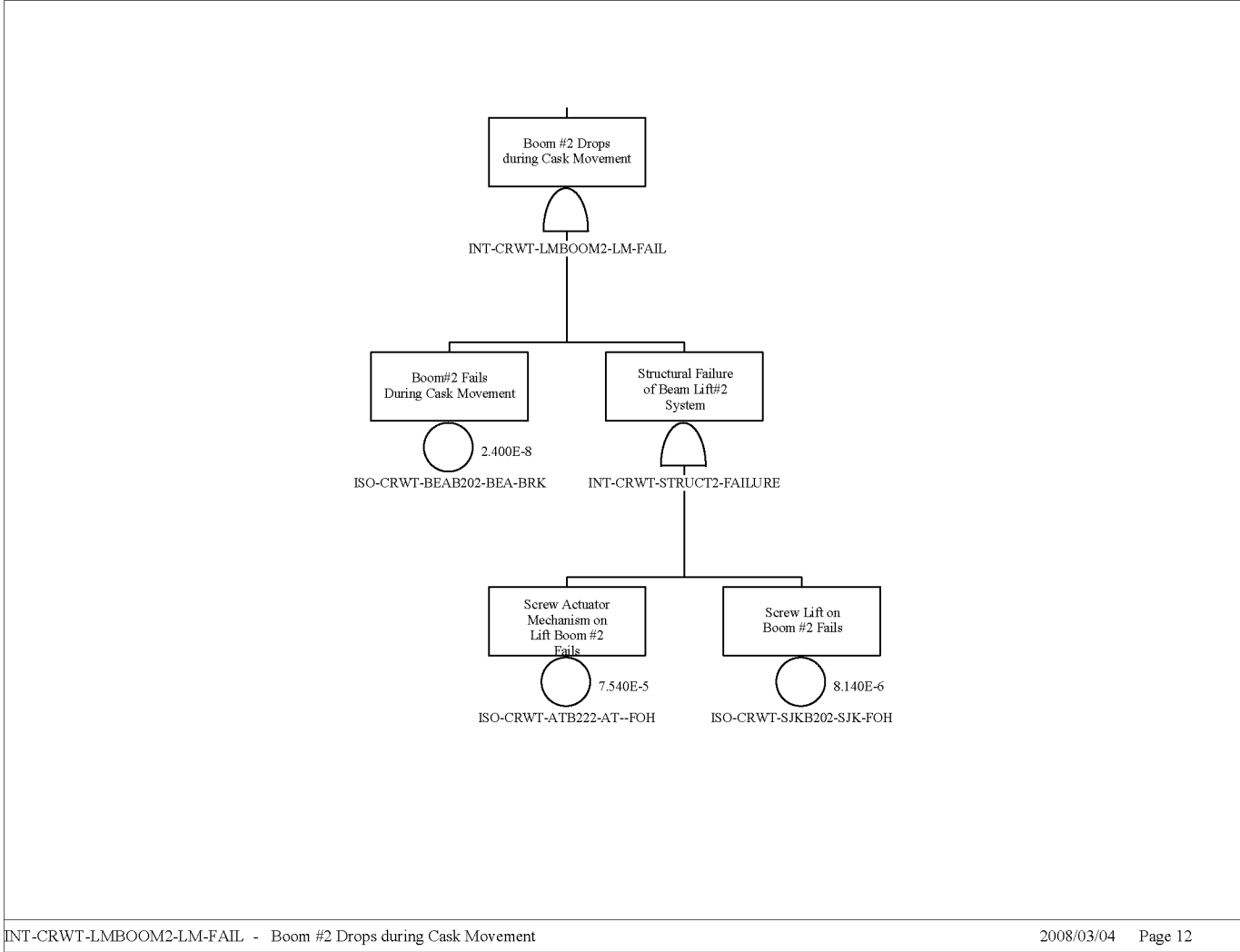


B2-30

Source: Original

Figure B2.4-11. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 4 of 12

March 2008

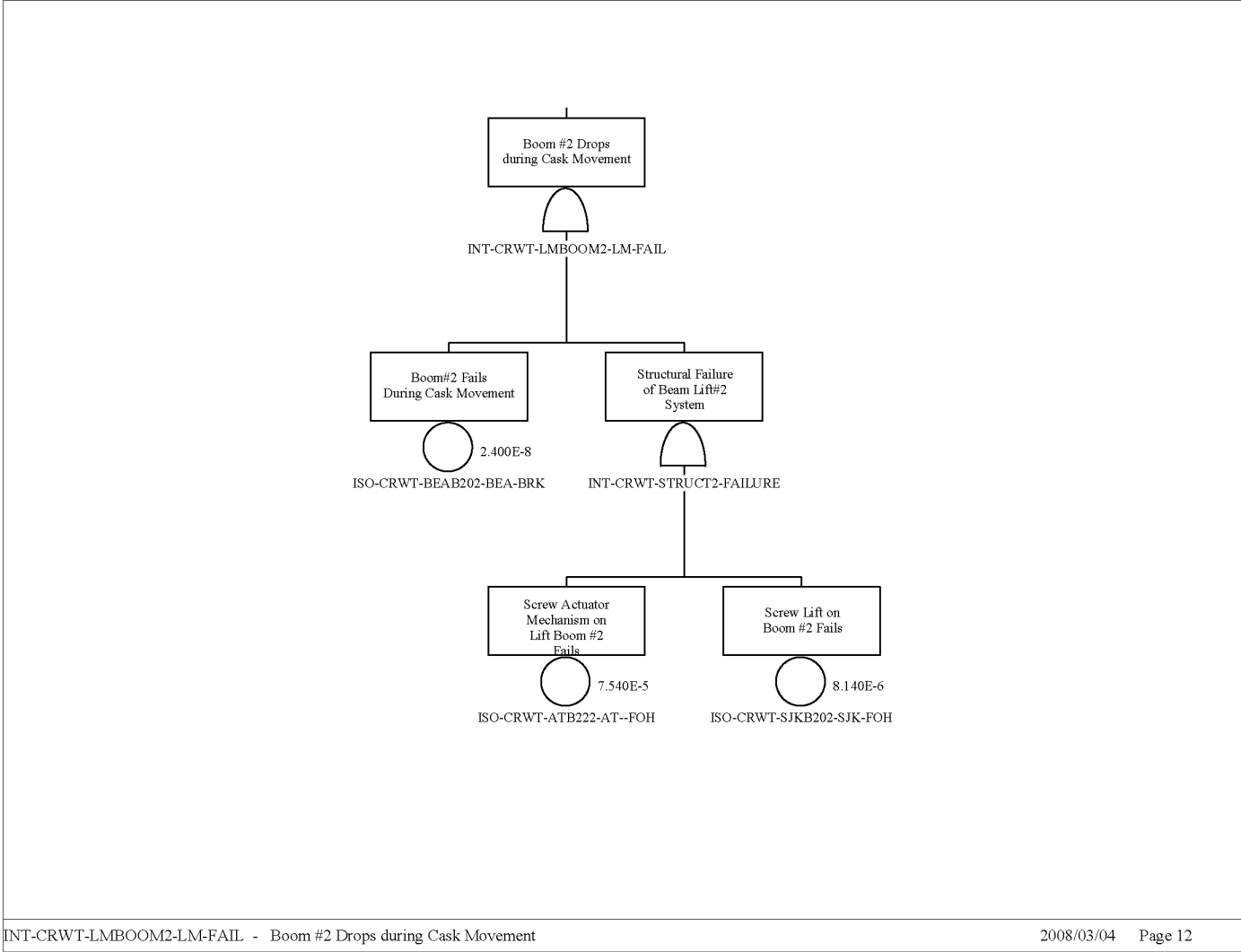


B2-31

March 2008

Source: Original

Figure B2.4-12. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 5 of 12

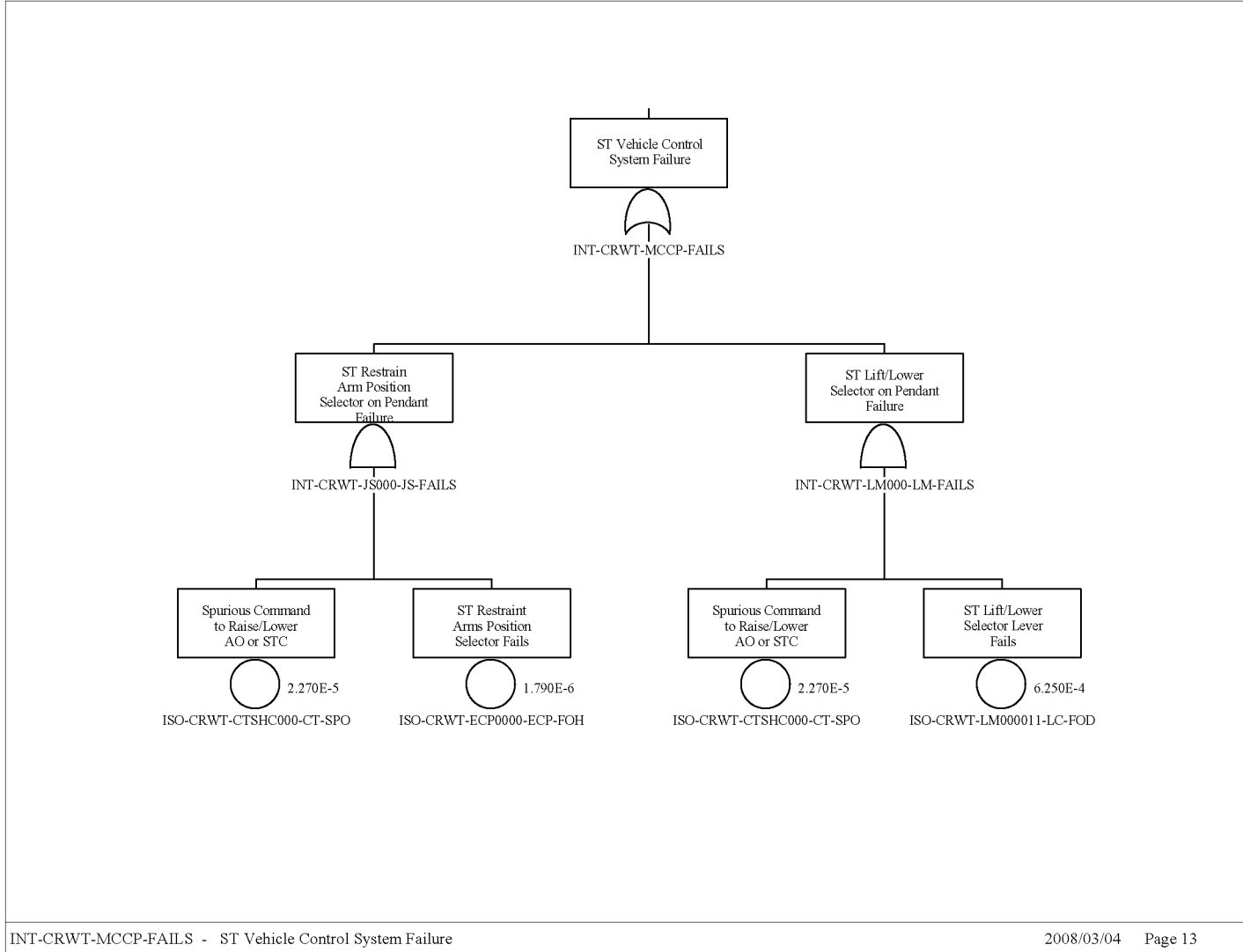


Source: Original

Figure B2.4-13. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 6 of 12

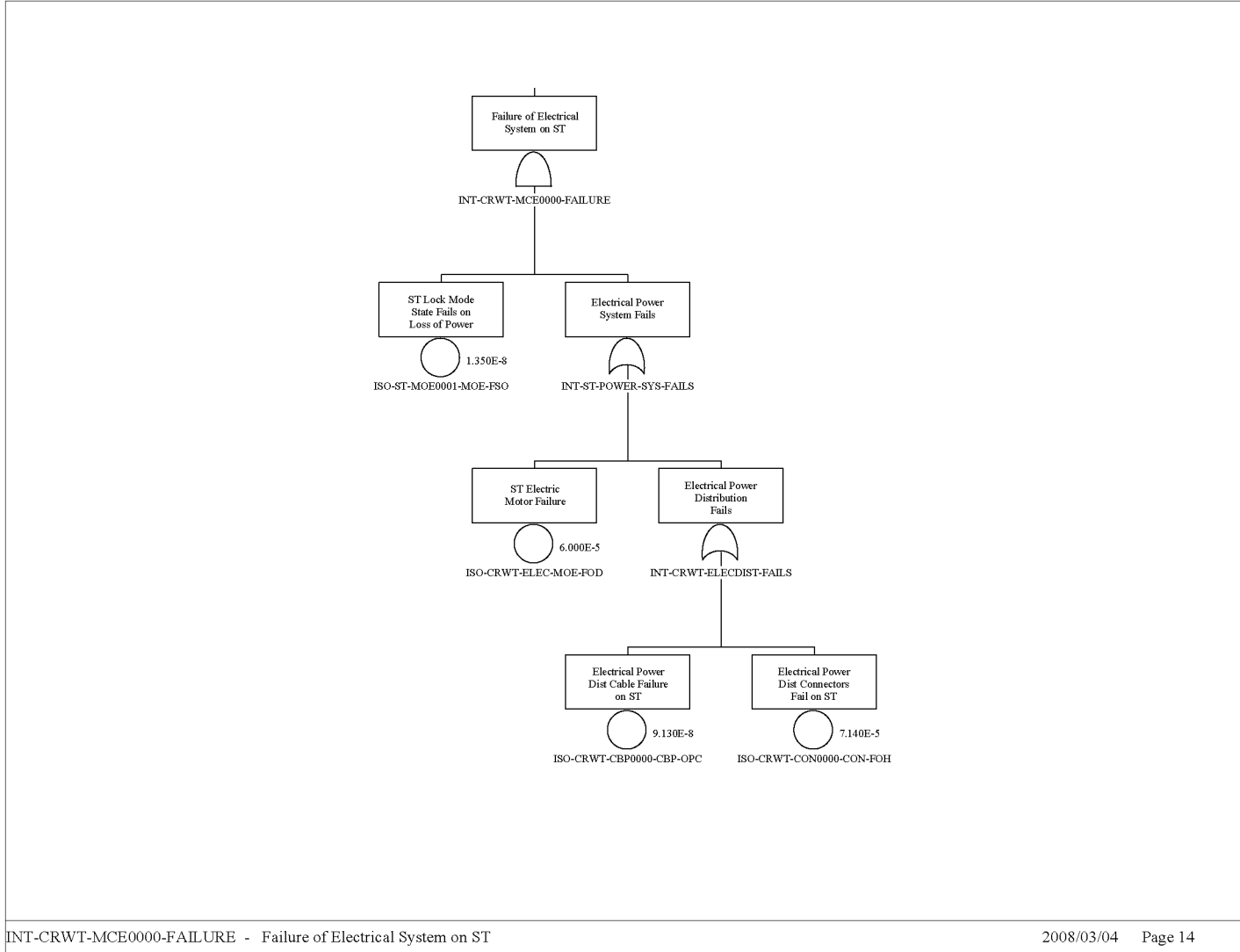
B2-32

March 2008



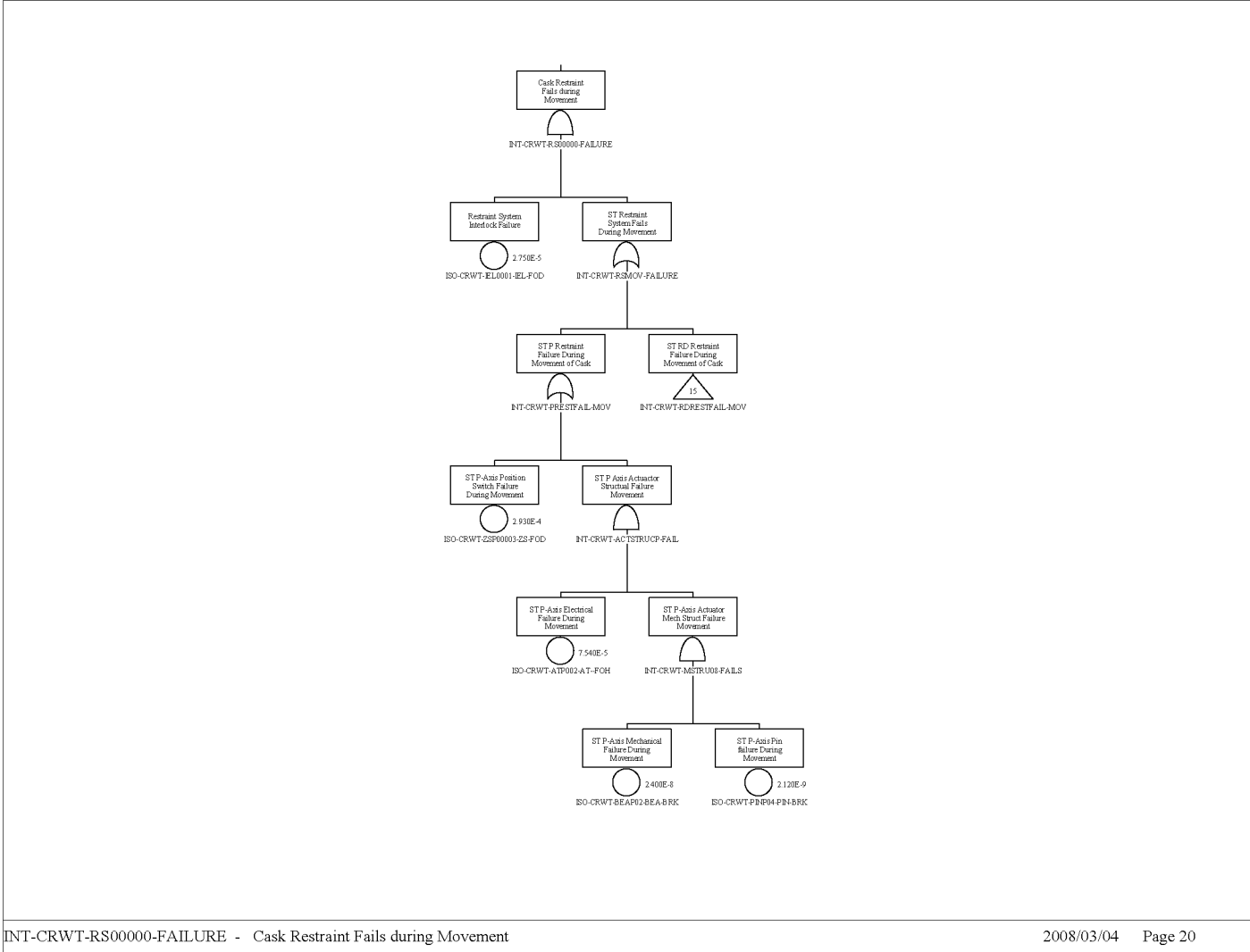
Source: Original

Figure B2.4-14. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 7 of 12



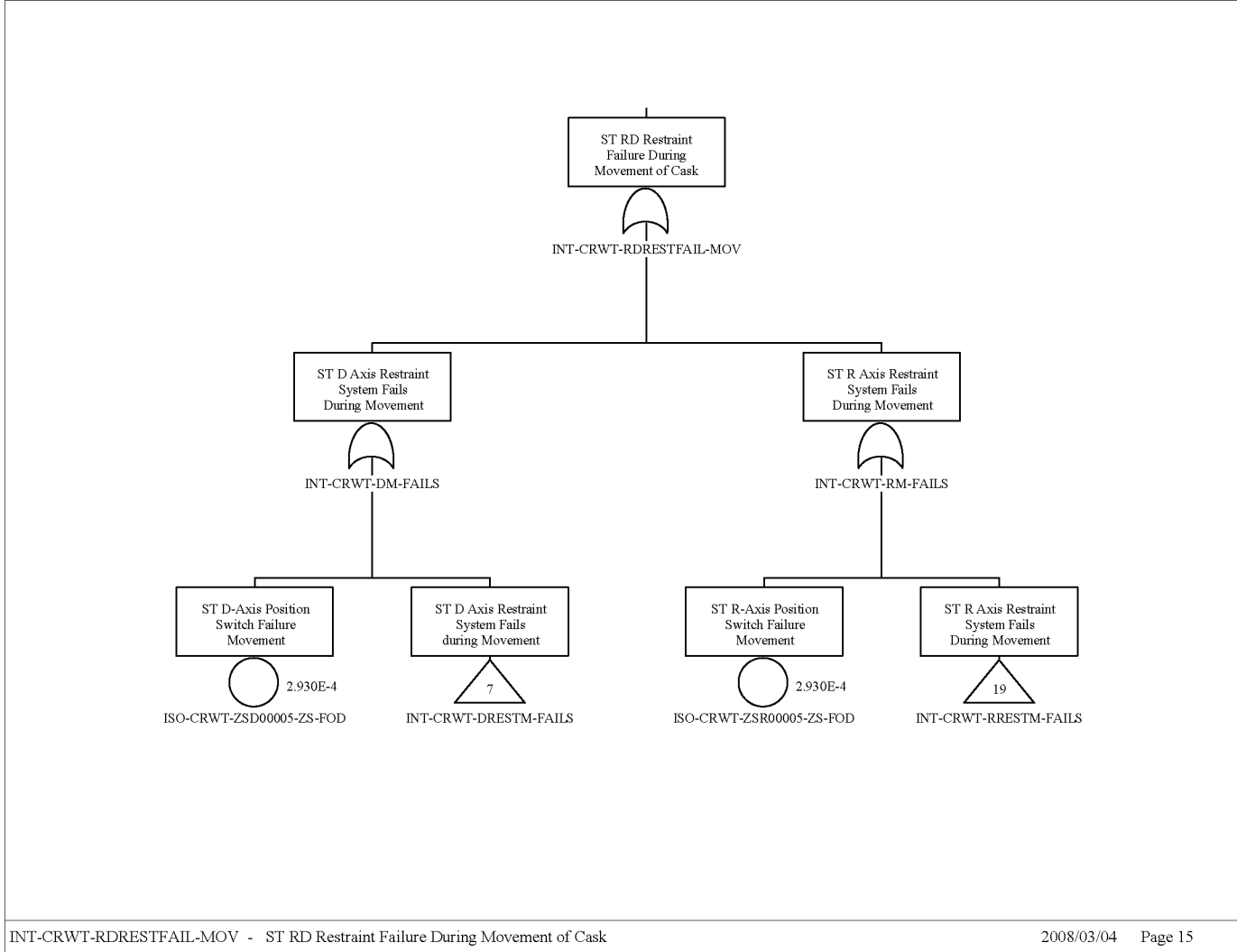
Source: Original

Figure B2.4-15. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 8 of 12



Source: Original

Figure B2.4-16. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 9 of 12

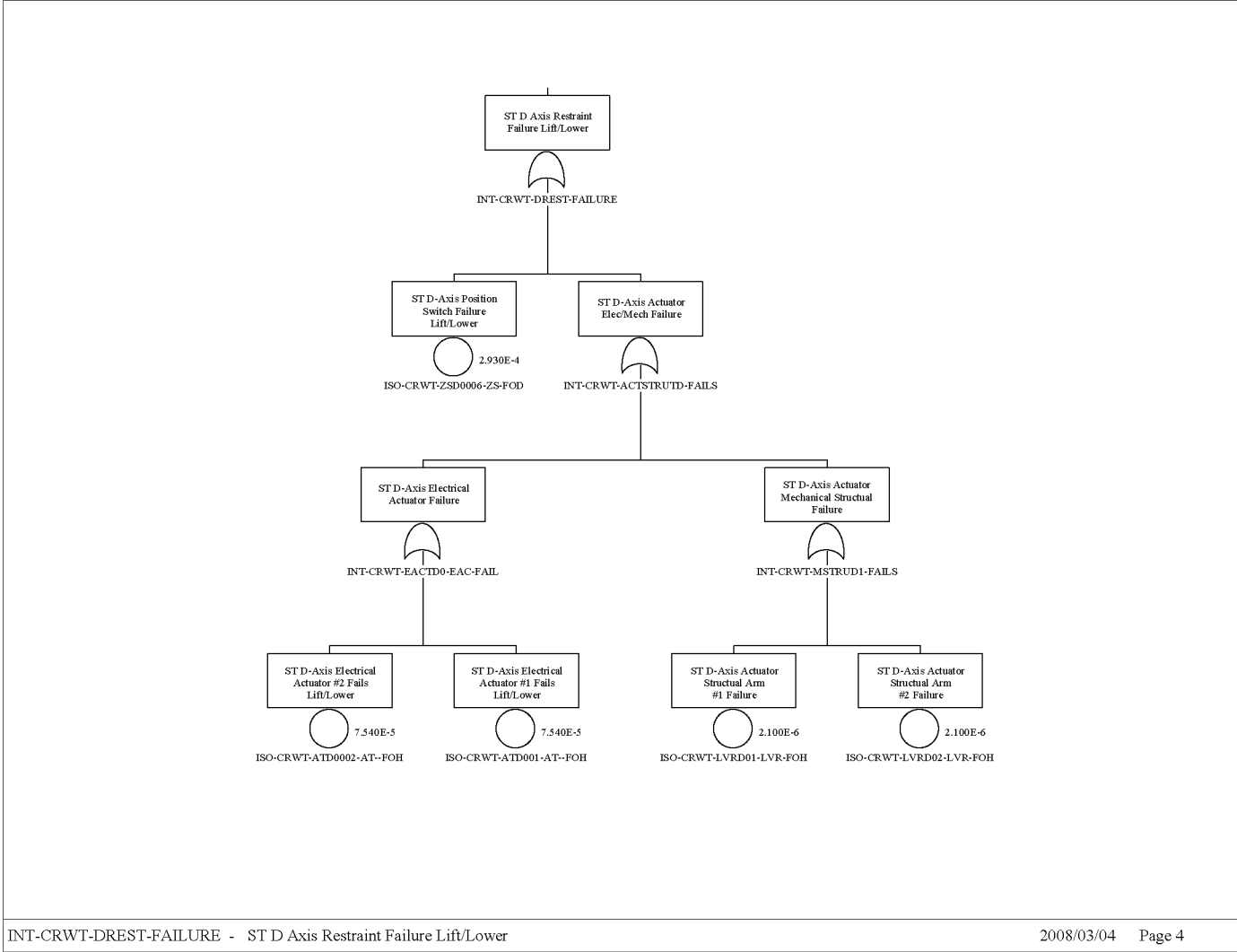


B2-36

March 2008

Source: Original

Figure B2.4-17. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 10 of 12



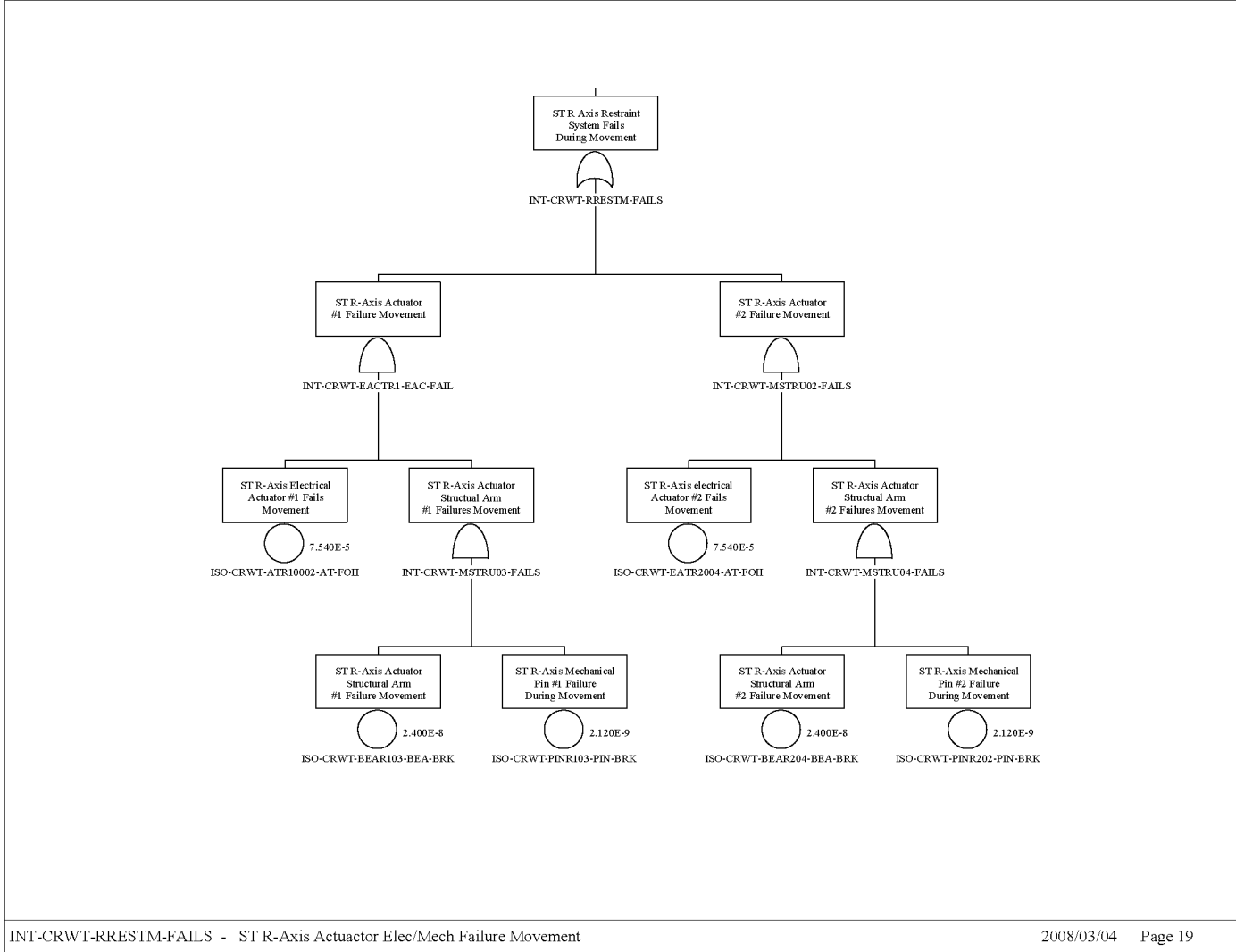
B2-37

Source: Original

Figure B2.4-18. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 11 of 12

March 2008





B2-38

March 2008

Source: Original

Figure B2.4-19. INTRASITE-ST-AO-DROP Site Transporter Drop Load during Lift/Movement Sheet 12 of 12

## **B3 CASK TRACTOR AND CASK TRANSFER TRAILER FAULT TREE ANALYSIS**

### **B3.1 REFERENCES**

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

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

#### **Design Inputs**

B3.1.1 BSC 2007. *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope*. 170-MJ0-HAT0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070518.0002.

B3.1.2 BSC 2007. *Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailers*. 000-3PS-HAT0-00300-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0004.

### **B3.2 CASK TRACTOR AND CASK TRANSFER TRAILER DESCRIPTION**

#### **B3.2.1 Overview**

The cask tractor and cask transfer trailer provide the following functions as described in Section 3.1.1 of *Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailer* (Ref. B3.1.2):

The function of the cask tractor, coupled with the cask transfer trailer, is to:

- Move a transportation cask loaded with a horizontal DPC from a surface facility to a horizontal aging module (HAM) located on Aging Pad 17R.
- Retrieve a horizontal DPC from the HAM, place it into the horizontal shielded transfer cask (HSTC), and transport to the WHF.

For fault tree models in SAPHIRE, the cask tractor and cask transfer trailer are collectively referred to in the code as an HCTT.

#### **B3.2.2 Physical Description**

The cask tractor is a large, four-wheel drive diesel tractor designed specifically for pulling the cask transfer trailer. The cask tractor has redundant brakes in addition to having a fail-safe emergency brake. The cask tractor has mounted non-driven hydraulic pendular axles, with a

minimum of four tires per axles to ensure that the cask remains level during transportation across uneven terrain. In addition to the pendular axles, the trailer has three other hydraulic systems: (1) stabilizing jacks, (2) a cask support skid and positioning system, and (3) a hydraulic ram. The cask tractor and cask transfer trailer are depicted in *Aging Facility Cask Transfer Trailers Mechanical Equipment Envelope* (Ref. B3.1.1).

### B3.3 DEPENDENCE AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with SSCs. The five areas considered are addressed in Table B3.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B3.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Hydraulic pendular axles	Vertical support and leveling during transport and load/unload	—	—	—	—
Hydraulic stabilizing jacks	Redundant vertical support during load/unload	—	—	—	—
Cask tractor brakes	Sufficient to stop conveyance with failed cask transfer trailer brakes	—	—	—	—
Cask transfer trailer brakes	Sufficient to stop conveyance on failed cask tractor brakes	—	—	—	—
Vehicle steering, control and speed limiter	Tractor/ trailer control	—	—	Collision Over speed	—

Source: Original

## **B3.4 CASK TRACTOR AND CASK TRANSFER TRAILER FAILURE SCENARIOS**

A cask tractor and cask transfer trailer collision is the only failure scenario modeled in the fault tree.

### **B3.4.1 Cask Tractor and Cask Transfer Trailer Collision**

#### **B3.4.1.1 Description**

There are two situations modeled where a cask tractor and cask transfer trailer collision may occur, and each has a unique vehicle configuration: (1) unloading the aging overpack at the HAMs (the cask transfer trailer is unhitched from the cask tractor), and (2) during transport between the facilities and HAMs when the cask tractor is pulling the cask transfer trailer.

#### **B3.4.1.2 Success Criteria**

A collision is defined as any undesired contact of the cask tractor and cask transfer trailer with another vehicle, facility structure, or piece of equipment. Any of the steering, braking, and hydraulic systems can cause this to occur, in addition to operator error.

#### **B3.4.1.3 Design Features and Requirements**

The cask tractor brakes are a redundant-brake design and include a backup system with a split master cylinder and an indicator light inside the cabin to warn an operator if one of the systems fails ((Ref. B3.1.2), Section 3.9.1.8.b)

The design features and requirements of the parking brakes are as follows:

- The parking brakes are fail safe – The parking brakes are spring-applied with hydraulically released calipers mounted on each axle input. (*Yucca Mountain Project Engineering Specification for Cask Tractor and Cask Transfer Trailers* (Ref. B3.1.2), Section 3.9.1.9.b).
- The cask tractor and cask transfer trailer brakes are redundant and either are capable of stopping the conveyance.
- The stabilizing jacks and pendular axles are redundant vertical support systems during loading and unloading operations.
- The cask transfer trailer has four pendular axles and eight axle hydraulic actuators. The pendular axle hydraulic system can sustain one actuator failure and still function properly.
- There are four stabilizing jacks. Failure of any one of the stabilizing jacks results in the failure of the stabilizing jack system.

### B3.4.1.4 Fault Tree Model

The top event in this fault tree is “Cask Tractor and Cask Transfer Trailer Collision” (INT-HCTT-COLLISION). This top event is defined as an undesired contact at any speed between the cask tractor and cask transfer trailer with another vehicle, facility structure, or piece of equipment. Faults modeled in this tree include axle and stabilizing jack hydraulic failures and vehicle control failures.

### B3.4.1.5 Basic Event Data

A number of basic events are used in this fault tree, including two CCF events and two human failure events as listed in Table B3.4-1.

Table B3.4-1. Basic Event Probabilities for Collision of the Cask Tractor and Cask Transfer Trailer, INT-HCTT-COLLISION

Name	Description	Calc. Type <sup>a</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-BRK001--BRK-FOD	Tractor brake a fails	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
ISO-CRWT-BRK002--BRK-FOD	Tractor brake b fails	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
ISO-CRWT-BRK003--BRK-FOD	Trailer brakes fail	1	1.460E-06	1.460E-06	0.000E+00	0.000E+00
ISO-CRWT-BRKCCF--BRK-FOD	CCF of both tractor brakes	1	6.900E-08	6.900E-08	0.000E+00	1.000E+00
ISO-CRWT-LPATH--ATH-CCF	CCF of pendular axle hydraulics during load/unload	1	3.778E-05	3.778E-05	0.000E+00	0.000E+00
ISO-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	3	1.780E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	3	1.778E-03	0.000E+00	8.910E-04	2.000E+00
ISO-CRWT-LSJATH1-ATH-FOH	Stabilizing jack 1 failure	3	8.906E-04	0.000E+00	8.910E-04	1.000E+00
ISO-CRWT-LSJATH2-ATH-FOH	Stabilizing jack 2 failure	3	8.906E-04	0.000E+00	8.910E-04	1.000E+00
ISO-CRWT-LSJATH3-ATH-FOH	Actuator (hydraulic) failure	3	8.906E-04	0.000E+00	8.910E-04	1.000E+00

Table B3.4-1. Basic Event Probabilities for Collision of the Cask Tractor and Cask Transfer Trailer, INT-HCTT-COLLISION (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-LSJATH4-ATH-FOH	Stabilizing jack 4 failure	3	8.906E-04	0.000E+00	8.910E-04	1.000E+00
ISO-CRWT-TRCT-STEER-FAIL	Tractor steering system failure	1	1.000E-05	1.000E-05	0.000E+00	0.000E+00
ISO-CRWT-TRLR-STEER-FAIL	Trailer steering system failure	1	1.000E-05	1.000E-05	0.000E+00	0.000E+00
ISO-HTTCOLLIDE--G65-FOH	Speed limiter fails	3	1.160E-05	0.000E+00	1.160E-05	1.000E+00
ISO-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HCTT while leaving the facility	1	3.000E-03	3.000E-03	0.000E+00	0.000E+00
ISO-OPHTINTCOL01-HFI-NOD	Operator causes collision of HCTT due to overspeed	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00

NOTE: <sup>a</sup> 1 is direct input probability; and 3 is lambda and mission time.

Calc. = calculation; CCF = common-cause failure; HCTT = cask tractor and cask transfer trailer.

Source: Original

#### B3.4.1.5.1 Human Failure Events

Two human failure events are modeled in the cask tractor and cask transfer trailer collision failure scenario as follows:

1. Operator causes collision of the cask tractor and cask transfer trailer while leaving a facility, ISO-OPHTCOLLIDE1-HFI-NOD.
2. Operator causes collision of the cask tractor and cask transfer trailer due to over speed, ISO-OPHTINTCOL01-HFI-NOD.

Both human failure events, ISO-OPHTCOLLIDE1-HFI-NOD and ISO-OPHTINTCOL01-HFI-NOD were modeled using screening values of 3E-03 and 1, respectively.

#### B3.4.1.5.2 Common-Cause Failures

Three CCF events are modeled in the cask tractor and cask transfer trailer collision failure scenario as follows:

1. CCF of the primary and redundant tractor brakes, ISO-CRWT-BRKCCF--BRK-FOD.
2. CCF of two or more pendular axle hydraulics, ISO-CRWT-LPATH--ATH--CCF.

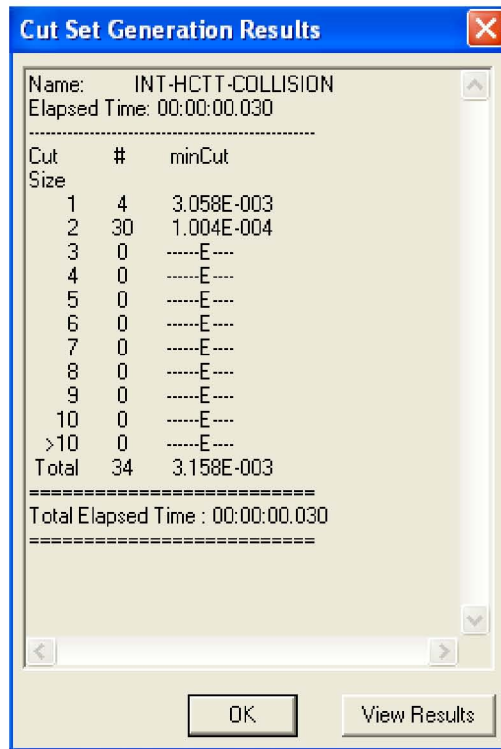
### B3.4.1.6 Uncertainty and Cut Set Generation Results

Figure B3.4-1 contains the uncertainty results obtained from running the fault trees for the cask tractor and cask transfer trailer collision. Figure B3.4-2 provides the cut set generation results for the cask tractor and cask transfer trailer collision tree.

Uncertainty Results			
Name	INT-HCTT-COLLISION		
Random Seed	1234	Events	16
Sample Size	10000	Cut Sets	34
Point estimate	3.158E-003		
Mean Value	4.659E-003		
5th Percentile Value	4.499E-004		
Median Value	2.113E-003		
95th Percentile Value	1.116E-002		
Minimum Sample Value	9.589E-005		
Maximum Sample Value	9.584E-001		
Standard Deviation	2.470E-002		
Skewness	2.693E+001		
Kurtosis	8.729E+002		
Elapsed Time	00:00:01.030		
<input type="button" value="OK"/>			

Source: Original

Figure B3.4-1. Uncertainty Results for the Cask Tractor and Cask Transfer Trailer Collision Fault Tree INT-HCTT-COLLISION



Source: Original

Figure B3.4-2. Cut Set Generation Results for Cask Tractor and Cask Transfer Trailer Collision Fault Tree INT-HCT-COLLISION

### B3.4.1.7 Cut Sets

Table B3.4-2 contains the top 20 cut sets generated for the collision of the cask tractor and cask transfer trailer, representing nearly 99% of the total system failure probability.

Table B3.4-2. Cut Sets for Collision of Cask Tractor and Cask Transfer Trailer (INT-HCTT-COLLISION)

% Total	% Cut Set	Probability/Frequency	Basic Event	Description	Event Probability
95.01	95.01	3.000E-03	ISO-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HCTT while leaving the facility	3.000E-03
96.21	1.20	3.778E-05	ISO-CRWT-LPATH--ATH--CCF	CCF of pendular axle hydraulics during load/unload	3.778E-05
96.58	0.37	1.160E-05	ISO-HTTCOLLIDE---G65-FOH	Sped limiter fails	1.160E-05
			ISO-OPHTINTCOL01-HFI-NOD	Operator causes collision of HCTT due to over speed	1.000E+00
96.90	0.32	1.000E-05	ISO-CRWT-TRCT-STEER-FAIL	Tractor steering system failure	1.000E-05
97.22	0.32	1.000E-05	ISO-CRWT-TRLR-STEER-FAIL	Trailer steering system failure	1.000E-05
97.32	0.10	3.170E-06	ISO-CRWT-LPATH7--ATH-FOH	Pendular axle hydraulic 7 failure	1.780E-03



Table B3.4-2. Cut Sets for Collision of Cask Tractor and Cask Transfer Trailer (INT-HCTT-COLLISION)  
(Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.42	0.10	3.170E-06	ISO-CRWT-LPATH6--ATH-FOH	Pendular axle hydraulic 6 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.52	0.10	3.170E-06	ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.62	0.10	3.170E-06	ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.72	0.10	3.170E-06	ISO-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.82	0.10	3.170E-06	ISO-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
97.92	0.10	3.170E-06	ISO-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-03
			ISO-CRWT-LPATH8--ATH-FOH	Pendular axle hydraulic 8 failure	1.780E-03
98.02	0.10	3.170E-06	ISO-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-03
			ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-03
98.12	0.10	3.170E-06	ISO-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-03
			ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-03
98.22	0.10	3.170E-06	ISO-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-03
			ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-03
98.32	0.10	3.170E-06	ISO-CRWT-LPATH4--ATH-FOH	Pendular axle hydraulic 4 failure	1.780E-03
			ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-03
98.42	0.10	3.170E-06	ISO-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-03
			ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-03

Table B3.4-2. Cut Sets for Collision of Cask Tractor and Cask Transfer Trailer (INT-HCTT-COLLISION)  
(Continued)

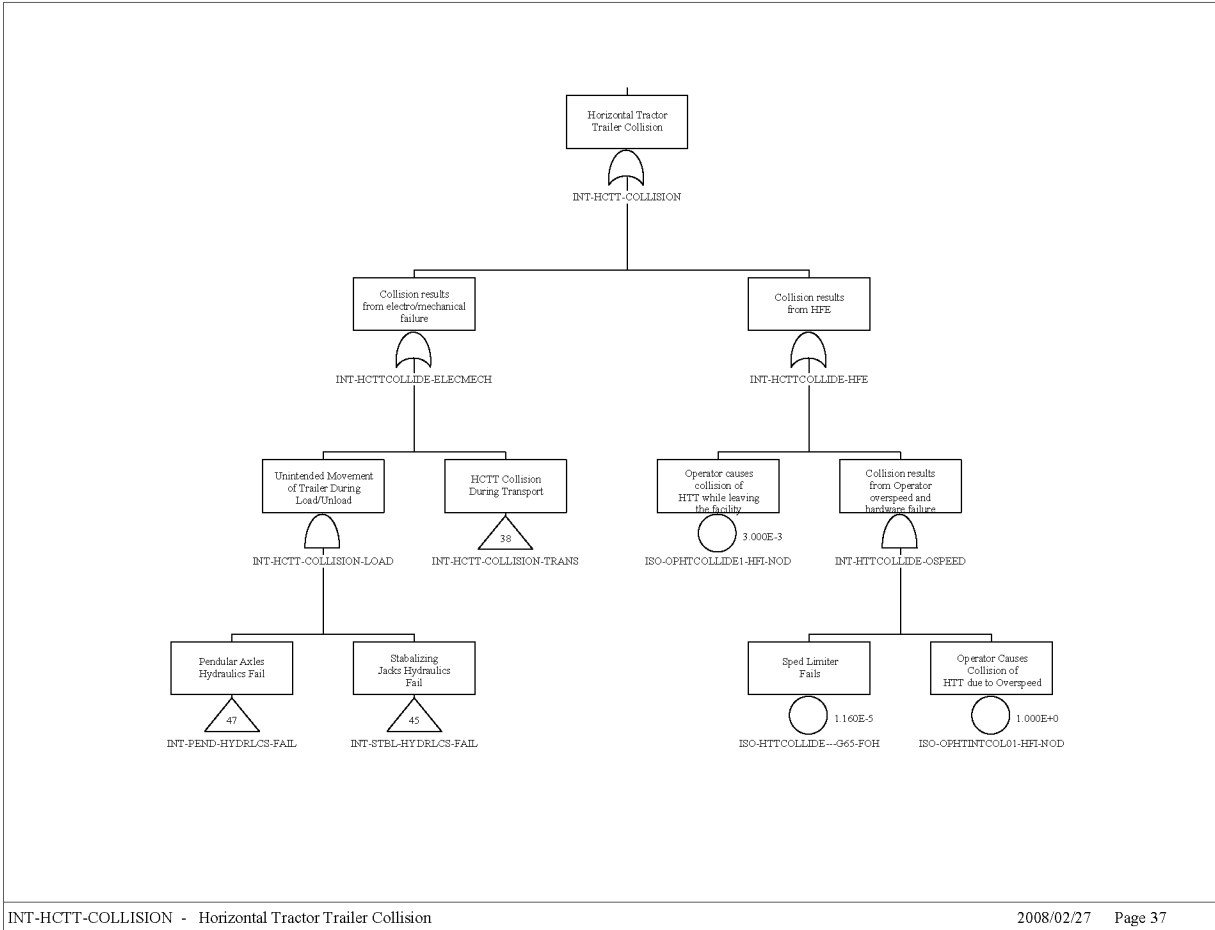
<b>% Total</b>	<b>% Cut Set</b>	<b>Probability/ Frequency</b>	<b>Basic Event</b>	<b>Description</b>	<b>Event Probability</b>
98.52	0.10	3.170E-06	ISO-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-03
			ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-03
98.62	0.10	3.170E-06	ISO-CRWT-LPATH1--ATH-FOH	Pendular axle hydraulic 1 failure	1.780E-03
			ISO-CRWT-LPATH5--ATH-FOH	Pendular axle hydraulic 5 failure	1.780E-03
98.72	0.10	3.170E-06	ISO-CRWT-LPATH2--ATH-FOH	Pendular axle hydraulic 2 failure	1.780E-03
			ISO-CRWT-LPATH3--ATH-FOH	Pendular axle hydraulic 3 failure	1.780E-03

NOTE: CCF = common-cause failure; HCTT = cask tractor and cask transfer trailer; No. = number.

Source: Original

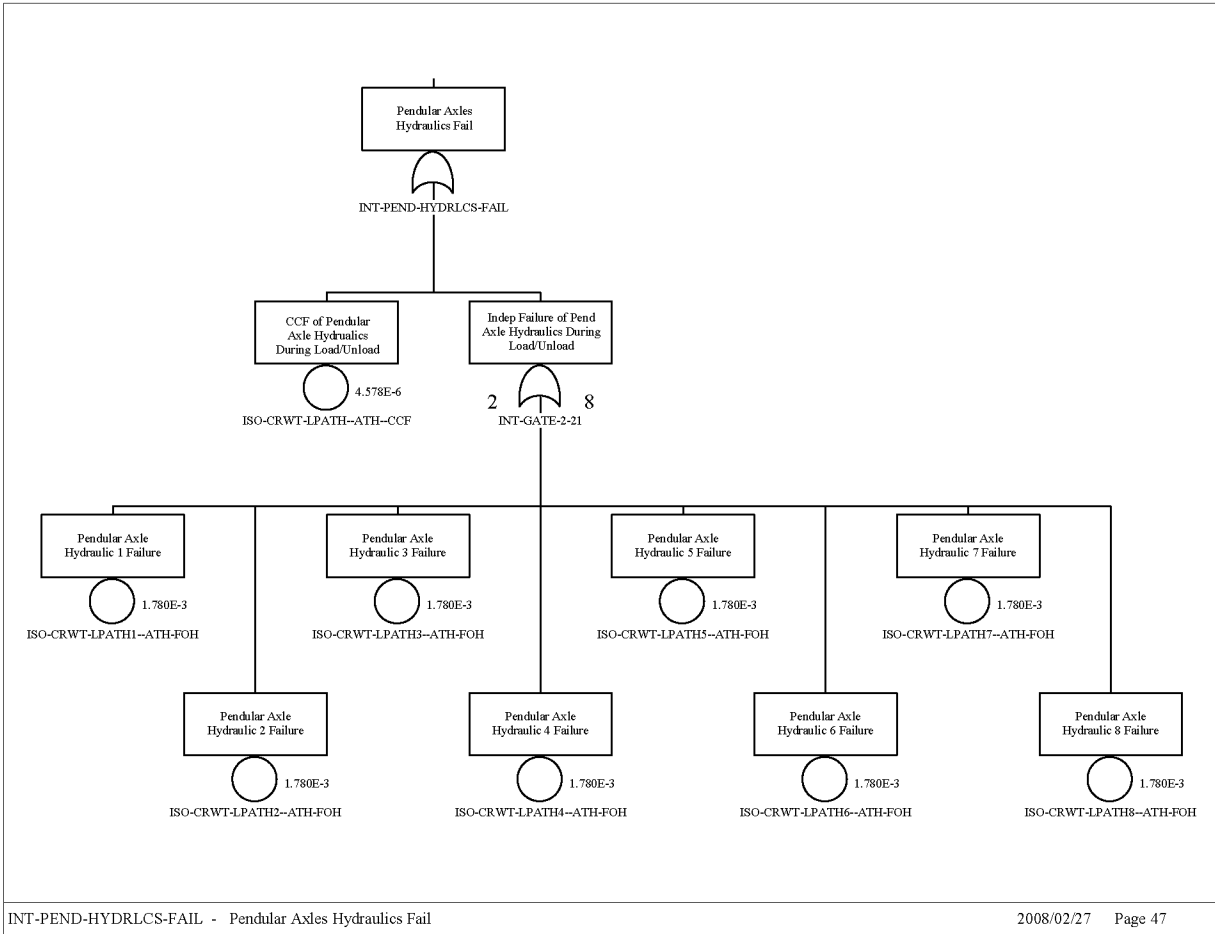
### B3.4.1.8 Fault Trees

The fault tree for the cask tractor and cask transfer trailer collision is presented in Figures B3.4-3 through B3.4-7.



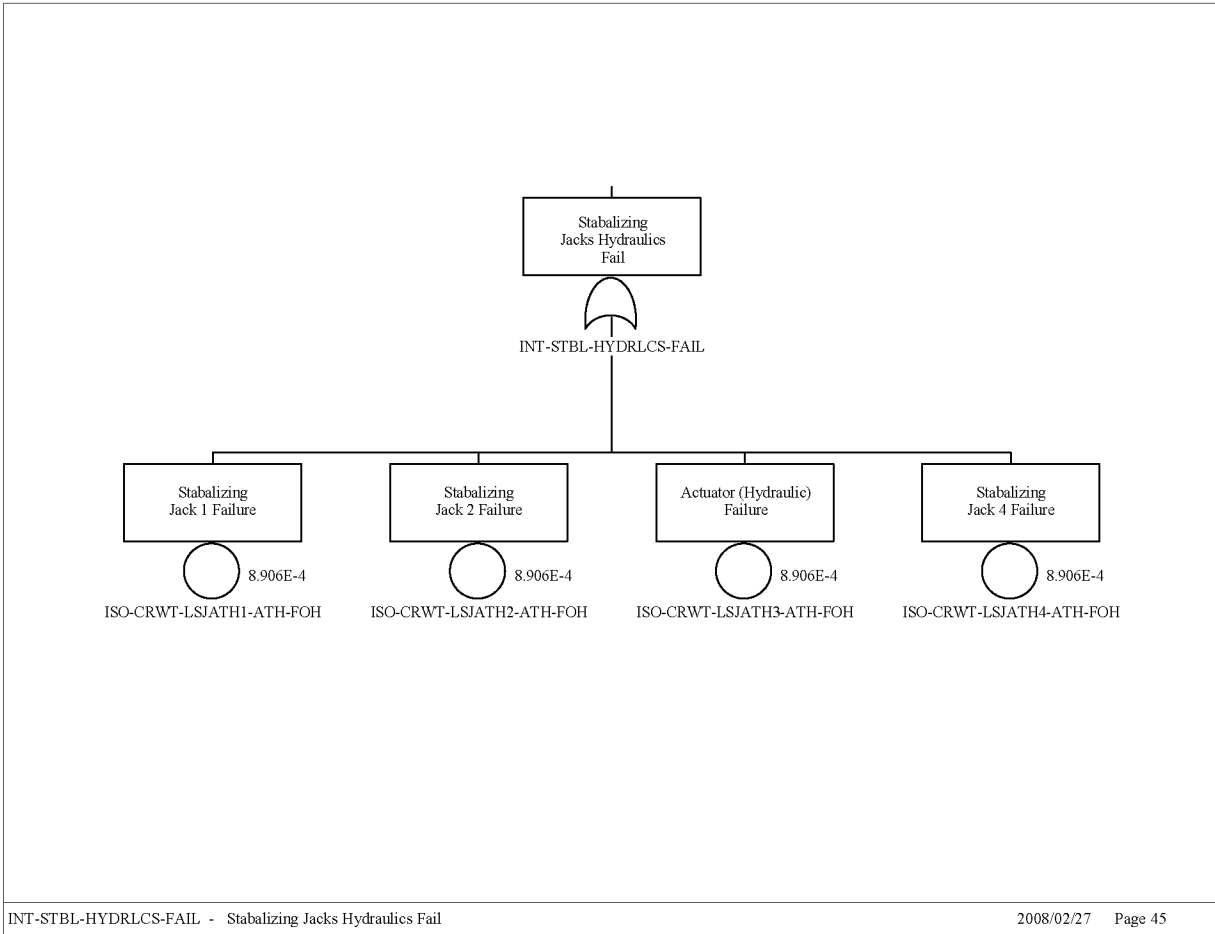
Source: Original

Figure B3.4-3. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION)  
Sheet 1 of 5



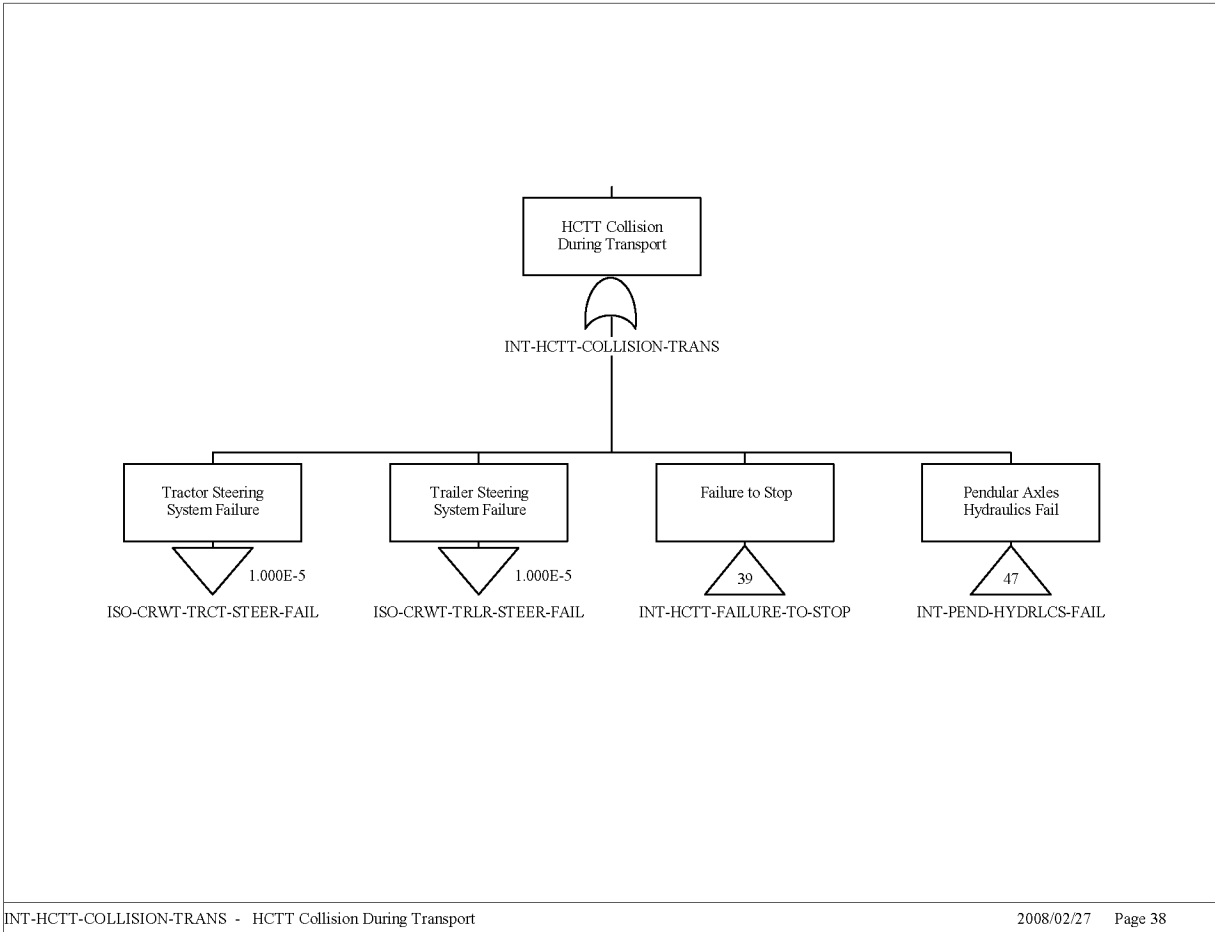
Source: Original

Figure B3.4-4. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION)  
Sheet 2 of 5



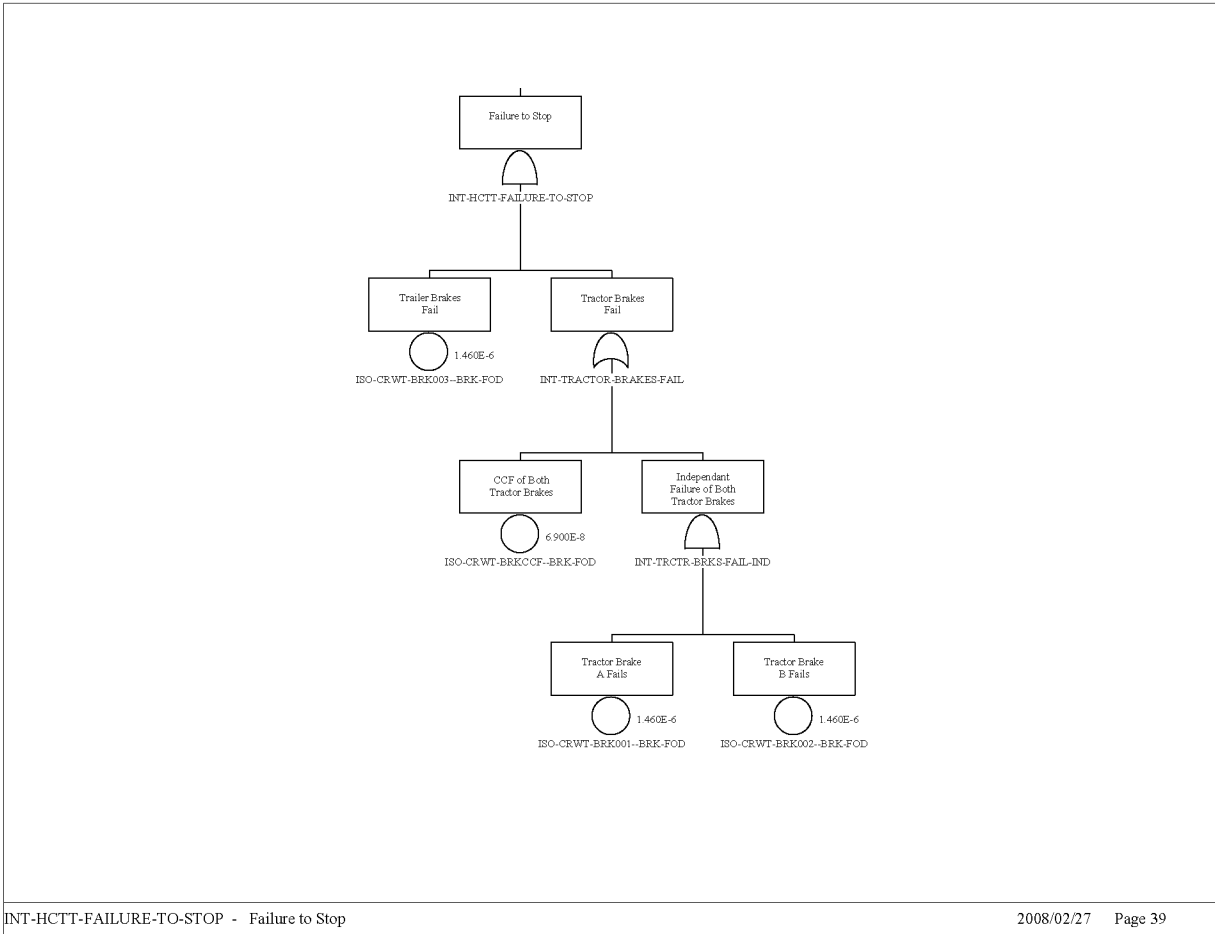
Source: Original

Figure B3.4-5. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION)  
Sheet 3 of 5



Source: Original

Figure B3.4-6. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION)  
Sheet 4 of 5



Source: Original

Figure B3.4-7. Fault Tree for Cask Tractor and Cask Transfer Trailer Collision (INT-HCTT-COLLISION)  
Sheet 5 of 5

## B4 ADDITIONAL FAULT TREES

Eleven additional fault trees were developed to address events that could impact Intra-Site Operations. These fault trees are identified in Table B4-1. All of these trees are top level trees; the results of quantifying these trees were input directly into the EXCEL spreadsheet used to quantify Intra-Site Operations event sequences as initiating events. Some provide the link between the top level events in the event trees and the system fault trees described in Sections B1 through B3. This relationship is identified in Table B4-1.

Table B4-1. Top Level and Linking Fault Trees

Fault Tree	Description	Events considered	System Fault Trees Used as Input
INTRASITE-PMRC-COLLIDE	SPMRC collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMRC-COLLISION (B1.4.1)
INTRASITE-DETRAIL	SPMRC derails during transit from receipt area to facility	SPMRC derailment	None
INTRASITE-PMTT-COLLIDE	SPMTT collisions during transport of a TC from receipt area to facility	Collisions during transit or with facility door	INT-1-SPMTT-COLLISION (B1.4.2)
INTRASITE-JIB-CRANE	Drop of heavy load onto TC during receipt processing and transit to facility	Crane drops onto TC	None
INTRASITE-ST-COLLIDE	ST collisions in transport of Aging Overpack from facility to Aging Facility	Collisions during transit or with facility door	INT-2-ST-COLLISION (B2.4)
INTRASITE-HCTT-COLLISION	HCTT collisions in transport of horizontal casks from facility to Aging Facility	HCTT collision during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HCTT-DROP	HCTT drops in transport of horizontal casks from facility to Aging Facility	HCTT drops during transport and set up at Aging Facility	INT-HCTT-COLLISION (B3.4)
INTRASITE-HAM-INSERT	Canister damaged during insertion into HAM	Operator or equipment failure during canister insertion into HAM	None
INTRASITE-HAM-AUX-EQUIPMENT	HAM damaged during canister loading/unloading operations	Impacts from crane operation	None
INTRASITE-HEPA-TRANSFER	Damage to LLW during transit from WHF to LLWF or offsite	Vehicle collisions during transit	None
INTRASITE-COLL-TRANSFER	Damage to LLW during transit from WHF to LLWF	Forklift or vehicle collisions during transit	None

NOTE: HAM = horizontal aging module; HCTT = cask tractor and cask transfer trailer; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer; ST = site transporter; TC = transportation cask; WHF = Wet Handling Facility.

Source: Original

The basic events used in each of these additional fault trees are provided in Table B4-2.



Table B4-2. Basic Events for Additional Fault Trees

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
DISTANCE	Distance from receipt area to facility	V	2.000E+00	2.000E+00	0.000E+00	0.000E+00
ISO-DISTANCE--TO--LLWF	Distance from facilities to LLWF	V	2.000E+00	2.000E+00	0.000E+00	0.000E+00
ISO-HAM-IMPACT-1	Crane impact at HAM due to crane failure -1	1	2.600E-05	2.600E-05	0.000E+00	0.000E+00
ISO-HAM-IMPACT-2	Crane impact at HAM due to crane failure-2	1	2.600E-05	2.600E-05	0.000E+00	0.000E+00
ISO-HAM-IMPACT-3	Crane impact at HAM due to crane failiure-3	1	2.600E-05	2.600E-05	0.000E+00	0.000E+00
ISO-HAM-RAM-INSERT	Motor (hydraulic) failure	3	5.389E-04	0.000E+00	5.390E-04	1.000E+00
ISO-HEPA-XFER-L-FORKLIFT	Puncture of drum at LLWF	1	1.200E-05	1.200E-05	0.000E+00	0.000E+00
ISO-HTC-MOVER-COLL-DROP	Split movement results between collision and drop	1	5.000E-01	5.000E-01	0.000E+00	0.000E+00
ISO-OP-HAM-INSERT-HFI-NOD	Operator misaligns transport and HAM opening	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
ISO-OP-HAMIMPACT-HFI-NOD	Operator causes HAM impact with crane	1	3.000E-03	3.000E-03	0.000E+00	0.000E+00
ISO-PMRC-DERAIL-PER-MILE	Derailment of a railcar per mile	1	1.180E-05	1.180E-05	0.000E+00	0.000E+00
ISO-OP-SICOMPDROP-HFI-NOD	Operator drops object onto TC <sup>b</sup>	1	0.000E+00	0.000E+00	0.000E+00	0.000E+00
ISO-VEH-COLISION-COL-RAT	Vehicle collision rate per mile	1	7.000E-07	7.000E-07	0.000E+00	0.000E+00
ISO-VEH-ONSITE-BUFFER	Distance from buffer area to facilities	V	2.000E+00	2.000E+00	0.000E+00	0.000E+00
ISO-VEH-ONSITE-MILES	Distance between facility and Aging Facility	V	2.000E+00	2.000E+00	0.000E+00	0.000E+00

NOTE: <sup>a</sup> V is a scalar value; 1 is direct input probability; and 3 is lambda and mission time.

<sup>b</sup> Operator event is addressed as part of the generic jib crane drop data.

Calc. = calculation; Fail. = failure; HAM = horizontal aging module; LLWF = Low-Level Waste Facility; Miss. = mission; Prob. = probability; TC = transportation cask.

Source: Original

The resulting parameters that defined the distribution for each initiating event are provided in Table B4-3.

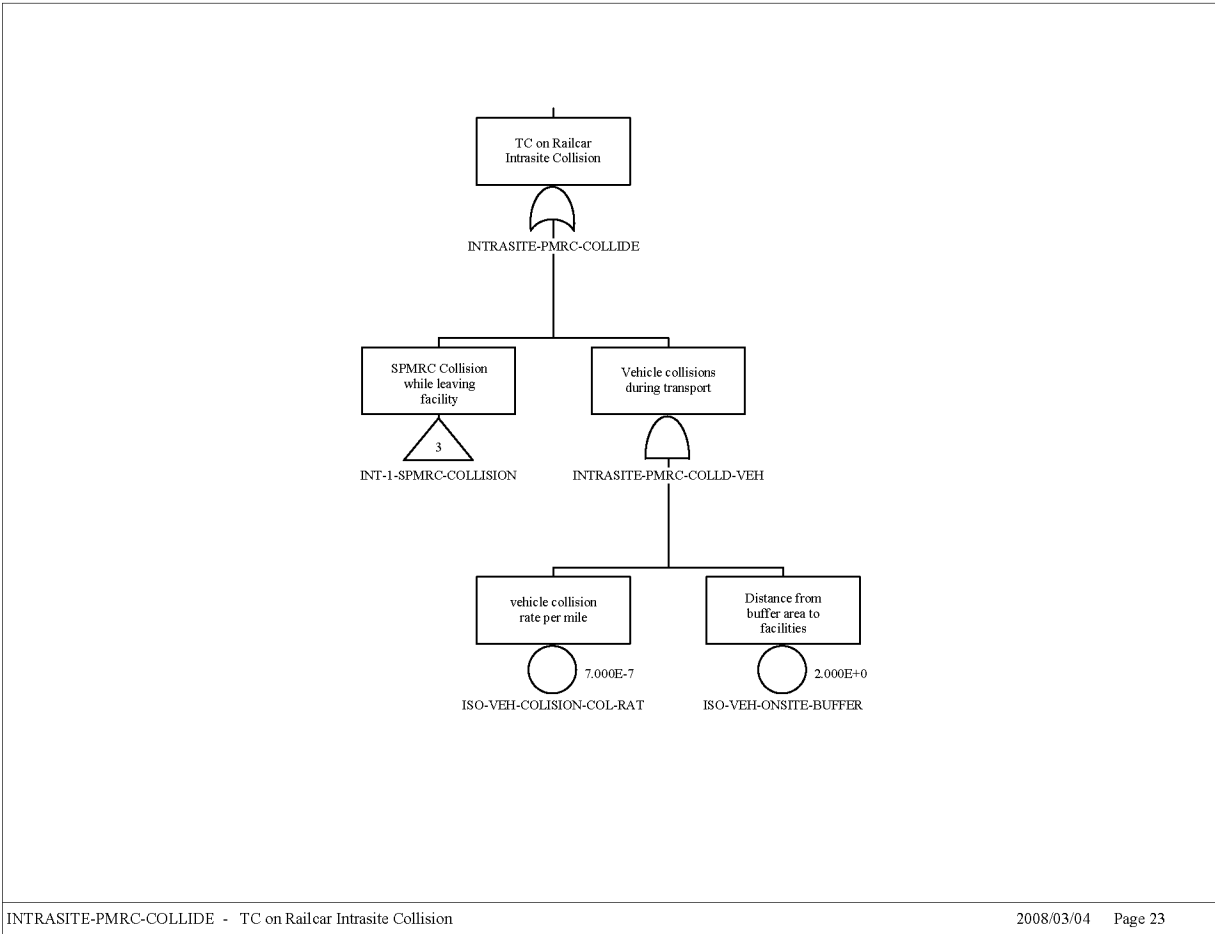
Table B4-3. Resulting Distribution Parameters Used in Quantification Spreadsheet

Fault Tree Name	Mean <sup>a</sup>	Median <sup>a</sup>	Std. Dev. <sup>a</sup>
INTRASITE-COLL-TRANSFER	1.00E-05	8.00E-06	2.00E-05
INTRASITE-DERAIL	2.00E-05	2.00E-05	3.00E-06
INTRASITE-HAM-AUX-EQUIP	3.00E-03	1.00E-03	7.00E-03
INTRASITE-HAM-INSERT	2.00E-03	9.00E-04	2.00E-03
INTRASITE-HCTT-COLLISION	3.00E-03	1.00E-03	2.00E-02
INTRASITE-HCTT-DROP	3.00E-03	1.00E-03	2.00E-02
INTRASITE-HEPA-TRANSFER	1.00E-06	5.00E-07	3.00E-06
INTRASITE-JIB-CRANE	3.00E-05	2.00E-05	2.00E-05
INTRASITE-SPMRC-COLLIDE	4.00E-03	2.00E-03	2.00E-02
INTRASITE-SPMTT-COLLIDE	4.00E-03	2.00E-03	1.00E-02
INTRASITE-ST-AO-DROP	4.00E-08	2.00E-08	1.00E-07
INTRASITE-ST-COLLIDE	5.00E-03	2.00E-03	1.00E-03

NOTE: <sup>a</sup> Values are rounded to one significant figure.  
Std. Dev. = standard deviation.

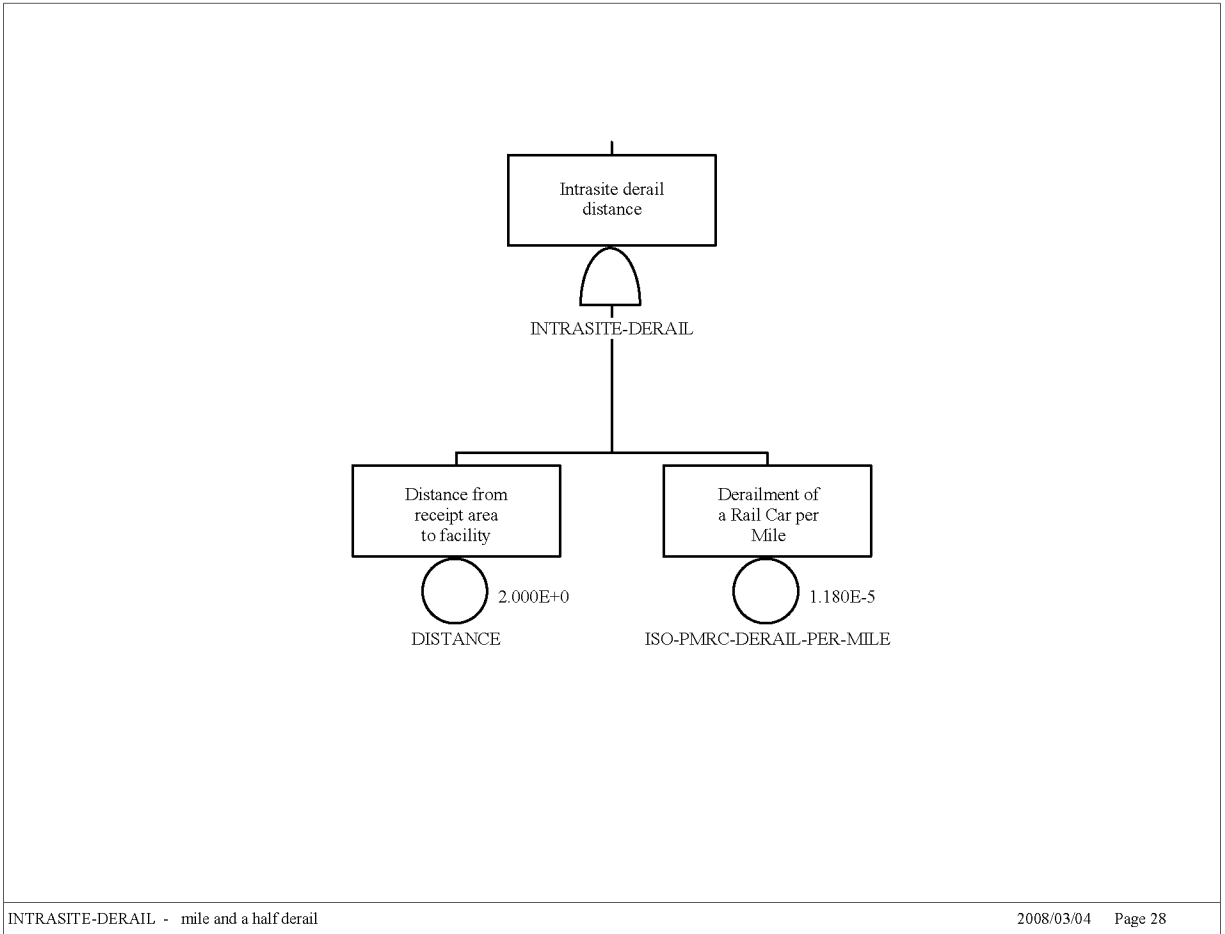
Source: Original

The eleven additional fault trees are presented in Figures B4-1 through B4-11.



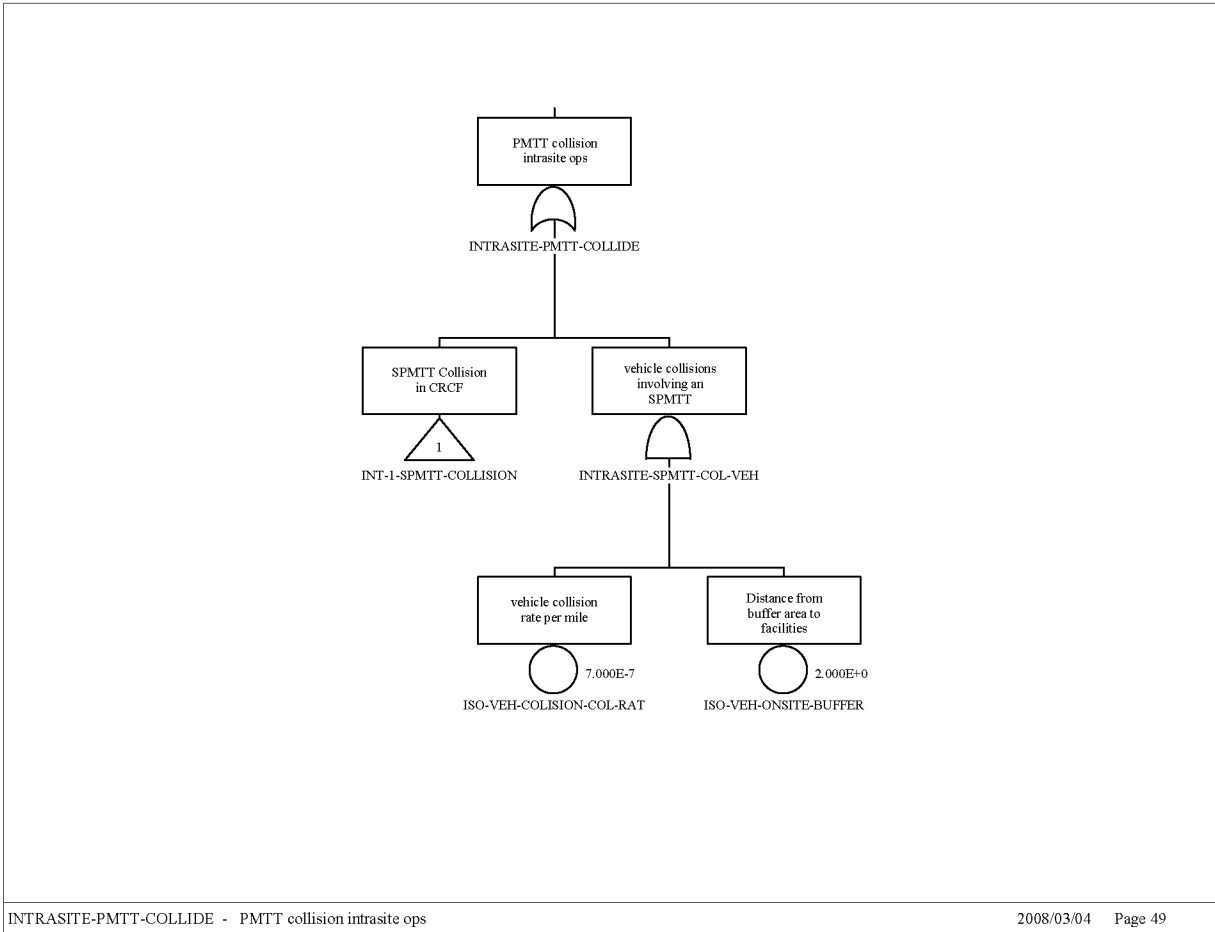
Source: Original

Figure B4-1. Fault Tree for INTRASITE-PMRC-COLLIDE



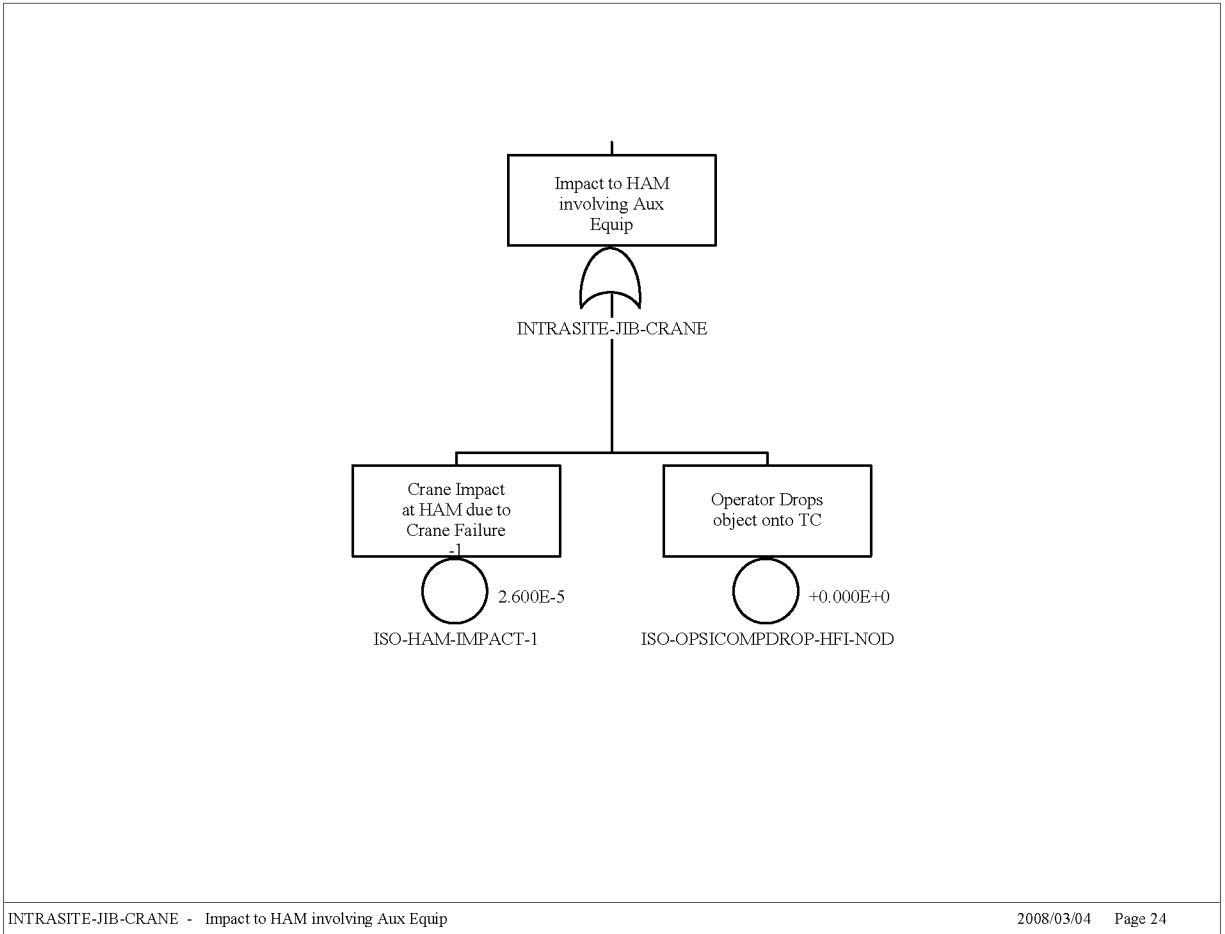
Source: Original

Figure B4-2. Fault Tree for INTRASITE-DETRAIL



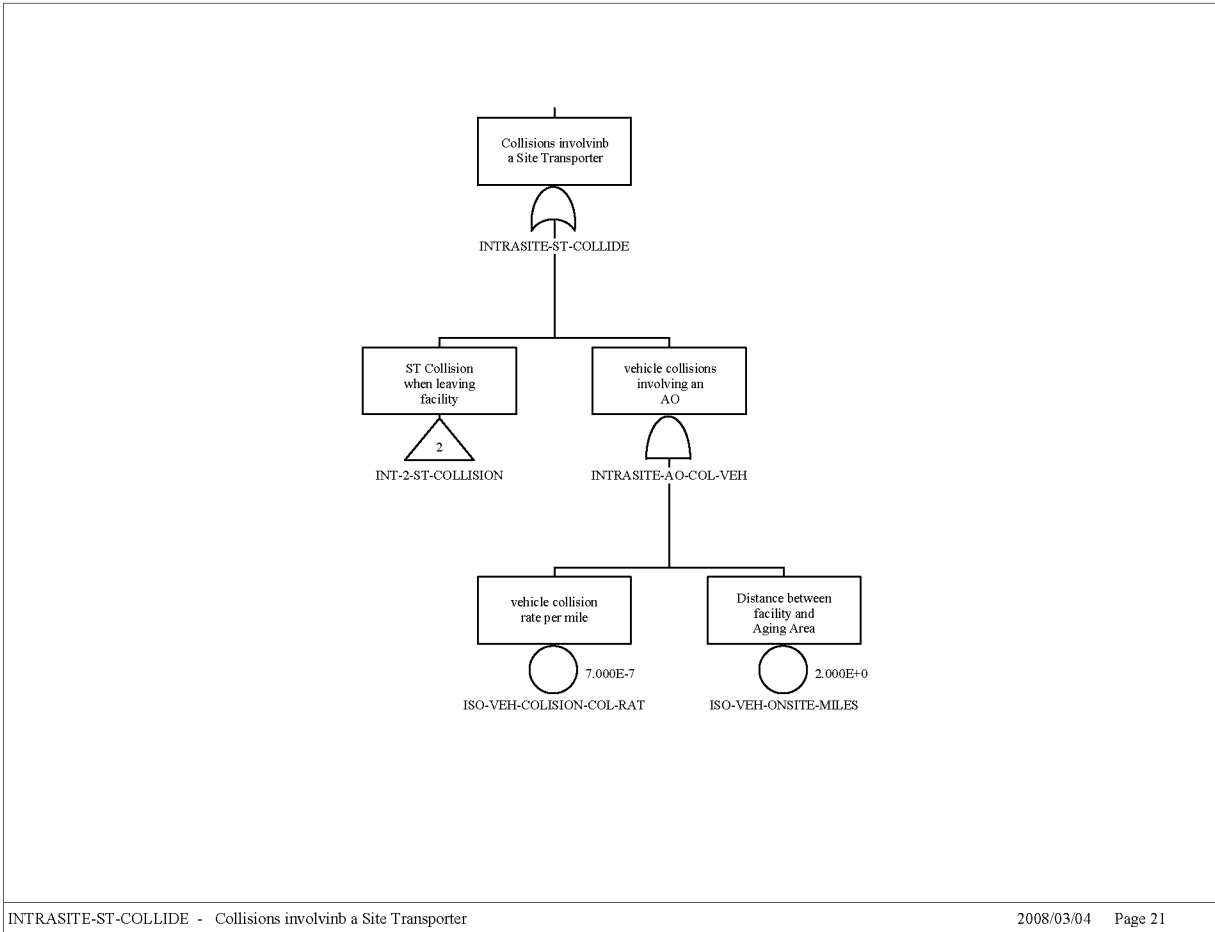
Source: Original

Figure B4-3. Fault Tree for INTRASITE-PMITT-COLLIDE



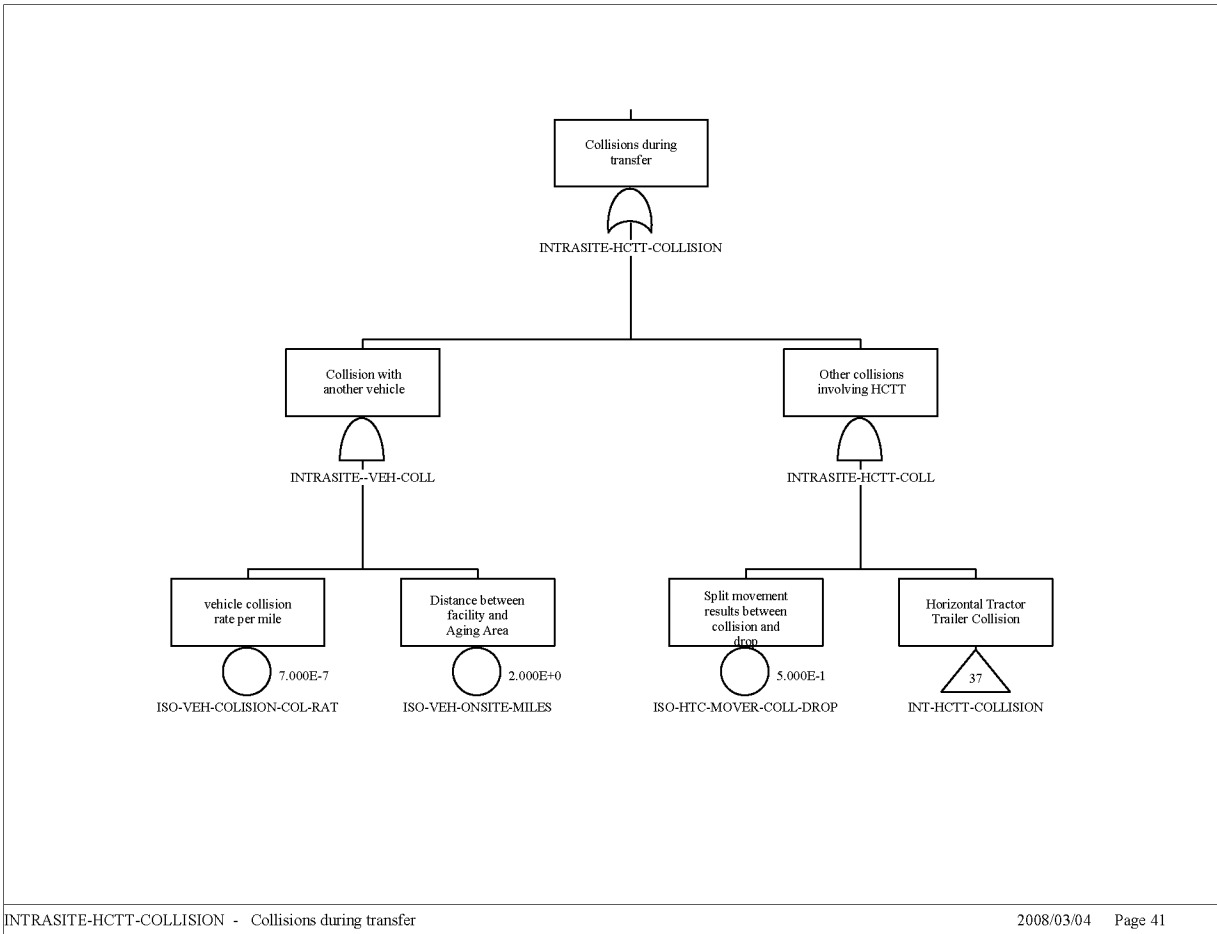
Source: Original

Figure B4-4. Fault Tree for INTRASITE-JIB-CRANE



Source: Original

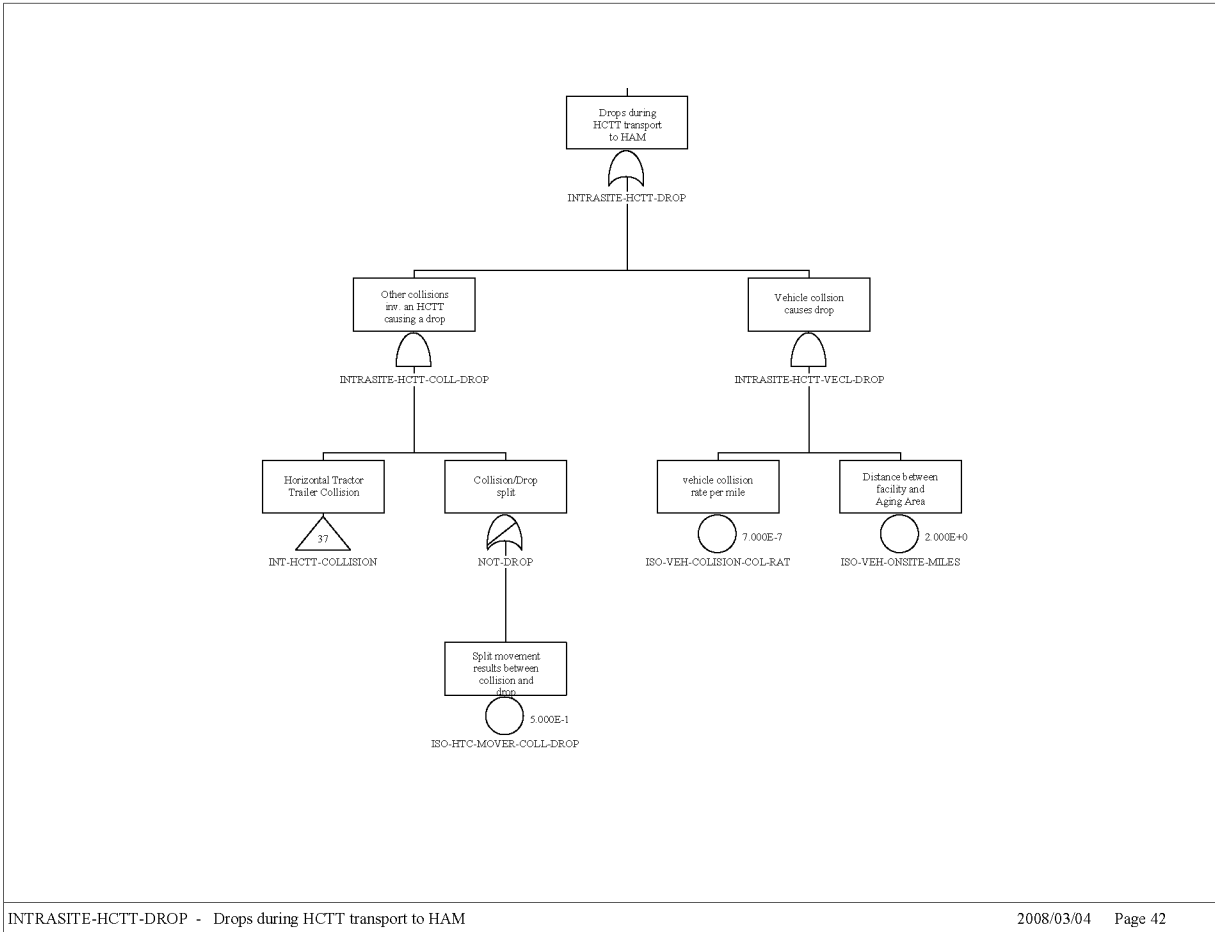
Figure B4-5. Fault Tree for INTRASITE-ST-COLLIDE



Source: Original

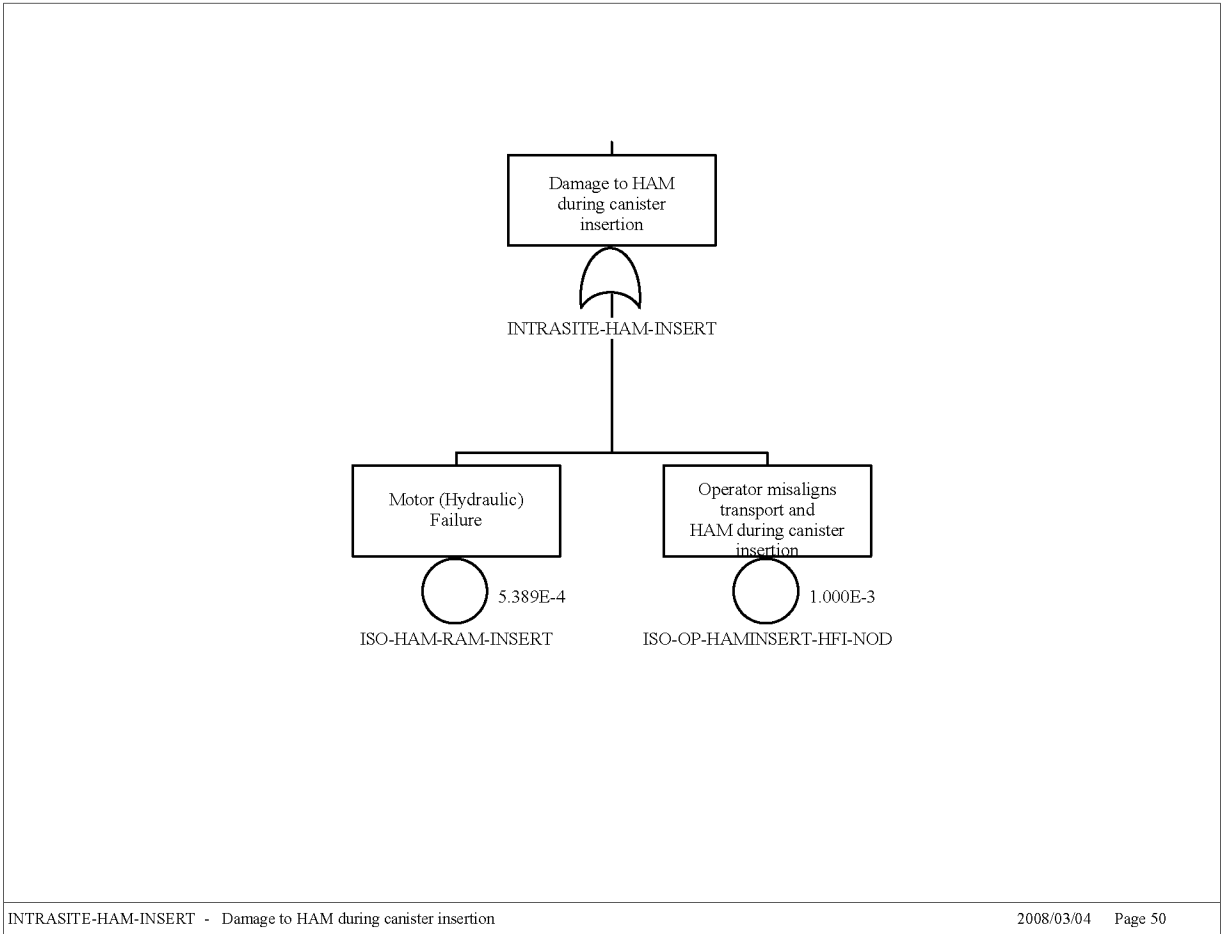
Figure B4-6. Fault Tree for INTRASITE-HCTT-COLLISION





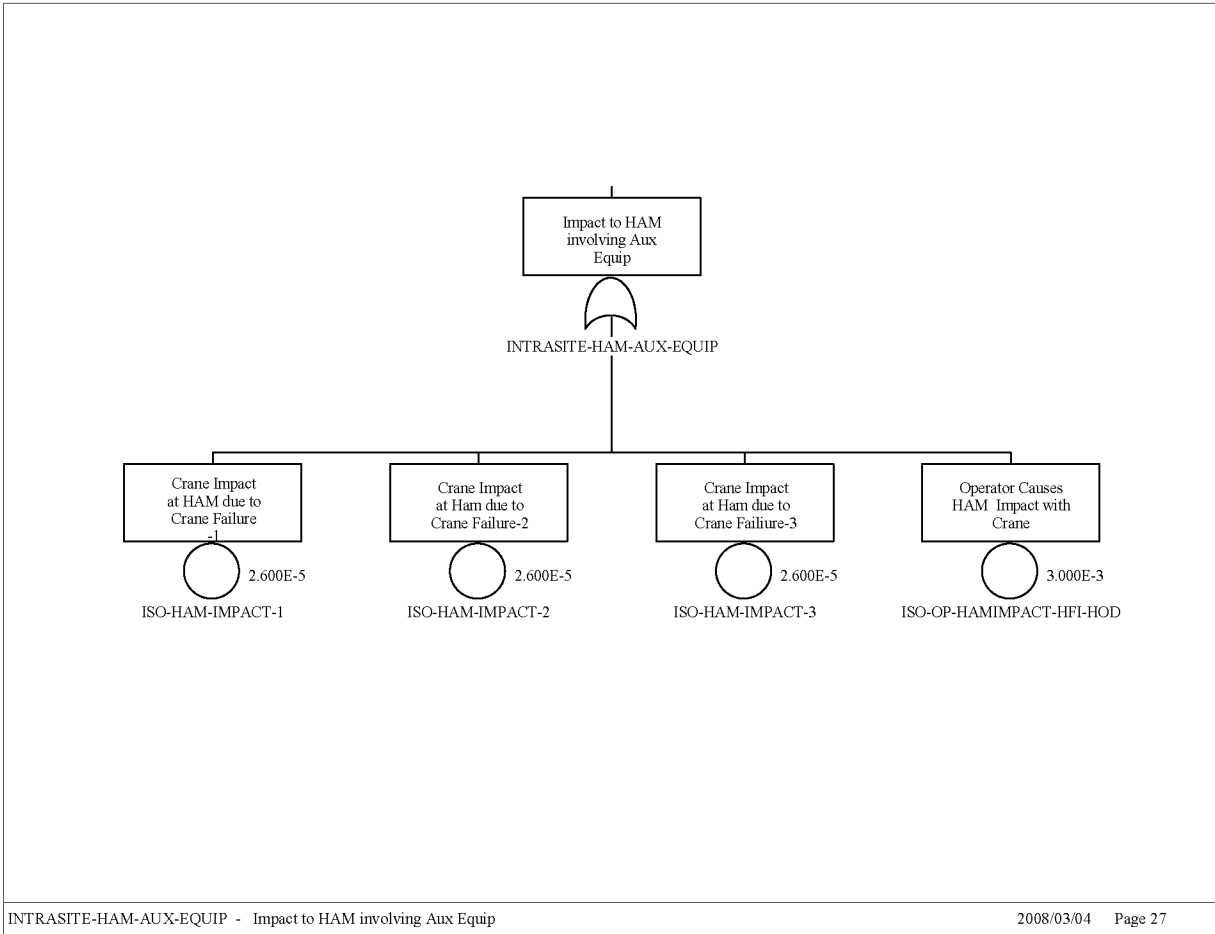
Source: Original

Figure B4-7. Fault Tree for INTRASITE-HCTT-DROP



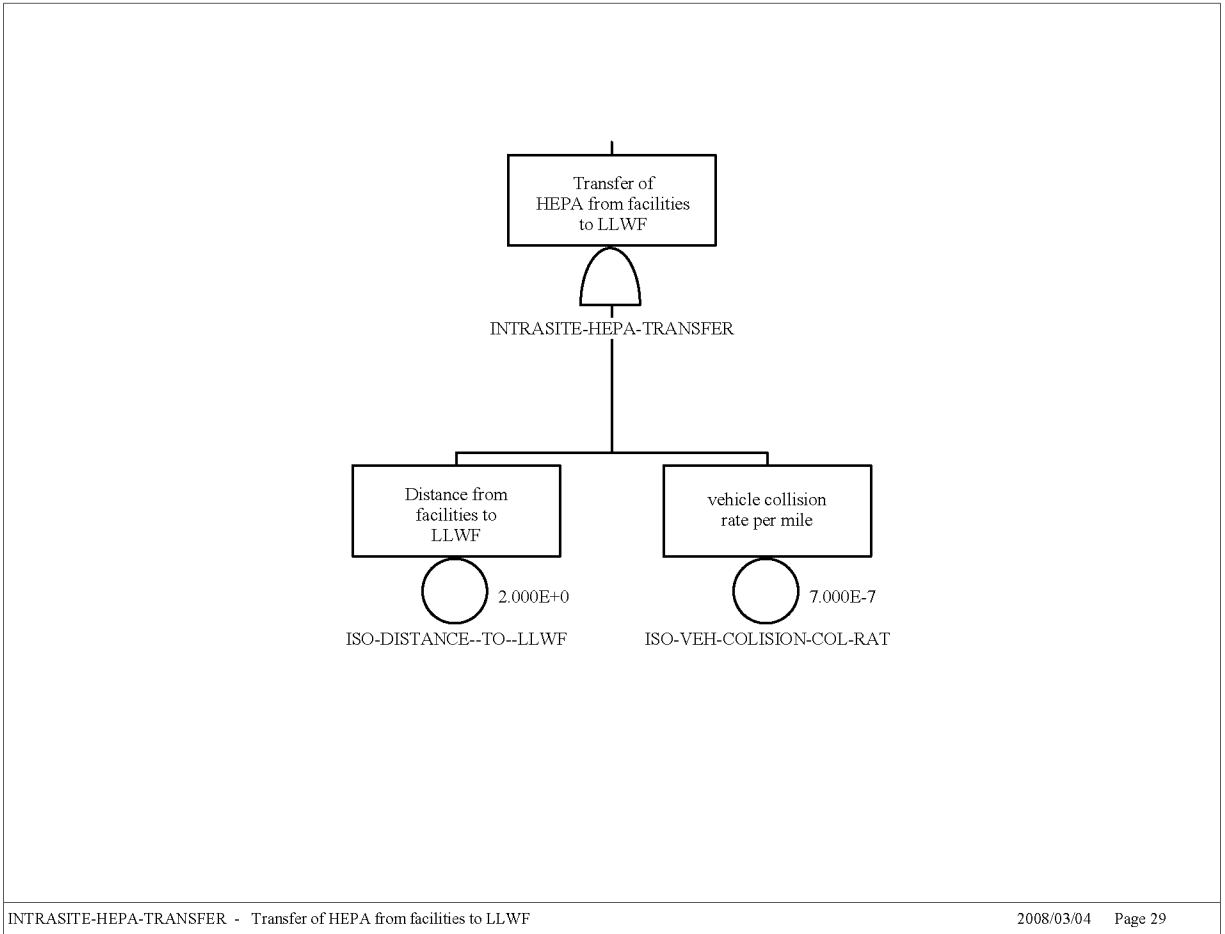
Source: Original

Figure B4-8. Fault Tree for INTRASITE-HAM-INSERT



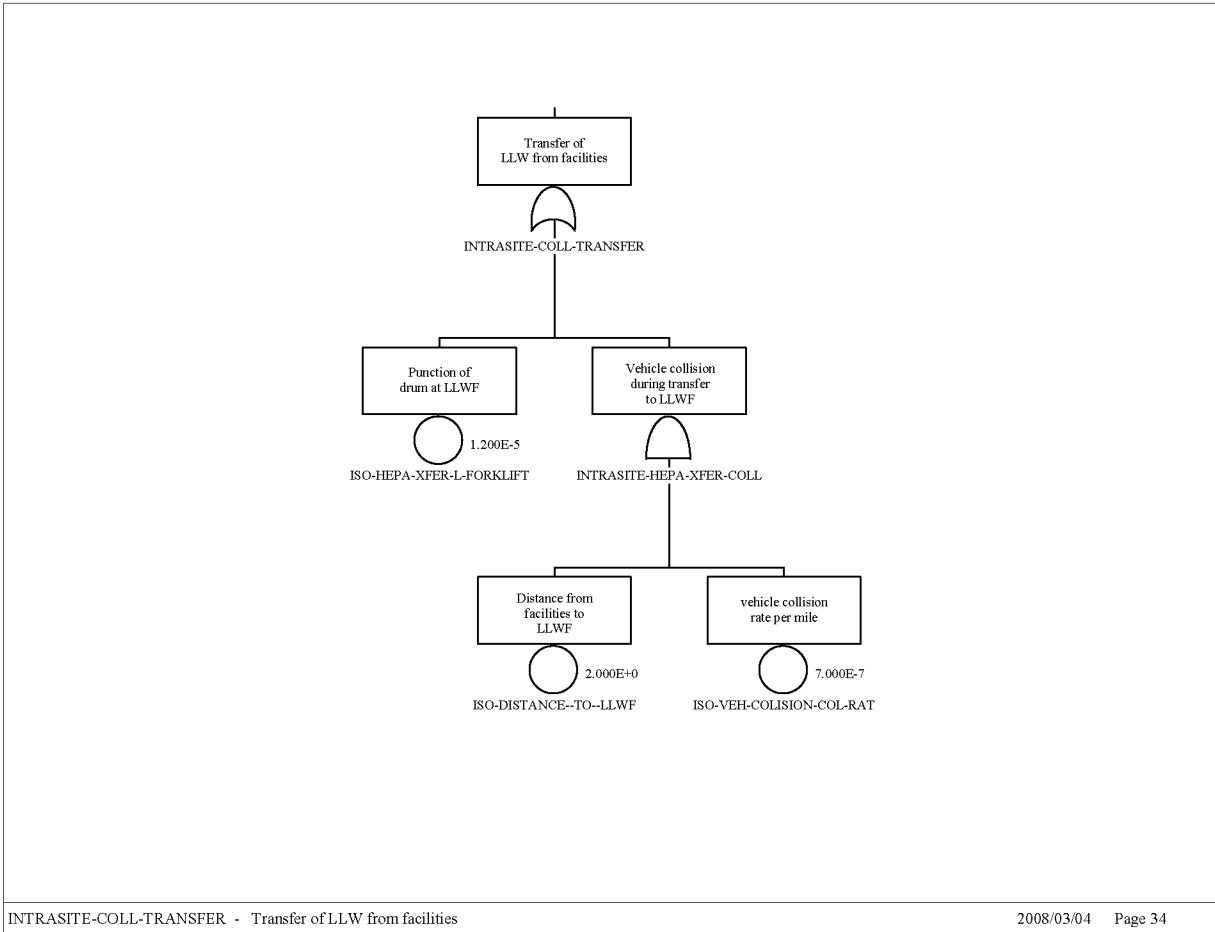
Source: Original

Figure B4-9. Fault Tree for INTRASITE-HAM-AUX-EQUIPMENT



Source: Original

Figure B4-10. Fault Tree for INTRASITE-HEPA-TRANSFER



Source: Original

Figure B4-11. Fault Tree for INTRASITE-COLL-TRANSFER

**ATTACHMENT C**  
**ACTIVE COMPONENT RELIABILITY DATA ANALYSIS**

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	C-5
C1 INDUSTRY-WIDE COMPONENT RELIABILITY DATA .....	C-6
C1.1 COMPONENT DEFINITION .....	C-6
C1.2 INDUSTRY-WIDE RELIABILITY DATA .....	C-13
C1.3 CRANE AND SPENT FUEL TRANSFER MACHINE DROP ESTIMATES .....	C-18
C2 BAYESIAN DATA COMBINATION .....	C-21
C2.1 PARAMETER ESTIMATION USING DATA FROM DIFFERENT SOURCES .....	C-23
C2.2 PARAMETER ESTIMATION IN CASE ONLY ONE DATA SOURCE IS AVAILABLE .....	C-30
C3 COMMON CAUSE FAILURE DATA .....	C-31
C4 ACTIVE COMPONENT RELIABILITY ESTIMATES INPUT TO SAPHIRE .....	C-34
C5 REFERENCES; DESIGN INPUTS .....	C-47

## FIGURES

	<b>Page</b>
C2.1-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line) .....	C-30
C3-1. Alpha Factor.....	C-32



**TABLES**

	<b>Page</b>
C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM).....	C-9
C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database .....	C-13
C1.2-2. Data Source Comparison for Check Valve .....	C-16
C1.2-3. Failure Rates Extracted from Various Data Sources for Check Valve.....	C-17
C1.2-4. Guidelines for Industry-wide Data Selection.....	C-17
C2.1-1. Comparison of Results of Parametric Empirical Bayes and Results Reported by Lopez Droguett et al.....	C-25
C3-1. Alpha Factor Table .....	C-33
C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models .....	C-36

## ACRONYMS AND ABBREVIATIONS

### Acronyms

CCF	common-cause failure
CTM	canister transfer machine
CTT	cask transfer trolley
DOE	U.S. Department of Energy
GROA	geologic repository operations area
HEPA	high-efficiency particulate air filter
HLW	high-level radioactive waste
HVAC	heating, ventilation, and air conditioning
MCC	motor control centers
MCO	multicanister overpack
NRC	U.S. Nuclear Regulatory Commission
PCSA	Preclosure Safety Analysis
PRA	probabilistic risk assessment
SFTM	spent fuel transfer machine
SNF	spent nuclear fuel
TEV	transport and emplacement vehicle
TYP	component type code
TYP-FM	component type and failure mode code
UPS	uninterruptible power supply
YMP	Yucca Mountain Project

### Abbreviations

AC	alternating current
DC	direct current
hr	hour

## **ATTACHMENT C**

### **ACTIVE COMPONENT RELIABILITY DATA ANALYSIS**

The purpose of component-level reliability data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. In this report, the term data is taken to mean reliability data analyzed as part of the preclosure safety analysis (PCSA) from published sources. The fault tree models described in Section 4.3.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. This attachment provides a summary of the approach for developing these active component reliability estimates by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represented the range of the industry-wide information. The discussion also addresses the method used for estimating the probability of common-cause failures among multiple components. Finally, a table is given showing the template data values input to the Yucca Mountain Project (YMP) PCSA SAPHIRE models (Section 4.2).

#### **C1 INDUSTRY-WIDE COMPONENT RELIABILITY DATA**

While data from the facility being studied is the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP activities are atypical of nuclear power plant activities and no operating history exists, it was necessary to develop the required data from the experience of other industries.

##### **C1.1 COMPONENT DEFINITION**

The purpose of component-level data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. To do this, it is necessary to clearly define component types, boundaries, and failure modes. The system analysis fault tree basic events identify the component and failure mode combinations requiring data, and the analysts' descriptions provide an understanding of the component operating environments. In response to these identified data needs, the data analysts compile data at the component failure mode level for input to the SAPHIRE models. However, this is best achieved via an iterative process between the system and data analysts to ensure that all basic events are properly quantified with appropriate failure data estimates.

1. **Component Type.** Corresponds to the category of equipment at the level for which data is required by the logic model and at which data will be developed by the data analyst. Examples of such component types are motor-driven pumps, cameras, diesel generators, and heat exchangers. For certain complex components, a larger component type such as the canister transfer machine (CTM) is likely to be broken down by the system analyst in the logic model into constituent component types including motors and brakes, not only to facilitate the data analysis but to evaluate the contribution of various subcomponents to the overall component failure.

2. **Component Boundaries.** The boundary definition task is closely connected with the tasks of defining systems boundaries and fault tree construction. Therefore this task is performed jointly with the system analysts.
3. **Failure Mode.** Failure mode is defined as an undesirable component state (e.g., normally closed motor operated valve doesn't open on demand because of valve mechanical damage that occurred before the demand itself).
4. **Selection of Model and Parameters.** Stochastic models of failures of different systems component are defined for component failure probability estimation depending on the system operational mode. A set of available models is given in SAPHIRE for Windows and includes the following:
  - A. **Components of stand-by systems.** The main parameter of stand-by system is the unavailability upon demand. Such system unavailability can be modeled by fault tree, where basic events probabilities are equal to system components unavailabilities averaged by time. This model treats the time to failure as a random value with exponential distribution. Such component unavailability is the function of time. In case of periodic test, unavailability is a periodic function of time. For simplifying the calculation, time dependency is usually replaced by the average value over the considered interval. For periodically tested components, the interval average is the average value for the test interval.

Three types of stand-by system components are identified:

- 1) **Periodically tested stand-by components.** For such components it is necessary to estimate following parameters: failure rate, probability of failure per demand, average restoring time (for repair), and average outage time due to test and maintenance.
- 2) **Non-tested stand-by component.** For such components, the exposure time is set to unit projected operation time for calculation of unavailability. But often the component is tested indirectly or replaced. For example, if the system gets a real actuation signal, the state of the non-tested component can be determined. In this case, the average time to failure for a component is set to the average interval between system actuations. In some instances, the component can be replaced along with the tested components. In this case, test interval for non-tested component is set to average time to failure of tested component.
- 3) **Monitored components.** State of some stand-by components is tested continuously (monitoring). In this case component failure is revealed immediately.

- B. Components of systems in operation. For systems in operation, the most important parameter is the probability of failure during the defined mission time. This probability may be estimated based on fault trees or another logic model, where basic event probabilities are set to unavailabilities of components over the interval mission time. Failures of operating components are modeled using an exponentially distribution with a failure rate different from the failure rate in stand-by mode.

Operating systems contain two main types of components: restorable and non-restorable.

- 1) Non-restorable components. Components that cannot be restored in case of failure. Exponential distribution of time between failures for such components is characterized by failure rate,  $\lambda$ .
  - 2) Restorable components. Components that may be restored in case of failure. In this case restoration means restoration without outage of operation.
- C. Stand-by systems following demand. Stand-by systems must fulfill a specific function during the defined time after successful start. During this time such systems are described in the same way as operating systems.
- D. Constant probability per demand. The model treats component failure probability as a fixed probability for every demand. For such components, tests are excluded from consideration.

For YMP, the operational mode of failure and standby failures predominate; therefore, constant failure rates and constant probabilities per demand were constructed.

Component types and failure modes were initially identified based upon a listing of the components considered to be likely to be encountered in the analysis. This list was compiled from expertise in database development and familiarity with general component requirements in a variety of facilities. As the fault tree modeling progressed, this list was augmented and tailored to the specific active components included in the PCSA models based on the YMP design.

Correspondingly, it was necessary to develop an active component and failure mode coding scheme that would be consistent with the fault tree model basic events, the needs of the SAPHIRE models, as well as with standard repository naming conventions for YMP equipment types.

The YMP PCSA basic event naming convention was therefore developed to incorporate the following information in the 24 character basic event (BE) name (consistent with the BE field in SAPHIRE):

- Area code – physical design or construction area where a component would be installed
- System locator code – operational systems and processes

- Component function identifiers – component function
- Sequence code – numeric sequence and train assignment
- Component type code – three character identifier for general component type, such as battery, actuator, or pump
- Failure mode code – three character identifier for the way in which the component is considered in the fault tree models to have failed, (e.g., FTS for fails to start or FOD for fails on demand).

The area, system locator, and component function codes were obtained from engineering standards from the YMP repository as a whole to be consistent with overall site naming conventions. The sequence codes were taken from the component identification numbers on project drawings, if the design had progressed to that point at the time of the data development and modeling.

Active component type codes were developed to be consistent with the component function identifiers, but since the type codes were limited to three digits and the function identifiers were occasionally four-characters long, in some instances it was necessary to truncate the identifier to construct the type code.

Failure mode codes (FM) were developed using prior database conventions or abbreviations that would be as intuitively obvious as possible.

Both type (TYP) and failure mode were limited to three characters each in order to be consistent with the input constraints and conventions of the SAPHIRE template database feature, which allows the same component failure data to be applied to all items in the model.

A list of the component type and failure mode combinations is provided in Table C1.1-1.

Industry-wide data sources were then collected and reviewed to identify failure rates per hour or failure probabilities per demand that would be relevant to each of the 146 TYP-FM combinations.

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM)

TYP-FM	Component Name & Failure Mode
AHU-FTR	Air Handling Unit Failure to Run
ALM-SPO	Alarm/Annunciator Spurious Operation
AT-FOH	Actuator (Electrical) Failure
ATH-FOH	Actuator (Hydraulic) Failure
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation
AXL-FOH	Axle Failure
B38-FOH	Bearing Failure
BEA-BRK	Lifting Beam/Boom Breaks
BLD-RUP	Air Bag Ruptures

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
BLK-FOD	Block or Sheaves Failure on Demand
BRH-FOD	Brake (Hydraulic) Failure on Demand
BRK-FOD	Brake Failure on Demand
BRK-FOH	Brake (Electric) Failure
BRP-FOD	Brake (Pneumatic) Failure on Demand
BRP-FOH	Brake (Pneumatic) Failure
BTR-FOD	Battery No Output Given Challenge
BTR-FOH	Battery Failure
BUA-FOH	AC Bus Failure
BUD-FOH	DC Bus Failure
BYC-FOH	Battery Charger Failure
C52-FOD	Circuit Breaker (AC) Fails on Demand
C52-SPO	Circuit Breaker (AC) Spurious Operation
C72-SPO	Circuit Breaker (DC) Spurious Operation
CAM-FOH	Cam Lock Fails
CBP-OPC	Cables (Electrical Power) Open Circuit
CBP-SHC	Cables (Electrical Power) Short Circuit
CKV-FOD	Check Valve Fails on Demand
CKV-FTX	Check Valve Fails to Check
CON-FOH	Electrical Connector (Site Transporter) Failure
CPL-FOH	Coupling (Automatic) Failure
CPO-FOH	Control system Onboard (TEV or Trolley) Failure
CRD-FOH	Badge/Card Reader Failure
CRJ-DRP	Jib Crane Load Drop
CRN-DRP	200-Ton Crane Load Drop
CRN-TBK	200-Ton Crane Two-Blocking Load Drop
CRS-DRP	Crane using Slings Load Drop
CRW-DRP	Waste Package Crane Load Drop
CRW-TBK	Waste Package Crane Two-Blocking Load Drop
CSC-FOH	Cask Cradle Failure
CT-FOD	Controller Mechanical Jamming
CT-FOH	Controller Failure
CT-SPO	Controller Spurious Operation
CTL-FOD	Logic Controller Fails on Demand
DER-FOM	Derailment Failure per Mile
DG-FTR	Diesel Generator Fails to Run
DG-FTS	Diesel Generator Fails to Start
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days
DM-FOD	Drum Failure on Demand
DM-MSP	Drum Misspooling (Hourly)
DMP-FOH	Damper (Manual) Fails to Operate

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)
DMS-FOH	Demister (Moisture Separator) Failure
DRV-FOH	Drive (Adjustable Speed) Failure
DRV-FSO	Drive (Adjustable Speed) Failure to Stop on Demand
DTC-RUP	Duct Ruptures
DTM-FOD	Damper (Tornado) Failure on Demand
DTM-FOH	Damper (Tornado) Failure
ECP-FOH	Position Encoder Failure
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)
FAN-FTR	Fan (Motor-Driven) Fails to Run
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand
FRK-PUN	Forklift Puncture
G65-FOH	Governor Failure
GPL-FOD	Grapple Failure on Demand
GRB-FOH	Gear Box Failure
GRB-SHH	Gear Box Shaft/Coupling Shears
GRB-STH	Gear Box Stripped
HC-FOD	Hand Held Radio Remote Controller Fails to Stop (on Demand)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation
HEP-LEK	Filter (HEPA) Leaks [Bypassed]
HEP-PLG	Filter (HEPA) Plugs
HOS-LEK	Hose Leaking
HOS-RUP	Hose Ruptures
IEL-FOD	Interlock Failure on Demand
IEL-FOH	Interlock Failure
LC-FOD	Level Controller Failure on Demand
LRG-FOH	Lifting Rig or Hook Failure
LVR-FOH	Lever (Two Position; Up-Down) Failure
MCC-FOH	Motor Control Centers (MCCs) Failure
MOE-FOD	Motor (Electric) Fails on Demand
MOE-FSO	Motor (Electric) Fails to Shut Off
MOE-FTR	Motor (Electric) Fails to Run
MOE-FTS	Motor (Electric) Fails to Start (Hourly)
MOE-SPO	Motor (Electric) Spurious Operation
MSC-FOH	Motor Speed Control Module Failure
MST-FOH	Motor Starter Failure
NZL-FOH	Nozzle Failure
PIN-BRK	Pin (Locking or Stabilization) Breaks
PLC-FOD	Programmable Logic Controller Fails on Demand
PLC-FOH	Programmable Logic Controller Fails to Operate
PLC-SPO	Programmable Logic Controller Spurious Operation



Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
PMD-FTR	Pump (Motor Driven) Fails to Run
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand
PPL-RUP	Piping (Lined) Catastrophic
PPM-PLG	Piping (Water) Plugs
PPM-RUP	Piping (Water) Ruptures
PR-FOH	Passive Restraint (Bumper) Failure
PRM-FOH	eProm (HVAC Speed Control) Failure
PRV-FOD	Pressure Relief Valve Fails on Demand
PV-SPO	Pneumatic Valve Spurious Operation
QDV-FOH	Quick Disconnect Valve Failure
RCV-FOH	Air Receiver Fails to Supply Air
RLY-FTP	Relay (Power) Fails to Close/Open
SC-FOH	Speed Control Failure
SC-SPO	Speed Control Spurious Operation
SEL-FOH	Speed Selector Fails
SEQ-FOD	Sequencer Fails on Demand
SFT-COL	Spent Fuel Transfer Machine Collision/Impact
SFT-DRP	Spent Fuel Transfer Machine Fuel Drop
SFT-RTH	Spent Fuel Transfer Machine Fuel Raised Too High
SJK-FOH	Screw jack (TEV) Failure
SRF-FOH	Flow Sensor Failure
SRP-FOD	Pressure Sensor Fails on Demand
SRP-FOH	Pressure Sensor Fails
SRR-FOH	Radiation Sensor Fails
SRS-FOH	Over Speed Sensor Fails
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand
SRT-FOH	Temperature Sensor/Transmitter Fails
SRT-SPO	Temperature Sensor Spurious Operation
SRU-FOH	Ultrasonic Sensor Fails
SRV-FOH	Vibration Sensor (Accelerometer) Fails
SRX-FOD	Optical Position Sensor Fails on Demand
SRX-FOH	Optical Position Sensor Fails
STU-FOH	Structure (Truck or Railcar) Failure
SV-FOD	Solenoid Valve Fails on Demand
SV-FOH	Solenoid Valve Fails
SV-SPO	Solenoid Valve Spurious Operation
SWA-FOH	Switch, Auto-Stop Fails (CTT end of Hose Travel)
SWG-FOH	13.8kV Switchgear Fails
SWP-FTX	Electric Power Switch Fails to Transfer
SWP-SPO	Electric Power Switch Spurious Transfer
TD-FOH	Transducer Failure

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
TDA-FOH	Transducer (Air Flow) Failure
TDP-FOH	Transducer (Pressure) Fails
TDT-FOH	Transducer (Temperature) Fails
THR-BRK	Third Rail Breaks
TKF-FOH	Fuel Tank Fails
TL-FOH	Torque Limiter Failure
TRD-FOH	Tread (Site Transporter)
UDM-FOH	Damper (Backdraft) Failure
UPS-FOH	Uninterruptible Power Supply (UPS) Failure
WNE-BRK	Wire Rope Breaks
XMR-FOH	Transformer Failure
XV-FOD	Manual Valve Failure on Demand
ZS-FOD	Limit Switch Failure on Demand
ZS-FOH	Limit Switch Fails
ZS-SPO	Limit Switch Spurious Operation

NOTE: AC = alternating current; DC = direct current; CTT = cask transfer trailer; HEPA = high efficiency particulate air (filter); HVAC = heating, ventilation, and air conditioning; MCC = motor control center; TEV = transport and emplacement vehicle; UPS = uninterruptible power supply.

Source: Original

## C1.2 INDUSTRY-WIDE RELIABILITY DATA

Industry-wide data sources are documents containing industrial or military experience on component performance. Usually they are previous safety/risk analyses and reliability studies performed nationally or internationally, but they can also be standards or published handbooks. For the YMP PCSA, an industry-wide database was constructed using a library of industry-wide data sources of reliability data from nuclear power plants, equipment used by the military, chemical processing plants, and other facilities. The sources used are listed in Table C1.2-1.

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
<i>Guidelines for Process Equipment Reliability Data with Data Tables.</i> [CCPS] (Ref. C5.1)
<i>Savannah River Site, Generic Data Base Development (U)</i> [SRS Reactors] (Ref. C5.5)
<i>The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve Component.</i> NUREG/CR-3154 (Ref. C5.6)
<i>Waste Form Throughputs for Preclosure Safety Analysis.</i> [BSC 2007](Ref. C5.7)
<i>Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.</i> [EPRI PRA] (Ref. C5.8)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

<b>Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database</b>
<i>Component Failure and Repair Data for Coal-Fired Power Units.</i> EPRI AP-2071 [EPRI Pipe Failure Study] (Ref. C5.10)
<i>Mechanical Reliability: Theory, Models and Applications.</i> [AIAA] (Ref. C5.11)
<i>Military Handbook, Reliability Prediction of Electronic Equipment.</i> MIL-HDBK-217F [MIL-HDBK-217F] (Ref. C5.12)
<i>The In-Plant Reliability Data Base for Nuclear Power Plant Components - Pump Component.</i> NUREG/CR-2886. (Ref. C5.13)
<i>Some Published and Estimated Failure Rates for Use in Fault Tree Analysis</i> [DuPont] (Ref. C5.14)
<i>Analysis of Station Blackout Risk. Volume 2 of Reevaluation of Station Blackout Risk at Nuclear Power Plants.</i> NUREG/CR-6890 (Ref. C5.15)
<i>Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.</i> NUREG/CR-6928. (Ref. C5.16)
"Train Accidents by Cause from Form FRA F 6180.54." [Federal Railroad Administration] (Ref. C5.17)
<i>Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999.</i> [McKenna] (Ref. C5.20)
Ruggedized Card Reader/Ruggedized Keypad Card Reader. [HID] (Ref. C5.21)
<i>IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems.</i> [IEEE-493] (Ref. C5.22)
<i>IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.</i> [IEEE-500] (Ref. C5.23)
<i>The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report- Diesel Generators, Batteries, Chargers and Inverters.</i> NUREG/CR-3831 (Ref. C5.24)
Instruments and Software Solutions (for Emergency Response and Health Physics [LAURUS] (Ref. C5.25)
<i>A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.</i> NUREG-1774. (Ref. C5.26)
<i>Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980.</i> NUREG/CR-1363 (Ref. C5.28)
<i>The Reliability Data Handbook.</i> [Moss] (Ref. C5.32)
<i>Control of Heavy Loads at Nuclear Power Plants.</i> NUREG-0612. (Ref. C5.35)
<i>Handbook of Reliability Prediction Procedures for Mechanical Equipment</i> [NSWC-98-LE1] (Ref. C5.37)
"Using the EDA to Gain Insight into Failure Rates" [Rand] (Ref. C5.38)
<i>Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data.</i> NUREG/CR-4639, (Ref. C5.39)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

<b>Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database</b>
<i>Nonelectronic Parts Reliability Data 1995.</i> NPRD-95. [NPRD -95] (Ref. C5.40)
<i>Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.</i> [SAIC Umatilla] (Ref. C5.41)
<i>Offshore Reliability Data Handbook.</i> 2nd Edition [OREDA-92] (Ref. C5.42)
<i>Offshore Reliability Data Handbook.</i> 4th Edition. [OREDA-2002] (Ref. C5.43)
<i>Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1972-April 30, 1980.</i> NUREG/CR-1205. (Ref. C5.45)
<i>N-Reactor Level 1 Probabilistic Risk Assessment: Final Report.</i> [N-Reactor] (Ref. C5.46)

NOTE: The code in brackets [XXXX] is used to aid the reader in identifying references in Table C4-1.

Source: Original

It was necessary to analyze the industry-wide data to compare the relevancy of the component data selected from the industry-wide data sources with the equipment in the YMP PCSA models.

The data source scope had to be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might have been used for electronics data versus mechanical data, so long as its use was justified by the detail and the applicability of the information provided. Lastly, the quality of the data source was considered to be a measure of the source’s credibility. Higher quality data sources are based on equipment failures documented by a facility’s maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort was made to use the highest quality data source available for each active component type and failure mode.

Data were selected from the industry-wide data sources using the following criteria:

- The component type (TYP) and failure mode (FM) identified in the data source had to match those in the basic events specified in the fault tree. For every component modeled, a comparison was made between the modeled component and the component found in the data source to ensure its suitability for the PCSA. Also, every attempt was made to match the failure modes. Often, the source described the failure mode as “all modes,” whereas the fault tree required “fails to operate.” In cases such as this, sources with more general failure modes were not used unless they were the only available sources.
- The data source had to be widely available, not proprietary. This ensured traceability and accessibility.

- Mid level or low level quality data sources were used only when high level sources were not available.
- The operating environment is an important factor in the selection of data sources. The environment of a component refers not only to its physical state, but also its operational state. The operating conditions of a component include the plant’s maintenance policy and testing policy. If either of these states differed from the modeled facility’s state, then the data were reconsidered and usually rejected (unless no alternative existed).

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, was to evaluate the similarity between the YMP operating environment and that represented in each data source to ensure data appropriateness.

An example of how data were retrieved from the various data sources is described in the following example for check valves. The failure modes modeled in the PCSA for the check valve are fails per hour (FOH), fails to check (FTX), leaks (LEK), and spurious operation (SPO).

Table C1.2-2 shows a comparison between the failure rates for the check valve and its failure modes from three different industry-wide data sources.

Table C1.2-2. Data Source Comparison for Check Valve

Data Source	Equipment Description	Failure Modes	Data Values Provided	Equipment Boundary Given?	Taxonomy Given?
(Ref. C5.1)	Valve-non-operated, Check	<ul style="list-style-type: none"> <li>• Fails to Check</li> <li>• Significant Back Leakage</li> </ul>	Lower, Mean, Upper	Yes	Yes
(Ref. C5.23)	Driven Equipment Valves, Check	“All Modes”	Low, Recommended, High	No	Yes
(Ref. C5.5)	Check	<ul style="list-style-type: none"> <li>• Fails to Open</li> <li>• Fails to Close</li> <li>• Plugs</li> <li>• Internal Leakage</li> <li>• Internal Rupture</li> <li>• External Leakage</li> <li>• External Rupture</li> </ul>	Mean	No	No

NOTE: AICHe = American Institute of Chemical Engineers; IEEE = Institute of Electrical and Electronics Engineers.

Source: Original

Table C1.2-3 shows actual numbers extracted from industry-wide data sources for five failure modes for check valves.

Table C1.2-3. Failure Rates Extracted from Various Data Sources for Check Valve

Failure Mode Description	Failure Mode Code	Data Source	Lower	Median	Upper	EF
Fails to Close (Hourly)	FOH	(Ref. C5.5)	$1.27 \times 10^{-7}$	$7.74 \times 10^{-7}$	$4.70 \times 10^{-6}$	6.1
Leaks	LEK	(Ref. C5.5)	$6.98 \times 10^{-7}$	$3.49 \times 10^{-6}$	$1.75 \times 10^{-5}$	5.0
Fails to Open (Hourly)	FOH	(Ref. C5.5)	$1.27 \times 10^{-7}$	$7.74 \times 10^{-7}$	$4.70 \times 10^{-6}$	6.1
Transfers Closed	SPO	(Ref. C5.23)	$8.00 \times 10^{-8}$	$7.81 \times 10^{-7}$	$3.27 \times 10^{-4}$	5.0
Transfers Open	SPO	(Ref. C5.23)	$8.00 \times 10^{-8}$	$7.81 \times 10^{-7}$	$3.27 \times 10^{-4}$	5.0

NOTE: EF = error factor.

Source: Original

At this stage of the analysis, it remains to decide which data is appropriate to keep and include in the data pool and which are discarded. The criteria for this process are discussed below.

The guidelines shown in Table C1.2-4 are based on observations of the analysts of their preferences and rationales during the data selection process among the data available at the time.

Table C1.2-4. Guidelines for Industry-wide Data Selection

Data Selection Guidelines	
1.	Preference for greater than zero failures (but not always able to exclude on this basis)
2.	Population of at least 5
3.	Denominator greater than 1,000 hours or 100 demands
4.	If mean or median values, some expression of uncertainty surrounding these values (either upper or lower bounds or lognormal error factor)
5.	Data analyst's confidence in the applicability of the data to the YMP based on: <ul style="list-style-type: none"> <li>• Component design</li> <li>• Driver/operator</li> <li>• Size</li> <li>• Component application</li> <li>• Active versus passive service</li> <li>• Materials/fluids moved (e.g., water versus caustic versus viscous)</li> <li>• Component boundary</li> <li>• What's included and excluded in component definition (e.g., motor, electrical connections)</li> <li>• Failure modes</li> <li>• Operating environment</li> <li>• Physical (e.g., heat, humidity, corrosive)</li> <li>• Functional (e.g., operation, maintenance, and testing frequency)</li> </ul>

NOTE: YMP = Yucca Mountain Project.

Source: Original

Given the fact that the YMP will be a relatively unique facility (although portions will be similar to the spent fuel handling and aging areas of commercial nuclear plants), the data development perspective was to collect as much relevant industry-wide failure estimate information as possible to cover the spectrum of equipment operational experience. It is assumed that the YMP equipment would fall within this spectrum (Assumption 3.2.1). The scope of the sources

selected for this data set was deliberately broad to increase the probability that YMP operational experience would fall within the bounds. A combined estimate that reflected the uncertainty ranges defined by the data source values was developed. This process is addressed further in the Bayesian estimation Section C2.

Every attempt was made to find more than one data source for each TYP-FM, although the unique nature of many equipment types made this difficult. Data was extracted from several sources in many cases, then combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs were quantified with one data source, 8% with two data sources, 8% with three data sources, and 31% with four or more data sources.

### **C1.3 CRANE AND SPENT FUEL TRANSFER MACHINE DROP ESTIMATES**

Industry-wide data was used to quantify the likelihood of experiencing a drop from the 200-ton crane while handling waste forms and their associated containers and for estimating drop probability for jib cranes and cranes used to maneuver waste packages. In addition, drop likelihoods for the spent fuel transfer machine (SFTM) were estimated using industry-wide data.

The rationale for using industry-wide data for these estimates was that a significant amount of crane experience exists within the commercial nuclear power industry and other applications and that this experience could be used to bound the anticipated crane performance at YMP. Further, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants.

Handling incidents that resulted in a drop were included in the drop probability regardless of cause; they may have been caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

The industry-wide data for cranes was taken from NUREG-0612 (Ref. C5.35), *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774 (Ref. C5.26), and the *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8). NUREG-0612 (Ref. C5.35) has several appendices that contain crane data from the Occupational Safety and Health Act Administration, the U.S. Navy, Waste Isolation Pilot Plant, Licensee Event Reports, and from the results of a fault tree analysis. The *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8) provides estimates from Savannah River Site crane experience in addition to fault tree analysis. Crane failure information was also obtained from quantitative risk study performed for the U.S. Army chemical weapons destruction program (Ref. C5.41).

The information from each of these sources was evaluated in terms of quality, applicability to YMP, and to ensure that the events cited included both equipment failures and human failures. For the industry-wide data provided in terms of the number of events, another major factor was the ability to reasonably and justifiably estimate a meaningful denominator of number of lifts

(demands) conducted by the crane population considered in the data source. If this could not be done, the source information could not be used.

A key consideration in evaluating the industry-wide crane data for the 200-ton cranes was the NOG-1 (Ref. C5.3) design requirements that will be placed upon the YMP cranes versus the crane design features reflected in the input data sources. NUREG-1774 (Ref. C5.26, Table 12, pp. 61 – 63) provides a list of the nuclear power plants that had upgraded their cranes to single-failure-proof status consistent with licensee response to U.S. Nuclear Regulatory Commission (NRC) *NRC Bulletin 96-02* (Ref. C5.9) which requested specific information relating to their heavy loads programs and plans consistent with the recommendations of NUREG-0554 (Ref. C5.34). This information was used to constrain the denominator of the number of very heavy load lifts from NUREG-1774 (54,000) by using a percentage of percent of nuclear power plants reporting single failure proof cranes out of total plants (42/110).

Conversely, a separate category of non-single-failure-proof cranes for the waste package manipulating cranes was developed using the remaining percentage (68/110) to adjust the number of lifts. The jib crane lifts were estimated using the NUREG-1774 (Ref. C5.26, Appendix D) table of the types of cranes involved in accidents; mobile and tower cranes using jibs are cited as being involved in ~76% of accidents while bridge and gantry (used for very heavy loads) are ~19%. The percentage of accidents that did not involve jib cranes was therefore believed to reside somewhere between 19% and 24% (100% – 76%). So, the 20,620 lifts estimated for very heavy loads by single failure proof cranes was divided by 21.2% to yield a round number estimate of 97,250 jib crane lifts.

The number of crane drop incidents used as the numerator of the 200-ton crane drop estimate from NUREG-1774 (Ref. C5.26) was also restricted to those involving very heavy loads (defined in NUREG-1774 as >30 tons) of single-failure-proof cranes. Drops occurring during sling lifts were parsed into a separate category and used to estimate the sling lift-related drop likelihood.

Load drop likelihood due to two-blocking was also estimated using industry-wide data. NUREG-0612 (Ref. C5.35) describes a two-blocking event as: “The act of continued hoisting to the extent that the upper head block and the load block are brought into contact, and unless additional measures are taken to prevent further movement of the load block, excessive loads will be created in the rope reeving system, with the potential for rope failure and dropping of the load.” Two-blocking events in the various data sources were evaluated based upon the type of crane involved, as was done for the drop likelihood estimates.

As a result, several categories of crane drop estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

CRN-DRP	200-ton Crane Load Drop	3.2E-05/demand
CRN-TBK	200-ton Crane Two Block Causing Load Drop	4.4E-07/demand
CRS-DRP	200-ton Crane using Slings Load Drop	1.2E-04/demand
CRJ-DRP	Jib Crane Load Drop	2.6E-05/demand
CRW-DRP	Waste Package Crane (Not Single Failure Proof) Load Drop	1.1E-04/demand



CRW-TBK Waste Package Crane (Not Single Failure Proof) 4.5E-05/demand  
Two Block Causing Load Drop

In each of these cases, as with the other active component reliability estimates, an effort was made to include a variety of operating experience and combine it together using a parametric empirical Bayes approach. However, for the CRS, CRJ and CRW estimates, since only NUREG-1774 (Ref. C5.26), data was considered to be applicable, a Jeffrey's non-informative prior approach for the Beta distribution was used, since the estimates were per lift (demand).

These crane incident estimates were combined in the SAPHIRE models with the number of estimated YMP crane lifts.

One potential issue regarding the applicability of the industry-wide crane data was the inclusion of hard-wired interlock features on the YMP cranes that might not exist at the nuclear power plants or naval installations from which the industry-wide experience resulted. In other instances, there was concern that interlocks included in the design for use in normal operations, on grapples to verify installation or engagement, could be defeated during maintenance actions where bypasses are permitted to move tools or pallets, since a particular grapple interlock is not standard in industry but is unique to YMP. Further, PCSA is not crediting the grapple interlock function and it was considered that having such interlocks in place would not make the estimated failure probability worse. Therefore the estimates from industry-wide data were considered to be reasonable in that they provided experience-based, and perhaps somewhat pessimistic measures of anticipated crane performance.

Estimates were also developed from industry-wide data source information for the likelihood of SFTM drop, collision, and raising the fuel too high but not dropped (for potential personnel exposure considerations). The primary source for this information was NUREG-1774 (Ref. C5.26, Table 4), which provides brief descriptions of SFTM incidents at U.S. nuclear power plants from 1968 through 2002. A separate study (McKenna/Framatome) (Ref. C5.20) was reviewed, which also included SFTM incidents at U.S. nuclear power plants categorized in terms of Human Error, Equipment Failure, or Misload. Some of these were the same incidents included in NUREG-1774 (Ref. C5.26) so care was taken not to double-count any events. Each of the incidents described was reviewed in detail to evaluate their relevance to the failure modes of interest to the study and their applicability to spent fuel transfers. Incidents related to all types of fuel transfers, such as refueling or new fuel receipt, were used to estimate upper bounds (95th percentiles of a lognormal distribution) and to develop the error factor uncertainty information input to SAPHIRE along with the mean value.

It should be noted that events prior to 1985 were removed from consideration since the number of plants in operation (and therefore the number of lifts per year) would significantly differ from that cited in McKenna/Framatome (Ref. C5.20). Also, McKenna/Framatome stated that reporting practices were inconsistent prior to 1985.

The number of fuel movements used as the denominator of the SFTM estimates was based upon information from McKenna/Framatome (Ref. C5.20), which gave 1,198,723 fuel movements for the 15 year study data window, from 1985 through 1999, or a rough estimate of 79,914.87 per year. Since the numerator information from NUREG-1774 (Ref. C5.26) was based upon

17 years of data, from 1985 through 2002, the estimated denominator was calculated for consistency as  $79,914.87 \times 17$  or 1,358,553 SFTM lifts.

As a result, several categories of SFTM event estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

SFT-COL	SFTM Collision/Impact	2.9E-06/demand
SFT-DRP	SFTM Load Drop	5.2E-06/demand
SFT-RTH	SFTM Fuel Raised Too High (but not dropped)	7.4E-07/demand

These SFTM incident estimates were combined in the SAPHIRE models with the number of estimated YMP fuel assembly transfers, specifically: 66,188 based on two transfers each of 33,094 assemblies (Ref. C5.7, Table 4, pg. 27).

The results of the industry-wide data search are documented, organized by component type and failure mode, and can be found in the Excel spreadsheet file “YMP Active Comp Database.xls”, located on the CD in Attachment H.

## C2 BAYESIAN DATA COMBINATION

The application of industry-wide data sources or expert elicitation introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes’ theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

A typical application of Bayes’ theorem is illustrated as follows: a failure rate for a given component is needed for fault tree (e.g., a fan motor in the heating, ventilation, and air conditioning (HVAC) system). There is no absolute value but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes’ theorem provides a mechanism for systematically treating the uncertainty and applying  $\lambda_j$  data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the “prior” probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trial if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur in over a certain exposure, operational, or test duration.

3. Update the probability distribution for the failure rate based on the new body of evidence using the mathematical expression of Bayes' theorem.

The mathematical expression for applying Bayes' theorem to data analysis is briefly described here. Let  $\lambda_j$  be one failure rate of a set of possible failure rates of the fan motor (component j). Initially, the state of knowledge of the "true value" of  $\lambda_j$  is expressed by the probability distribution  $P(\lambda)$ , the "prior." The choice of the analytic or discrete form of the prior distribution is made by the data analyst. Let  $E$  be a new body of evidence, e.g., a new set of test data or field observations. The new evidence improves the data analyst's state of knowledge. The revised, or "updated," probability distribution for the "true value" of  $\lambda_j$  is represented as  $P(\lambda_j|E)$ . Bayes' theorem gives:

$$P(\lambda_j | E) = \frac{P(\lambda_j)L(E | \lambda_j)}{\sum_j P(\lambda_j)P(E | \lambda_j)} \quad (\text{Eq. C-1})$$

In summary, Equation C-1 states that the knowledge of the "updated" probability of  $\lambda_j$ , given the new information  $E$ , equals the "prior" probability of  $\lambda_j$  before any new information times the likelihood function,  $L(E|\lambda_j)$ . The likelihood function expresses the probability of observing the number of failures in the evidence if the failure rate  $\lambda_j$  has a certain value. The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The numerator in Equation C-1 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of  $\lambda_j$  equals unity.

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in NUREG/CR-6823 (Ref. C5.4). For the YMP PCSA, the method known as "parametric empirical Bayes" was used. This permitted a variety of different sources to be statistically combined and compared, whether the inputs were expressed as the number of failures and exposure time or demands, or as a mean and error factor. Examples of the methods used for several combinatorial cases are provided below.

## C2.1 PARAMETER ESTIMATION USING DATA FROM DIFFERENT SOURCES

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution,  $g$ , representing the source-to-source variability, also called population variability, of the component reliability (Ref. C5.4, Section 8.1). The objective of this section is to outline the methodology for developing the population-variability distribution of active components in the preclosure safety analysis. In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. This distribution is to be updated, as operating experience becomes available, to produce a reliability distribution specific to the component operated under geologic repository operations area (GROA) conditions. For the time being however, the components anticipated for use at the GROA are yet to be procured and operated. As a consequence, the population-variability distributions developed in this section both aim at and are limited to encompassing the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the preclosure safety analysis. As indicated in “Bayesian Parameter Estimation in Probabilistic Risk Assessment.” (Ref. C5.44, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example, the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

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

For each data source, the reliability information about a component’s failure rate or failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. C5.44, Section 4.2). When no exposure data are available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution ((Ref. C5.44, Section 4.4) and (Ref. C5.27, pp. 312, 314, and 315)).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. C5.4, Section 8.2.1), which have the advantage of resulting in relatively simpler

calculations. This technique however is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of “The Combined Use of Data and Expert Estimates in Population Variability Analysis,”(Ref. C5.27, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the population-variability distribution in its lognormal form is noted  $g(x, \nu, \tau)$ , where  $x$  is the reliability parameter for the component (failure rate or failure probability), and  $\nu$  and  $\tau$ , the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided in the latter case that any tail truncation above  $x = 1$  has a negligible effect (Ref. C5.44, p. 99). The validity of this can be confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98 percent of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

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

$$L_i(\nu, \tau) = \int_0^1 \text{Binom}(x, r, n) \times g(x, \nu, \tau) dx \quad (\text{Eq. C-2})$$

where  $\text{Binom}(x, r, n)$  represents the binomial distribution evaluated for  $r$  failures out of  $n$  demands, given a failure probability equal to  $x$ , and  $g(x, \nu, \tau)$  is defined as previously indicated. This equation is similar to that shown in “Bayesian Parameter Estimation in Probabilistic Risk Assessment.” (Ref. C5.44, Equation 37). If the component reliability was expressed in terms of a failure rate and the data source provided exposure data, the binomial distribution in Equation C-2 would be replaced by a Poisson distribution. If the data source provided expert opinion only (no exposure data), the binomial distribution in Equation C-2 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine  $\nu$  and  $\tau$  (Ref. C5.44, p. 101). The maximum likelihood estimators for  $\nu$  and  $\tau$  are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each data source (Ref. C5.27, Equation 4). To find the maximum likelihood estimators for  $\nu$  and  $\tau$ , it

is equivalent and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of  $\nu$  and  $\tau$  completely determines the population-variability distribution  $g$  for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution  $g$ , which are calculated using the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to  $\exp(\nu + \tau^2/2)$  and the error factor is equal to  $\exp(1.645 \times \tau)$ .

The selection of the parametric empirical Bayes method to determine the population-variability distribution is now discussed. This method provides a single “best” solution, while other techniques, such as the hierarchical Bayes method (Ref. C5.4, Section 8.3) differ by using a weighted mix of distributions of the chosen model, which incorporate epistemic (state of knowledge) uncertainty about the model. The parametric empirical Bayes method does not embed epistemic uncertainty but was nevertheless employed because of its satisfactory results for the majority of active components modeled in the preclosure safety analysis. The general adequacy of the method was confirmed by comparing its results to those obtained based on an example using a state-of-knowledge-informed approach (Ref. C5.27). The example involves twelve hypothetical data sources, each documenting the failure rate of motor-driven pumps either in terms of expert judgment or exposure data (Ref. C5.27, Table 1). Table C2.1-1 compares the percentiles predicted by the parametric empirical Bayes method and those found in “The Combined Use of Data and Expert Estimates in Population Variability Analysis.” (Ref. C5.27, Table 4). Overall, the percentiles appear to be similar, with a key metric of the distributions, their mean, being nearly identical, and the medians being comparable. Percentiles at the tails of the distributions show more differences, the parametric empirical Bayes method yielding a population-variability distribution more spread out overall than the state-of-knowledge-informed distribution (Ref. C5.27).

Table C2.1-1. Comparison of Results of Parametric Empirical Bayes and Results Reported by Lopez Droguett et al.

Population-Variability Value	Parametric Empirical Bayes Method <sup>a</sup>	Lopez Droguett Results <sup>b</sup>
Mean	$6.00 \times 10^{-5}$	$6.05 \times 10^{-5}$
1 <sup>st</sup> percentile	$1.32 \times 10^{-7}$	$3.16 \times 10^{-7}$
5 <sup>th</sup> percentile	$4.75 \times 10^{-7}$	$1.38 \times 10^{-6}$
10 <sup>th</sup> percentile	$9.38 \times 10^{-7}$	$2.67 \times 10^{-6}$
50 <sup>th</sup> percentile (median)	$1.04 \times 10^{-5}$	$1.61 \times 10^{-5}$
90 <sup>th</sup> percentile	$1.14 \times 10^{-4}$	$7.79 \times 10^{-5}$
95 <sup>th</sup> percentile	$2.26 \times 10^{-4}$	$1.36 \times 10^{-4}$
99 <sup>th</sup> percentile	$8.10 \times 10^{-4}$	$4.85 \times 10^{-4}$

NOTE: <sup>a</sup> Derivation of the results is given in the following section, Example of Development of Population-Variability Distribution.

<sup>b</sup> (“The Combined Use of Data and Expert Estimates in Population Variability Analysis.” *Reliability Engineering and System Safety*, 83 (Ref. C5.27, Table 1)

Source: (Ref. C5.27, Table 1).

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, “External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom,” *Reliability Engineering and System Safety*, 47 (Ref. C5.19, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between  $2 \times 10^{-8}$ /hr (5th percentile) and  $6 \times 10^{-5}$ /hr (95th percentile). Using the definition of the error factor given in NUREG/CR-6823, (Ref. C5.4, Section A.7.3), this corresponds to an error factor of  $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$ . Therefore, in the preclosure safety analysis, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55 are too diffuse to adequately represent the population-variability distribution of a component. In such instances (two such cases in the entire PCSA database, when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution and therefore is unaffected by the value taken by the error factor. Based on NUREG/CR-6823, (Ref. C5.4, Section A.7.3), the median is calculated as  $\exp(v)$ , where  $v$  is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the preclosure safety analysis is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in NUREG/CR-6823, (Ref. C5.4, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for a component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using a data source that yields a more diffuse likelihood. In the other cases, the lognormal distribution approximately encompasses the likelihood functions yielded by the data sources, showing that the parametric empirical Bayes method is adequate. An illustration of a graph plotting the population-variability distribution along with the likelihood functions from data, based on the example of the Lopez Droguett et al. paper (Ref. C5.27) is provided below.

### Example of Development of Population-Variability Distribution

Mathcad is used to calculate the population-variability distribution of active components. An illustration of such a calculation is given using the example in “The Combined Use of Data and Expert Estimates in Population Variability Analysis.” (Ref. C5.27, Table 1). In this example, several data sources supply information about the reliability of motor-driven pumps, as follows:

Four data sources supply point estimates of the failure rates, along with a range (error) factor. This information is given in the following matrix, where the first column contains the estimated hourly failure rate (considered to be a median value) and the second column the associated error factor:

$$A := \begin{pmatrix} 3.0 \cdot 10^{-5} & 5 \\ 2.1 \cdot 10^{-5} & 3 \\ 2.0 \cdot 10^{-5} & 10 \\ 2.53 \cdot 10^{-5} & 10 \end{pmatrix}$$

In addition, eight data sources supply exposure data, which are given in the following matrix, where a recorded number of failures is shown in the first column, and the associated operating time (in hours) is shown in the second.

$$B := \begin{pmatrix} 0 & 76000 \\ 0 & 152000 \\ 0 & 74000 \\ 2 & 74000 \\ 0 & 48000 \\ 3 & 76000 \\ 9 & 10200 \\ 2 & 48000 \end{pmatrix}$$

The population-variability distribution  $g$  of the failure rate  $x$  is approximated by a lognormal distribution whose unknown parameters,  $\nu$  and  $\tau$ , respectively the mean and standard deviation of the associated normal distribution, are to be determined. Calculating  $\nu$  and  $\tau$  involves calculating the likelihood function associated with the reliability information in each data source. This is done as follows:

For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate  $x$ , and characterized by its median value and associated error factor shown in the matrix  $A$ . In Mathcad, the parameters required for defining a lognormal distribution are the mean and standard deviation of the associated normal distribution. Based on the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3), the mean of the associated normal distribution is the natural logarithm of the median failure rate, and the standard deviation of the associated normal distribution is  $\ln(EF)/1.645$ , where  $EF$  is the error factor.



Because the unknowns to be determined are  $\nu$  and  $\tau$ , the likelihood function is expressed as a function unconditional on the value of  $x$ . This is done by integrating the likelihood function over all possible values of  $x$  (i.e., theoretically, from 0 to infinity) and weighting by the probability of having a value of  $x$ , conditional on observing  $\nu$  and  $\tau$ . In practice, to facilitate the numerical integration on Mathcad, the integration is performed on a range that encompasses credible values for  $x$ . In this example, the failure rate range considered varies from  $10^{-8}$ /hr to  $10^{-2}$ /hr. Thus, the likelihood functions, unconditional on  $x$ , for each of the data source in the matrix  $A$ , are calculated as follows:

$$a := 1..4 \quad fe(a, x) := dlnorm\left(x, \ln(A_{a,1}), \frac{\ln(A_{a,2})}{1.645}\right) \quad (\text{Eq. C-3})$$

$$LA(a, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fe(a, x) \cdot dlnorm(x, \nu, \tau) dx \quad (\text{Eq. C-4})$$

(In the above formulas,  $a$  is an index used to particularize a likelihood function to a data source in the matrix  $A$ .)

For a data source providing exposure data (given in the form of a number  $n$  of recorded failures over an exposure time  $t$ ), the likelihood function is a Poisson distribution, expressing the probability that  $n$  failures are observed when the expected number of failures is  $x$  times  $t$ . Here also, the likelihood needs to be expressed as a function unconditional on the failure rate  $x$ , which is done by integrating  $x$  out, in a similar manner as above:

$$b := 1..8 \quad fd(b, x) := dpois(B_{b,1}, B_{b,2} \cdot x) \quad (\text{Eq. C-5})$$

$$LB(b, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fd(b, x) \cdot dlnorm(x, \nu, \tau) dx \quad (\text{Eq. C-6})$$

(In the above formulas,  $b$  is an index used to particularize a likelihood function to a data source in the matrix  $B$ .)

The maximum likelihood method is used to calculate  $\nu$  and  $\tau$ . This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source (this is because the data sources are independent from each other). It is equivalent and computationally convenient to find the maximum likelihood estimators for  $\nu$  and  $\tau$  by using the sum of the log-likelihood (logarithm of the likelihood) of each data source.

Therefore, the log-likelihood function to be maximized is:

$$L(\nu, \tau) := \sum_{a=1}^4 \ln(LA(a, \nu, \tau)) + \sum_{b=1}^8 \ln(LB(b, \nu, \tau)) \quad (\text{Eq. C-7})$$

To maximize a function, Mathcad requires guess values and a range over which to search for maxima. The quantity  $\nu$  represents the logarithm of a failure rate, which is expected to be in the  $10^{-6}$  /hr range. Therefore, a guess value for  $\nu$  is:

$$\nu := \ln(10^{-6}) \quad \nu = -13.8$$

Based on a typical error factor value of 10, a guess value for  $\tau$  is:

$$\tau := \frac{\ln(10)}{1.645} \quad \tau = 1.4$$

A reasonable range over which to perform the likelihood maximization is as follows:

$$\begin{array}{ll} \text{Given} & \nu > -20 & \nu < -1 \\ & \tau > 0.01 & \tau < 5 \end{array}$$

The maximum likelihood estimators for  $\nu$  and  $\tau$  are:

$$\begin{array}{ll} L := \text{Maximize}(L, \nu, \tau) & \nu := L_1 & \nu = -11.478 \\ & \tau := L_2 & \tau = 1.874 \end{array}$$

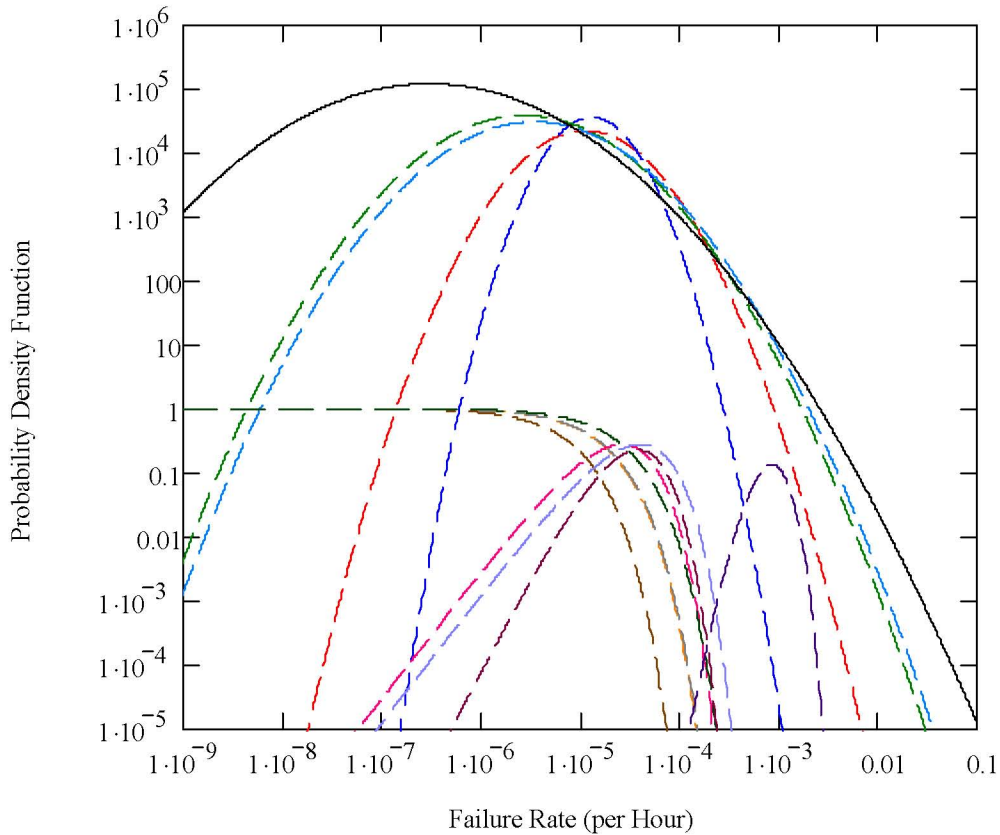
Therefore, the mean and error factors of the population-variability distribution for the failure rate are (based on the formula in NUREG/CR-6823 (Ref. C5.4, Section A.7.3)):

$$\begin{array}{ll} m := \exp\left(\nu + \frac{2}{\tau}\right) & m = 6.00 \times 10^{-5} \quad \text{per hour} \\ EF := \exp(1.645 \cdot \tau) & EF = 21.8 \end{array}$$

Notable percentiles of the population-variability distribution are as follows (expressed as hourly failure rates) and shown in Figure C2.1-1:

$$\begin{array}{ll} 1^{\text{st}} \text{ percentile:} & qlnorm(0.01, \nu, \tau) = 1.32 \times 10^{-7} \\ 5^{\text{th}} \text{ percentile:} & qlnorm(0.05, \nu, \tau) = 4.75 \times 10^{-7} \\ 10^{\text{th}} \text{ percentile:} & qlnorm(0.10, \nu, \tau) = 9.38 \times 10^{-7} \\ 50^{\text{th}} \text{ percentile:} & qlnorm(0.50, \nu, \tau) = 1.04 \times 10^{-5} \end{array}$$

90<sup>th</sup> percentile:  $qlnorm(0.90, \nu, \tau) = 1.14 \times 10^{-4}$   
 95<sup>th</sup> percentile:  $qlnorm(0.95, \nu, \tau) = 2.26 \times 10^{-4}$   
 99<sup>th</sup> percentile:  $qlnorm(0.99, \nu, \tau) = 8.10 \times 10^{-4}$



Source: Original

Figure C2.1-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

## C2.2 PARAMETER ESTIMATION IN CASE ONLY ONE DATA SOURCE IS AVAILABLE

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data (i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities) the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffrey's noninformative prior distribution. As indicated in NUREG/CR-6823 (Ref. C5.4,

Section 6.2.2.5.2), this noninformative prior conveys little prior belief or information, thus allowing the data to speak for themselves.

As mentioned in “Bayesian Parameter Estimation in Probabilistic Risk Assessment,” (Ref. C5.44, Section 4.2), the likelihood function associated with exposure data is either a Poisson distribution (in the case of failure rates), or a binomial distribution (in the case of failure probabilities).

Applying Bayes’ theorem with Jeffrey’s noninformative prior in conjunction with a Poisson likelihood function characterized by  $r$  recorded failures over an exposure time  $t$  results in a closed-form posterior distribution, namely a gamma distribution, characterized by a shape parameter equal to  $0.5 + r$ , and a scale parameter equal to  $t$ ; the mean of this distribution is  $(0.5 + r)/t$  (Ref. C5.4, Sections 6.2.2.5.2 and A7.6). In SAPHIRE, this distribution is characterized by its mean and by its shape parameter (i.e.,  $0.5 + r$ ).

Applying Bayes’ theorem with Jeffrey’s noninformative prior in conjunction with a binomial likelihood function characterized by  $r$  recorded failures out of  $n$  demands results in a closed-form posterior distribution, namely a beta distribution, characterized by a parameter “ $a$ ” equal to  $0.5 + r$ , and a parameter “ $b$ ” equal to  $n - r + 0.5$ ; the mean of this distribution is  $(0.5 + r)/(n + 1)$  (Ref. C5.4, Sections 6.3.2.3.2 and A7.8). In SAPHIRE, this distribution is characterized by its mean and by the parameter “ $b$ ” (i.e.,  $n - r + 0.5$ ).

### **C3 COMMON CAUSE FAILURE DATA**

Dependent failures are modeled in event tree and fault tree logic models, with potential dependent failures modeled explicitly via the logic models, whenever possible. For example, failure of the HVAC system is explicitly dependent upon failures in the electrical supply systems that are modeled in the fault trees. Similarly, the effects of erroneous calibration or other human failure events can be explicitly included in the system fault tree models and the basic event probabilities considered during the human reliability analysis. Otherwise, potential dependencies known as common-cause failures are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate common cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. C5.18), the Multiple Greek Letter method (Ref. C5.29) and (Ref. C5.30), and the Alpha Factor method (Ref. C5.31). These methods do not require an explicit knowledge of the dependence failure mode. For the YMP PCSA, common-cause failure rates or probabilities were estimated using the alpha factor method described in NUREG/CR-5485 (Ref. C5.31).

The vast majority of the equipment types for which common cause failure basic events were modeled in the YMP PCSA are not covered by the detailed component-specific alpha factor sources based on commercial nuclear plant equipment. Therefore, it was necessary to use alpha factors to address the common cause failure estimates for crane hoist wire ropes, gear boxes, over-torque sensors and the like.

The alpha factor method provides a model to treat common cause failure (CCF) probabilities of *k*-of-*m* components. In addition, industry-wide alpha factors have been developed for the U.S. Nuclear Regulatory Commission from experience data collected at nuclear power plants. The data analysis reported in NUREG/CR-5485 (Ref. C5.31) consisted of:

1. Identifying the number of redundant components in each subsystem being reported (e.g., two, three, or four (this is termed the CCF group size, CCCG of size *m*)).
2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, i.e., *k* = 1 for one component at a time, *k* = 2 for two components at a time, *k* = 3 for three components at a time, up to *m* for failure of all components in a given CCF group.
3. Estimating the alpha factor for a given component type based on its definition as the fraction of total failure events that involve *k* component failures due to common cause, for a system of *m* redundant components, using the alpha factor equation from NUREG/CR-5485 (Ref, C5.31, Table 5-10), as shown in Figure C3-1.

$$\alpha_k^m = \frac{n_k}{\sum_{j=1}^m n_j} \quad k = 1, \dots, m$$

Source: NUREG/CR-5485, p. 70 (Ref. C5.31)

Figure C3-1. Alpha Factor

4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produced industry-wide prior distributions for the alpha factors for each CCCG size, based on all CCF events in their database. Events were mapped to a given CCCG size, the maximum likelihood estimator obtained and fit to a constrained noninformative prior distribution. The parameter  $A_T$  of a Dirichlet distribution was then calculated for each alpha and the results combined using the geometric mean. The results are the industry-wide mean alpha factors and uncertainty bounds reported in of NUREG/CR-5485 (Ref. C5.31, Table 5-11) shown in Table C3-1:

Table C3-1. Alpha Factor Table

Table 5-11. Generic prior distributions for various system sizes.

CCCG Size m	α-Factor	Distributions Parameters		Percentiles			Mean
		a	b	P <sub>05</sub>	P <sub>50</sub>	P <sub>95</sub>	
2	α <sub>1</sub>	9.5300	0.470	8.20E-01	9.78E-01	1.00E-00	0.95300
	α <sub>2</sub>	0.4700	9.530	1.42E-04	2.16E-02	1.81E-01	0.04700
3	α <sub>1</sub>	15.2000	0.800	8.42E-01	9.67E-01	9.99E-01	0.95000
	α <sub>2</sub>	0.3872	15.613	2.10E-05	8.79E-03	1.01E-01	0.02420
	α <sub>3</sub>	0.4128	15.587	3.45E-05	1.01E-02	1.05E-01	0.02580
4	α <sub>1</sub>	24.7000	1.300	8.67E-01	9.61E-01	9.95E-01	0.95000
	α <sub>2</sub>	0.5538	25.446	1.44E-04	1.08E-02	7.81E-02	0.02130
	α <sub>3</sub>	0.2626	25.737	2.98E-07	1.99E-03	4.82E-02	0.01010
	α <sub>4</sub>	0.4836	25.516	6.29E-05	8.42E-03	7.17E-02	0.01860
5	α <sub>1</sub>	38.042	1.958	8.86E-01	9.58E-01	9.91E-01	0.95106
	α <sub>2</sub>	0.7280	39.272	3.72E-04	1.10E-02	6.05E-02	0.01820
	α <sub>3</sub>	0.4120	39.588	1.32E-05	3.93E-03	4.22E-02	0.01030
	α <sub>4</sub>	0.2336	39.766	4.57E-08	8.97E-04	2.89E-02	0.00584
	α <sub>5</sub>	0.5840	39.416	1.24E-04	7.66E-03	5.27E-02	0.01460
6	α <sub>1</sub>	50.4724	2.528	8.97E-01	9.58E-01	9.89E-01	0.95231
	α <sub>2</sub>	0.7791	52.221	3.76E-04	9.20E-03	4.78E-02	0.01470
	α <sub>3</sub>	0.5406	52.459	6.04E-05	5.02E-03	3.79E-02	0.01020
	α <sub>4</sub>	0.3127	52.687	9.28E-07	1.56E-03	2.66E-02	0.00590
	α <sub>5</sub>	0.2433	52.757	5.77E-08	7.67E-04	2.24E-02	0.00459
	α <sub>6</sub>	0.6519	52.348	1.66E-04	6.93E-03	4.27E-02	0.01230
7	α <sub>1</sub>	74.5360	3.464	9.12E-01	9.59E-01	9.86E-01	0.95559
	α <sub>2</sub>	0.9906	77.009	6.44E-04	8.84E-03	3.79E-02	0.01270
	α <sub>3</sub>	0.6817	77.318	1.39E-04	5.05E-03	2.99E-02	0.00874
	α <sub>4</sub>	0.4891	77.511	2.21E-05	2.82E-03	2.42E-02	0.00627
	α <sub>5</sub>	0.2941	77.706	3.39E-07	8.97E-04	1.74E-02	0.00377
	α <sub>6</sub>	0.2051	77.795	3.84E-09	2.94E-04	1.35E-02	0.00263
	α <sub>7</sub>	0.8034	77.197	2.89E-04	6.52E-03	3.32E-02	0.01030
8	α <sub>1</sub>	97.6507	4.349	9.20E-01	9.60E-01	9.84E-01	0.95736
	α <sub>2</sub>	1.1118	100.888	7.25E-04	7.91E-03	3.13E-02	0.01090
	α <sub>3</sub>	0.7915	101.209	2.07E-04	4.87E-03	2.52E-02	0.00776
	α <sub>4</sub>	0.6253	101.375	6.92E-05	3.34E-03	2.17E-02	0.00613
	α <sub>5</sub>	0.4417	101.558	8.51E-06	1.76E-03	1.74E-02	0.00433
	α <sub>6</sub>	0.2581	101.742	6.09E-08	4.74E-04	1.21E-02	0.00253
	α <sub>7</sub>	0.1969	101.803	1.59E-09	1.93E-04	1.00E-02	0.00193
	α <sub>8</sub>	0.9241	101.076	3.82E-04	6.12E-03	2.78E-02	0.00906

Source: NUREG/CR-5485 (Ref. C5.31)

These values were used in the YMP PCSA by multiplying the mean failure rate for the TYP-FM data by the appropriate alpha factor for k-of-n components for failure-on-demand events (e.g., pump failure to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run) as per the guidance in NUREG/CR-5485 (Ref. C5.31). For example, for a 2-out-of-2 failure on demand event, the mean alpha factor of 0.047 shown in the far right column of Table C3-1 associated with α<sub>2</sub> was multiplied by the mean failure probability for the appropriate component type and failure mode (from Table C4-1) to yield the common cause failure probability.

This approach was considered to provide conservative CCF data for all the component types for which common causes were modeled. This was considered particularly important since the

YMP has never operated and therefore the applicability of conventional nuclear plant alpha factors could not be justified.

The conservatism of this approach can be demonstrated by comparing the alpha factors used for the PCSA diesel generator CCF events to those posted on the U.S. Nuclear Regulatory Commission website for use in Probabilistic Risk Assessment studies of commercial nuclear power plants in the U.S.

The alpha factor used for the PCSA for 2 of 2 diesel generators failing to start was the 0.047 value cited earlier, while the mean alpha factor for a CCCG=2 cited by the NRC (Ref. C5.36) is 0.0136.

Diesel generators are the only component types for which such a comparison can be made since the other YMP component types for which common cause failures were modeled were not covered by the NRC equipment-specific alpha factors.

#### **C4 ACTIVE COMPONENT RELIABILITY ESTIMATES INPUT TO SAPHIRE**

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data had to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

- BEA – attributes to assign information to the proper SAPHIRE fields
- BED – descriptions of the component type name and failure mode
- BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement such that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the YMP PCSA case was the TYP-FM coding). Examples of descriptions used for the PCSA template data were Clutch Failed to Operate, Relay Spurious Operation, Position Sensor Fails on Demand, and Wire Rope Breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the Lognormal Error Factor, or the shape parameter of the Beta or Gamma distributions.

Geometric means of the input parameters from the industry-wide data sources were initially used as screening values for each TYP-FM and were entered into the .BEI file, along with a default Error Factor of 10. Once the Bayesian combination process was completed for all 275 TYP-FM combinations, mean and uncertainty parameter information was entered into the .BEA files, and tested in SAPHIRE before being distributed to the systems analysts.

Failure probability per demand information was entered as SAPHIRE Calculation Type 1 for a simple probability and failure rate per hour information was entered as SAPHIRE Calculation Type 3 as a mean failure rate in the lambda field. Calc Type 3 uses the formula  $P = 1 - \exp(-\lambda T_m)$ , where  $\lambda$  is the mean failure rate (or lambda) and  $T_m$  is the mission time. Mission time is defined in the SAPHIRE Basics manual as "...the period of time that a component is required to operate in order to characterize the component operation as successful." Since the template data was to be used for all YMP facilities while the mission times would be system-specific, the mission time field in the three template data files was left blank and these times were instead input individually by the systems analysts.

The correlation class field was also used for the YMP template data files "to account for data dependencies among like events in the database" during the uncertainty analysis, as stated in the SAPHIRE Basics manual. This meant that all components in the same correlation class would be treated the same during the uncertainty analysis. This feature of SAPHIRE is based upon the observations documented (Ref. C5.2) that in the risk models, all components of the same type are quantified with the same failure rate or probability, therefore it is appropriate to group together the experience of all the nominally identified components in the same facility. Therefore, all components of the same type and failure mode are aggregated into a single number, meaning that the dependency between components of the same class must somehow be addressed. For example, if multiple motor-operated valves needed to open for success and all are assigned the same failure probability, then these basic events needed to be correlated via being assigned the same correlation class in the .BEI file. However, if different probabilities were to be used for different motor-operated valves based on the data, then the basic events would not be correlated. In all cases, a correlation class identifier, using the TYP-FM acronyms, was input to the .BEI file to indicate that all equipment within the same TYP-FM should be correlated by the SAPHIRE model. SAPHIRE then would sample from one distribution and then use this sampled probability for all other basic events with the same correlation class.

The template data was also identified by TYP-FM combination and was utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the code, then by using the Modify Event feature to link the template data to each basic event in the fault tree. This permitted each active component of the same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the industry-wide data investigation and Bayesian combination process.

Table C4-1 shows the active component reliability estimates that were input to SAPHIRE as template data for fault tree model quantification.



Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
AHU-FTR	Air Handling Unit Failure to Run	G	5.00E-01 <sup>b</sup>		3.80E-06 <sup>b</sup>	1 source; N/D	NUREG/CR-6928 (Ref. C5. 16)
ALM-SPO	Alarm/Annunciator Spurious Operation	L	1.30E+01		4.74E-07	5 sources N/D; 1 source mean	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40)
AT-FOH	Actuator (Electrical) Failure	L	1.24E+01		7.54E-05	3 sources; N/D	NPRD-95 (Ref. C5.40)
ATH-FOH	Actuator (Hydraulic) Failure	L	3.81E+01		8.91E-04	4 sources; N/D	NPRD-95 (Ref. C5.40)
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation	L	5.00E+00		1.34E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
AXL-FOH	Axle Failure	G	5.00E-01 <sup>b</sup>		1.60E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
B38-FOH	Bearing Failure	L	1.13E+01		2.50E-06	8 sources; N/D	NPRD-95 (Ref. C5.40)
BEA-BRK	Lifting Beam/Boom Breaks	G	1.50E+00		2.40E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
BLD-RUP	Air Bag Ruptures	B	1.10E+04	1.36E-04		1 source; N/D	BSC 2007 (Ref. C5.7)
BLK-FOD	Block or Sheaves Failure on Demand	B	1.30E+06	1.15E-06		1 source; N/D	NPRD-95 (Ref. C5.40)
BRH-FOD	Brake (Hydraulic) Failure on Demand	L	5.50E+01	8.96E-06		3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
BRK-FOD	Brake Failure on Demand	L	6.30E+00	1.46E-06		3 sources; mean + EF	EPRI PRA (Ref. C5.8)
BRK-FOH	Brake (Electric) Failure	G	2.50E+00		4.40E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
BRP-FOD	Brake (Pneumatic) Failure on Demand	L	2.55E+00	5.02E-05		4 sources; N/D	NPRD-95 (Ref. C5.40)
BRP-FOH	Brake (Pneumatic) Failure	L	2.55E+00		8.38E-06	4 sources; N/D	NPRD-95 (Ref. C5.40)
BTR-FOD	Battery No Output Given Challenge	B	6.05E+01	8.20E-03		1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
BTR-FOH	Battery Failure	L	4.30E+00		4.29E-06	12 sources N/D; 8 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5. 16), SAIC Umatilla (Ref. C5.41)
BUA-FOH	AC Bus Failure	L	3.08E+00		6.10E-07	3 sources; N/D	IEEE 493 (Ref. C5. 22), NUREG/CR-6928 (Ref. C5. 16)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
BUD-FOH	DC Bus Failure	L	8.70E+01		2.40E-07	1 source mean + EF	IEEE-500 (Ref. C5.23)
BYC-FOH	Battery Charger Failure	L	1.00E+01		7.60E-06	1 source mean + EF	CCPS (Ref. C5.1)
C52-FOD	Circuit Breaker (AC) Fails on Demand	L	9.80E+00	2.24E-03		19 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
C52-SPO	Circuit Breaker (AC) Spurious Operation	L	2.29E+01		5.31E-06	12 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-6928 (Ref. C5.16), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
C72-SPO	Circuit Breaker (DC) Spurious Operation	L	1.20E+00		1.07E-06	3 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
CAM-FOH	Cam Lock Fails	L	8.30E+01		3.19E-06	4 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
CBP-OPC	Cables (Electrical Power) Open Circuit	G	5.00E-01		9.13E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CBP-SHC	Cables (Electrical Power) Short Circuit	G	5.00E-01		1.88E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CKV-FOD	Check Valve Fails on Demand	L	1.36E+01	6.62E-04		4 sources N/D; 7 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
CKV-FTX	Check Valve Fails to Check	L	1.50E+01	2.20E-03		1 source; mean + EF	CCPS (Ref. C5.1)
CON-FOH	Electrical Connector (Site Transporter) Failure	G	5.00E-01		7.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
CPL-FOH	Coupling (Automatic) Failure	L	5.00E+00		1.90E-06	1 source mean + EF	AIAA (Ref. C5.11)
CPO-FOH	Control System Onboard [TEV or Trolley] Failure	G	9.85E+01		2.10E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CRD-FOH	Card Reader Failure	L	5.00E+00		4.55E-05	1 source mean + EF	HID (Ref. C5.21)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
CRJ-DRP	Jib Crane Drop	B	9.72E+04	2.60E-05		1 source; N/D	NUREG-1774 (Ref. C5.26)
CRN-DRP	200 Ton Crane Drop	L	4.35E+01	3.21E-05		2 sources N/D; 4 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26), EPRI PRA (Ref. C5.8)
CRN-TBK	200 Ton Crane Two Block Drop	L	1.15E+01	4.41E-07		1 source N/D; 3 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26)
CRS-DRP	200 Ton Crane Sling Drop	B	2.06E+04	1.21E-04		1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-DRP	WP (Non-Single Failure Proof) Crane Drop	B	3.34E+04	1.05E-04		1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-TBK	WP (Non-Single Failure Proof) Crane Two Block Drop	B	3.34E+04	4.49E-05		1 source; N/D	NUREG-1774 (Ref. C5.26)
CSC-FOH	Cask Cradle Failure	G	1.50E+00		4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CT-FOD	Controller Mechanical Jamming	L	5.00E+00 <sup>b</sup>	4.00E-06		1 source; mean + EF	EPRI PRA (Ref. C5.8)
CT-FOH	Controller Failure	L	1.00E+01		6.88E-05	1 source mean + EF	CCPS (Ref. C5.1)
CT-SPO	Controller Spurious Operation	L	1.00E+01		2.27E-05	1 source mean + EF	CCPS (Ref. C5.1)
CTL-FOD	Logic Controller Fails on Demand	L	1.10E+01	2.03E-03		3 sources; N/D	NUREG/CR-6928 (Ref. C5.16)
DER-FOM	Derailment Failure per Mile	G	3.97E+03		1.18E-05	1 source; N/D	Federal Railroad Administration (Ref. C5.17)
DG-FTR	Diesel Generator Fails to Run	L	1.51E+01		4.08E-03	8 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
DG-FTS	Diesel Generator Fails to Start	L	3.50E+00	8.38E-03		9 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days	G	5.05E+01		8.27E-04	1 source, N/D	NUREG/CR-6890 (Ref. C5.15)
DM-FOD	Drum Failure on Demand	L	1.00E+01	4.00E-08		2 sources mean + EF	EPRI PRA (Ref. C5.8)
DM-MSP	Drum Misspooling (Hourly)	G	5.00E-01		6.86E-07	1 source, N/D	NPRD-95 (Ref. C5.40)
DMP-FOH	Damper (Manual) Fails to Operate	L	4.30E+00		5.94E-06	3 sources mean + EF	IEEE-500 (Ref. C5.23), N-Reactor (Ref. C5.46), Moss (Ref. C5.32)
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)	L	3.20E+00		8.38E-08	2 sources N/D; 2 sources mean + EF	NUREG/CR-3154 (Ref. C5.6), NUREG/CR-1363 (Ref. C5.28), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
DMS-FOH	Demister (Moisture Separator) Failure	L	5.00E+00		9.12E-06	1 source mean + EF	EPRI AP-2071 (Ref. C5.10)
DRV-FOH	Drive (Adjustable Speed) Failure	G	5.0E-01		2.5E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
DRV-FSO	Drive (Adjustable Speed) Failure to Stop on Demand	B	2.5E+02		3.4E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
DTC-RUP	Duct Ruptures	L	2.6E+01		3.7E-06	9 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5), SAIC Umatilla (Ref. C5.41)
DTM-FOD	Damper (Tornado) Failure on Demand	L	5.0E+00	8.7E-04		1 source; mean + EF	IEEE-500 (Ref. C5.23)
DTM-FOH	Damper (Tornado) Failure	L	7.9E+00		2.3E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
ECP-FOH	Position Encoder Failure	G	5.0E-01		1.8E-06	2 sources; N/D	NPRD-95 (Ref. C5.40)

C-39

March 2008

Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis

000-PSA-MGR0-00900-000-00A

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)	L	5.0E+00	2.5E-04		1 source; mean + EF	EPRI PRA (Ref. C5.8)
FAN-FTR	Fan (Motor-Driven) Fails to Run	L	4.6E+01		7.21E-05	11 sources N/D; 6 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand	L	1.0E+01	2.0E-03		7 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
FRK-PUN	Forklift Puncture	L	1.06E+01		1.20E-05	1 source mean + EF	SAIC Umatilla (Ref. C5.41)
G65-FOH	Governor Failure	G	1.82E+02		1.16E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
GPL-FOD	Grapple Failure on Demand	B	1.30E+06	1.15E-06		1 source; N/D	NPRD-95 (Ref. C5.40)
GRB-FOH	Gear Box Failure	L	1.40E+01		2.21E-04	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
GRB-SHH	Gear box Shaft/Coupling Shears	L	5.00E+00		2.40E-06	1 source; mean + EF	EPRI PRA (Ref. C5.8)
GRB-STH	Gear Box Stripped	L	5.00E+00		7.86E-08	1 source; mean + EF	NPRD-95 (Ref. C5.40)
HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	L	8.39E+01	1.74E-03		1 source N/D; 3 sources mean + EF	EPRI PRA (Ref. C5.8), NPRD-95 (Ref. C5.40)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation	G	5.00E-01		5.23E-07	1 source N/D	NPRD-95 (Ref. C5.40)
HEP-LEK	Filter (HEPA) Leaks [Bypassed]	L	1.00E+01		3.00E-06	1 source; mean + EF	SRS Reactors (Ref. C5.5)
HEP-PLG	Filter (HEPA) Plugs	L	9.5E+00		4.3E-06	3 sources N/D; 2 sources mean + EF	IEEE-500 (Ref. C5.23), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)

C-40

March 2008

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
HOS-LEK	Hose Leaking	L	2.47E+01		1.48E-05	same as HOS-RUP with factor of 10	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
HOS-RUP	Hose Ruptures	L	2.47E+01		1.48E-06	2 sources N/D; 3 sources mean + EF	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
IEL-FOD	Interlock Failure on Demand	L	5.0E+00	2.8E-05		1 source; mean + EF	NPRD-95 (Ref. C5.40)
IEL-FOH	Interlock Failure	L	5.50E+01		3.43E-05	4 sources; N/D	NPRD-95 (Ref. C5.40)
LC-FOD	Level Controller Failure on Demand	B	6.07E+03	6.25E-04		1 source; N/D	NUREG/CR-6928 (Ref. C5.16)
LRG-FOH	Lifting Rig or Hook Failure	G	4.65E+01		7.45E-07	1 source; N/D	NPRD-95 (Ref. C5.40)
LVR-FOH	Lever (two position; up-down) Failure	G	9.85E+01		2.10E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
MCC-FOH	Motor Control Centers (MCCs) Failure	L	1.00E+01		7.49E-06	composite of Relay (RLY-FTP) + Motor Starter (MST FOH) + Limit Switch (ZS-FOH)	
MOE-FOD	Motor (Electric) Fails on Demand	L	5.00E+00	6.00E-05		1 source; mean + EF	EPRI PRA (Ref. C5.8)
MOE-FSO	Motor (Electric) Fails to Shut Off	L	1.07E+01		1.35E-08	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MOE-FTR	Motor (Electric) Fails to Run	L	9.50E+00		6.50E-06	8 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), OREDA-2002 (Ref. C5.43)
MOE-FTS	Motor (Electric) Fails to Start (Hourly)	L	1.90E+01		7.14E-06	5 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40)
MOE-SPO	Motor (Electric) Spurious Operation	L	1.07E+01		6.74E-07	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MSC-FOH	Motor Speed Control Module Failure	G	5.00E-01		1.28E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
MST-FOH	Motor Starter Failure	L	1.33E+00		1.43E-07	2 sources; N/D	IEEE 493 (Ref. C5.22)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
NZL-FOH	Nozzle Failure	L	7.50E+00		2.85E-06	5 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PIN-BRK	Pin (Locking or Stabilization) Breaks	L	1.46E+00		2.12E-09	4 sources; N/D	NPRD-95 (Ref. C5.40)
PLC-FOD	Programmable Logic Controller Fails on Demand	B	1.35E+03	3.69E-04		1 source; N/D	NPRD-95 (Ref. C5.40)
PLC-FOH	Programmable Logic Controller Fails to Operate	L	1.00E+01		3.26E-06	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PLC-SPO	Programmable Logic Controller Spurious Operation	L	1.00E+01		3.65E-07	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PMD-FTR	Pump (Motor Driven) Fails to Run	L	9.9E+00		3.5E-05	6 sources N/D; 87 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand	L	3.80E+00	2.50E-03		7 sources N/D; 80 sources mean + EF	N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PPL-RUP	Piping (Lined) Catastrophic	L	1.50E+01		4.42E-07	1 source; mean + EF	CCPS (Ref. C5.1)
PPM-PLG	Piping (Water) Plugs	L	1.35E+01		7.26E-07	1 source N/D; 2 sources mean + EF	DuPont (Ref. C5.14), EPRI Pipe Failure Study (Ref. C5.10), SAIC Umatilla (Ref. C5.41)
PPM-RUP	Piping (Water) Ruptures	L	2.00E+01		8.75E-10	1 source; mean + EF	NUREG/CR-6928 (Ref. C5.16)
PR-FOH	Passive restraint (bumper) Failure	G	2.09E+02		4.45E-10	1 source; N/D	NPRD-95 (Ref. C5.40)

C-42

March 2008

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
PRM-FOH	eProm (HVAC Speed Control) Failure	G	5.00E-01		5.38E-07	1 source; N/D	MIL-HDBK-217F (Ref. C5.12)
PRV-FOD	Pressure Relief Valve Fails on Demand	L	2.72E+01	6.54E-03		6 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
PV-SPO	Pneumatic Valve Spurious Operation	G	5.00E-01		2.92E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
QDV-FOH	Quick Disconnect Valve Failure	L	3.56E+00		4.26E-06	4 sources N/D	NPRD-95 (Ref. C5.40)
RCV-FOH	Air Receiver Fails to Supply Air	L	1.00E+01		6.00E-07	1 source; mean + EF	IEEE-500 (Ref. C5.23)
RLY-FTP	Relay (Power) Fails to Close/Open	G	5.00E-01		8.77E-06	1 source N/D	NPRD-95 (Ref. C5.40)
SC-FOH	Speed Control Failure	G	5.00E-01		1.28E-04	1 source N/D	NPRD-95 (Ref. C5.40)
SC-SPO	Speed Control Spurious Operation	G	5.00E-01		3.20E-05	1 source N/D	NPRD-95 (Ref. C5.40)
SEL-FOH	Speed Selector Fails	L	5.34E+00		4.16E-06	3 sources N/D	NPRD-95 (Ref. C5.40)
SEQ-FOD	Sequencer Fails on Demand	B	7.49E+02	3.33E-03		1 source N/D	NUREG/CR-6928 (Ref. C5.16)
SFT-COL	Spent Fuel Transfer Machine (SFTM) Collision or Impact	L	4.00E+00	2.94E-06		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SFT-DRP	Spent Fuel Transfer Machine (SFTM) Drop	L	3.00E+00	5.15E-06		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SFT-RTH	Spent Fuel Transfer Machine (SFTM) Raised Fuel Too High	L	7.00E+00	7.36E-07		2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SJK-FOH	Screw Jack [TEV] Failure	G	5.00E-01		8.14E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SRF-FOH	Flow Sensor Failure	G	5.00E-01		1.07E-06	1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
SRP-FOD	Pressure Sensor Fails on Demand	B	1.25E+02	4.00E-03		1 source; N/D	NPRD-95 (Ref. C5.40)
SRP-FOH	Pressure Sensor Fails	L	1.21E+01		2.95E-06	8 sources N/D	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16)
SRR-FOH	Radiation Sensor Fails	L	5.00E+00		2.00E-05	1 source; mean + EF	Laurus (Ref. C5.25)
SRS-FOH	OverSpeed Sensor Fails	G	1.28E+02		2.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)



Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand	L	2.10E+00	7.33E-04		2 sources N/D	NUREG/CR-6928 (Ref. C5.16), OREDA-92 (Ref. C5.42)
SRT-FOH	Temperature Sensor/Transmitter Fails	L	1.41E+01		7.05E-07	4 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43)
SRT-SPO	Temperature Sensor Spurious Operation	L	2.80E+01		2.23E-06	1 source; mean + EF	OREDA-2002 (Ref. C5.43)
SRU-FOH	Ultrasonic Sensor Fails	G	5.00E-01		9.62E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
SRV-FOH	Vibration Sensor (Accelerometer) Fails	L	1.07E+01		9.40E-05	4 sources N/D	NPRD-95 (Ref. C5.40)
SRX-FOD	Optical Position Sensor Fails on Demand	B	3.18E+03	1.10E-03		1 source; N/D	SAIC Umatilla (Ref. C5.41)
SRX-FOH	Optical Position Sensor Fails	L	5.00E+00		4.70E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
STU-FOH	Structure (truck or railcar) Failure	G	1.50E+00		4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
SV-FOD	Solenoid Valve Fails on Demand	L	1.17E+01	6.28E-04		4 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NSWG-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
SV-FOH	Solenoid Valve Fails	L	1.70E+01		4.87E-05	1 source; mean + EF	CCPS (Ref. C5.1)
SV-SPO	Solenoid Valve Spurious Operation	L	3.00E+00		4.09E-07	1 source; mean + EF	CCPS (Ref. C5.1)
SWA-FOH	Auto-Stop Switch (CTT hose travel) Fails	G	6.50E+00		3.12E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SWG-FOH	13.8kV Switchgear Fails	G	2.85E+01		1.31E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-FTX	Electric Power Switch Fails to Transfer	G	6.50E+00		3.59E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-SPO	Electric Power Switch Spurious Transfer	G	6.50E+00		1.55E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
TD-FOH	Transducer Failure	L	4.70E+00		9.84E-05	3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)

C-44

March 2008

Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis

000-PSA-MGR0-00900-000-00A

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
TDA-FOH	Transducer (Air Flow) Failure	L	6.21E+00		1.65E-04	2 sources N/D	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDP-FOH	Transducer (Pressure) Fails	L	5.35E+01		2.20E-04	23 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDT-FOH	Transducer (Temperature) Fails	L	2.95E+01		1.04E-04	12 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
THR-BRK	Third Rail Breaks	L	1.00E+01		1.01E-08	1 source; mean + EF	NPRD-95 TRK-BRK adjusted with failure information from Federal Railroad Administration Safety Data website (Ref. C5.17)
TKF-FOH	Fuel Tank Fails	L	1.11E+01		4.40E-07	15 sources; N/D	NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
TL-FOH	Torque Limiter Failure	G	8.05E+01		8.05E-05	1 source N/D	NPRD-95 (Ref. C5.40)
TRD-FOH	Tread (Site Transporter)	L	3.40E+00		5.89E-07	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), Rand (Ref. C5.38)
UDM-FOH	Damper (Backdraft) Failure	L	7.90E+00		2.26E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
UPS-FOH	Uninterruptible Power Supply (UPS) Failure	L	5.08E+00		2.02E-06	10 sources; N/D	NPRD-95 (Ref. C5.40)
WNE-BRK	Wire Rope Breaks	L	5.00E+00	2.00E-06		1 source; mean + EF	EPRI PRA (Ref. C5.8)
XMR-FOH	Transformer Failure	L	1.53E+01		2.91E-07	13 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
XV-FOD	Manual Valve Failure on Demand	L	1.00E+01	6.48E-04		3 sources N/D; 12 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
ZS-FOD	Limit Switch Failure on Demand	L	5.7E+00	2.9E-04		3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5)

C-45

March 2008

Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis

000-PSA-MGR0-00900-000-00A

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist Type	Uncert Value	Demand Probability	Hourly Failure Rate	Number of Inputs	Input Data Sources <sup>a</sup>
ZS-FOH	Limit Switch Fails	L	6.03E+00		7.23E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)
ZS-SPO	Limit Switch Spurious Operation	L	5.56E+00		1.28E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)

NOTE: <sup>a</sup> Refer to Section C1.2 for specific citation to data sources.

<sup>b</sup> There are minor differences between the specific values tagged by this footnote and those used to quantify the SAPHIRE model. Such differences are not meaningful in the context of this analysis because (a) the difference pertains only to the uncertainty of the component reliability or (b) the uncertainty in the reliability value is much greater than difference between the value given here and that used in the model.

B = Beta Distribution; EF = Lognormal Error Factor; G = Gamma Distribution; L = Lognormal Distribution; N/D = Numerator/Denominator

Source: Original

## C5 REFERENCES; DESIGN INPUTS

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

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

- C5.1 \*AIChE (American Institute of Chemical Engineers) 1989. *Guidelines for Process Equipment Reliability Data with Data Tables*. G-07. New York, New York: American Institute of Chemical Engineers, Center for Chemical Process Safety. TIC: 259872. ISBN: 978-0-8169-0422-8.
- C5.2 \*Apostolakis, G. and Kaplan, S. 1981. "Pitfalls in Risk Calculations." *Reliability Engineering*, 2, 135-145. [Barking], England: Applied Science Publishers. TIC: 253648.
- C5.3 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.
- C5.4 \*Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.
- C5.5 \*Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U)*. WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.
- C5.6 \*Borkowski, R.J.; Kahl, W.K.; Hebble, T.L.; Fragola, J.R.; Johnson, J.W. 1983. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve-Component*. NUREG/CR-3154; ORNL/TM-8647. Oak Ridge, TN: Oak Ridge National Laboratory. ACC: MOL.20071129.0315.
- C5.7 BSC 2007 (Bechtel SAIC Company). *Waste Form Throughputs for Preclosure Safety Analysis*. 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.
- C5.8 \*Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report*. 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.
- C5.9 \*Crutchfield, D.M. 1996. "Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment." NRC Bulletin 96-02. Washington,

- D.C.: U.S. Nuclear Regulatory Commission. Accessed February 12, 2008.  
ACC: MOL.20080213.0021. URL: <http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1996/bl96002.html>
- C5.10 \*Derdiger, J.A.;Bhatt, K.M.;Siegfriedt, W.E. 1981. *Component Failure and Repair Data for Coal-Fired Power Units*. EPRI AP-2071. Palo Alto, CA: Electric Power Research Institute. TIC: 260070.
- C5.11 \*Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications*. AIAA Education Series. Washington, D.C.: American Institute of Aeronautics & Astronautics. TIC: 259878.
- C5.12 \*DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment*. MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.
- C5.13 \*Drago, J.P.; Borkowski, R.J.; Fragola, J.R.; and Johnson, J.W. 1982. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report — The Pump Component*. NUREG/CR-2886. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0222.
- C5.14 \*E.I. DuPont de Nemours & Company (Inc.) 1981. *Some Published and Estimated Failure Rates for Use in Fault Tree Analysis*. Washington, DE: E.I. DuPont de Nemours & Company (Inc). (DIRS 184415)
- C5.15 \*Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Station Blackout Risk*. Volume 2 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants*. NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0165.
- C5.16 \*Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; Rasmuson, D.M.; and Atwood, C.T. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*. NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.
- C5.17 \*Federal Railroad Administration. 2004. “Train Accidents by Cause from Form FRA F 6180.54.” Washington, D.C.: U.S. Department of Transportation, Federal Railroad Administration. Accessed 03/12/2004. ACC: MOL.20040311.0211. URL: <http://safetydata.fra.dot.gov/OfficeofSafety/Query/Default.asp>
- C5.18 \*Fleming, K.N. 1975. *A Reliability Model for Common Mode Failures in Redundant Safety Systems*. GA-A13284. San Diego, California: General Atomic Company. ACC: MOL.20071219.0221.
- C5.19 \*Fragola, J.R. and McFadden, R.H. 1995. “External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom.” *Reliability Engineering and System Safety*, 47, 255-273. [New York, New York]: Elsevier. TIC: 259675.

- C5.20 \*Framatome ANP (Advanced Nuclear Power) 2001. *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999*. [Lynchburg, Virginia]: Framatome Advanced Nuclear Power. ACC: MOL.20011018.0158.
- C5.21 \*HID Corporation [n.d.]. *Ruggedized Card Reader/Ruggedized Keypad Card Reader. Dorado 740 and 780*. Irvine, California: HID Corporation. TIC: 260007.
- C5.22 \*IEEE (Institute of Electrical and Electronics Engineers) Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205. ISBN: 1-55937-969-3.
- C5.23 \*IEEE Std 500-1984 (Reaffirmed 1991). 1991. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 256281.
- C5.24 \*Kahl, W.K. and Borkowski, R.J. 1985. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report - Diesel Generators, Batteries, Chargers, and Inverters*. NUREG/CR-3831. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071212.0181.
- C5.25 \*Laurus Systems [n.d.]. *Instruments and Software Solutions for Emergency Response and Health Physics*. Ellicott City, Maryland: Laurus Systems. TIC: 259965.
- C5.26 Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.
- C5.27 \*Lopez Droguett, E.; Groen, F.; and Mosleh, A. 2004. "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety*, 83, 311-321. New York, New York: Elsevier. TIC: 259380.
- C5.28 \*Miller, C.F.; Hubble, W.H.; Trojovsky, M.; and Brown, S.R. 1982. *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980*. NUREG/CR-1363, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0223.
- C5.29 \*Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques*. Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.
- C5.30 \*Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Procedural Framework and Examples*. Volume 1 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

- C5.31 \*Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106.
- C5.32 \*Moss, T.R. 2005. *The Reliability Data Handbook*. 1st Edition. New York, New York: ASME Press (American Society of Mechanical Engineers). ISBN: 0-7918-0233-7. TIC: 259912.
- C5.33 Not Used.
- C5.34 NRC (U.S. Nuclear Regulatory Commission) 1979. *Single-Failure-Proof Cranes for Nuclear Power Plants*. NUREG-0554. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 232978.
- C5.35 NRC 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.
- C5.36 NRC 2005. *CCF Parameter Estimation 2005*. Washington, D.C.: Nuclear Regulatory Commission (NRC). ACC: MOL.20080213.0022.
- C5.37 \*NSWC (Naval Surface Warfare Center) 1998. *Handbook of Reliability Prediction Procedures for Mechanical Equipment*. NSWC-98/LE1. West Bethesda, Maryland: Naval Surface Warfare Center, Carderock Division. TIC: 245703.
- C5.38 \*Peltz, E.; Robbins, M.; Boren, P.; Wolff, M. 2002. "Using the EDA to Gain Insight into Failure Rates." *Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer*. Santa Monica, CA: RAND. TIC: 259917. ISBN: 0-8330-3115-5.
- C5.39 \*Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data*. NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.
- C5.40 \*Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995*. NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.
- C5.41 \*SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment*. Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.
- C5.42 \*SINTEF Industrial Management 1992. *OREDA, Offshore Reliability Data Handbook*. 2nd Edition. Trondheim, Norway: OREDA. ISBN: 825150188.1
- C5.43 \*SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook*. 4th Edition. Trondheim, Norway: OREDA. ISBN: 8214027055. TIC: 257402.

- C5.44 \*Siu, N.O. and Kelly, D.L. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment." *Reliability Engineering and System Safety*, 62, 89-116. New York, New York: Elsevier. TIC: 258633.
- C5.45 \*Trojovsky, M. 1982. *Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1980*. NUREG/CR-1205, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20080207.0024.
- C5.46 \*Zentner, M.D.; Atkinson, J.K.; Carlson, P.A.; Coles, G.A.; Leitz, E.E.; Lindberg, S.E.; Powers, T.B.; and Kelly, J.E. 1988. *N Reactor Level 1 Probabilistic Risk Assessment: Final Report*. WHC-SP-0087. Richland, Washington: Westinghouse Hanford Company. ACC: MOL.20080207.0021.



**ATTACHMENT D**  
**PASSIVE EQUIPMENT FAILURE ANALYSIS**

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	D-6
D1 LOSS OF CONTAINMENT DUE TO DROPS AND IMPACTS .....	D-8
D1.1 LAWRENCE LIVERMORE NATIONAL LABORATORY ANALYSIS OF CANISTERS AND CASKS .....	D-9
D1.2 IDAHO NATIONAL LABORATORY ANALYSIS OF SPENT NUCLEAR FUEL CANISTERS AND MULTICANISTER OVERPACKS .....	D-13
D1.3 PROBABILITIES OF FAILURE OF HIGH LEVEL WASTE CANISTERS DUE TO DROPS .....	D-20
D1.4 PROBABILITIES OF FAILURE OF WASTE PACKAGES DUE TO DROPS AND IMPACTS .....	D-21
D1.5 PREDICTING OUTCOMES OF OTHER SITUATIONS BY EXTRAPOLATING STRAINS FOR MODELED SCENARIOS .....	D-27
D1.6 MISCELLANEOUS SCENARIOS .....	D-28
D2 PASSIVE FAILURE DUE TO FIRE .....	D-30
D2.1 ANALYSIS OF CANISTER FAILURE DUE TO FIRE .....	D-30
D2.2 SHIELDING DEGRADATION IN A FIRE .....	D-68
D3 SHIELDING DEGRADATION DUE TO IMPACTS .....	D-72
D3.1 DAMAGE THRESHOLDS FOR LOS .....	D-73
D3.2 SEVERITY OF DAMAGE VERSUS IMPACT VELOCITY .....	D-74
D3.3 ESTIMATE OF THRESHOLD SPEEDS FOR LOSS OF SHIELDING DUE TO IMPACTS .....	D-78
D3.4 PROBABILITY OF LOSS OF SHIELDING .....	D-80
D4 REFERENCES .....	D-86
D4.1 DESIGN INPUTS .....	D-86
D4.2 DESIGN CONSTRAINTS .....	D-92

## FIGURES

	<b>Page</b>
D1.1-1.	Original and Shifted Cumulative Distribution Functions (CDF) for Capacity (or Fragility) Plotted as a Function of True Strain ..... D-10
D2.1-1.	Comparison Between Results Calculated Using the Simplified Heat Transfer Model and ANSYS – Fire Engulfing a TAD Canister in a Waste Package ..... D-43
D2.1-2.	Plot of Larson-Miller Parameter for Type 316 Stainless Steel ..... D-55
D2.1-3.	Yield, Ultimate, and Flow Stress for Type 316 Stainless Steel ..... D-56
D2.1-4.	Probability Distribution for the Failure Temperature of Thin-Walled Canisters..... D-59
D2.1-5.	Probability Distribution for the Failure Temperature of Thick-Walled Canisters..... D-60
D2.1-6.	Probability Distribution for Maximum Canister Temperature – Thin-Walled Canister in a Waste Package ..... D-62
D2.1-7.	Distribution of Radiation Energy from Fire..... D-67
D3.2-1.	Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph ..... D-76
D3.2-2.	Truck Steel/Lead/Steel Inner Shell Strain versus Impact Speed ..... D-77
D3.2-3.	Rail Steel/Lead/Steel Strain versus Impact Speed ..... D-78
D3.4-1.	Summary Event Tree Showing Model Logic for Canisters and Aging Overpacks ..... D-81

**TABLES**

	<b>Page</b>
D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1 .....	D-10
D1.2-1. Container Configurations and Loading Conditions .....	D-13
D1.2-2. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for Representative Canister within an Aging Overpack .....	D-14
D1.2-3. Failure Probabilities with and without Triaxiality Factor, with and without Fragility Curve Adjustment, for Representative Canister .....	D-15
D1.2-4. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Representative Canister inside the Transportation Cask .....	D-16
D1.2-5. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Transportation Cask .....	D-17
D1.2-6. Strains at Various Canister Locations Due to Drops .....	D-18
D1.2-7. Failure Probabilities for the DOE Spent Nuclear Fuel (DSNF) Canisters and Multicanister Overpack (MCO) .....	D-19
D1.4-1. Waste Package Probabilities of Failure for Various Drop and Impact Events .....	D-23
D1.5-1. Calculated Strains and Failure Probabilities for Given Side Impact Velocities .....	D-28
D2.1-1. Probability Distribution for Fire Duration - Without Automatic Fire Suppression .....	D-33
D2.1-2. Probability Distribution for Fire Duration - With Automatic Fire Suppression .....	D-35
D2.1-3. Effective Thermal Properties for 21-PWR Fuel in a TAD .....	D-39
D2.1-4. Model Inputs – Bare Canister .....	D-46
D2.1-5. Model Inputs – Canister in a Waste Package .....	D-47
D2.1-6. Model Inputs – Canister in Transportation Cask .....	D-48
D2.1-7. Model Inputs – Canister in a Shielded Bell .....	D-50
D2.1-8. Summary of Canister Failure Probabilities in Fire .....	D-62
D2.1-9. Model Inputs – Bare Fuel Cask .....	D-65
D2.1-10. Summary of Fuel Failure Probabilities .....	D-66
D2.1-11. Probabilities that Radiation Input Exceeds Failure Energy for Cask .....	D-68
D3.2-1. Maximum Plastic Strain in Inner Shell of Sandwich Wall Casks .....	D-75
D3.3-1. Drop Height to Reach a Given Impact Speed .....	D-80
D3.3-2. Impact Speeds on Real Target for Equivalent Damage for Unyielding Targets .....	D-80

**TABLES (Continued)**

	<b>Page</b>
D3.4-1. Probabilities of Degradation or Loss of Shielding.....	D-85

---

## ACRONYMS AND ABBREVIATIONS

### Acronyms

ASME	American Society of Mechanical Engineers
CDF	cumulative distribution function
COV	coefficient of variation
CTM	canister transfer machine
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EPS	equivalent (or effective) plastic strain
ETF	expended toughness fraction
FEA	finite element analysis
HLW	high-level radioactive waste
INL	Idaho National Laboratory
LLNL	Lawrence Livermore National Laboratory
MCO	multicanister overpack
PCSA	preclosure safety analysis
PDF	probability density function
PWR	pressurized water reactor
SAR	Safety Analysis Report
SFC	spent fuel canister
SLS	steel-lead-steel
SNF	spent nuclear fuel
TAD	transportation, aging, and disposal
TEV	transport and emplacement vehicle
WPTT	waste package transfer trolley

---

## ACRONYMS AND ABBREVIATIONS (Continued)

### Abbreviations

C	Celsius
cm	centimeter
F	Fahrenheit
ft	foot, feet
hr, hrs	hour, hours
J	joule
K	Kelvin
kg	kilogram
kV	kilovolt
kW	kilowatt
LOS	loss of shielding
m	meter
min	minute, minutes
m/s	meters/second
mrem	millirem
MPa	megapascal
mph	miles per hour
psig	pounds per square inch gauge
rem	roentgen equivalent man
W/m K	watt per meter Kelvin
W/m <sup>2</sup> K	watt per square meter Kelvin

## **ATTACHMENT D**

### **PASSIVE EQUIPMENT FAILURE ANALYSIS**

Many event sequences described in Section 6.1 include pivotal events that arise from loss of integrity of a passive component, namely one of the aging overpacks, casks, or canisters that contain a radioactive waste form. Such pivotal events involve (1) loss of containment of radioactive material that may result in airborne releases, or (2) loss of shielding effectiveness. Both types of pivotal events may be failure modes caused by either physical impact to the container or by thermal energy transferred to the container. This attachment presents the results of passive failure analyses that provide conditional probability of loss of containment or loss of shielding. Many scenarios were selected for analysis as representative or bounding for anticipated scenarios in the risk assessment. Results of some scenarios may not have been used in the final event sequence quantification.

#### **D1 LOSS OF CONTAINMENT DUE TO DROPS AND IMPACTS**

The category of passive equipment includes canisters and casks used during transport, aging, and disposal of spent nuclear fuel. The canisters and casks contain the spent fuel and provide containment of radioactive material. During transport and handling, the canisters and casks could be subjected to drops, impacts, or fires, which may result in loss of containment. The probabilities of loss of containment due to various physical or thermal challenges are evaluated primarily through structural and thermal analysis and drop test data.

Passive equipment (e.g., transportation casks, storage canisters, and waste packages) may fail from abnormal use such as defined by the event sequences. Studies were performed and passive equipment failure probabilities were determined using the methodologies summarized in Section 4.3.2.2. The probability of loss of containment (breach) was determined for several types of containers, including transportation casks (analyzed without impact limiters), shielded transfer casks, waste packages, TAD canisters, DPCs, DOE standardized canisters, MCOs, HLW canisters, and naval SNF canisters. The mechanical breach of TAD canisters, DPCs and naval SNF canisters were analyzed as representative canisters as described in Section D1.1. The structural analysis of DOE standardized canisters and MCOs for breaches is described in Section D1.2 and then the probabilistic methodology of Section D1.1 was applied. Transportation casks, site transfer casks (STCs) and horizontal STCs were analyzed as representative transportation casks as describe in Section D1.1. The probabilistic estimation of breach from mechanical loads of all other waste containers is described in Sections D1.3 through D1.6. The analysis of loss or degradation of shielding of casks and overpacks against mechanical loads is described in Section D3. The probabilistic analysis of fire severity and the associated effects on casks, canisters, and overpacks with respect to both containment breach and shielding degradation or loss is described in Section D2. The analysis of mechanical failures and thermal failures included the specific configuration defined by the event sequences. For example, if the event sequence occurred during a process in which the canister is within a transportation casks or aging overpack, the analysis is performed in that configuration.



## **D1.1 LAWRENCE LIVERMORE NATIONAL LABORATORY ANALYSIS OF CANISTERS AND CASKS**

Lawrence Livermore National Laboratory (LLNL) performed the FEA using Livermore Software–Dynamic Finite Element Program (LS-DYNA) to model drops and impacts for casks and canisters with selected properties for use as representative containers expected to be delivered to Yucca Mountain (Ref. D4.1.27). LS-DYNA, which has been used in nuclear facility and non-nuclear industrial applications, is appropriate to model nonlinear, transient responses of a passive component to a structural challenge such as a drop or an impact. Existing commercial casks and canisters that would likely be used on the Yucca Mountain Project (YMP) were identified and characterized. The cases analyzed are listed in Table D1.2-1.

Appropriate finite element models were developed for the representative cask, selected container types, configurations, and drop types. The level of detail for each model was selected to understand deformation and damage patterns, possible failure mode(s) in each structural element, and failure-related response. Special attention was required to properly model the bottom-weld and closure regions to ensure that coarser mesh of the simplified model would capture failure-related response with acceptable accuracy. A consistent failure criterion for each case was identified as part of the detailed analyses. The effective plastic strain in each element, in combination with material ductility data, was used to predict failure measures.

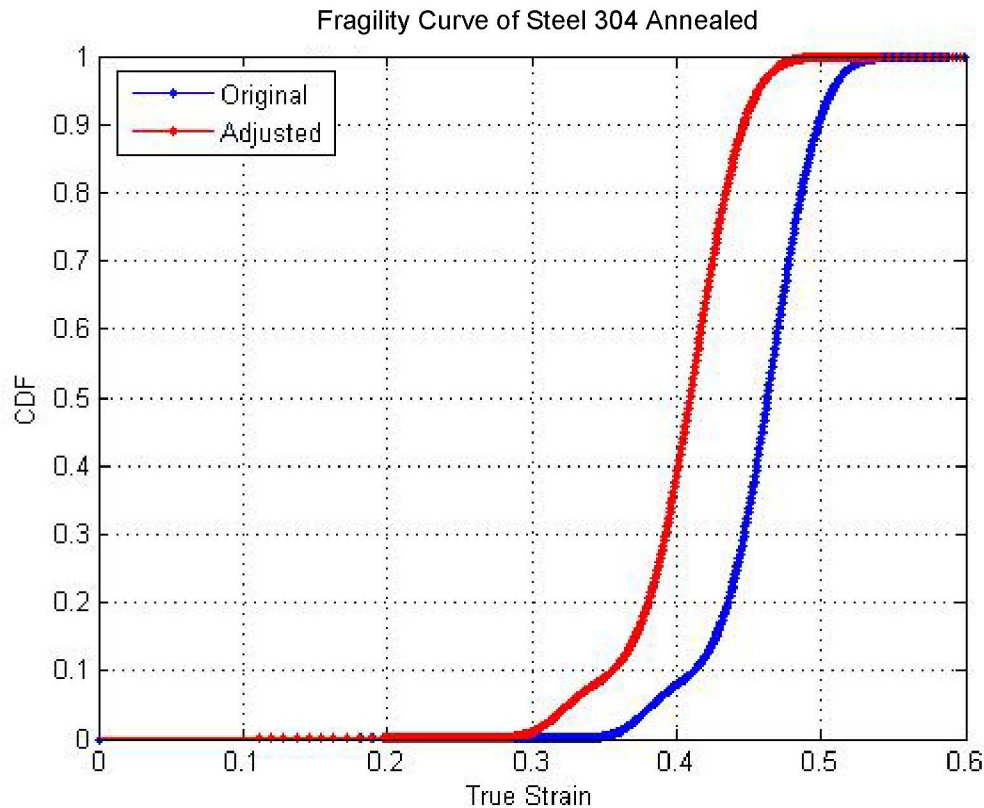
The maximum strain for each scenario was compared with the capacity distribution based on material properties to obtain containment failure probabilities using the methodology described in Section 4.3.2.2. For simplicity and consistency in interpreting results, the impact-surface conditions, including both the ground and the falling 10-ton load for the analyses, were considered infinitely stiff and unyielding, which is conservative.

The results of these cases are summarized in Tables D1.2-2 through D1.2-4. The bases for these results are summarized in the following paragraphs. If a probability for the event sequence is less than  $1.0 \times 10^{-8}$ , additional conservatism is incorporated in the PCSA by using a failure probability of  $1.0 \times 10^{-5}$ , which are termed “LLNL, adjusted”. This additional conservatism is added to account for a) future evolutions of cask and canister designs, and b) uncertainties, such as undetected material defects, undetected manufacturing deviations, and undetected damage associated with handling before the container reaches the repository, which are not included in the tensile elongation data.

LLNL developed a fragility curve for the base metal by fitting a mixture of two normal probability density functions (PDFs) to the engineering (tensile) strain data (Ref. D4.1.4). Both the data and their corresponding log-transforms were found to be non-normally distributed ( $p < 10^{-4}$ ) by the Shapiro-Wilk test (Ref. D4.1.62). These data collected at 100°F were determined to be reasonably well modeled as a sample from a weighted mixture of two normal distributions, one with a mean of 46% and a standard deviation of 2.24% (weight = 7.84%), and the other with a mean of 59.3% and a standard deviation of 4.22% (weight = 92.16%), with the goodness of fit ( $p = 0.939$ ) assessed by the Kolmogorov-Smirnov 1 sample test (Ref. D4.1.33).

The stainless steel used in the LLNL (Ref. D4.1.27) analysis is alloy 304L. The un-annealed alloys have relatively shorter elongations at failure than annealed 304L. Therefore, the base

Figure D1.1-1 fragility cumulative distribution function (CDF) model was adjusted to different steels used in a typical design and to meet the code specification of the material model used in LS-DYNA. The adjustment consisted of shifting the distribution by -8.3% (Ref. D4.1.27, p. 93). Thus the initial fragility curve was shifted by 8.3% to a lower value of minimum elongation. The fragility curves before and after the shift are shown in and tabulated in Table D1.1-1. 316L stainless steel might be used for construction of some canisters and casks, but the stress-strain curves would be similar.



Source: Ref. D4.1.27, Figure 6.3.7-3

Figure D1.1-1. Original and Shifted Cumulative Distribution Functions (CDF) for Capacity (or Fragility) Plotted as a Function of True Strain

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1

True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.00	-1.70	0.0000E+00	1.6754E-15	0.36	0.05	1.0506E-02	1.0973E-01
0.01	-1.65	2.0924E-16	1.8688E-15	0.37	0.10	2.3978E-02	1.4282E-01
0.02	-1.60	4.1848E-16	2.0622E-15	0.38	0.15	4.3259E-02	1.9679E-01
0.03	-1.55	6.2772E-16	2.2555E-15	0.39	0.19	6.2863E-02	2.7687E-01
0.04	-1.50	8.3696E-16	2.4489E-15	0.40	0.24	7.9100E-02	3.8310E-01

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1 (Continued)

True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.05	-1.45	1.0462E-15	2.6422E-15	0.41	0.29	9.5539E-02	5.0814E-01
0.06	-1.41	1.2554E-15	2.8356E-15	0.42	0.34	1.2068E-01	6.3823E-01
0.07	-1.36	1.4647E-15	3.0290E-15	0.43	0.39	1.6410E-01	7.5736E-01
0.08	-1.31	1.6739E-15	3.2223E-15	0.44	0.44	2.3393E-01	8.5309E-01
0.09	-1.26	1.8832E-15	3.4157E-15	0.45	0.48	3.3371E-01	9.2036E-01
0.10	-1.21	2.0924E-15	3.6090E-15	0.46	0.53	4.5893E-01	9.6161E-01
0.11	-1.16	2.3016E-15	3.8024E-15	0.47	0.58	5.9615E-01	9.8363E-01
0.12	-1.11	2.5109E-15	2.8601E-14	0.48	0.63	7.2682E-01	9.9385E-01
0.13	-1.07	2.7201E-15	2.3645E-13	0.49	0.68	8.3454E-01	9.9797E-01
0.14	-1.02	2.9294E-15	1.6225E-12	0.50	0.73	9.1117E-01	9.9941E-01
0.15	-0.97	3.1386E-15	9.7686E-12	0.51	0.78	9.5806E-01	9.9985E-01
0.16	-0.92	3.3478E-15	5.2952E-11	0.52	0.82	9.8270E-01	9.9997E-01
0.17	-0.87	3.5571E-15	2.6233E-10	0.53	0.87	9.9379E-01	9.9999E-01
0.18	-0.82	3.7663E-15	1.2513E-09	0.54	0.92	9.9807E-01	1.0000E+00
0.19	-0.78	2.1733E-14	6.9107E-09	0.55	0.97	9.9948E-01	1.0000E+00
0.20	-0.73	2.1209E-13	2.6769E-08	0.56	1.02	9.9988E-01	1.0000E+00
0.21	-0.68	1.7358E-12	1.1600E-07	0.57	1.07	9.9998E-01	1.0000E+00
0.22	-0.63	1.1373E-11	4.8126E-07	0.58	1.11	1.0000E+00	1.0000E+00
0.23	-0.58	6.4625E-11	1.9316E-06	0.59	1.16	1.0000E+00	1.0000E+00
0.24	-0.53	4.1126E-10	7.5246E-06	0.60	1.21	1.0000E+00	1.0000E+00
0.25	-0.48	2.4773E-09	2.8566E-05	0.61	1.26	1.0000E+00	1.0000E+00
0.26	-0.44	1.2132E-08	1.0566E-04	0.62	1.31	1.0000E+00	1.0000E+00
0.27	-0.39	5.2343E-08	3.7635E-04	0.63	1.36	1.0000E+00	1.0000E+00
0.28	-0.34	2.4478E-07	1.2625E-03	0.64	1.41	1.0000E+00	1.0000E+00
0.29	-0.29	1.0945E-06	3.8474E-03	0.65	1.45	1.0000E+00	1.0000E+00
0.30	-0.24	4.7123E-06	1.0185E-02	0.66	1.50	1.0000E+00	1.0000E+00
0.31	-0.19	1.9709E-05	2.2466E-02	0.67	1.55	1.0000E+00	1.0000E+00
0.32	-0.15	7.9860E-05	4.0237E-02	0.68	1.60	1.0000E+00	1.0000E+00
0.33	-0.10	3.1104E-04	5.9110E-02	0.69	1.65	1.0000E+00	1.0000E+00
0.34	-0.05	1.1366E-03	7.5125E-02	0.70	1.70	1.0000E+00	1.0000E+00
<b>0.35</b>	<b>0.00</b>	<b>3.7379E-03</b>	<b>8.9858E-02</b>				

NOTE: The mean for true strain is 0.35, shown in bold. The standard deviation (std) of true strain is 0.21.

Source: Ref. D4.1.27, Table 6.3.7.3-1

The weldment at best can have the same mechanical properties as the hosting metal (native metal), but it is usually more brittle than the hosting metal. The failure likelihood of the weldment substructure was considered, reflecting weighting factors of both 1.0 and 0.75 applied to estimated true strain at failure.

The capacity function is based on coupon tensile strength tests in uniaxial tension. However, cracking of a stainless steel may not be determined simply by comparing the calculated plastic strain to the true strain of failure, because the equivalent (or effective) plastic strain (EPS) is calculated from a complex 3-D state of stress, while the true strain at failure was based on data from a 1-D state of stress. A 3-D state of stress may constrain plastic flow in the material and lower the EPS at which failure occurs. This loss of ductility is accounted for by the use of a triaxiality factor, which is the ratio of normal stress to shear stress on the octahedral plane, normalized to unity for simple tension. For the purpose of determining the probability of structural failure, LLNL (Ref. D4.1.27) set the ductility ratio to 0.5. This is equivalent to a triaxiality factor of 2, which corresponds to a state of biaxial tension.

Failure of containment can occur when strain in a component is of sufficient magnitude that it results in breakage or puncture of the container. The probability of failure is calculated based on the maximum strain for a single finite element brick obtained from LS-DYNA simulations. Fracture propagation takes place on the milliseconds time-scale and thus propagates across the canister wall thickness very quickly, compared to the time-frame of the LS-DYNA simulations. Furthermore, the fragility curve is obtained on the basis of a maximum average strain over the thickness of the respective specimens, which are 2 in. long stainless steel 304L specimens. Although LS-DYNA results provide multiple values of the strain through the thickness of the canister wall (the wall thickness being represented by multiple finite element layers), it is more conservative to use the maximum strain value at a single finite element brick than the average of the multiple values across the thickness of the wall.

The probability of failure for each impact scenario is evaluated by finding the maximum strain at a location in which a through-wall crack would constitute a radionuclide release. A probability of failure is determined from the CDF of capacity or fragility curve (as discussed below) from the global maximum strain.

A conservative approach and aid to computational efficiency is achieved by performing calculations focusing on the regions of the container having high strain (and deformation) after a drop (“hot zones”). An importance sampling strategy was used which places greater-than-random emphasis on ranges of input-variable values, and/or on combinations of such value ranges, that are more likely to affect output. This approach is an alternative to Monte Carlo methods with the important advantage that possible combinations of upper-bound variable values are in fact incorporated into each probabilistic estimate of expected model output (which is not always guaranteed by uniform sampling).

Using the general probabilistic approach summarized here, LLNL (Ref. D4.1.27) calculated failure probabilities for representative canisters in an aging overpack, and in a transportation cask, and for the representative canister itself, as presented in Tables D1.2-2 through D1.2-5. For the drop of a 10-metric-ton load onto a cask, the falling mass is modeled as a rigid (unyielding) wall, oriented normal to longitudinal axis of the cask.

## D1.2 IDAHO NATIONAL LABORATORY ANALYSIS OF SPENT NUCLEAR FUEL CANISTERS AND MULTICANISTER OVERPACKS

Drop tests of prototype canisters conducted by the Idaho National Laboratory (INL) confirmed that the stainless steel shell material can undergo significant strains without material failure leading to loss of containment. These drop tests also validated analytical models used to predict strains under various drop scenarios. Table D1.2-6 shows scenarios selected to address potential drop scenarios at YMP facilities and the predicted strains.

INL performed FEA (using ABAQUS/Explicit, which, like LS-DYNA, has been used in nuclear facility and non-nuclear industrial applications, and is appropriate to model nonlinear, transient responses of a passive component to a structural challenge such as a drop or an impact) of 23-foot drops, three degrees off vertical, to determine the extent of strain at various positions in the bottom head, cylindrical shell, and joining weld. The strain was evaluated and reported for the inside, outside, and middle layers (Ref. D4.1.64). The U.S. Department of Energy (DOE) standardized spent nuclear fuel (SNF) canisters were modeled at 300°F, the maximum skin temperature expected due to the heat evolved by the fuel (based on review of thermal analyses performed by transportation casks vendors), resulting in diminished casing material strength. It was found that greater strains would be expected in the multicanister overpacks (MCOs) at ambient temperatures than at elevated temperatures.

During a canister drop event, the majority of the kinetic energy at impact performs work on the material, which causes the worst locations to exhibit plastic strain. A good measure of this work is equivalent plastic strain, which is a cumulative strain measure that takes into account the deformation history starting at impact. From the peak equivalent plastic strain, LLNL (Ref. D4.1.27) developed failure probabilities using the method described in Section D1.1 for an 18 in. and 24 in. DOE standard canister and an MCO. Results are summarized in Table D1.2-7.

Table D1.2-1. Container Configurations and Loading Conditions

Container	Configuration	Drop Type/Impact Condition <sup>a</sup>	Drop Height
AO (aging overpack) cell with canister inside	Representative canister inside AO	A IC 1: End with vertical orientation	3-ft vertical
		A IC 2: Slapdown from a vertical orientation and 2.5 mph horizontal velocity	0-ft vertical
Transportation cask with spent nuclear fuel (SNF) canister inside	Representative canister inside representative cask	T IC 1a: End, with 4 degree off-vertical orientation	12-ft vertical
		T.IC 1b: Same as T.IC 1a	13.1-ft vertical
		T.IC 1c: Same as T.IC 1a	30-ft vertical
		T IC 2a: End, with 4 degree off-vertical orientation, and approximated slapdown	13.1-ft vertical
		T.IC 2b: Same as T.IC 2a, with no free fall	0-ft vertical
		T IC 3: Side, with 3 degree off-horizontal orientation	6-ft vertical
DPC (Dual purpose canister)	Representative canister	D IC 1a: End, with vertical orientation	32.5-ft vertical
		D IC 1b: Same as D.IC 1a	40-ft vertical

Table D1.2-1. Container Configurations and Loading Conditions (Continued)

Container	Configuration	Drop Type/Impact Condition <sup>a</sup>	Drop Height
TAD (Transportation, aging, and disposal) canister		D IC 2a: End, with 4 degree off-vertical orientation	23-ft vertical
		D IC 2b: Same as D.IC 2a	10-ft vertical
		D IC 2c: Same as D.IC 2a	5-ft vertical
		D IC 3: 40 ft/min horizontal collision inside the CTM bell	No drop
		D IC 4: Drop of 10-metric-ton load onto top of canister	10-ft vertical
		D.IC 2a: Hourglass-control study for end drop, with 4 degree off-vertical orientation	23-ft vertical
		D.IC 2a: Friction coefficient sensitivity study for end drop, with 4 degree off-vertical orientation	23-ft vertical
		D.IC 2a: Mesh density study for end drop, with 4 degree off-vertical orientation	23-ft vertical
DSNF (DOE spent nuclear fuel) canister	INL-analyzed case	O.IC 1: End, with 3-degree-off vertical orientation	23-ft vertical

NOTE: A = aging overpack; (AO) CTM = canister transfer machine; ft = foot; D = dual purpose canister; IC = impact condition; min = minute; mph = miles per hour; O = DOE SNF canister; SNF = spent nuclear fuel; T = transportation cask.

Source: <sup>a</sup> Ref. D4.1.27, Table 4.3.3-1a.

Table D1.2-2. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for Representative Canister within an Aging Overpack

Container Type/ Impact Condition <sup>a</sup>	Impact Condition Description	Max EPS <sup>b</sup>	Failure Probability <sup>b</sup>			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
A.IC 1	3-ft end drop, with vertical orientation	0.16%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
A.IC 2	Slapdown from a vertical orientation and 2.5-mph horizontal velocity	0.82%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$

NOTE: <sup>a</sup>"A" stands for aging overpack. "IC" stands for impact condition, which are defined in Table D1.2-1.

<sup>b</sup>Values of Max EPS and failure probability are applicable to the SNF canister.

Source: Ref. D4.1.27, Table 6.3.7.6-1.

Table D1.2-3. Failure Probabilities with and without Triaxiality Factor, with and without Fragility Curve Adjustment, for Representative Canister

Container Type/ Impact Condition <sup>a</sup>	Impact Condition Description	Max EPS <sup>b</sup>	Failure Probability <sup>b</sup>			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
D.IC 1a	32.5-ft end drop, with vertical orientation	2.13%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 1b	40-ft end drop, with vertical orientation	2.65%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 2a	23-ft end drop, with 4-degree off-vertical orientation	24.19%	$<1 \times 10^{-8}$	$7.71 \times 10^{-1}$	$9.72 \times 10^{-6}$	$9.96 \times 10^{-1}$
D.IC 2b	10-ft end drop, with 4-degree off-vertical orientation	19.71%	$<1 \times 10^{-8}$	$7.01 \times 10^{-2}$	$1.73 \times 10^{-8}$	$3.19 \times 10^{-1}$
D.IC 2c	5-ft end drop, with 4-degree off-vertical orientation	15.76%	$<1 \times 10^{-8}$	$4.10 \times 10^{-5}$	$<1 \times 10^{-8}$	$3.12 \times 10^{-2}$
D.IC 3	40-ft/min horizontal side collision	0.16%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 4	10-ft drop of 10-metric-ton load onto top of canister	0.75%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
D.IC 2a S1-L1	Same as D.IC 2a	24.19%	$<1 \times 10^{-8}$	$7.71 \times 10^{-1}$	$9.72 \times 10^{-6}$	$9.96 \times 10^{-1}$
D.IC 2a S2-L1	Same as D.IC 2a	21.52%	$<1 \times 10^{-8}$	$1.66 \times 10^{-1}$	$2.44 \times 10^{-7}$	$7.62 \times 10^{-1}$
D.IC 2a S3-L1	Same as D.IC 2a	16.53%	$<1 \times 10^{-8}$	$3.37 \times 10^{-4}$	$<1 \times 10^{-8}$	$6.02 \times 10^{-2}$
D.IC 2a S1-L2	Same as D.IC 2a	23.34%	$<1 \times 10^{-8}$	$5.52 \times 10^{-1}$	$3.07 \times 10^{-6}$	$9.78 \times 10^{-1}$
D.IC 2a S1-L3	Same as D.IC 2a	25.15%	$<1 \times 10^{-8}$	$9.28 \times 10^{-1}$	$3.48 \times 10^{-5}$	1.00
D.IC 2a S2-L3	Same as D.IC 2a	22.57%	$<1 \times 10^{-8}$	$3.50 \times 10^{-1}$	$1.07 \times 10^{-6}$	$9.28 \times 10^{-1}$
D.IC 2a S3-L3	Same as D.IC 2a	18.08%	$<1 \times 10^{-8}$	$1.22 \times 10^{-2}$	$<1 \times 10^{-8}$	$1.14 \times 10^{-1}$
D.IC 2a S2-L4	Same as D.IC 2a	24.07%	$<1 \times 10^{-8}$	$7.44 \times 10^{-1}$	$8.27 \times 10^{-6}$	$9.95 \times 10^{-1}$
D.IC 2a S3-L4	Same as D.IC 2a	19.50%	$<1 \times 10^{-8}$	$6.29 \times 10^{-2}$	$1.37 \times 10^{-8}$	$2.77 \times 10^{-1}$

NOTE: <sup>a</sup>“D” stands for dual purpose canister. “IC” stands for impact condition, which are defined in Table D1.2-1.

<sup>b</sup>Values of Max EPS and failure probability are applicable to the SNF canister. A range of canister shell and bottom plate thicknesses were evaluated. The values shown are for the configuration that yielded the highest strains (0.5-inch shell thickness and 2.313 inch bottom plate thickness)

See Table 6.3.3.5-1 of Ref. D4.1.27 for definitions of H1, F1, M1, etc. See Table 6.3.3.6-1 of Ref. D4.1.27 for definitions of S1, L1, etc.

Source: *Seismic and Structural Container Analyses for the PCSA* (Ref. D4.1.27, Table 6.3.7.6-3)

Table D1.2-4. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Representative Canister inside the Transportation Cask

Container Type/ Impact Condition <sup>a</sup>	Impact Condition Description	Max EPS <sup>b</sup>	Failure Probability <sup>b</sup>			
			Original CDF Fragility Curve w/o Adjustment		CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality	w/o Triaxiality	with Triaxiality
T.IC 1a	12-ft end drop, with 4-degree off-vertical orientation	3.53%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1b	13.1-ft end drop, with 4-degree off-vertical orientation	4.06%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1c	30-ft end drop, with 4-degree off-vertical orientation	5.77%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 2a	13.1-ft end drop, with 4-degree off-vertical orientation, and approximated slapdown	4.35%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 2b	Approximated slapdown from vertical orientation	1.25%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 3	6-ft side drop, with 3-degree off-horizontal orientation	2.07%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 4	10-ft drop of 10-metric-ton load onto top of cask	0.96%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5a	30-ft end drop, with vertical orientation	3.55%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5b	30-ft end drop, with 4-degree off-vertical orientation	5.77%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5c	30-ft end drop, with 45-degree off-vertical orientation	6.41%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5d	30-ft end drop, with center of gravity over corner (i.e., point of impact)	6.63%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$

NOTE: <sup>a</sup>“T” stands for transportation cask. “IC” stands for impact condition, which are defined in Table D1.2-1.  
<sup>b</sup>Values of Max EPS and failure probability are applicable to the SNF canister.

Source: Ref. D4.1.27, Table 6.3.7.6-2



Table D1.2-5. Failure Probabilities with and without Triaxiality Factor, with and without the Fragility Curve Adjustment, for the Transportation Cask

Container Type/ Impact Condition <sup>a</sup>	Impact Condition Description	Max EPS <sup>b</sup>	Failure Probability	
			CDF Fragility Curve Adjusted for Minimum Elongation (-8.3% Shift)	
			w/o Triaxiality	with Triaxiality
T.IC 1a	12-ft end drop, with 4-degree off-vertical orientation	9.20%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1b	13.1-ft end drop, with 4-degree off-vertical orientation	9.37%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 1c	30-ft end drop, with 4-degree off-vertical orientation	11.25%	$<1 \times 10^{-8}$	$9 \times 10^{-7}$
T.IC 2a	13.1-ft end drop, with 4-degree off-vertical orientation, and approximated slapdown	9.94%	$<1 \times 10^{-8}$	$3 \times 10^{-8}$
T.IC 2b	Approximated slapdown from vertical orientation	5.30%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 3	6-ft side drop, with 3-degree off-horizontal orientation	7.42%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 4	10-ft drop of 10-metric-ton load onto top of cask	1.76%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5a	30-ft end drop, with vertical orientation	3.17%	$<1 \times 10^{-8}$	$<1 \times 10^{-8}$
T.IC 5b	30-ft end drop, with 4-degree off-vertical orientation	11.25%	$<1 \times 10^{-8}$	$9 \times 10^{-7}$
T.IC 5c	30-ft end drop, with 45-degree off-vertical orientation	70.56%	1	1
T.IC 5d	30-ft end drop, with center of gravity over corner (i.e., point of impact)	44.88%	0.9	1

NOTE: <sup>a</sup>“T” stands for transportation cask. “IC” stands for impact condition, which are defined in Table D1.2-1.  
<sup>b</sup>Values of Max EPS and failure probability are applicable to the structural body of the transportation cask, which excludes the shield and shield shell.

Source: Probabilities calculated using Table D1.1-1 based on strains reported in *Seismic and Structural Container Analyses for the PCSA* (Ref. D4.1.27, Table 6.3.7.6-2)

Table D1.2-6. Strains at Various Canister Locations Due to Drops

Canister	Component	Maximum PEEQ Strains (%)			Load Case/ Conditions
		Outside Surface	Mid-Surface	Inside Surface	
18-inch DOE STD canister	Lower head	8	3	6	300°F, 23-foot drop, 3 degrees off-vertical Material: ASME Code minimum strengths
	Lower head-to-main shell weld	2	2	3	
	Main shell	2	2	3	
	Upper head-to-main shell weld	0	0	0	
	Upper head	1	0.2	2	
24-inch DOE STD canister	Lower head	2	0.7	1	300°F, 23-foot drop, 3 degrees off-vertical Material: ASME Code minimum strengths
	Lower head-to-main shell weld	0.2	0.3	0.5	
	Main shell	0.2	0.3	0.5	
	Upper head-to-main shell weld	0	0	0	
	Upper Head	0	0	0	
MCO	Lower head	35	16	14	70°F, 23-foot drop, 3 degrees off-vertical Material: Actual material properties (significantly higher than ASME Code minimums)
	Lower head-to-main shell weld	21	11	11	
	Main shell	13	15	29	
	Upper head-to-main shell weld	0	0	0	
	Upper head	0	0	0	

NOTE: ASME = The American Society of Mechanical Engineers; DOE STD = U.S. Department of Energy standard; MCO = multiccanister overpack; PEEQ = peak equivalent.

Source: Ref. D4.1.64, Tables 13, 14, and 16

Table D1.2-7. Failure Probabilities for the DOE Spent Nuclear Fuel (DSNF) Canisters and Multicanister Overpack (MCO)

Component	Peak Equivalent Plastic Strain (%)			Probability of Failure					
				Original CDF			CDF adjusted to min elongation		
	Outside Surface	Middle	Inside Surface	Outside Surface	Middle	Inside Surface	Outside Surface	Middle	Inside Surface
<b>18-inch standard canister containment PEEQ strains, 3 degrees off vertical drop, 300°F</b>									
Lower Head	8	3	6	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Lower Head-to-Main Shell Weld	2	2	3	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Main Shell	2	2	3	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head-to-Main Shell Weld	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head	1	0.2	2	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
<b>24-inch standard canister containment PEEQ strains, 3 degrees off vertical drop, 300°F</b>									
Lower Head	2	0.7	1	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Lower Head-to-Main Shell Weld	0.2	0.3	0.5	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Main Shell	0.2	0.3	0.5	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head-to-Main Shell Weld	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Upper Head	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
<b>4 MCO containment PEEQ strains, 3 degrees off vertical drop, 70°F</b>									
Bottom	35	16	14	3.74E-03	<1E-08	<1E-08	8.99E-02	<1E-08	<1E-08
Bottom-to-Main Shell	21	11	11	<1E-08	<1E-08	<1E-08	1.16E-07	<1E-08	<1E-08
Main Shell	13	15	29	<1E-08	<1E-08	1.09E-06	<1E-08	<1E-08	3.85E-03
Collar	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08
Cover	0	0	0	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08	<1E-08

NOTE: ASME = The American Society of Mechanical Engineers; CDF = cumulative distribution function; DOE STD = U.S. Department of Energy standard; MCO = multicanister overpack; PEEQ = peak equivalent.

Source: Ref. D4.1.27, Tables 6.3.7.6-4 and 6.3.7.6-5

### D1.3 PROBABILITIES OF FAILURE OF HIGH LEVEL WASTE CANISTERS DUE TO DROPS

The probability of failure for drops of high-level radioactive waste (HLW) canisters was assessed by evaluating actual drop test data. Several series of tests were conducted including vertical, top, and corner drops of steel containers. The reports on these tests are summarized in *Leak Path Factors for Radionuclide Releases from Breached Confinement Barriers and Confinement Areas* (Ref. D4.1.17). No leaks were found after 27 tests, 14 of which were from 23 feet and 13 of which were from 30 feet. These tests can be interpreted as a series of Bernoulli trials, for which the outcome is the breach, or not, of the tested canister. The observation of zero failures in 13 tests was interpreted using a beta-binomial conjugate distribution Bayes analysis.

A uniform prior distribution, which indicates prior knowledge that the probability of failure is between 0 and 1, may be represented as a Beta(r,s) distribution in which both r and s equals 1. The conjugate pair likelihood function for a Beta(r,s) distribution is a Binomial(n, N) where n represents the number of failures within the tests and N represents the number of tests. The posterior distribution resulting from the conjugate pairing is also a Beta distribution with parameters r' and s', which are defined as follows:

$$r' = r + n \quad \text{and} \quad s' = s + N - n \quad (\text{Eq. D-1})$$

The mean,  $\mu$ , and standard deviation,  $\sigma$ , of the posterior distribution are determined using the following equations:

$$\mu = r' / (r' + s') \quad \text{and} \quad \sigma = \{r's' / [(r' + s' + 1)(r' + s')^2]\}^{1/2} \quad (\text{Eq. D-2})$$

For n = 0 and N = 13, Equation D-2 results in  $\mu = 0.067$  and  $\sigma = 0.062$ . For n = 0 and N = 27,  $\mu = 0.034$  and  $\sigma = 0.033$ . These values are used for the failure probability of a dropped HLW canister, for example during its transfer by a canister transfer machine.

One element of the Nuclear Safety Design Basis (Section 6.9) requires that the transportation cask, which will deliver HLW and DOE standardized canisters, be designed to preclude contact between the canister and a transportation cask lid or other heavy object that might fall. Similarly, other large heavy objects are precluded from damaging these canisters, when residing within a co-disposal waste package by the design of the waste package, which includes separator plates that extend well above the canisters. These scenarios are not quantitatively analyzed herein.

The combined INL and LLNL analyses discussed previously conclude that a DOE SNF canister has a probability of breach less than 1E-08 for a 23 foot drop, 4 degrees off-normal (i.e., 4 degrees from vertical) onto an unyielding rigid surface. The LLNL results demonstrate that generally strains from impact and probability of failure is higher for off-normal drops than normal (i.e., vertical) drops for the same height. The LLNL results further show that a 10 ton load dropped from 10 feet onto a representative canister also results in a probability of breach of less than 1E-08. INL analysis EDR-NSNF-087 entitled Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository states that

canister integrity was maintained for a 30 foot drop test onto a rigid, unyielding surface. The report discusses drop of a HLW canister on a DOE SNF canister and drop of a DOE SNF canister onto another one. Drops of these canisters onto canisters in the IHF or CRCF would occur with drop heights of less than 10 feet. Two main differences are noted between a drop of a DOE SNF and a drop of a HLW canister onto a DOE SNF. The first is that substantially lower kinetic energy of impact of the latter drop would result in significantly less skirt deformation. The non-flat bottom nature of the HLW/DOE SNF interaction would have a different skirt deformation pattern than the flat bottomed drop. INL concludes that the skirt would be expected to absorb the bulk of the heaviest HLW canister (4.6 tons) drop energy and DOE SNF canister integrity would be maintained. A difference between a 10 ton drop of a load onto a representative canister and a drop onto a DOE SNF canister results from the difference diameters of the target as well as different materials and lid thicknesses. Nevertheless, INL concludes that the impact from 10 feet of a HLW canister onto a DOE SNF canister is less challenging than impact from a 30 foot drop. Since the probability from a 23 foot drop was calculated to be less than 1E-08, it is conservative to use a value of 1E-05 for the probability of failure of an HLW on DOE SNF impact. The increased value is assigned to account for uncertainties owing to the differences noted above.

#### **D1.4 PROBABILITIES OF FAILURE OF WASTE PACKAGES DUE TO DROPS AND IMPACTS**

The probabilities of containment failure are evaluated by comparing the challenge load with the capacity of the waste package to withstand that challenge in a manner similar to that described in *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis - Level of Information and Reliability Estimation*. HLWRS-ISG-02 (Ref. D4.1.56), and summarized in Section 4.3.2.2. Three scenarios are evaluated for the potential loss of containment by waste packages due to drops and impacts:

- Two-foot horizontal drop
- 3.4-mph end-to-end impact
- Rockfall on waste package in subsurface tunnels.

An additional scenario, drop of a waste package shield ring onto a waste package, is considered in Section D1.4.4.

For this assessment, the potential load has been determined by FEA in the calculations cited below as the sources of inputs. The load is expressed in terms of stress intensities and as expended toughness fraction (ETF), which is the ratio of the stress intensity to the true tensile strength. The ETF is used to obtain the failure probability by the following:

$$P = \int_{-\infty}^x N(t) dt \quad \text{and} \quad x = \frac{ETF - 1}{COV} \quad (\text{Eq. D-3})$$

where

$P$	=	probability of failure
$N(t)$	=	standard normal distribution with mean of zero and standard deviation of one
$T$	=	variable of integration
$ETF$	=	expended toughness fraction
$COV$	=	coefficient of variation = ratio of standard deviation to mean for strain capacity distribution, applied here to stress capacity or true tensile strength

The capacity is the true tensile strength of the material, the stress the material can withstand before it separates. The minimum true tensile strength,  $\sigma_u$ , for the Alloy 22 typically used for the outer corrosion barrier (OCB) of the waste package is 971 MPa (Ref. D4.1.20, Section 7.7, p. 162). The variability in the capacity is expressed as the standard deviation of a normal distribution that includes strength variation data and variability of the toughness index,  $I_T$ , computed without triaxiality adjustments (uniaxial test data). The standard deviation as percent of the mean of  $\sigma_u$  is 25% (Ref. D4.1.20, Section 7.6, p. 162). The distribution of elongations used for defining the fragility curve in the LLNL analysis was expressed as two normal distributions, the larger of which was with a mean of 59.3% elongation and a standard deviation of 4.22% elongation, or a COV of 0.0712 (Ref. D4.1.27, Section 6.3.7.3). Thus the 0.073 reported for the OCB material is conservative compared with the LLNL data and is used for the COV in the expression above. The possibility of waste package weld defects is not explicitly considered in the analysis. However, as noted in Section D.1.4.5, weld defects are not expected to contribute significantly to the probability of waste package failure due to drops or other impacts.

#### D1.4.1 Waste Package Drop

A study investigating the structural response of the naval long waste package to a drop while it is being carried on the emplacement pallet, found the ETF for the outer corrosion barrier (OCB) to be 0.29 for a 10 m/s flat impact (Ref. D4.1.20, Table 7-15, pg. 117), equivalent to a 16.7-foot drop. This corresponds to a failure probability of less than  $1 \times 10^{-8}$ . The failure of the OCB is used to define the loss of containment, taking no credit for the inner vessel and the canister within. The description of the transport and emplacement vehicle (TEV) provided in *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (Ref. D4.1.12) mentions that the floor plate is lifted by four jacks and guided by a roller. The guide roller precludes tilted drops of the flat bed of the TEV. As was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of  $1 \times 10^{-5}$  is used for the probability that the waste package containment would fail due to a two-foot horizontal drop, which is much less severe than the modeled 16.7-foot drop.

#### D1.4.2 Rockfall onto a Waste Package

A seismic event during the preclosure period could cause rocks to fall from the ceiling of a drift onto the waste packages stored there prior to deployment of the drip shields. The extent of

damage has been predicted for several levels of impact energy of falling rocks (Ref. D4.1.26). The maximum credible impact energy from a falling rock is about  $1 \times 10^6$  joules (J) (Ref. D4.1.21, p. 57). The maximum ETF resulting from rockfall impacting with approximately  $1 \times 10^6$  J is about 0.11 (Ref. D4.1.26, p. 54, Table 5), corresponding to a failure probability less than  $1 \times 10^{-8}$ . As was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of  $1 \times 10^{-5}$  should be used for the probability that the waste package containment would fail due to rockfall on the waste package.

### D1.4.3 Results for the Three Assessed Scenarios

The failure probabilities for the three scenarios, derived from the results in the cited reports, are summarized in Table D1.4-1.

Table D1.4-1. Waste Package Probabilities of Failure for Various Drop and Impact Events

Event	Probability of Failure
2-Foot Horizontal Drop	$< 1 \times 10^{-5}$
3.4-mph end-to-end impact	$< 1 \times 10^{-5}$
20 metric ton Rockfall on Waste Package with and without Rock Bolt <sup>a</sup> Impacting the Waste Package	$< 1 \times 10^{-5}$

NOTE: <sup>a</sup>A rock bolt is a long anchor bolt, for stabilizing rock excavations, which may be tunnels or rock cuts.

Source: Original

### D1.4.4 Drop of a Waste Package Shield Ring onto a Waste Package

After the co-disposal waste package has been welded closed in the Waste Package Positioning Room, the shield ring is lifted from it before the waste package transfer trolley is moved into the load out area. Grapple failures might cause the drop to occur at a variety of orientations relative to the top of the waste package. A frequency of canister breach from a potential drop as high as 10 feet is considered here. For a canister breach to occur, the shield ring must penetrate the 1-inch thick outer lid made of SB 575 (Alloy 22) and the 9 inch thick stainless steel inner lid (SA 240) before having an opportunity to impact the canister (Ref. D4.1.13). There are six inches separating the inner and outer lids. In the radial center area of that space, which would be directly above the DOE SNF canister, is a stainless steel lifting device attached to the inner lid. This adds another layer of energy absorption.

The shield ring weighs approximately 15 tons and is made of stainless steel with a lighter weight neutron absorber material. The impact energy of a 15-ton shield ring dropping 10 feet would be 0.4 MJ. The frequency of penetration of the sides of a waste package from a 20 metric ton rock impacting the side of the waste package with impact energy of 1 MJ is less than  $1 \times 10^{-8}$  (Table D1.4-1). The sides of a waste package are approximately three inches thick compared to a cumulative thickness (excluding lifting fixture) of 10 inches at the top. Although the impact energy could be more focused, the impact energy for the shield ring against the top of the waste package is less than the impact energy of the rockfall against the side and the top is much thicker than the side. The probability of failure due to shield ring impact against the top of the waste

package is expected to be no worse than for the impact of a rock against the side. A conservative value of  $1 \times 10^{-5}$  is used in the analysis for this probability.

#### **D1.4.5 Waste Package Weld Defects**

Waste package closure involves engaging and welding the inner lid spread ring, inerting the waste package with helium, setting and welding the outer lid to the outer corrosion barrier, performing leak testing on the inner vessel closure, performing nondestructive examination of welds, and conducting postweld stress mitigation on the outer lid closure weld.

The weld process of the waste package closure subsystem is controlled as a special process by the Quality Assurance Program (Ref. D4.1.29, Section 9.0). The activities performed by the system are controlled by approved procedures.

The principal components of the system include welding equipment; nondestructive examination equipment for visual, eddy current, and ultrasonic inspections of the welds and leak detection; stress mitigation equipment for treatment of the outer lid weld; inerting equipment; and associated robotic arms. Other equipment includes the spread ring expander tool, leak detection tools, cameras, and the remote handling system. The system performs its functions through remote operation of the system components.

The capability of the waste package closure subsystem will be confirmed by demonstration testing of a full-scale prototype system. The prototype includes welding, nondestructive examinations, inerting, stress mitigation, material handling, and process controls subsystems. The objective of the waste package closure subsystem prototype program is to design, develop, and construct the complete system required to successfully close the waste package. An iterative process of revising and modifying the waste package closure subsystem prototype will be part of the design process. When prototype construction is finalized, a demonstration test of the closure operations will be performed on only the closure end of the waste package; thus, the mock-up will be full diameter but not full height as compared to the waste package. The purpose of the demonstration test is to verify that the individual subsystems and integrated system function in accordance with the design requirements and to establish closure operations procedures. This program is coordinated with the waste package prototype fabrication program.

The principal functions of the waste package closure subsystem are to:

- Perform a seal weld between the spread ring and the inner lid, the spread ring and the inner vessel, and the spread ring ends; perform a seal weld between the purge port cap and the inner lid; and perform a narrow groove weld between the outer lid and the outer corrosion barrier.
- Perform nondestructive examination of the welds to verify the integrity of the welds and repair any minor weld defects found.
- Purge and fill the waste package inner vessel with helium gas to inert the environment.



- Perform a leak detection test of the inner lid seals to ensure the integrity of the helium environment in the inner vessel.
- Perform stress mitigation of the outer lid groove closure weld to induce compressive residual stresses.

The gas tungsten arc welding process is used for waste package closure welds and weld repairs. Welding is performed in accordance with procedures qualified to the *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section IX), as noted below:

- The spread ring and purge port cap welds are two-pass seal welds.
- The outer lid weld is a multipass full-thickness groove weld.

Welding process procedures will be developed that identify the required welding parameters. The process procedures will:

- Identify the parameters necessary to consistently achieve acceptable welds.
- State the control method for each weld parameter and the acceptable range of values.

The welds are inspected in accordance with examination procedures developed using *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section V and Section III, Division 1, Subsection NC) as a guide, with modification as appropriate:

- Seal welds—visual inspection
- Groove welds—visual, eddy current, and ultrasonic inspection.

A weld dressing end effector is used for weld repairs. The defect is removed, resulting in an excavated cavity of a predetermined contour. The excavated cavity surface is inspected using the eddy current inspection end effectors. Then the cavity is welded and inspected in accordance with the welding and inspection procedures.

The stress mitigation process for the outer lid closure weld is controlled plasticity burnishing. Controlled plasticity burnishing is a patented method of controlled burnishing to develop specifically tailored compressive residual stress with associated controlled amounts of cold work at the outer surface of the waste package outer lid closure weld.

The inner vessel of the waste package is evacuated and backfilled with helium through a purge port on the inner lid. The inerting process is in accordance with the inerting process described in NUREG-1536 (Ref. D4.1.54, Sections 8.0 and V.1). After the waste package inner vessel is backfilled by helium, both the spread ring welds and the purge port plug are leak tested in accordance with *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section V, Article 10, Appendix IX) to verify that no leakage can be detected that exceeds the rate of  $10^{-6}$  std cm<sup>3</sup>/s.

Waste package closure welding, nondestructive examination, stress mitigation, and inerting are conducted in accordance with approved administrative controls. The processes for waste package closure welding, nondestructive examination, stress mitigation, and inerting will be

developed in accordance with the codes and standards identified below. The processes are monitored by qualified operators, and resulting process data are checked and verified as acceptable by qualified individuals.

Waste package closure welding, nondestructive examination, stress mitigation, and inerting normal operating procedures will specify, for example, the welding procedure specification, nondestructive examination procedure, qualification and proficiency requirements for operators and inspectors, and acceptance and independent verification records for critical process steps.

The waste package closure subsystem-related welds, weld repairs, and inspections are performed in accordance with *2001 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.5, Section II, Part C; Section III, Division I, Subsection NC; Section IX; Section V).

The inerting of the waste package is performed in accordance with the applicable sections of NUREG-1536 (Ref. D4.1.54).

PCSA event sequences involving waste packages include challenges ranging from low velocity collisions to a 20 metric ton rockfall to a spectrum of fires. Waste package failure probabilities are calculated to be very low. Furthermore, a significant conservatism in the analysis is that the containment associated with the canister is not included in the probability of containment breach. In other words, if the waste package breaches, radionuclide release is analyzed as if the canister has breached (if the event sequence is in Category 1 or 2). Analytically, the canister is not relied upon for event sequences involving waste packages. The analytical results from the LLNL analysis show a significant reduction in canister strains is achieved by transportation cask and aging overpack protection. Although not analyzed, a similar ameliorating effect on the canister would be expected to be provided by the waste package.

The weld, inspection and repair process ensures no significant defects to a high reliability. The event sequence analysis shows that all event sequences associated with waste package breach are Beyond Category 2. In the context of the event sequence analysis, a significant defect is one that would have increased the probability of breach of the canister within the waste package by orders of magnitude. Even for significant weld defects, the protection offered by the waste package to the canister containment function would remain. Therefore, the effect of waste package weld failure on loss of canister containment during event sequences is not further considered.

#### **D1.4.6 Waste Package End-to-End Impact**

An oblique impact of a long naval SNF waste package inside TEV) was modeled to assess the structural response (Ref. D4.1.19). Most of the runs were with initial impact velocity of 3.859 m/s corresponding to a drop height of 0.759 m (2.49 ft). The maximum ETF for the 3.859 m/s (12.66 ft/sec) oblique impact in the OCB is about 0.7 (Ref. D4.1.19, page 37, Table 7-3, runs 1, 2, and 3), corresponding to a failure probability of about  $2 \times 10^{-5}$ . The oblique impact should be bounding for a direct end impact. Using equation D-4, an ETF of 0.11 is estimated for the hypothesized 3.4 mph end-to-end collision (two TEVs each traveling 1.7 mph), corresponding to a failure probability of less than  $1 \times 10^{-8}$ . The failure of the OCB is used to define the loss of containment, taking no credit for the inner vessel and the canister within. As

was done for the results from LLNL, to introduce an additional measure of conservatism, a failure probability of  $1 \times 10^{-5}$  is used for the probability that the waste package containment would fail due to a 3.4-mph end-to-end impact.

### D1.5 PREDICTING OUTCOMES OF OTHER SITUATIONS BY EXTRAPOLATING STRAINS FOR MODELED SCENARIOS

Equation 17 in Section 6.3.2.2 demonstrates use of the probability of failure at a given drop height together with the COV to predict probabilities at other drop heights. A similar approach can be used to extrapolate from one strain to another to find the corresponding failure probability. The work done on damaging the container expressed in the form of strain should be roughly proportional to the energy input to the material due to the impact. The impact energy is proportional to the drop height or to the square of the impact velocity. Finite element modeling demonstrated that the increase in strain is actually less than proportional to increase in drop height (Tables D1.2-3 and D1.2-4), so increasing the strain proportionally with drop height or the square of impact velocity is conservative. The strain is extrapolated by multiplying it by the square of the ratio of the velocity of interest to the reference velocity.

$$\tau_i = \tau_{ref} \left( \frac{v_i}{v_{ref}} \right)^2 \quad (\text{Eq. D-4})$$

where

- $\tau_i$  = strain at velocity of interest (dimensionless)
- $\tau_{ref}$  = strain at reference velocity (dimensionless)
- $v_i$  = velocity of interest (same units as  $v_{ref}$ )
- $v_{ref}$  = reference velocity (same units as  $v_i$ )

In case D.IC.3, a 0.16% strain ( $\tau_{ref}$ ) was predicted for a side impact of 40 ft/min ( $v_{ref}$ ). Using Equation D-4 to extrapolate for an impact velocity of 2.5 miles/hr gives an estimated strain of 4.84%.

The estimated strain is then compared with the fragility curve tabulated in D1.1-1. A failure rate of less than  $1 \times 10^{-8}$  is predicted for a strain of 4.84%. Probabilities of failure for a range of impact velocities are listed in Table D1.5-1.

Table D1.5-1. Calculated Strains and Failure Probabilities for Given Side Impact Velocities

Impact Velocity		% strain	Probability of failure
(ft/sec)	(ft/min)		
0.67	40	0.16	$< 1 \times 10^{-8}$
1	60	0.36	$< 1 \times 10^{-8}$
2	120	1.44	$< 1 \times 10^{-8}$
4	240	5.76	$< 1 \times 10^{-8}$
6	360	13	$< 1 \times 10^{-8}$
8	480	23	$< 1 \times 10^{-5}$

Source: Original

A similar approach is applied to estimate failure probabilities for vertical drops greater than 40 feet. The strains are extrapolated using the ratio of drop heights rather than the squared ratio of impact velocities in Equation D-4.

For the DPC, the maximum EPS is 2.65% for a 40-foot end drop (case D.IC.1b in Table D1.2-3). Strains of 2.98% and 3.31% are estimated for 45- and 50-foot drops, respectively. Doubling the strains to account for triaxiality and comparing these strains with Table D1.1-1 shows the probabilities of failure are both  $< 1 \times 10^{-8}$ . As before, conservative probabilities of  $1 \times 10^{-5}$  are used in the event sequence quantification.

For the DOE standard canister the maximum strain is 8% in the lower head of the 18-inch canister resulting from a 23-foot drop 3 degrees off vertical (Table D1.2-6). By the same approach as above, 10.4%, 15.7%, and 17.4% strains are estimated for 30-foot, 45-foot, and 50-foot drops. Doubling these strains and comparing with Table D1.1-1 yields the failure probabilities of  $1 \times 10^{-7}$ ,  $3 \times 10^{-2}$ , and  $9 \times 10^{-2}$  for the 30-foot, 45-foot, and 50-foot drops, respectively. A conservative probability of  $1 \times 10^{-5}$  is used for the 30-foot drop of the DOE standardized canister.

## D1.6 MISCELLANEOUS SCENARIOS

### D1.6.1 Localized Side Impact on a Transportation Cask

One of the requirements specified for transportation casks is they be robust enough to survive a 40-inch horizontal drop onto an unyielding 6-inch diameter upright cylinder (Ref. D4.2.2, Paragraph 71.73). The impact energy for such a scenario involving a 250,000 pound cask (a typical weight for a loaded cask) – the NAC STC has a loaded weight of 260,000 pounds (Ref. D4.1.50, p. 1.1-1) is about 1.1 MJ. The maximum weight of a forklift is considerably less than 20,000 kg. At a maximum speed of 2.5 mph (1.12 m/s), the maximum impact energy would be 12.5 kJ, a factor of 90 less than the impact energy for the 40-inch drop of the cask. If the resultant strain is proportional to the impact energy and the drop event in the Safety Analysis Report (SAR) is just below the failure threshold (i.e. the median impact energy for failure), the impact energy due to the 2.5-mph impact would be a maximum of  $1/90^{\text{th}}$  of the median failure impact energy, or  $1 - 1/90$  COVs less than a normalized median of 1. Equation D-3 is applicable

substituting the ratio of impact energy to median failure impact energy for the factor ETF. Using  $1/90$  ( $=0.011$ ) in place of the ETF in Equation D-3 gives a probability of failure of much less than  $1 \times 10^{-8}$  due to impact of a forklift against a transportation cask. If the impact speed were 9 mph instead of 2.5 mph, the impact energy would be about  $1/7^{\text{th}}$  of the energy in the SAR drop event, 0.14 would be used in place of the ETF in Equation D-3, and the probability of failure would still be less than  $1 \times 10^{-8}$ .

### **D1.6.2 Screening Argument for TAD Weld Defects**

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

The process control program for the closure welds produced by the TAD canister closure system is controlled as a special process by the Quality Assurance Program (Ref. D4.1.29, Section 9.0).

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

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

The qualification of the TAD canister final closure welds is in accordance with ISG-18 (Ref. D4.1.55) as specified in *Basis of Design for the TAD Canister-Based Repository Design Concept* (Ref. D4.1.15, Section 33.2.2.36). Adherence to this guidance is deemed to provide reasonable assurance that weld defects occur at a low rate. However, TAD canister weld cracks are considered an initiating event after the TAD canister welding process in the Wet Handling

Facility (WHF). If this occurs, the radionuclide release would be minimal because the incoming casks and canisters have already been opened. After TAD canisters are welded, they are placed in aging overpacks and moved by the site transporter to the Canister Receipt and Closure Facility (CRCF). The probability of TAD canister failure during removal from the aging overpack handling in the CRCF and placement into a waste package is considered in the CRCF event sequence analysis. The conditional probability of TAD canister failures during handling in the CRCF has been shown to be small. The low probability of weld defects and their size would not alter this result. After the TAD canister is placed in the waste package, the containment is considered to be the waste package and the TAD canister is no longer relied upon in event sequences involving mechanical impacts.

## **D2 PASSIVE FAILURE DUE TO FIRE**

A risk assessment must consider a range of fires that can occur, as well as variations in the dynamics of the heat transfer and uncertainties in the failure temperature of the target. This section presents an analysis to determine the probability that a waste container will lose containment integrity or lose shielding in a fire. Section D2.1 addresses loss of containment and Section D2.2 addresses loss of shielding.

### **D2.1 ANALYSIS OF CANISTER FAILURE DUE TO FIRE**

A common approach to safety analysis in regards to the effect of a fire is to postulate a specific fire (in terms of duration, combustible loading, heat rate, and other fire parameters) and then apply it to a specific configuration of a target. Then, a simple comparison is made between the temperature that the target reaches as a result of the fire, and the failure temperature of the target. Based on this comparison, a conclusion is made that either the target always fails, or never fails, or fails at some specific time. While such an approach may be appropriate for demonstrating that a specific design code has been met, it is not appropriate for a risk informed PCSA.

There are two parts to the assessment of the canister failure probability (sometimes referred to as the canister *fragility*): determining the thermal response of the canister to the fire and determining the temperature at which the canister will fail. In calculating the thermal response of the canister, variations in the intensity and duration of the fire are considered along with conditions that control the rate of heat transfer to the container (e.g., convective heat transfer coefficients, view factors, emissivities). In calculating the failure temperature of the canister, variations in the material properties of the canister material are considered along with variations in the loads that lead to failure.

#### **D2.1.1 Uncertainty in Fire Severity**

In the fragility analysis, fire severity is characterized by the fire temperature and duration, since these factors control the amount of energy that the fire could transfer to a target cask or canister. Uncertainty distributions were developed for the fire temperature and fire duration based on a review of generic and YMP-specific information.

### **D2.1.1.1 Uncertainty in Fire Duration**

In the context of this study, this duration of the fire is from the perspective of the target (i.e., the cask or canister that could be compromised by the fire). Therefore, the fire duration used in the analysis is the amount of time a particular container is exposed to the fire, and not necessarily the amount of time a fire burns. As an example, a fire that propagates through a building over a four-hour period is not a four-hour hazard to a particular target. In calculating the exposure time for a specific target, it does not matter whether the fire started in the room where the target is, or it started in another room and ended where the target is, or the fire passed through the target room between its beginning and end. The exposure duration is how long the fire burns while consuming combustibles in the vicinity of the target. This allows a single probability distribution to be developed for the fire duration, regardless of how the fire arrived at the target, based on estimates of the duration of typical single-room fires.

In order to develop this curve, data on typical fire durations is required. A number of sources were used to derive insights regarding the range of expected durations of typical fires. The following sources were used:

- NUREG/CR-4679 (Ref. D4.1.53) reviewed the results of fire tests conducted by a number of organizations on a variety of types and amounts of combustible materials. Although focused on nuclear power plants, the materials assessed are typical of those found at a variety of industrial facilities.
- NUREG/CR-4680 (Ref. D4.1.52) reports on the results of a series of tests conducted by Sandia National Laboratories using a series of fuel source packages representative of trash found around nuclear power plants. Once again, these packages are typical of what might be found around other types of industrial facilities.

The tests were not extensive, and represented only particular configurations. In general, the fire durations were found to depend upon the amount, type, and configuration of the available combustible material.

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

### **D2.1.1.2 Fire Duration without Automatic Fire Suppression**

The first uncertainty distribution was developed for fires in which automatic fire suppression is not available. The vast majority of the tests conducted were for this case. The following summarizes information presented in the three references listed above.

Sandia National Laboratories conducted two large-scale cable fire tests using an initial fire source of five gallons of heptane fuel, and an additional fuel loading of two vertical cable trays with a 12.5% fill consisting of 43-10-foot lengths of cable per tray (Ref. D4.1.53, Section 2.2.1). The only difference between the tests was that one test used unqualified cable and the other used IEEE-383 qualified cable. In the unqualified cable test, the cables reached peak heat release at

approximately four minutes, and the rate decayed toward reaching zero at approximately 17 minutes. In the qualified cable test, the cables reached peak heat release at approximately seven minutes, and the rate decayed toward reaching zero at approximately 16 minutes.

Factory Mutual Research Corporation conducted tests for large-scale configurations of cable trays (Ref. D4.1.53, Section 2.2.3). One set of tests involved a configuration of 12 fully loaded horizontal trays in two stacked tiers. NUREG/CR-4679 (Ref. D4.1.53) provides detailed results for three of the “free-burn” tests (no automatic fire suppression). The first test reached and maintained the peak heat release rate at six minutes to 20 minutes, and reached zero at 25 minutes. The second test reached and maintained the peak heat release rate at seven minutes to 25 minutes, and reached zero at 34 minutes. The third test reached and maintained the peak heat release rate at 26 minutes to 40 minutes, and reached zero at 60 minutes.

Lawrence Berkeley Laboratory conducted tests on electrical cabinets (Ref. D4.1.53, Section 2.2.5). Two tests were conducted. The first was a single cabinet with only thermocouple wire and leads and no internal cabinet fuel loading. The fire that exposed the cabinet was two trash bags with loosely packed paper in a 32-gallon polyethylene trash receptacle, plus two cardboard boxes of packing “peanuts.” This fire reached a peak heat release rate at seven minutes, and reached zero at 19 minutes. The second test involved two cabinets separated by a steel barrier. The cabinets contained a total of 64 lengths of cable (48 and 16). The source fire in this test was similar in nature to the first test, but had a heavier container and loose paper instead of the “peanuts.” This fire had two peaks, at six minutes and 18 minutes, with the second being much larger than the first. The fire decayed toward reaching zero between 25 minutes and 30 minutes.

The Department of Health and Human Services sponsored a series of tests on various types of furnishing materials (Ref. D4.1.53, Section 3). While the specific types of furnishings are unlikely to be found in a YMP preclosure facility, these results are instructive for combinations of combustible materials that could be found. The first test was on a molded fiberglass chair with a metal frame. The fire reached a peak heat release rate in two minutes, and reached zero at 10 minutes. The second test was for a wood frame chair with latex foam cushions. This fire reached a peak heat release rate in four minutes and reached zero at 40 minutes. The final test was on four stackable, metal frame chairs with cushions that appeared to consist of a wood base, foam core, and vinyl cover. The fire reached a relatively steady state peak heat release rate from four minutes to 23 minutes, and reached zero at 38 minutes.

Sandia National Laboratories performed a series of nine tests on representative transient fuel fires (Ref. D4.1.52). Five different fuel packages were used for the tests. The first two fuel packages used mixed wastes representative of cleaning materials that might be left by maintenance personnel during routine operations. The first package was about 1.8 kilograms, and the second about 2.2 kilograms. The other difference between the two packages was the first package had more cardboard, whereas the second had more plastic. In both tests on the first package, the fire reached a peak heat release rate at approximately four minutes. However, they reached zero at different times (greater than 30 minutes versus approximately 20 minutes). In the two tests on the second package, the time of peak heat release was different (a high peak at four minutes versus a relatively low peak at 10 to 20 minutes), but they both reached zero at approximately the same time (50 minutes).



The third fuel package was designed to represent normal combustibles that might be in control or computer rooms, and consisted primarily of cardboard and stacked paper, with some crumpled paper. Total mass was about 7.9 kilograms. In both tests, the fire reached a peak heat release rate in approximately two minutes, but reached zero at different times (16 minutes versus 20 minutes).

The fourth fuel package was designed to represent mixed waste that might be found in a control room, computer room, security room, or similar location. It consisted primarily of a plastic trash can filled with paper and rags. Total mass was about 1.6 kilograms. In both tests, the fire reached a peak heat release rate in approximately three minutes and remained relatively steady for most of the duration of the fire, but reached zero at different times (54 minutes versus 70 minutes).

The fifth fuel package was designed to represent larger industrial waste containers that might be found in a variety of places in an industrial facility. It consisted primarily of a large plastic receptacle filled with wood, cardboard, paper, and oily rags. Total mass was about 6.5 kilograms. Only one test was conducted with this fuel package, and the fire reached two separate peak heat release rates (at 35 and 50 minutes) and decayed toward reaching zero at 80 minutes.

The preceding test data were reviewed and a probability distribution for the fire duration was developed based on engineering judgment. This distribution is characterized by 10% to 90% hazard levels of 10 minutes and 60 minutes, respectively (i.e., it was concluded that 10% of the fires would result in a target exposure duration of less than 10 minutes and 90% of the fires would result in a target exposure duration of less than 60 minutes). These values were fitted to a lognormal distribution with a mean and standard deviation of 3.192 and 0.6943, respectively. The mean of this distribution is approximately 31 min, the median (50<sup>th</sup> percentile) is approximately 24 min, and the error factor (i.e., the ratio of the 95<sup>th</sup> percentile over the median) is about 3.1. The resultant probability distribution is presented in Table D2.1-1 as the probability of target exposure durations over a set of discrete intervals. The 30-minute design basis fire duration mandated in 10 CFR 71.73 (Ref. D4.2.2) corresponds to the 62nd percentile value of this distribution.

Table D2.1-1. Probability Distribution for Fire Duration - Without Automatic Fire Suppression

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (minutes)	Interval Probability <sup>a</sup>
10	0.1	0 to 10	0.1
20	0.39	10 to 20	0.29
30	0.62	20 to 30	0.23
40	0.76	30 to 40	0.14
50	0.85	40 to 50	0.09
60	0.903	50 to 60	0.053
70	0.936	60 to 70	0.033
90	0.97	70 to 90	0.034
120	0.989	90 to 120	0.019
150	0.9956	120 to 150	0.0066

Table D2.1-1. Probability Distribution for Fire Duration - Without Automatic Fire Suppression (Continued)

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (minutes)	Interval Probability <sup>a</sup>
180	0.998	150 to 180	0.0024
210	0.999	180 to 210	0.001
270	0.99974	210 to 270	0.00074
360	0.99995	270 to 360	0.00021
∞	1	>360	5E-05

NOTE: <sup>a</sup> The interval probability is the difference between the cumulative probability at the top of the interval and the cumulative probability at the bottom of the interval.

Source: Original

### D2.1.1.3 Fire Duration with Automatic Suppression

The second uncertainty distribution that was developed is for fires where automatic suppression is available. There were only a limited number of tests conducted for this case.

Factory Mutual Research Corporation conducted tests for large-scale configurations of cable trays, as discussed in the previous sections. In addition to the tests conducted without suppression, a number of tests were conducted with suppression. NUREG/CR-4679 (Ref. D4.1.53, pp. 26-31) provides detailed results for six of these “extinguishment tests.” All these tests involved a configuration of 12 fully loaded horizontal trays in two stacked tiers. Two of the six also involved the addition of two fully loaded vertical cable trays. The cables were polyvinyl chloride (PVC) - jacket with polyethylene insulation. The results of the first four tests were that the fires reached their peak heat release rates at 8, 9, 12, and 12 minutes. The associated times when the heat release rate dropped to zero were 10, 12, 16, and 29 minutes, respectively. The results of the final two tests were peak heat release rates at 9 and 16 minutes, with zero being reached at 24 and 36 minutes, respectively.

These were the only extinguishment tests reported in the references. Therefore, an analysis of a wooden box-type fire conducted by Parsons also was examined. This is not an actual test, but rather a calculation of a “typical” fire where credit was given for the actuation of fire suppression. The calculation gave a peak heat release rate occurring at 7 minutes and extending to 15 minutes. The calculation showed the fire decaying towards zero at approximately 20 minutes.

These test data were reviewed and a probability distribution for the fire duration was developed based on engineering judgment. Although the data are somewhat sparse, they were taken in the overall context of how the actuation of suppression affected the tests conducted and how that compared to the free-burn tests. This was extrapolated to the other free-burn tests. It was judged likely that the operation of automatic suppression would have little effect on the lower end of the distribution, as such fires would likely burn out without actuating suppression. However, there would be a significant effect for the longer fires. It was concluded that a reasonable estimate of the 10 to 90% hazard levels was 10 minutes and 30 minutes (i.e., it was concluded that it was a reasonable interpretation of the data to state that 10% of the fires would result in target exposure

duration of less than 10 minutes and 90% of the fires would result in target exposure duration of less than 30 minutes). These values were fitted to a lognormal distribution with a mean and standard deviation of 2.849 and 0.4286, respectively. The resultant uncertainty distribution is presented in Table D2.1-2 as the probability of target exposure durations over a set of discrete intervals.

Table D2.1-2. Probability Distribution for Fire Duration - With Automatic Fire Suppression

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (min)	Interval Probability <sup>a</sup>
10	0.1	0 to 10	0.1
15	0.37	10 to 15	0.27
20	0.63	15 to 20	0.26
25	0.81	20 to 25	0.18
30	0.901	25 to 30	0.091
40	0.975	30 to 40	0.074
50	0.993	40 to 50	0.018
60	0.9982	50 to 60	0.0052
80	0.9998	60 to 80	0.0016
100	0.99998	80 to 100	0.00018
∞	1	>100	2E-05

NOTE: <sup>a</sup> The interval probability is the difference between the cumulative probability at the top of the interval and the cumulative probability at the bottom of the interval.

Source: Original

### D2.1.2 Uncertainty in Fire Temperature

As used in the fire fragility analysis, the fire temperature is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. D4.1.61, p. 2-56). A review of the available fire temperature data for liquid and solid fuels is discussed below.

Experimental measurements of liquid hydrocarbon pool fires with radii from 0.25 to 40.0 m indicate effective blackbody radiation temperatures between 1,200°K and 1,600°K (927°C and 1,327°C) (Ref. D4.1.61, p. 2-56). Testing of rail tank cars engulfed in a liquid hydrocarbon pool fire indicates an effective blackbody temperature of 816°C to 927°C (1,089°K to 1,200°K) (Ref. D4.1.2).

Heat release data for combustible solid materials such as wood, paper, or plastic are plentiful, but fire temperature data have generally not been presented. However, *The SFPE Handbook of Fire Protection Engineering* (Ref. D4.1.61, pp. 3-82 to 3-87) discusses the hot gas temperatures associated with fully-developed compartment fires that do include combustion of solid materials. Fully-developed fires involve essentially all combustible material in a compartment, so the peak hot gas temperature should be reasonably indicative of the *effective* fire temperature. The data indicate typical peak temperatures between 400°C and 1,200°C (750°F and 2,190°F). (The

400°C value applies to small, short duration fires and is too low to represent a true fire temperature.)

Fires within one of the YMP facilities are likely to involve both combustible solid and liquid materials. Judgment suggests that most postulated fires should generally resemble the compartment fires discussed in *The SFPE Handbook of Fire Protection Engineering* (Ref. D4.1.61, Section 2, Chapter 7). This implies that the assigned temperature distribution should be strongly influenced by the 400°C and 1,200°C range. However, combustible liquids (e.g., diesel fuel in a site transporter) may also contribute significantly to some fires, so the upper bound of the fire temperature distribution should include the higher temperatures indicated by the pool fire data. Based on this reasoning, the fire temperature distribution is normally distributed with a mean of 1,072°K (799°C) and a standard deviation of 172°K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C mandated in 10 CFR 71.73 (Ref. D4.2.2).

This fire temperature probability distribution has a value of 400°C for the 5th percentile and 1,327°C for the 99.9th percentile. The first value represents the lower end of the compartment fire temperature range while the second corresponds to the upper end of the liquid pool fire effective blackbody temperature range. Therefore, the distribution applies to fires involving both liquid and solid fuels.

It should be noted that data from fire testing indicate that the fire temperature is not constant over the duration of the fire. The fire temperature generally increases to a peak value and then decreases considerably as the combustible material is consumed. In the fire fragility analysis, herein, the fire temperature is treated as constant, which tends to increase the maximum target temperature.

### **D2.1.3 Correlation of Fire Temperature and Duration**

Testing has shown that fire temperature and duration are negatively correlated. Intense fires with high fire temperatures tend to be short-lived because the high temperature results from very rapid burning of the combustible material. In contrast, long duration fires generally result from slower burning of the combustible material. In the probabilistic fire fragility analysis discussed below, the fire temperature and duration were correlated with a conservative correlation coefficient of -0.5. It is conservative because this correlation allows some fires that have both a high temperature and long duration.

### **D2.1.4 Uncertainty in the Thermal Response of the Canister**

The probability distributions discussed in Section D2.1.1 characterize the uncertainty in the fire severity. In order to determine the probability that a canister fails due to a fire, models are needed to calculate the uncertainty in the thermal response of the container to a fire and the uncertainty in the failure temperature of the container.

The following sections describe the two simplified heat transfer models used to determine the thermal response of the canister to the fire. The heat transfer models have been simplified in order to allow a probabilistic analysis using Monte Carlo sampling. The two models discussed

below apply to bare canisters or canisters inside a waste package, transportation cask, or a canister transfer machine (CTM) shielded bell. The simplified model was validated by comparison with a more complete model as discussed in Section D2.1.4.3.

#### D2.1.4.1 Heat Transfer to Bare Canisters

Bare canisters near or engulfed in a fire can be heated primarily by two heat transfer mechanisms: convection and radiation. Convection heating occurs when hot gases from the fire circulate and come into contact with the canister surface. Due to gravitational effects, the hot gases from the fire are expected to rise and collect near the ceiling of the room. Thus, unless a canister is engulfed in the fire, the hot gases are unlikely to come into direct contact with the canister, and radiation should be the dominant mode of heating. Further, radiation from the flame (luminous portion of the fire gases) is expected to far exceed radiation from the hot gas layer near the ceiling. For that reason, radiative heating by the hot gas layer is not considered in the fragility analysis. The heat transfer model described in the following sections are believed to capture the important aspects of the heat transfer from the fire.

Due to substantial conduction within the metal wall of the canister, the canister wall is modeled as a single effective temperature (thin-wall approximation) during heatup. Using this approach, the canister temperature ( $T_c$ ) was advanced in time using the following Euler finite-difference formulation:

$$T_c = \frac{q_{c,net} \Delta t}{m_c c_{p,c}} + T_{c,i} \quad (\text{Eq. D-5})$$

where

- $m_c$  = mass of the canister wall
- $c_{p,c}$  = specific heat of the canister material
- $\Delta t$  = time step
- $T_{c,i}$  = canister temperature at the beginning of the time step, and
- $q_{c,net}$  = net rate of energy deposition into the canister.

The net rate of energy deposition into the canister during the fire is given by the following equation:

$$q_{c,net} = q_{r,fire} + q_{c,fire} - q_{r,f} \quad (\text{Eq. D-6})$$

where

- $q_{r,fire}$  = radiative heat transfer to the canister from the fire
- $q_{c,fire}$  = net convective heat transfer to the canister (positive if the canister is engulfed by the fire and negative if the canister is not engulfed by the fire)
- $q_{r,f}$  = radiative heat transfer from the canister to material stored in the canister.

The terms on the right-hand-side of this equation are defined below.

An earlier formulation of Equation D-6 included convective heat transfer from the canister wall to the gas inside the canister and from this gas to the spent fuel inside the canister. The addition of this heat transfer term did not significantly affect the heating rate of either the canister or the fuel, but did significantly increase the calculation time for the analysis. For that reason, convective heat transfer to the gas inside the canister was not included in the subsequent probabilistic analysis.

In this analysis, the important parameters are: (1) the fire temperature, size, and location relative to the canister, (2) treatment of the fire surface as a blackbody, and (3) treatment of the canister surface as diffuse and gray. Thus, the net rate of radiative heat transfer to the canister surface,  $q_{r,fire}$ , is given by:

$$q_{r,fire} = \epsilon_c A_c F_{c-fire} F_s \sigma (T_{fire}^4 - T_c^4) \quad (\text{Eq. D-7})$$

where

$\epsilon_c$	=	emissivity of the canister surface
$A_c$	=	surface area of the canister
$F_{c-fire}$	=	view factor between the canister and the fire, which is the related to the fraction of radiation leaving the fire that strikes the canister surface
$F_s$	=	suppression scale factor (discussed below)
$\sigma$	=	Stefan-Boltzmann constant
$T_{fire}$	=	effective blackbody temperature of the fire
$T_c$	=	canister temperature.

In Equation D-6,  $q_{c,fire}$  is the energy input due to convective heating from the fire, which is given by:

$$q_{c,fire} = A_c F_s h_{conv} (T_{fire} - T_c) \quad (\text{Eq. D-8})$$

where  $h_{conv}$  is the convective heat transfer coefficient and all other terms are defined as above.

The final term in Equation D-6 is the rate of heat transfer from the canister to the spent fuel or high level waste. This term is given by the following equation:

$$q_{r,f} = \frac{A_c F_{c-f} \sigma (T_c^4 - T_f^4)}{1/\epsilon_c + 1/\epsilon_f - 1} \quad (\text{Eq. D-9})$$

where  $F_{c-f}$  is the view factor between the canister and the fuel,  $\epsilon_f$  is the emissivity of the fuel, and  $T_f$  is the temperature of the fuel being heated by the canister (outer portion of the fuel).

As the canister becomes hotter and heat is transferred to the fuel, the fuel temperature will also increase according to the following equation:

$$T_f = \frac{(q_{r,f} + q_{DH})\Delta t}{m_f c_{p,f}} + T_{f,i} \quad (\text{Eq. D-10})$$

where  $q_{DH}$  is the decay heat generated in the fuel,  $m_f$  is the mass of fuel heated by the canister (outer portion of the fuel),  $c_{p,f}$  is the specific heat of the fuel, and  $T_{f,i}$  is the fuel temperature at the beginning of the time step.

Equation D-10 uses the mass of fuel being heated by the canister and the corresponding decay heat in this portion of the fuel. This equation ignores heat transfer from the heated fuel to unheated fuel. That is, there is no energy exchange between the outer fuel and the inner fuel.

The fuel mass to use in Equation D-10 can be estimated by calculating the thermal penetration depth within the fuel during the fire. In a number of previous studies (for example, (Ref. D4.1.25)), the fuel region inside the canister has been treated as a homogeneous material with effective thermal properties. The effective thermal properties used in these studies were determined for many different fuel configurations based on the results from detailed thermal analyses. Table D2.1-3 presents the effective thermal properties for 21-PWR fuel in the TAD canister (Ref. D4.1.25).

Table D2.1-3. Effective Thermal Properties for 21-PWR Fuel in a TAD

Property	Value
Density, $\rho$	3,655 kg/m <sup>3</sup>
Specific Heat, $c_p$	438 J/kg K
Thermal Conductivity, $k$	4.29 W/m K
Thermal Diffusivity, $\alpha$	$2.6 \times 10^{-6}$ m <sup>2</sup> /s

NOTE: PWR = pressurized water reactor; TAD = transportation, aging, and disposal (canister).

Source: Ref. D4.1.25, Table 17, and Equation 2 of Section 6.2.2.

Based on the effective thermal properties listed in the table, estimation of the thermal penetration depth during a typical fire is given by the following equation:

$$\delta = \sqrt{\alpha t} \quad (\text{Eq. D-11})$$

where  $\alpha$  is the effective thermal diffusivity and  $t$  is the time (3,600 seconds). Based on the effective thermal diffusivity shown in the table, a thermal penetration depth of approximately 9.5 cm is calculated. The fuel volume corresponding to this penetration depth is calculated by multiplying the canister interior surface area by the penetration depth. The effective fuel mass is then calculated by multiplying this volume by the effective density of the fuel. The resulting fuel mass is approximately 9,700 kg.

### D2.1.4.2 Heat Transfer to a Canister inside a Cask, Waste Package, or Shielded Bell

The calculation of the heating of a canister inside another container or structure is slightly more complex than that for a canister directly exposed to fire. When inside another container, the canister is not directly heated by the fire. Rather, the container is first heated by the fire and then the interior surface of the heated container radiates heat to the canister and also convects heat to any air or other gas in the annular region between the outer container and canister. When there are multiple heat transfer barriers (e.g., the waste package, which has an outer barrier and an inner barrier), heat transfer between the barriers must also be considered. The following discussion includes the presence of an inner and outer barrier, as is the case for a waste package.

The calculation of canister heating was accomplished by first calculating the temperature of the outer barrier when exposed to a fire. Then, the energy radiated from the outer barrier to the inner barriers was calculated. Next, the energy radiated from the inner barrier to the canister was calculated. Models that included convective heat transfer to and from the gas in the annular spaces between these regions demonstrated that convective heating and cooling had little effect on the heating of the canister, but caused calculation times to be significantly longer. As a result, the convective heat transfer was removed from the models and the temperature increase of the inner barrier and canister were calculated based on radiative heating only.

It should also be noted that many transportation casks have neutron or gamma shielding composed of a low melting point material such as borated polyethylene. This material is likely to melt very quickly so its effect on heat transfer was not considered in the model. In reality, this layer of material would have a substantial resistance to heat transfer, at least initially. Ignoring this thermal resistance is therefore conservative.

The heating of the outer barrier is calculated in the same general manner as that of a bare canister exposed directly to a fire. Due to the substantial conduction within the metal barrier, the thin-wall approximation was applied. Using this approach, the outer barrier temperature ( $T_{ob}$ ) was advanced in time using the following Euler finite-difference formulation:

$$T_{ob} = \frac{(q_{ob} - q_{ib})\Delta t}{m_{ob}c_{p,ob}} + T_{ob,i} \quad (\text{Eq. D-12})$$

where

- $q_{ob}$  = radiation and convection to the outer barrier from the fire
- $q_{ib}$  = radiation to the inner barrier from the outer barrier
- $m_{ob}$  = mass of the outer barrier
- $c_{p,ob}$  = specific heat of the outer barrier
- $\Delta t$  = time step
- $T_{ob,i}$  = outer barrier temperature at the beginning of the time step.



Equation D-12 does not consider convective heat transfer to the air inside the container. Initial calculations showed that convective heat transfer to the air in the container would be small compared to the radiation heat loss term, so convective heat transfer was neglected.

If (1) the fire temperature, size, and location relative to a container are known, (2) the fire surface can be treated as a blackbody, and (3) the outer barrier surface can be considered diffuse and gray, then the net rate of radiative heat transfer to the outer barrier surface ( $q_{ob}$ ) can be approximated as:

$$q_{ob} = \varepsilon_{ob} A_{ob} F_{fc} F_s \sigma (T_f^4 - T_{ob}^4) \quad (\text{Eq. D-13})$$

where

- $\varepsilon_{ob}$  = emissivity of the outer barrier surface
- $A_{ob}$  = surface area of the outer barrier
- $F_{fc}$  = view factor for radiative heat transfer, which is related to the fraction of radiation leaving the fire that strikes the outer barrier surface
- $F_s$  = suppression scale factor (discussed below)
- $\sigma$  = Stefan-Boltzmann constant
- $T_f$  = fire (flame) temperature
- $T_{ob}$  = temperature of the outer barrier.

Once the temperature of the outer barrier is known, the heating of the inner barrier can be found in the same manner. Instead of a fire temperature, the temperature of the heated outer barrier is used and the net rate of radiative heat transfer from the outer barrier interior surface to inner barrier ( $q_{ib}$ ) can be approximated as:

$$q_{ib} = \frac{A_{ob} F_{oi} \sigma (T_{ob}^4 - T_{ib}^4)}{1/\varepsilon_{ib} + 1/\varepsilon_{ob} - 1} \quad (\text{Eq. D-14})$$

where

- $\varepsilon_{ib}$  = emissivity for of the inner barrier
- $F_{oi}$  = view factor for radiation between the outer and inner barriers (discussed below)
- $T_{ib}$  = inner barrier surface temperature.

The temperature of the inner barrier is calculated using an equation similar to Equation D-12; however, in this equation, the thermal radiation incident on the inner barrier comes from the outer barrier rather than the fire and the heat loss from the inner barrier is to the spent fuel or high level waste canister.

Finally, the temperature of the canister is calculated using the following equation, which has a form similar to Equation D-12:

$$T_c = \frac{(q_{ib} + q_{DH})\Delta t}{m_c c_{p,c}} + T_{c,i} \quad (\text{Eq. D-15})$$

where  $q_{DH}$  is the total decay heat generated by the contents of the canister and all other terms are defined as in preceding equations.

In Equation D-15, the heat capacity of the contents of the canister is conservatively neglected so that all decay heat is transmitted to the canister wall. In reality, some fraction of the decay heat would be transmitted to the contents of the canister (e.g., the spent fuel or high level waste), increasing the temperature of the contents. Neglecting this term is conservative since it increases the temperature increase of the canister itself.

Note also that, in order to simplify the model, heat transfer from the canister to its contents is ignored in Equation D-15. In reality, some heat would be transferred from the canister wall to the spent fuel or high level waste inside the canister. Neglecting this heat removal is conservative since it increases the temperature increase of the canister.

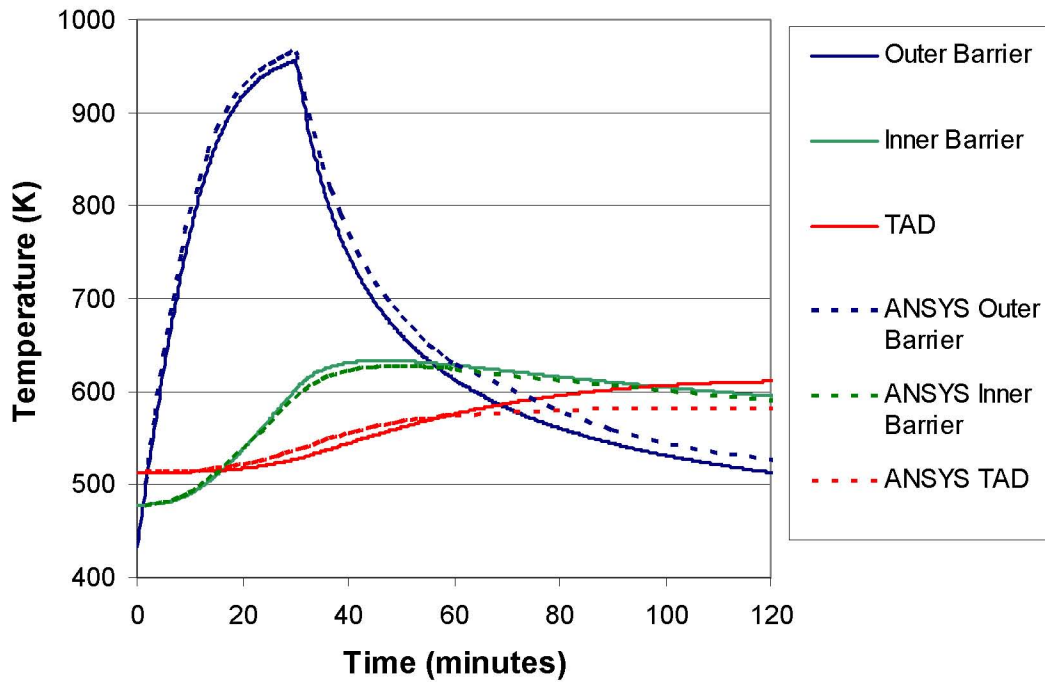
Unlike the bare canister case in which heating of the canister ends when the fire ends, heating of a canister that is inside other containers will increase after the fire ends as heat is transmitted from the heated outer and inner barrier. After the fire has been extinguished, heat will be lost by the outer barrier due to a combination of radiation to cooler surfaces and convection to the air in the room. A temperature of 400°K was used as the surface and air boundary condition. The surfaces were modeled as blackbodies in the radiation heat transfer calculation. Convective heat transfer was calculated based on a heat transfer coefficient of 2.0 W/m<sup>2</sup> K. The fragility analysis showed that the predicted canister failure probability was not sensitive to either the boundary condition temperature or the convective heat transfer coefficient.

#### **D2.1.4.3 Validation of the Simplified Heat Transfer Models**

In order to validate the simplified heat transfer models discussed above, results were compared to results calculated using more detailed models. In one such comparison, results calculated using the model for heating of a canister in a waste package were compared to the results from a similar ANSYS calculation (Ref. D4.1.25, Attachment V). ANSYS is a finite-element analysis software application use in nuclear facility and non-nuclear industrial applications to model temperature evolutions of complex systems. The simplified model was set up to match the inputs to the ANSYS calculation as closely as possible. The only differences between the two included:

- The ANSYS run was made with temperature-dependent specific heats whereas average specific heats were used in the simplified model.
- The ANSYS run treated the TAD canister and its contents as a homogeneous material with average properties, whereas the simplified model treated the TAD canister but ignored heat transfer to its contents.

Figure D2.1-1 shows a comparison of the calculated time-dependent temperatures from these two calculations. The figure shows that the simplified model accurately predicts the results from the more detailed analysis. Because heat transfer from the TAD canister to its contents is ignored in the simplified model, the canister reaches slightly higher temperatures with the simplified model compared to the more detailed model.



NOTE: TAD = transportation, aging, and disposal canister.

Source: Original

Figure D2.1-1. Comparison Between Results Calculated Using the Simplified Heat Transfer Model and ANSYS – Fire Engulfing a TAD Canister in a Waste Package

A similar comparison was made between the results reported in the HI-STAR safety analysis report (SAR) (Ref. D4.1.38, Table 3.5.4) and results calculated using the simplified model. These calculations simulated a design basis 30-minute fire. The maximum canister temperature reported in the HI-STAR SAR was 419°F (215°C). This temperature was predicted to occur approximately 3 hours after the start of the fire. The simplified model predicted a peak canister temperature of 213.5°C at approximately 4 hours after the start of the fire. This comparison again demonstrates the accuracy of the simplified model in predicting the maximum canister temperature due to the fire.

Detailed ANSYS calculations were not performed for the bare canister configuration. However, it is possible to infer the accuracy of the simplified bare canister model based on the accuracy of the simplified model in predicting the thermal response of the outer barrier in the waste package

configuration. As shown in Figure D2.1-1, the simplified heat transfer accurately predicted the thermal response of the outer barrier both during the 30-minute fire and after.

#### **D2.1.4.4 Heat Transfer Model Inputs and Uncertainties**

The heat transfer models discussed in Sections D2.1.4.1 and D2.1.4.2 include a large number of input parameters. Some of these parameters are known to a high degree of confidence whereas others are considered to be uncertain. This uncertainty was explicitly considered in the probabilistic analysis discussed in Section D2.1.1. The following sections discuss the major inputs to the models and the treatment of the uncertainty in these inputs.

##### **D2.1.4.4.1 View Factor**

The radiation view factor from the container (e.g., cask or waste package) to the fire can be calculated if the size of the fire and distance between the fire and the container can be determined. The size (height and width) of the fire can be approximated using published correlations in the SFPE handbook (Ref. D4.1.61, Section 1, Chapter 6). The distance between the fire and the container depends on the location of combustible materials and ignition sources relative to the container.

Since the location of combustible materials and ignition sources relative to the container is difficult to predict and would vary from one room to another, a conservative approach in which the container was engulfed by the fire is followed. For a container completely engulfed by the fire the view factor is essentially 1.0. This is conservative for the long vertically-oriented containers because even an engulfing fire may engulf only the lower portion of the container.

A view factor of 1.0 was applied only to the cask, waste package, or a shielded bell that encase a canister. Bare canisters are treated differently. Since a canister is only bare as it is being withdrawn from a cask or inserted into a waste package, only a portion of the canister could be exposed to the fire at any given time. In this case, the view factor is given by fraction of the canister actually exposed to the fire. This fraction depends on the space between the top of the cask or waste package and the ceiling of the loading or unloading room. Generally, this fraction would be considerably less than 50%.

The radiation view factor between concentric cylinders (e.g., the inner and outer barrier of a waste package) can be estimated very easily if the cylinders are very long compared to their diameters. Under this condition, which is true of most configurations of interest in the current study, the view factor can be approximated by  $D_i/D_o$  where  $D_i$  and  $D_o$  are the inner and outer diameters of the two cylinders (Ref. D4.1.63, Configuration C-63).

##### **D2.1.4.4.2 Consideration of Fire Suppression on Canister Heating**

The effect of fire suppression on canister heating is treated using a suppression scale factor. The suppression scale factor is included in the heat transfer equations as an adjustment to the rate of heat transfer to the canister from the fire. The value of the suppression scale factor used in the model is based on testing at the Building and Fire Research Laboratory, which is part of the National Institute of Standards and Technology (Ref. D4.1.31).

The Building and Fire Research Laboratory tests considered a range of fires and a range of sprinkler system spray densities. Results were presented for the net heat release rate from the fire both before and after actuation of the fire suppression system. The fire suppression scale factor implicitly includes consideration of the time delay before actuation of the fire suppression system and the effectiveness of the system. Rooms with early actuation and effective fire suppression would have a very small suppression scale factor, whereas rooms with delayed actuation and/or ineffective fire suppression would have a large suppression scale factor (upper bound of 1.0 when no suppression is present).

Because no credit is taken for fire suppression in this analysis, the fire suppression scale factor was set equal to 1.0 in all of the analyses discussed in this document.

#### **D2.1.4.4.3 Convective Heat Transfer Coefficient during the Fire**

In testing of containers engulfed in a fire, considerable variations in the convective heat transfer coefficient have been measured. Values as high as  $30 \text{ W/m}^2 \text{ K}$  have been measured in vigorously burning pool fires (Ref. D4.1.51, pp. 19-21), although values on the order of  $20 \text{ W/m}^2 \text{ K}$  or less are considered more typical (Ref. D4.1.57, Table 3-2). For fire conditions in which the combustible material is burning more slowly, values on the order of  $5 \text{ W/m}^2 \text{ K}$  or lower have been measured (Ref. D4.1.51, p. 19). To capture the potential variability in the convective heat transfer coefficient, a probability distribution for the convective heat transfer coefficient was included in the model. A normal distribution applies with a mean and standard deviation of  $17.5 \text{ W/m}^2 \text{ K}$  and  $4.2 \text{ W/m}^2 \text{ K}$ , respectively. This distribution yields practical upper and lower bound values (0.1 and 99.9th percentiles) of approximately 5 and  $30 \text{ W/m}^2 \text{ K}$ .

#### **D2.1.4.4.4 Decay Heat**

The canisters processed through the preclosure facilities will contain spent fuel with varying decay heat levels. Based on information provided in the safety analysis reports for transportation casks, a probability distribution was developed for the decay heat level in the canister. A normal distribution applies with a mean and standard deviation of 17kW and 3kW, respectively. This distribution yields practical upper and lower bound values (0.1 and 99.9th percentiles) of approximately 8kW and 26kW.

#### **D2.1.4.4.5 Other Model Inputs**

Other inputs required by the heat transfer model include (1) the thermal and physical properties of all materials, (2) the dimensions of the canister, cask, waste package, or shielded bell, (3) the initial temperatures of each layer, (4) decay heat generated within the canister, and (5) the post-fire convective heat transfer coefficient and temperature. The values for these input parameters are provided in Tables D2.1-4 through D2.1-7. The tables also provide a brief rationale or a reference for the values used in the analysis.

As shown in the tables, calculations were performed for two spent fuel canister wall thicknesses: 0.5 inches (0.0127 m) and 1.0 inch (0.0254 m). This was done for two reasons. First, initial calculations showed that the wall thickness greatly influences both the heating and failure of the canister. Second, a review of the available canister information indicated a range of canister thicknesses from 0.5 inches to 1 inch. A substantial fraction of the older transport cask designs

have spent fuel canisters with wall thicknesses of 0.5 or 0.625 inches, whereas newer designs (e.g., the naval spent fuel canister or TAD canister) are expected to have a wall thickness of 1.0 inch.

Table D2.1-4. Model Inputs – Bare Canister

Model Parameter	Value	Basis/Rationale
<b>Canister Properties</b>		
Outer Diameter (m)	1.68	Minimum outer diameter listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Density (kg/m <sup>3</sup> )	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400C (Ref. D4.1.25, Table 8)
Emissivity	0.8	Estimated value for stainless steel that has undergone some oxidation
Initial Temperature (K)	513	Initial temperature upon removal from the cask. Estimated from <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Fuel Properties</b>		
Heated Mass (kg)		Calculated based on thermal penetration depth (see text)
Specific Heat (J/kg K)	438	Average for fuel region taken from <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Table 15)
Effective Surface Area (m <sup>2</sup> )	28.18	Projected area for radiation heat transfer. Calculated based on outer diameter of fuel region (1.67 m)
Emissivity	0.8	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Table 17)
Initial Temperature (K)	543	Estimated from <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Post-Fire Conditions</b>		
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)

Table D2.1-4. Model Inputs – Bare Canister (Continued)

Model Parameter	Value	Basis/Rationale
<b>Canister Properties</b>		
Heat Transfer Coefficient (W/m <sup>2</sup> K)	2.0	Approximate value based on correlations in (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-5. Model Inputs – Canister in a Waste Package

Model Parameter	Value	Basis/Rationale
<b>Canister Properties</b>		
Outer Diameter (m)	1.68	Minimum diameter listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs  1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Density (kg/m <sup>3</sup> )	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Outer Barrier of Waste Package</b>		
Outer Diameter (m)	1.8816	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0254	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Length (m)	5.4	Heated length adjacent to the TAD canister – same as TAD canister length
Density (kg/m <sup>3</sup> )	8690	Value for Alloy 22 (Ref. D4.1.5, Section II, Part B, SB-575, Section 7.1)
Specific Heat (J/kg K)	476	Value for Alloy 22 at 400°C (Ref. D4.1.36, p. 13)
Emissivity	0.87	Value for Alloy 22 (Ref. D4.1.45, p. 10-297)
Initial Temperature (K)	433	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)

Table D2.1-5. Model Inputs – Canister in a Waste Package (Continued)

Model Parameter	Value	Basis/Rationale
<b>Inner Barrier of Waste Package</b>		
Outer Diameter (m)	1.8212	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Wall Thickness (m)	0.0508	Listed in <i>TAD Waste Package Configuration</i> (Ref. D4.1.22), (Ref. D4.1.23), and (Ref. D4.1.24)
Length (m)	5.4	Heated length adjacent to the TAD canister – same as TAD canister length
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	478	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Post-Fire Conditions</b>		
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)
Heat Transfer Coefficient (W/m <sup>2</sup> K)	2.0	Approximate value based on correlations in <i>Introduction to Heat Transfer</i> (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-6. Model Inputs – Canister in Transportation Cask

Model Parameter	Value	Basis/Rationale
<b>Canister Properties</b>		
Outer Diameter (m)	1.68	Minimum diameter listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Density (kg/m <sup>3</sup> )	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)



Table D2.1-6. Model Inputs – Canister in Transportation Cask (Continued)

Model Parameter	Value	Basis/Rationale
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Transportation Cask Outer Shell</b>		
Outer Diameter (m)	2.438	From HI-STAR Transportation Cask SAR (Ref. D4.1.38, p. 1.2-3)
Wall Thickness (m)	0.0127	Minimum outer shell thickness listed in cask SARs
Length (m)	5.4	Length adjacent to the TAD canister
Density (kg/m <sup>3</sup> )	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)
Emissivity	0.8	Average value for carbon steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	381	Initial temperature in HI-STAR SAR (Ref. D4.1.38, Figure 3.5.3)
<b>Transportation Cask Gamma Shield</b>		
Outer Diameter (m)	2.148	From HI-STAR Transportation Cask SAR (Ref. D4.1.38, Drawing No.3913)
Wall Thickness (m)	0.19	A lower value for the combined thickness of gamma shield and inner containment listed in cask SARs
Length (m)	5.4	Length adjacent to the TAD canister
Density (kg/m <sup>3</sup> )	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)
Emissivity	0.8	Average value for carbon steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	405	Approximate average initial temperature in HI-STAR SAR (Ref. D4.1.38, Figure 3.5.3)
Ambient Temperature (K)	361	Post-fire temperature of 190°F - a value 100°F higher than the maximum interior facility temperature (Ref. D4.1.16, Section 3.2)
Heat Transfer Coefficient (W/m <sup>2</sup> K)	2.0	Approximate value based on correlations in <i>Introduction to Heat Transfer</i> (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SAR = Safety Analysis Report; SFC = spent fuel canister; SNF = spent nuclear fuel;  
TAD = transportation, aging, and disposal.

Source: Original

Table D2.1-7. Model Inputs – Canister in a Shielded Bell

Model Parameter	Value	Basis/Rationale
<b>Canister Properties</b>		
Outer Diameter (m)	1.68	Minimum diameter listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Wall Thickness (m)	0.0127 or 0.0254	0.5 inches is the thinnest canister wall thickness listed for current transport cask designs 1.0 inch is the anticipated TAD canister thickness and is also the thickness of the naval SFC
Length (m)	5.4	Typical length of TAD canister listed in <i>Transportation, Aging and Disposal Canister System Performance Specification</i> (Ref. D4.1.28, Section 3.1.1)
Density (kg/m <sup>3</sup> )	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.62	Average value for Type 316 stainless steel in <i>Mark's Standard Handbook for Mechanical Engineers</i> (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	513	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<b>Shielded Bell</b>		
Outer Diameter (m)	2.388	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (Ref. D4.1.11)
Wall Thickness (m)	0.273	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (Ref. D4.1.11)
Length (m)	7.62	From <i>CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope</i> (Ref. D4.1.11)
Density (kg/m <sup>3</sup> )	7980	Density of Type 316 stainless steel (Ref. D4.1.7, Table X1.1)
Specific Heat (J/kg K)	560	Approximate value for Type 316 stainless steel at 400°C (Ref. D4.1.25, Table 8)
Emissivity	0.67	Approximate value at elevated temperature (corresponds to little oxidation of the surface)
Initial Temperature (K)	306	Maximum interior facility temperature of 90°F (Ref. D4.1.16, Section 3.2)
<b>Post-Fire Conditions</b>		
Ambient Temperature (K)	367	Post-fire temperature of 190°F - a value 100°F higher than the maximum operating temperature listed above

Table D2.1-7. Model Inputs – Canister in a Shielded Bell (Continued)

Model Parameter	Value	Basis/Rationale
Heat Transfer Coefficient (W/m <sup>2</sup> K)	2.0	Approximate value based on correlations in <i>Introduction to Heat Transfer</i> (Ref. D4.1.41, pp. 456-457) (Results not sensitive to this value)

NOTE: SFC = spent fuel canister; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal.

Source: Original

### D2.1.4.5 Uncertainty in Canister Failure Temperature

Using the models discussed in Sections D2.1.4.1 and D2.1.4.2, the temperature increase of a canister due to a fire can be calculated. In order to determine whether the temperature is sufficient to cause the canister to fail, it is necessary to determine the canister temperature at which failure would occur. Two failure modes were considered:

1. *Creep-Induced Failure.* Creep is the plastic deformation that takes place when a material is held at high temperature for an extended period under tensile load. This mode of failure is possible for long duration fires.
2. *Limit Load Failure.* This failure mode occurs when the load exerted on a material exceeds its structural strength. As the temperature of the canister increases in temperature, its strength decreases. Failure is generally predicted at some fraction (usually around 70 percent) of the ultimate strength.

The modeling associated with these failure modes is described in the following subsections.

#### D2.1.4.5.1 Modeling Creep-Induced Failure

Creep failure could occur if the canister is maintained at a high temperature for a lengthy period of time. One way to predict creep failure is to calculate a creep damage index, which defines the ratio of the creep damage to the cumulative creep required for failure. Such a model has been used by researchers at Argonne National Laboratory to predict failure of steam generator tubes under accident conditions (Ref. D4.1.46). In the Argonne National Laboratory model, failure occurs when the creep damage index reaches a value of 1. Written in the form of an equation, this condition is given by:

$$\int_0^{t_f} \frac{dt}{t_R(T, \sigma)} = 1 \quad (\text{Eq. D-16})$$

where

- T = the temperature experienced by the canister (a function of time)  
 σ = the tensile stress exerted on the canister wall, and  
 t<sub>f</sub> = the canister failure time (the time at which the equality is satisfied).

The function in the denominator of Equation D-16 is

$$t_R = 10^{\frac{P_{LM}}{T}-20} \quad (\text{Eq. D-17})$$

where  $P_{LM}$  is the Larson-Miller parameter (Ref. D4.1.44), which is a material property of the canister material and is a function of the applied stress.

Since the canisters are pressurized to varying degrees with a combination of helium or air used to backfill the canister and gases released when the fuel fails, the pressure inside the canister will increase as the canister gets hotter. The internal pressure exerts a hoop stress in the radial direction that puts the canister wall under tension. It is this stress that controls failure of the canister wall. The hoop stress,  $\sigma$ , is calculated using the following equation:

$$\sigma = \frac{Pr_c}{h} \quad (\text{Eq. D-18})$$

where

- h = the thickness of the canister wall
- $r_c$  = the mean radius of the canister
- P = the pressure difference across the canister wall.

#### D2.1.4.5.2 Modeling Limit Load Failure

Limit load failure occurs when the load on a structure exceeds its ability to withstand that load. As with the creep failure mode, the load on the canister wall is a hoop stress and is calculated using Equation D-18.

The capability of the canister to withstand a load is given by a flow stress, which is defined by (Ref. D4.1.46, p. 3):

$$\bar{\sigma} = k(\sigma_y + \sigma_u) \quad (\text{Eq. D-19})$$

where

- k = a multiplication factor (0.5 in the current analysis)
- $\sigma_y$  = the yield strength (temperature dependent)
- $\sigma_u$  = the ultimate strength (temperature dependent).

The yield and ultimate strength are both temperature-dependent properties, so the flow stress is also a temperature-dependent property. For a typical 316 stainless steel, a value of 0.5 for k yields a flow stress that is approximately 0.7 times the ultimate strength. Failure is predicted if the hoop stress exceeds the flow stress.

This failure condition is consistent with the failure condition outlined in *2004 ASME Boiler and Pressure Vessel Code* (Ref. D4.1.6, Appendix F, paragraph F-1331). The ASME code specifies that for ferritic steels, the primary membrane stress intensity shall not exceed  $0.7 \sigma_u$ . For austenitic steels, the primary membrane stress intensity shall not exceed the greater of  $0.7 \sigma_u$  or  $\sigma_y + (\sigma_u + \sigma_y)/3$ . As is noted below, for type 316 stainless steels,  $0.7 \sigma_u$  is always the controlling condition.

#### **D2.1.4.5.3 Inputs to the Canister Failure Models**

The canister failure models require the following inputs:

- the value for the Larson-Miller parameter (a function of temperature and stress)
- the value for the flow stress (a function of temperature)
- the time-dependent internal pressure and temperature experienced by the canister.

The following discussion outlines how these values were determined.

##### **D2.1.4.5.3.1 Larson-Miller Parameter**

The value for the Larson-Miller parameter can be determined based on creep data provided by material suppliers. In the absence of data specific to the steels used for the spent fuel and high level waste canisters to arrive at Yucca Mountain, a literature review was performed to obtain representative creep rupture data for steels of the type expected to be used.

The primary focus of this data search was type 316 stainless steel since that is the steel most likely to be used for the spent fuel or high level waste canisters. Data were collected from the following sources:

- “Properties and Selection of Metals.” Volume 1 of *Metals Handbook* (Ref. D4.1.3).
- Reliability and Longevity of Furnace Components as Influenced by Alloy of Construction. H-3124 (Ref. D4.1.35).
- *Creep of the Austenitic Steel AISI 316L(N) -Experiments and Models* (Ref. D4.1.58).
- Assessment of Creep Behaviour of Austenitic Stainless Steel Welds (Ref. D4.1.59).
- *Materials Selection for High Temperature Applications* (Ref. D4.1.60).

The creep data provides the time required for creep rupture given a specified constant temperature and applied tensile stress.

Using this data, the value for the Larson-Miller parameter (Ref. D4.1.44) can be determined from the following equation:

$$P_{LM} = T[C + \log(t_f)] \quad (\text{Eq. D-20})$$

where

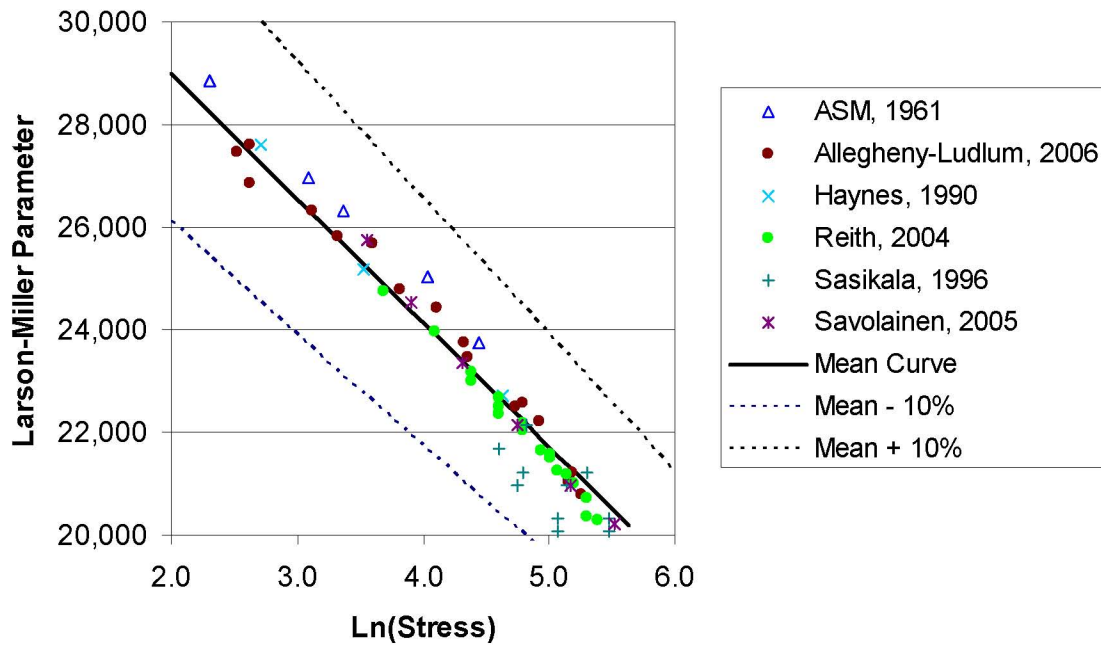
- T = temperature (K)
- $t_f$  = failure time (hours) determined in testing
- C = a constant that is approximately 20 for most stainless steels

Using this equation and the data collected in the literature review, values for the Larson-Miller parameter were calculated. The calculated values for the Larson-Miller parameter are shown in Figure D2.1-2. As shown in the figure, the Larson-Miller parameter decreases as the applied stress increases.

In order to apply the results shown in the table outside the range of stresses considered in the table, it is necessary to determine a correlation that best fits the data. The best-fit curve, which is also plotted in Figure D2.1-2, is given by the following equation:

$$P_{LM} = 33,845 - 2,423 \ln(\sigma) \quad (\text{Eq. D-21})$$

As shown in Figure D2.1-2, the value for the Larson-Miller parameter varies from one metal specimen to the next and from one vendor to the next. This variability is illustrated, in part, by the variability in the data shown in the figure. In addition, the research by Sasikala, et al. (Ref. D4.1.59) showed that stainless steel weld material is generally less creep-resistant than the base metal (this is illustrated by the five outlier points on the figure which were determined for the weld material rather than the base metal). The variability in the Larson-Miller parameter must be reflected in the uncertainty analysis for the canister failure temperature.



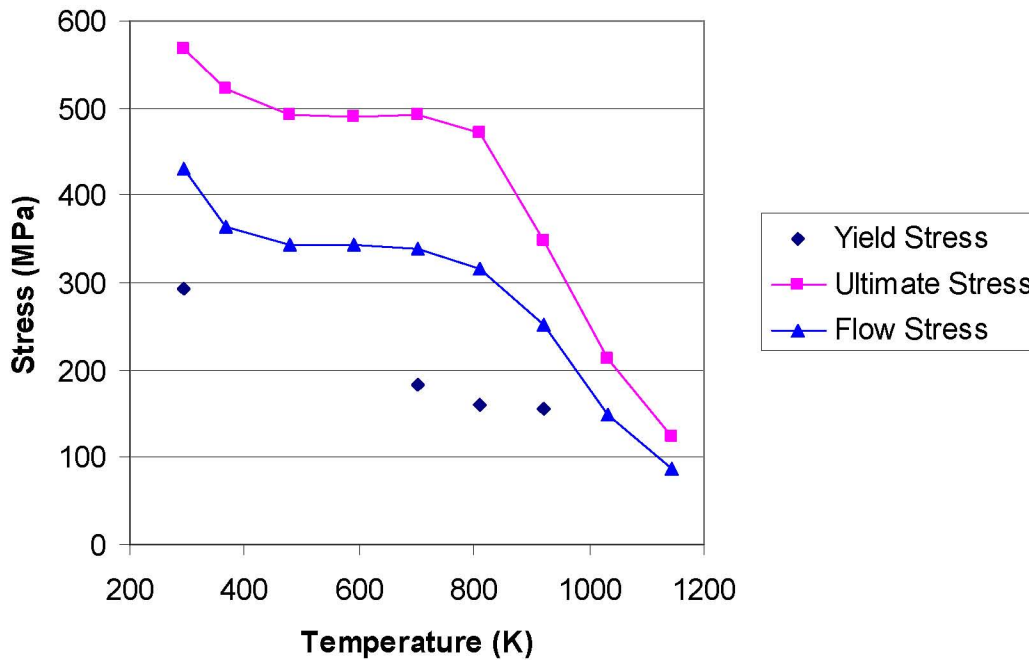
Source: Excel Spreadsheet *Creep rupture - Fast Heatup 1 inch.xls* found in Attachment H.

Figure D2.1-2. Plot of Larson-Miller Parameter for Type 316 Stainless Steel

The uncertainty in the Larson-Miller parameter is treated within the canister failure analysis by multiplying the calculated value for  $P_{LM}$  by a factor  $(1+a)$ , where the value for  $a$  is normally distributed with a mean of 0.0 and a standard deviation of 0.038. Using this formulation, 99% of all canister steels would have  $P_{LM}$  values within approximately 10% of the calculated value. This uncertainty is believed to reflect the variability between different canister steels as well as the variability between the base metal and the weld material.

#### D2.1.4.5.3.2 Flow Stress

In the canister failure analysis, the flow stress is the average of the yield and ultimate strength. Both the yield and ultimate strength are temperature-dependent and decrease rapidly above a temperature of about 800°K. Figure D2.1-3 presents typical curves for the yield and ultimate strength of Type 316 stainless steel as a function of temperature (Ref. D4.1.1). The figure also presents the calculated flow stress curve. For temperatures with no yield strength data, the flow stress equals 0.7 times the ultimate strength.



NOTE: MPa = megapascals.

Source: Original

Figure D2.1-3. Yield, Ultimate, and Flow Stress for Type 316 Stainless Steel

For the temperature range of interest, the flow stress curve can be fit to two straight lines: one line for temperatures between 350°K and 800°K and another for temperatures above 800°K. The equations for these two lines are provided below:

$$\bar{\sigma} = 395.9 - 0.0925T \quad \text{for } T < 800 \text{ K} \quad (R^2 = 0.889) \quad (\text{Eq. D-22a})$$

$$\bar{\sigma} = 899.1 - 0.7139T \quad \text{for } T \geq 800 \text{ K} \quad (R^2 = 0.989) \quad (\text{Eq. D-22b})$$

Note that the fit is particularly good for the upper temperature range, which is of greatest interest in the current analysis.

As with the value for the Larson-Miller parameter, the value for the flow stress is uncertain. The uncertainty in the flow stress was treated in the same manner at the uncertainty in the Larson-Miller parameter. Specifically, the mean value described by the equations provided above was multiplied by a factor  $(1 + a)$  where the value for  $a$  is normally distributed with a standard deviation of 0.038. This distribution results in 99% of all canister steels having a flow stress within 10% of the mean value given by the equations. This adequately reflects the variability in the material properties of Type 316 steels, the variability between the properties of the base metal and weld material, and the potential for other types of steel with lower or higher tensile strength to be used in manufacture of the canisters.



### D2.1.4.5.3.3 Pressure Difference and Temperature Histories

Creep failure and limit load failure depend on the time-dependent internal pressure and canister temperature. The canister temperature depends on the fire severity and also on whether the canister is bare or enclosed in a waste package or cask. The canister temperature is calculated using a separate analysis, as discussed above. Rather than attempting to couple the canister failure and canister heatup analyses into a single calculation, a separate canister failure analysis was completed. This analysis required the following inputs: the rate of temperature increase of the canister wall and the relationship between the internal canister pressure and the temperature of the canister wall.

Based on a series of runs with the canister heat transfer models discussed above, it was determined that the rate of temperature increase for a bare canister was likely to range from a low of around 25°K/min to a high of around 175°K/min. This range was input as a normal distribution with a mean of 100°K/min and a standard deviation of 25°K/min. Similar runs for the non-bare canister cases indicated a much slower heatup rate. For these cases, the canister heatup rate was input as a normal distribution with a mean of 10°K/min and a standard deviation of 2.5°K/min.

Analyses with a special version of the bare canister heat transfer model were also used to characterize the rate at which the temperature of the gas inside the canister would increase as a result of heating of the canister wall. This version of the model included convective heat transfer from the canister wall to the gas, from the canister wall to fuel assemblies inside the canister, and from the fuel assemblies to the gas inside the canister. These analyses showed a substantial lag in temperature between the canister wall and the gas.

The following equation was used to calculate the internal pressure of the canister based on the canister temperature:

$$P = P_0 \left[ 1 + C \left( \frac{T_{\text{can}} - T_{\text{can},0}}{T_{\text{can},0}} \right) \right] \quad (\text{Eq. D-23})$$

where

- $P_0$  = initial pressure inside the canister (including potential fuel failures)
- $T_{\text{can},0}$  = initial temperature of the canister wall
- $T_{\text{can}}$  = canister temperature at the current timestep
- $C$  = a constant that depends on the canister heating rate.

Note that if the value for  $C$  is set equal to 1.0 in this equation, the proportional change in pressure is equal to the proportional change in temperature. This would be true if the gas and canister temperatures increased at the same rate. Because the gas temperature lags behind the canister temperature, the value for  $C$  is always less than 1. Rather than attempting to model the variability in the value for  $C$ , the analysis used a bounding value of 0.5 for all analyses. This value bounded the range of values calculated in the separate heat transfer analysis.

The initial pressure,  $P_0$ , in Equation D-23 varies over a wide range depending on the amount of overpressure supplied when the canister is sealed, the extent of fuel rod failures, and the type of fuel stored in the canister. Since the canister failure analysis considers only the increase in gas temperature due to the fire, the initial pressure must reflect potential fuel failures during the fire.

The SARs prepared by transportation cask vendors were consulted for information on internal pressure under normal and accident conditions (see for example, Section 3.6.6 of *GA-9 Legal Weight Truck From-Reactor Spent Fuel Shipping Cask, Final Design Report* (Ref. D4.1.34)). The SARs provide information on the initial overpressure in the canister and the pressure increase associated with fuel rod failures. Based on this information, an uncertainty distribution for the initial pressure in the canister was developed. The uncertainty is characterized by a Weibull distribution with a minimum of 5 psig, a scale factor of 45 psig, and a shape factor of 2.4. This distribution is applied to all canisters considered in the preclosure safety analysis (PCSA).

### **D2.1.5 Probabilistic Fragility Analysis**

The mechanistic models described above produce results that are deterministic. That is, for a given set of input values, they yield a single answer. However, as has been shown, the inputs to the models are uncertain. Uncertainty in the input parameters could lead to a substantial variation in the predicted canister thermal response and failure temperature. Therefore, it is necessary to treat the analysis in a probabilistic manner. It is in the fragility analysis that all the parameters that affect the failure of the spent fuel or high level waste canister are addressed in a probabilistic fashion.

The fragility analysis consists of two separate probabilistic analyses: (1) an analysis to determine the probability distribution for the canister failure temperature, and (2) an analysis to determine the maximum temperature reached by the canister due to the fire. These two analyses are combined to determine the probability that the canister fails as a result of the fire.

Calculations were performed for canisters inside a waste package, a cask, or a shielded bell. As discussed earlier, two canister wall thicknesses were evaluated: 0.5 inches (hereafter referred to as *thin-walled* canisters) and 1.0 inch (hereafter referred to as *thick-walled* canisters). The following sections describe how these analyses are performed and present the calculated failure probabilities for the various canister configurations of interest.

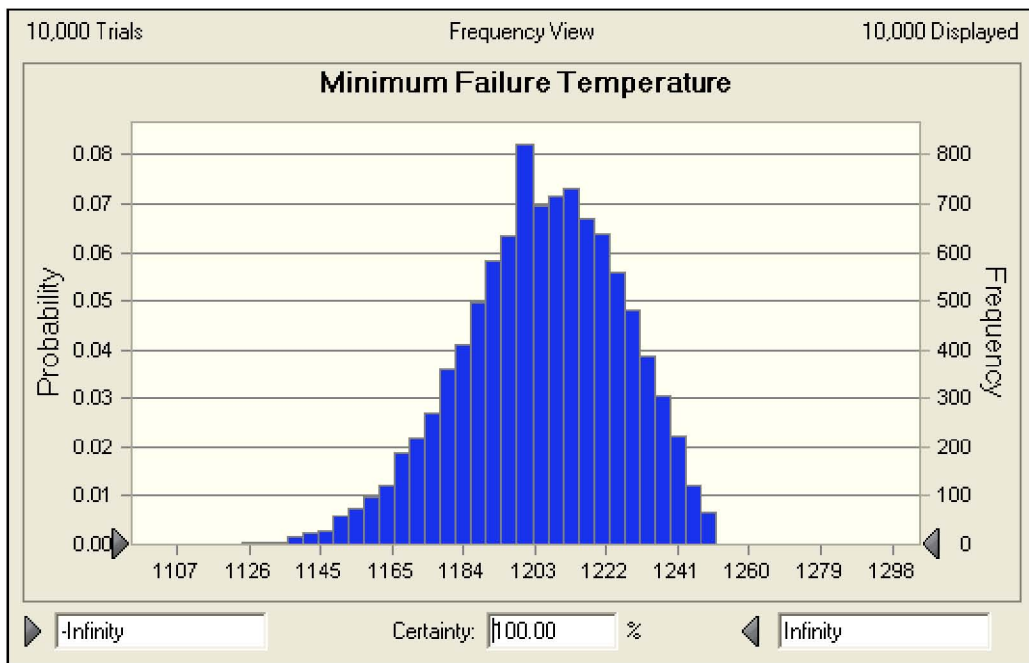
#### **D2.1.5.1 Probabilistic Analysis of Canister Failure Temperature**

The first step in the fragility analysis was to determine the probability distribution for the canister failure temperature. The probability distribution was determined using a Monte Carlo analysis in which the failure models outlined in Section D2.1.4 were repeatedly solved with parameter values sampled from the uncertainty distributions discussed in that section. The failure temperature for each sample was the lower of the two temperatures calculated based on creep rupture or limit load failure.

A Microsoft Excel add-in product, Crystal Ball, was used to perform Monte Carlo simulation. Latin hypercube sampling was used to ensure that parameter samples represented the assigned distributions adequately.

Figure D2.1-4 shows the calculated canister failure temperature distribution for canisters inside a waste package, transportation cask, or shielded bell. This calculation used the lower heating rate discussed in Section D2.1.4.5.3.3. The probability distribution shown in Figure D2.1-4 is well-characterized by a normal distribution with a mean of 1,203°K and a standard deviation of 22.85°K. This normal distribution provides a particularly good fit to the lower failure temperature portion of the distribution which is the most important for the canister failure analysis.

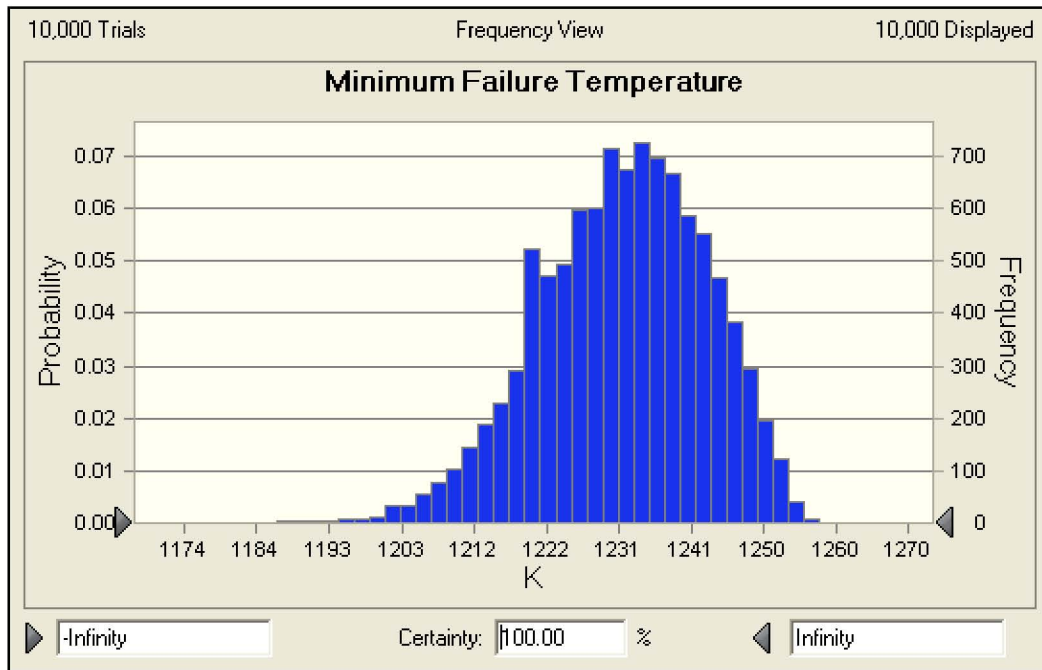
A similar analysis was performed for bare canisters. This calculation used the higher heating rate discussed in Section D2.1.4.5.3.3. The resulting probability distribution was nearly identical to the one shown in Figure D2.1-4. The reason for this is that canister failure was nearly always due to limit load failure rather than creep failure, so the difference in heating rates for the two configurations was not important.



Source: Original

Figure D2.1-4. Probability Distribution for the Failure Temperature of Thin-Walled Canisters

A similar analysis was performed for thick-walled canisters. As with the thin-walled canisters, the probability distribution for the canister failure temperature was found to be nearly independent of the canister heating rate. Figure D2.1-5 shows the calculated probability distribution. This probability distribution is well-characterized by a normal distribution with a mean of 1,232°K and a standard deviation of 12.3°K. This normal distribution provides a particularly good fit to the lower failure temperature portion of the distribution which is the most important for the canister failure analysis.



Source: Original

Figure D2.1-5. Probability Distribution for the Failure Temperature of Thick-Walled Canisters

### D2.1.5.2 Probabilistic Analysis to Determine the Maximum Canister Temperature and Canister Failure Probability

The next step in the fragility analysis was to determine the maximum temperature of the canister as a result of the fire. In this analysis, Monte Carlo techniques were used to repeatedly sample from the uncertainty distributions discussed in Section D2.1.4 while applying the canister heating models to determine the maximum temperature of the canister due to the fire. As with the failure temperature analysis, Crystal Ball was used to perform the Monte Carlo simulation.

For each Monte Carlo sample, the calculated maximum canister temperature was then compared to a canister failure temperature sampled from the probability distribution discussed in Section D2.1.5.1. The canister is considered failed if the maximum temperature of the canister exceeded the sampled failure temperature for that Monte Carlo sample. The failure probability was determined as the fraction of the samples for which failure was calculated.

This process was repeated for a sufficient number of samples to provide a good statistical basis for the failure probability. The rule of thumb used in determining the required number of samples was that at least 10 failures had to be calculated. Thus, if the failure probability was on the order of  $10^{-4}$ , 100 thousand ( $10^5$ ) samples were needed. The maximum number of samples for any run was set at 1 million. If no failures were calculated for one million samples, the failure probability was recorded as being less than  $10^{-6}$ .

Since each Monte Carlo sample has two possible outcomes (failure or no failure), each sample represents a Bernoulli trial. Since the probability of failure or no failure is the same for each trial, the outcome from the sampling process can be represented by a binomial distribution. The

binomial distribution is closely approximated by a normal distribution if the number of failures is greater than about five. The mean of the normal distribution is simply the number of failures divided by the total number of samples. The standard deviation of the normal distribution is given by the following equation:

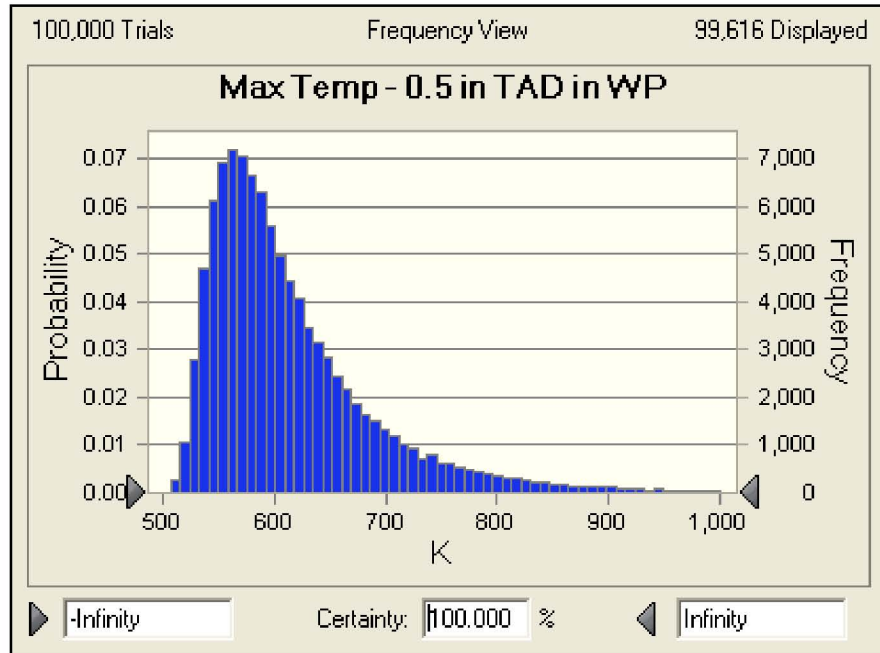
$$\sigma = \sqrt{\frac{\frac{n_{\text{fail}}}{N} \left( \frac{N - n_{\text{fail}}}{N} \right)}{N}} \quad (\text{Eq. D-24})$$

where  $n_{\text{fail}}$  is the number of failures,  $N$  is the total number of Monte Carlo samples, and  $p_{\text{fail}}$  is the calculated mean failure probability ( $n_{\text{fail}}/N$ ).

Figure D2.1-6 shows the calculated distribution for the maximum temperature reached by a thin-walled canister inside a waste package. The figure shows that the vast majority of the Monte Carlo samples had maximum temperatures well below 950°K. Only under extreme combinations of fire temperature and duration did the calculated maximum temperature approach the failure temperatures shown in Figure D2.1-4. Consequently there were only 32 calculated canister failures out of a total of 100,000 Monte Carlo samples. The resulting mean value for the canister failure probability is therefore 32/100,000 or  $3.2 \times 10^{-4}$ . The standard deviation calculated using Equation D-24 is  $5.7 \times 10^{-5}$ . The mean and standard deviation of the failure probability are shown in Table D2.1-8.

A similar analysis was performed for a thick-walled canister inside a waste package. Because of the thicker wall, the failure temperature of the canister is higher than for the thin-walled canister. In addition, the thick-walled canister heats up more slowly than the thin-walled canister because of its greater mass. These two factors combine to substantially lower the probability of failure for these canisters. In the Monte Carlo analysis, 20 failures were calculated for 200,000 samples, which results in a mean failure probability of  $1 \times 10^{-4}$  and a standard deviation of  $2.2 \times 10^{-5}$ .

Similar calculations have been performed for a canister inside a transportation cask and a canister inside the shielded bell of the CTM. The resulting mean and standard deviation for the canister failure probability are provided in Table D2.1-8.



Source: Original

Figure D2.1-6. Probability Distribution for Maximum Canister Temperature – Thin-Walled Canister in a Waste Package

Table D2.1-8. Summary of Canister Failure Probabilities in Fire

Configuration <sup>b</sup>	Monte Carlo Results		Failure Probability	
	Total Failures	Total Trials	Mean	Standard Deviation
Thin-Walled Canister in a Waste Package <sup>a</sup>	32	100,000	$3.2 \times 10^{-4}$	$5.7 \times 10^{-5}$
Thick-Walled Canister in a Waste Package <sup>a</sup>	20	200,000	$1.0 \times 10^{-4}$	$2.2 \times 10^{-5}$
Thin-Walled Canister in a Transport Cask	2	1,000,000	$2.0 \times 10^{-6}$	$1.4 \times 10^{-6}$
Thick-Walled Canister in a Transport Cask	1	1,000,000	$1.0 \times 10^{-6}$	$1.0 \times 10^{-6}$
Thin-Walled Canister in a Shielded Bell	27	200,000	$1.4 \times 10^{-4}$	$2.6 \times 10^{-5}$
Thick-Walled Canister in a Shielded Bell	27	300,000	$9.0 \times 10^{-5}$	$1.7 \times 10^{-5}$

NOTE: <sup>a</sup>For the 5-DHLW/DOE SNF waste package, this probability applies only to the DOE HLW canisters located on the periphery of the waste package. The DOE SNF canister in center of the waste package would not be heated appreciably by the fire.

<sup>b</sup>Configurations not addressed in this table include, any canister in a waste package that is inside the transfer trolley or any canister inside an aging overpack. In these configurations, the canister is protected from the fire by the massive steel transfer trolley or by the massive concrete overpack. Calculations have shown that the temperatures experienced by the canister in these configurations are well below the canister failure temperature. Although failures for these configurations could be screened on this basis, a conservative screening probability of  $1 \times 10^{-6}$  is used in the PCSA.

Source: Original

Note that Table D2.1-8 contains no failure probability for a bare canister configuration. The reason for this is that the canister is outside of a waste package or cask for only a short time. During that time, the canister is usually inside the shielded bell of the CTM. The preceding

analysis addressed a fire outside the shielded bell. When in that configuration, the canister is shielded from the direct effects of the fire. A fire inside the shielded bell, which could directly heat the canister, was not considered to be physically realizable for two reasons. First, the hydraulic fluid used in the CTM equipment is non-flammable (Ref. D4.1.48, p 30) and no other combustible material could be present inside the bell to cause a fire. Second, the annular gap between the canister and the bell only 3 inches wide, but is approximately 27 feet long. Given this configuration, it is unlikely that there would be sufficient inflow of air to sustain a large fire. There may be sufficient inflow to sustain a localized fire, but such a fire would not be adequate to heat the canister to failure.

The canister is also outside of a cask, waste package, or shielded bell as it is being moved from a cask into the shielded bell or from the shielded bell into a waste package. The time during which the canister would be in this configuration is extremely short (a matter of minutes) so a fire that occurs during this time is extremely unlikely. In addition, because the gap between the top of the waste package or cask and ceiling of the transfer cell is generally much shorter than the height of the canister, only a small portion of the canister surface would be exposed to the fire. Furthermore, this exposure would only be for the short time that the canister was in motion.

For these reasons, failure of a bare canister was not considered a physically realizable threat to breach of a canister and was not treated further.

The notes to Table D2.1-8 mention two other configurations for which fire-induced canister failure is not credible: a fire outside a waste package inside a waste package transfer trolley (WPTT) and a fire outside an aging overpack. These two special cases are discussed below.

The failure probability for a waste package in the WPTT was determined using the probabilistic methodology discussed above. For this calculation, the waste package calculation discussed earlier was modified by simply adding a thermal barrier outside the waste package to represent the WPTT. The fire heats the WPTT which then transfers heat by radiation to the outer barrier of the waste package. The WPTT was modeled as having an equivalent external diameter of 3.05 meters, a thickness of 20.3 cm (steel thickness only<sup>1</sup>), and a mass of 89,000 kg. The transfer trolley was considered to be made of a stainless steel with an average specific heat of 476 J/kg K. The probabilistic analysis was run for 1 million Monte Carlo samples and no failures were calculated. Though the maximum temperature calculated in this analysis was well below the failure temperatures shown in Figures D2.1-4 and D2.1-5, a conservative failure probability of  $1 \times 10^{-6}$  is used in the PCSA.

The probabilistic methodology discussed above could not be used for analysis of canister failure for a fire outside an aging overpack. The reason for this is that the concrete that comprises the majority of the aging overpack has a very low thermal conductivity. Therefore, the underlying premise of a relatively uniform temperature in each cylindrical region would be incorrect. Instead, a simple heat conduction calculation was performed to determine how far into the concrete heat could be conducted during a fire. The thermal penetration depth (from Equation D-11) was estimated based on a bounding 2-hour fire and concrete with the following

---

<sup>1</sup> There is also a 7.5-inch layer of borated polyethylene. Because this layer is likely to melt early in the fire transient, it is ignored in the analysis.

average properties: thermal conductivity = 1.2 W/m K; density = 2,200 kg/m<sup>3</sup>; and specific heat = 1,000 J/kg K. The thermal penetration depth calculated for these conditions was 6.3 cm. Since the aging overpack is expected to be at least 24 inches (61 cm) thick, the canister inside the aging overpack will not be heated significantly by the fire. A conservative failure probability of  $1 \times 10^{-6}$  is used in the PCSA.

Note that, in this calculation, the fire was modeled as being only on the outside of the aging overpack. Though the overpack has ventilation openings for natural circulation, this flow path is expected to provide sufficient resistance to airflow that (1) combustion could not be sustained inside the overpack even if fuel entered through the openings, and (2) hot gases would likely flow over the outer surface of the overpack rather than enter the ventilation openings and flow up through the annulus inside the overpack. In fact, because oxygen would be consumed by the fire near the bottom of the overpack, air may actually flow downward through the ventilation openings to supply air to the fire.

### **D2.1.5.3 Analysis To Determine Failure Probabilities For Bare Fuel in Casks Exposed To Fire**

Another fire-induced failure mode is of interest in the PCSA; namely, failure of a transport cask containing bare spent fuel assemblies. The analysis uses GA-4/GA-9 transportation casks to represent casks of this type. Should a transportation cask containing uncanistered spent nuclear fuel fail in a fire, it is of interest for determining the source term to know if the fuel cladding is heated above its failure temperature (approximately 700°C to 800°C).

A modified version of the model for failure of a canister in a transportation cask was used to determine the probability that fuel will exceed this failure temperature. In the modified spreadsheet, the canister was replaced by the mass of fuel that would be heated during the fire. As in the bare canister analysis discussed in Section D2.1.4.1, this mass was estimated based on the calculated thermal penetration depth. Based on the information provided in the GA-9 SAR report (Ref. D4.1.34, p. 3.6-3), the following average spent fuel properties were determined: thermal conductivity = 1.5 W/m K, density  $\times$  specific heat =  $9.9 \times 10^5$  J/m<sup>3</sup> K. For a 1-hour fire, the calculated thermal penetration depth is 7.4 cm and the effective fuel mass is 1,910 kg. Since the severe fires of greatest concern have durations of 1 hour or longer, this fuel mass represents a reasonable, but probably conservative, estimate.

Other modifications to the model included changes to model the geometry and materials used in the GA-4/GA-9 casks. The inputs to the model are presented in Table D2.1-9. As in the previous analyses, the model does not rely on neutron shield because it is liable to melt early in the transient.

The model was run for three different fuel failure temperatures: 700°C, 750°C, and 800°C. This range of failure temperatures represents the lower end of the values reported in the literature (Ref. D4.1.65, pp. 7-20 to 7-21). As shown in Table D2.1-10, the calculated fuel failure probabilities were less than 0.001.



Table D2.1-9. Model Inputs – Bare Fuel Cask

Model Parameter	Value	Basis/Rationale
<b>Fuel Properties</b>		
Heated Mass (kg)	1,910	Calculated based on thermal penetration depth (see text)
Specific Heat (J/kg K)	438	Average for fuel region taken from <i>Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Table 15)
Effective Surface Area (m <sup>2</sup> )	10.0	Projected area for radiation heat transfer. Calculated based on equivalent outer diameter of fuel region (0.66 m)
Emissivity	0.8	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNL Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Table 17)
Initial Temperature (K)	400	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)
<b>Transportation Cask Outer Shell</b>		
Outer Diameter (m)	1.12	Equivalent diameter estimated based on GA-9 SAR (Ref. D4.1.34, Figure 1.2-9)
Wall Thickness (m)	0.0032	Minimum outer shell thickness listed in cask SAR (Ref. D4.1.34)
Length (m)	4.25	Length adjacent to the fuel region
Density (kg/m <sup>3</sup> )	7850	Density of 516 carbon steel (Ref. D4.1.6, Section II, Part A, SA-20, 14.1)
Specific Heat (J/kg K)	604	Approximate value for 516 carbon steel at 400°C (Ref. D4.1.25, Table 10)
Emissivity	0.8	Average value for carbon steel in Avallone and Baumeister, (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	344	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)
<b>Transportation Cask Gamma Shield<sup>a</sup></b>		
Outer Diameter (m)	0.902	Equivalent diameter estimated based on GA-9 SAR (Ref. D4.1.34, Figure 1.2-9)
Wall Thickness (m)	0.107	Combined thickness of stainless steel and depleted uranium shields (steel: 0.0445 m; DU: 0.0622 m)(Ref. D4.1.34)
Length (m)	4.25	Length adjacent to the fuel region
Mass × Specific Heat (J/K)	3.45 × 10 <sup>6</sup>	Based on calculated masses of steel and DU and specific heats listed in GA-9 SAR (Ref. D4.1.34, Tables 2.2-1 and 3.2-2)
Emissivity	0.8	Average value for carbon steel in Avallone and Baumeister, (Ref. D4.1.8, Table 4.3.2)
Initial Temperature (K)	360	Estimated from fig 3.4-4 in GA-9 SAR (Ref. D4.1.34)
<b>Post-Fire Conditions</b>		
Ambient Temperature (K)	361	Post-fire temperature of 190°F from <i>Discipline Design Guide and Standards for Surface Facilities HVAC Systems</i> Ref. D4.1.16, Section 3.2). This value is 100 °F higher than the maximum interior facility temperature

Table D2.1-9. Model Inputs – Bare Fuel Cask (Continued)

Model Parameter	Value	Basis/Rationale
Heat Transfer Coefficient (W/m <sup>2</sup> K)	2.0	Natural convection based on anticipated post-fire surface temperature and standard convective heat transfer correlations (Results not sensitive to this value)

NOTE: <sup>a</sup> Composite properties representing both the stainless steel cask wall and depleted uranium gamma shield.

DU = depleted uranium

Source: Original

Table D2.1-10. Summary of Fuel Failure Probabilities

Fuel Failure Temperature	Monte Carlo Results		Failure Probability	
	Total Failures	Total Trials	Mean	Standard Deviation
700°C	54	100,000	$5.4 \times 10^{-4}$	$7.4 \times 10^{-5}$
750°C	27	100,000	$2.7 \times 10^{-4}$	$5.2 \times 10^{-5}$
800°C	13	100,000	$1.3 \times 10^{-4}$	$3.6 \times 10^{-6}$

Source: Original

#### D2.1.5.4 Analysis To Determine Failure Probabilities For Casks Exposed To Fire

NUREG/CR-6672 (Ref. D4.1.65, Section 6) provides an analysis of seal failure in bare fuel transportation casks. The analysis uses a simple 1-D axisymmetric heat transfer model that is similar to the simple model used in the fire fragility analysis presented in Section D2. The simple model is used to determine the length of time the cask could be exposed to an 800°C or 1,000°C fire before seal failure would be predicted.

The report notes that the elastomer seals used in many transportation casks degrade completely at 500°C, but that the degradation rate increases significantly at 350°C (Ref. D4.1.65, p. 2-9). Other seal degradation information provided by cask vendors indicates that the maximum design temperature for the metallic o-ring seals in the TN-68 casks is 536°F (280°C) (Ref. D4.1.66, p. 3-2). This is the maximum safe temperature for continuous operation. The actual failure temperature for these seals would be much higher. Based on this information, seal failure is anticipated at temperatures of around 350°C to 450°C.

NUREG/CR-6672 indicates that the seals in a steel/depleted uranium (DU) truck cask would reach 350°C if exposed to a 1,000°C fire for 0.59 hours (Ref. D4.1.65, Table 6.5). In a steel/lead/steel (SLS) truck cask, this temperature would be reached in 1.04 hours. The times for rail casks were longer at 1.06 hours for an SLS rail cask and 1.37 hours for a monolithic steel rail cask.

The probability distributions for fire temperature and fire duration discussed in section D2.1.1 can be used to determine the probability that the fire conditions listed in the preceding paragraph would be exceeded. This is accomplished by first determining the probability distribution (using

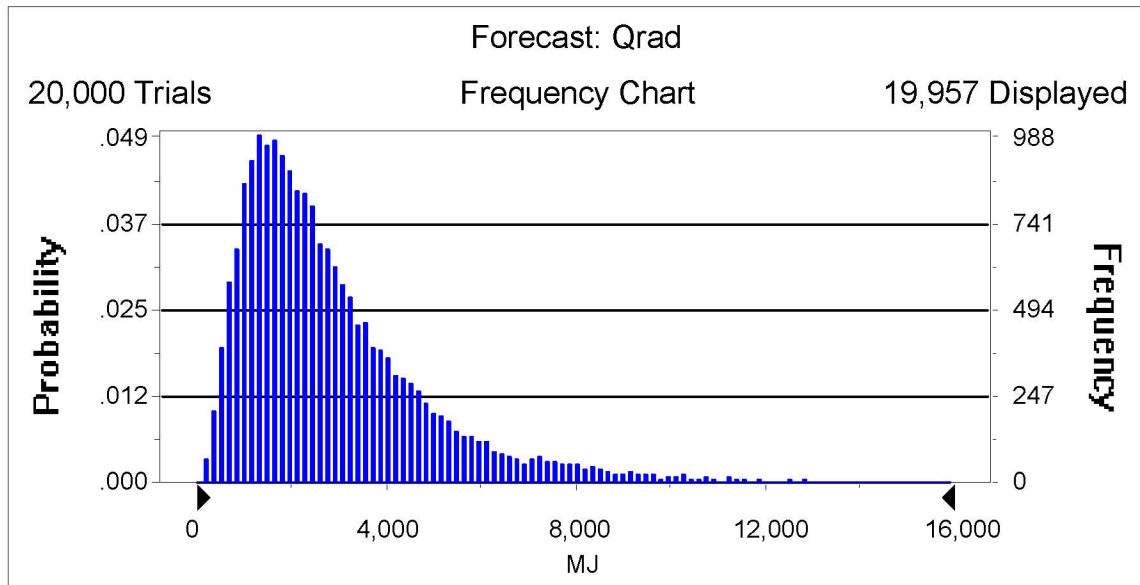
Crystal Ball) for the maximum thermal radiation energy from the fire using the following equation:

$$Q_{\text{rad}} = \sigma A T_{\text{fire}}^4 t_{\text{fire}} \quad (\text{Eq. D-25})$$

where

- $\sigma$  = the Stefan-Boltzmann constant ( $5.668 \times 10^{-8} \text{ W/m}^2 \text{ K}^4$ )
- $A$  = cask surface area exposed to the fire
- $T_{\text{fire}}$  = fire temperature (sampled from the probability distribution)
- $t_{\text{fire}}$  = fire duration (sampled from the probability distribution)

The probability distribution for  $Q_{\text{rad}}$  is shown in the figure below:



Source: Original

Figure D2.1-7. Distribution of Radiation Energy from Fire

Next, the value for  $Q_{\text{rad}}$  corresponding to the NUREG/CR-6672 fire temperature and duration for seal failure is calculated. The probability distribution for  $Q_{\text{rad}}$  can then be used to determine the probability that the fire will be severe enough to cause seal failure (i.e., will exceed the value for  $Q_{\text{rad}}$  calculated based on the NUREG/CR-6672 conditions).

The values for  $Q_{\text{rad}}$  corresponding to a 1,000°C fire and the fire durations reported in NUREG/CR-6672 are listed below along with the probability of exceedance determined from the probability distribution. The exceedance probabilities can be used as an estimate of the seal failure probability for seals that fail at the temperature,  $T_{\text{fail}}$ , listed in Table D2.1-11. For example, for a SLS truck cask that has seals that fail at 350°C, the probability that the seals fail due to a fire is  $6.9 \times 10^{-3}$ .

By multiplying the highest seal failure probability in Table D2.1-11 (0.05) by the highest probability of fire-induced cladding failure in Table D2.1-11 ( $5.4 \times 10^{-4}$ ), it is shown that the joint conditional probability of a fire that causes additional cladding failure in a truck cask, given a fire, is less than  $3 \times 10^{-5}$ . Because the fire initiating event frequency over the preclosure period of such truck cask fires is less than 1 (see Attachment F for the facilities that contain these, i.e., WHF and Intra-Site operations), such fires are beyond Category 2 and not analyzed further.

Table D2.1-11. Probabilities that Radiation Input Exceeds Failure Energy for Cask

Cask Type	T <sub>fail</sub> (°C)	Temperature (°C)	Duration (hrs)	Q <sub>rad</sub> (MJ)	P <sub>exceed</sub>
Steel/DU Truck Cask	350	1,000	0.59	7,208	$5.0 \times 10^{-2}$
Steel/Lead/Steel Truck Cask	350	1,000	1.04	12,405	$6.9 \times 10^{-3}$
Steel/Lead/Steel Rail Cask	350	1,000	1.06	12,950	$5.6 \times 10^{-3}$
Monolithic Steel Rail Cask	350	1,000	1.37	16,737	$1.7 \times 10^{-3}$
Steel/DU Truck Cask	500	1,000	≈ 1.0 <sup>a</sup>	≈ 12,200	$7.1 \times 10^{-3}$
Steel/Lead/Steel Truck Cask	500	1,000	≈ 1.3 <sup>a</sup>	≈ 15,900	$2.2 \times 10^{-3}$

NOTE: <sup>a</sup> Estimated from Figure 6.6 in NUREG/CR-6672 (Ref. D4.1.65).

Source: Original

## D2.2 SHIELDING DEGRADATION IN A FIRE

The NUREG/CR-6672 (Ref. D4.1.65) transportation study performed analyses on the internal temperatures of cask for long duration fires of 1,000°C. The transportation study included scenarios for fire-only and fire-plus-impact in the calculation of the probability of loss of shielding (LOS).

### D2.2.1 Analysis of Loss of Shielding for Transportation Casks

All transportation casks contain separate gamma and neutron shields. The neutron shields are generally composed of a low melting point polymer material that would melt and offgas very quickly when exposed to a fire. For that reason, it is given that the neutron shield is always lost in fire scenarios. The composition of the gamma shield varies between cask designs, with some designs having layers of steel and depleted uranium, others having layers of steel and lead, or and others with layers of steel. Only casks containing lead could lose their gamma shielding in a fire.

As previously discussed, the thermal analyses for the transportation casks (Ref. D4.1.65, Table 6.5) shows that the internal regions of the cask reach the 350°C range in the range of 0.59 to 1.37 hours for the long duration 1,000°C fire. The least time represents the steel- depleted uranium casks and the longest the monolithic steel. The time to reach 350°C for steel-lead-steel (SLS) casks is about one hour. The time to reach the lead melting temperature (327.5°C) should be somewhat less than one hour but is not specified. However, NUREG/CR-6672 (Ref. D4.1.65) indicates that lead melting in itself does not result in significant LOS but the melting must be accompanied by outer shell puncture that permits the lead to flow out of the shield configuration.

NUREG/CR-6672 states that there are four characteristic fires of interest in the transportation risk analysis: 10 minutes as the duration of a typical automobile fire; 30 minutes for a regulatory fires; 60 minutes for an experimental pool fire for fuel from one tanker truck; and 400 minutes for an experimental pool fire from one rail tank car. These typical durations suggest that a real fire is unlikely to last long enough to result in a LOS condition for transportation scenarios.

### **D2.2.2 Probability of LOS in Fire Scenarios**

Melting of the lead shielding and loss of containment of the molten lead results in loss of shielding for SLS casks. Two mechanisms for escape of the molten lead are considered:

- Puncture of the outer shell
- Rupture lead containment due to internal pressure

Puncture of the 2-inch thick (or more) outer shell, in addition to exposure to fire, would allow molten lead to escape, resulting in LOS. The shell puncture would be an independent failure with a probability of  $10^{-8}$  for the low speeds at which the cask would be moving (Table 6.3-4). With the additional failure of exposure to fire, the LOS probability would be even less.

Containment of the molten lead could be lost due to thermal expansion of the lead coincident with the thermal weakening of the steel. Molten lead is cast into the cavity bounded by the inner and outer shells and the bottom plate ((Ref. D4.1.50, p. 1.1-4); (Ref. D4.1.49, p. 1.2-2); (Ref. D4.1.9, p. 1.2-5); and (Ref. D4.1.47, p. 1-5)). The lead contracts as it cools and solidifies. When the cask is exposed to a fire and the lead melts, it expands to reoccupy the volume when originally cast. When heated beyond the melting point, the liquid lead could continue to expand, exerting hoop stresses upon the inner and outer shells. The shells are thick and strong, e.g. the inner and outer shell thicknesses for the MP197 are 1.25 and 2.5 inches, respectively (Ref. D4.1.47, Drawing 1093-71-4, rev. 1), and the bottom plate thickness is 6.5 inches (Ref. D4.1.47, Drawing 1093-71-2, rev. 1). Consequently, failure of the steel is considered very unlikely.

As part of the PCSA, an attempt was made to analyze hydraulic failure of the molten lead containment due to a fire. Unfortunately, the thermal and physical properties of lead necessary for this analysis could not be found. Thus, hydraulic failure cannot be conclusively disproved. For that reason, a probability of 1.0 is used for LOS by transportation casks due to fire.

### **D2.2.3 Bases for Screening of Loss of Shielding Pivotal Events for Aging Overpacks in Fire Scenarios**

This section summarizes the rationale for screening loss of shielding pivotal events associated with heating of aging overpacks in a fire. Loss of shielding could occur if the concrete that comprises the majority of the aging overpack spalled as a result of the fire. Spalling would reduce the thickness of the concrete and, if sufficient spalling occurs, the thickness could be reduced below the level required for adequate shielding.

### **D2.2.3.1 Thickness of Concrete Required for Adequate Shielding**

The concrete thickness needed for adequate shielding can be estimated by determining the dose outside the overpack for different concrete thicknesses and comparing that dose to the exposure limits for radiation workers. For this calculation, the exposure rate on the surface of the aging overpack prior to the fire is 40 mrem/hr (Ref. D4.1.15, Section 33.2.4.17).

The dose outside the aging overpack is primarily due to Co-60 gamma radiation, the gamma attenuation due to concrete can be estimated based on data available from the National Institute of Standards and Technology (NIST) (Ref. D4.1.40). This reference lists a value for the mass attenuation coefficient of the concrete divided by the concrete density ( $\mu/\rho$ ) of  $0.058 \text{ cm}^2/\text{g}$  for the gammas produced by Co-60. Multiplying this value by an approximate concrete density of  $2.3 \text{ g/cm}^3$  (Ref. D4.1.39, Table 4.2.5) yields a value for the mass attenuation coefficient of  $0.133 \text{ cm}^{-1}$ . Based on this value, there is approximately a factor of 10 reduction in the gamma dose for each 17.2 cm (6.8 inches) of concrete.

If the outer 6.8 inches of concrete were to spall as a result of the fire, the dose at the surface of the aging overpack would increase to 400 mrem/hr. If an additional 6.8 inches of concrete were to spall, the dose on the surface would be 4 rem/hr. The original concrete thickness is 34 inches based on existing aging overpack drawings (Ref. D4.1.14). There is 27.2 inches of concrete remaining after the first 6.8 inches of spallation and 20.4 inches of concrete remaining after the second 6.8 inches of spallation.

The dose outside the aging overpack can be estimated by noting that the dose decreases as the square of the distance from the source. After 13.6 inches of concrete has spalled, the dose 20.4 inches from the surface of the aging overpack would be 1 rem/hr, and the dose 61.2 inches from the surface would be 250 mrem/hr. Therefore, even in the case of extensive concrete spalling, workers involved in fire fighting or post-fire activities could be in close proximity to the degraded aging overpack for a lengthy period of time without exceeding either the annual exposure limit of 5 rem or special exposure limits outlined in 10 CFR Part 20 (Ref. D4.2.1, Paragraph 20.1206).

### **D2.2.3.2 Extent of Concrete Spalling in a Fire**

The current aging overpack design has a steel liner outside the concrete shielding. Consequently, spalling and removal of concrete from the surface cannot occur unless the steel liner is removed or fails catastrophically. However, because alternative aging overpack designs have been considered without a steel outer liner, the potential for substantial spallation with a bare concrete shield was assessed.

Extensive spalling of structural concrete has been observed under some conditions when the structural concrete is exposed to intense fires. The most extensive spalling has been observed in tunnel fires, such as the Channel Tunnel fire in 1996. In such cases, a significant fraction of the concrete spalled when exposed to the intense heat from the long-duration fires.

Due to the potential significance of spalling in reducing the strength of concrete support structures, spallation of concrete has been the subject of considerable study. "Limits of Spalling

of Fire-Exposed Concrete." (Ref. D4.1.37) provides a good overview of the factors that control concrete spalling due to fire. Hertz indicates that there are three types of spalling that can occur: (1) aggregate spalling, (2) explosive spalling, and (3) corner spalling. Aggregate spalling occurs with some aggregates (such as flint or sandstone) and results in superficial craters on the surface of the concrete. Corner spalling occurs only on the convex corners of beams or other structures and is caused by a localized weakening and cracking of the concrete such that the corner breaks off under its own weight. This mode of spalling is not relevant for the aging overpacks. Explosive spalling occurs when sufficient pressure builds up inside the concrete to cause pieces of concrete to be ejected from the surface. Explosive spalling is believed to account for the extensive concrete loss observed in the Channel Tunnel fire. Of the three modes of spalling, only explosive spalling could produce the loss of concrete necessary to significantly reduce the shielding capability of the aging overpack.

"Predicting the fire resistance behaviour of high strength concrete columns," (Ref. D4.1.43) notes that explosive spalling occurs when sufficient pressure builds up in the pores of the concrete to cause ejection of concrete from the surface. Buildup of such a high pressure requires three things: (1) low concrete permeability, (2) high moisture content in the concrete, and (3) rapid heating and resulting large thermal gradients. In addition, "Limits of Spalling of Fire-Exposed Concrete." (Ref. D4.1.37) notes that spallation is more pronounced in concrete structures undergoing high compressive stress, such as support columns.

Low permeability prevents gas migration and allows pressure to build. High structural strength concretes, such as those used in tunnel construction, are known to have very low permeability and are therefore more prone to spalling. In contrast, normal strength concretes do not have low permeability and spallation is not observed (Ref. D4.1.43). Because the concrete used for shielding in the aging overpacks is not counted on for structural strength and is therefore classified as normal strength concrete<sup>2</sup>, spallation is unlikely to occur.

Moisture content is a major factor in pressure buildup because water vapor is the gas primarily responsible for high pore pressures in the concrete. The concrete in the aging overpacks is unlikely to have a high moisture content because it is heated both internally by decay heat and externally by solar heat. In addition, it is likely to have been sitting in the Nevada desert for a lengthy period of time.

Thus, although the fire will produce large thermal gradients in the concrete, these gradients are unlikely to result in pressure buildup sufficient to cause extensive spallation due to the expected high permeability and low moisture content of the aging overpack concrete. This would be true regardless of whether the outer steel liner is present or not.

### **D2.2.3.3 Conclusion**

The preceding discussion has shown that a substantial amount of concrete would have to spall during a fire to produce a hazard to workers involved in either fire fighting or post-fire activities. In addition, it was shown that spallation is very unlikely given the type of concrete to be used in

---

<sup>2</sup> For example, the compressive strength of the concrete used in the HI-STORM storage overpack (Ref. D4.1.39, Table 1.D.1) is listed as 3,300 psi or 22.75 MPa, which is well below the strength of 55 MPa usually defined as necessary for high strength concrete (Ref. D4.1.43).

the aging overpacks and the likelihood that the aging overpacks will have an outer steel liner. For these reasons, loss of aging overpack shielding in a fire is considered Beyond Category 2 and need not be analyzed further.

### **D3 SHIELDING DEGRADATION DUE TO IMPACTS**

Neutrons emitted from transportation casks are shielded by a resin surrounded by a steel layer. The neutron shielding is present in the top lid, bottom and shell. Neutron shields designed to 10 CFR Part 71 (Ref. D4.2.2) are robust against 10 CFR Part 71 hypothetical accident conditions related to impacts or drops, exhibiting factors of safety greater than 1 for Service Level D allowables. Meeting *2004 ASME Boiler and Pressure Vessel Code Service Level D* (Subsection NF) (Ref. D4.1.6) provides for twice the allowable stress intensity as normal operation but still results in an extremely low failure probability. In addition, neutron dose typically attenuates quickly with distance from the transportation cask so it is only a small fraction of the gamma dose to personnel more than two meters away. Evacuation to that distance is the way to reduce personnel dose from neutrons. For these reasons, the analysis below focuses on the principle threat to workers on the site, which is degradation of gamma shielding.

This section summarizes information on loss of shielding mechanisms that could occur in event sequences for repository waste handling operations. The information is derived from transportation cask accident risk analyses. This information provides insights and bases for estimating probabilities of passive failures that result in LOS for casks and overpacks in waste handling event sequences.

The repository facilities process three categories of waste containers that provide shielding: transportation casks (truck and rail) and aging overpacks. The event sequence diagrams for operations involving processing of transportation casks and aging overpacks include the pivotal event “loss of shielding” for event sequences that are initiated by physical impact or fire. LOS due to fire was addressed previously in section D2.2 of this attachment. The following discussion focuses specifically on LOS due to drops and impacts.

The information in this section is based in large part on results of finite-element analysis (FEA) performed for four generic transportation cask types for transportation accidents as reported in NUREG/CR-6672 (Ref. D4.1.65) and NUREG/CR-4829 (Ref. D4.1.32). The results of the FEA were used to estimate threshold drop heights and thermal conditions at which LOS may occur in repository event sequences, using damage severity levels keyed to the FEA results to determine the challenge needed to cause LOS. The four cask types included one steel monolith rail cask, one steel/depleted uranium truck cask, one SLS truck cask and one SLS rail cask. NUREG/CR-6672 states that the steel in any of the cask is thick enough to provide some shielding, but the depleted uranium and lead provide the primary gamma shielding for the multi-shell cask types. The referenced study performed structural and thermal analyses for both failure of containment boundaries and loss of shielding for accident scenarios involving rail cask and truck cask impacting unyielding targets at impact speeds of 30-60, 60-90, 90-120, and greater than 120 mph. The impact orientations included side (0–20 degrees), corner (20 degrees–85 degrees), and end (85 degrees–90 degrees). The referenced study also correlated the damage from impacts on real targets including soil and concrete.



The event sequences used in the transportation accident analyses included impact-only, impact plus-fire, and fire-only conditions. The results of the FEA indicate that LOS could occur in the impact-only at speeds as low as 30 mph with an unyielding target and in fire scenarios of sufficient intensity and duration. The structural analyses did not credit the energy absorption capability of impact limiters. Therefore, the results are deemed applicable to approximate the structural response of transportation and similar casks in drop scenarios.

The primary reference NUREG/CR-6672 (Ref. D4.1.65), however, does not provide a threshold below which no LOS could be assured. Therefore, information quoted in an evaluation by the Association of American Railroads (AAR) (Ref. D4.1.30) was used to establish thresholds for LOS conditions based on damage categories that are correlated to plastic strain in the inner shell of a cask. That information is based on a prior transportation accident analysis known as the Modal Study (Ref. D4.1.32). For potential PCSA applications, FEA results for inner shell strain versus impact speed were extended to estimate the lower bound of impact speed or drop heights to establish conditions at which LOS may occur in cask-drop scenarios in repository operations.

NUREG/CR-6672 (Ref. D4.1.65) addresses two modes of LOS in accident scenarios: deformations of lid and closure geometry that permit direct streaming of radiation; and/or reductions in cask wall thickness or relocation of the depleted uranium or lead shielding. The LOS due to lid/closure distortion can be accompanied by air-borne releases if the inner shell of the cask is also breached.

The results of the FEA reported in NUREG/CR-6672 (Ref. D4.1.65) provides some definitive results that are deemed to be directly applicable to the repository event sequence analyses:

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

Therefore, this analysis focuses on LOS for SLS casks to estimate the drop or collision conditions that could result in LOS from lead slumping. Figure D3.2-1 illustrates the effect of cask deformation and lead slumping for a SLS rail cask following an end-on impact at 120 mph onto an unyielding target from the result of the FEA reported in NUREG/CR-6672 (Ref. D4.1.65).

### **D3.1 DAMAGE THRESHOLDS FOR LOS**

The AAR study (Ref. D4.1.30) is used as a reference for this report. The information cited, however, was derived from an earlier transportation cask study known as the “Modal Study,”

(Ref. D4.1.32). The Modal Study assigned three levels of cask response characterized by the maximum effective plastic strain within the inner shell of a transport cask. The severity levels are defined as:

- S1—implies strain levels  $< 0.2\%$
- S2—implies strains between 0.2 and 2.0%
- S3—implies strain levels between 2.0 and 30%.

The amount of damage to a cask for the respective severity levels is summarized in the following:

S1:

- No permanent dimensional change
- Seal and bolts remain functional
- Little if any radiation release
- Less than 40 g axial force on lead for all orientations
- No lead slump
- Fuel basket functional; up to 3% of fuel rods may release into cask cavity
- Loads/releases within regulatory criteria.

S2:

- Small permanent dimensional changes
- Closure and seal damage, may result in release
- Limited lead slump
- Up to 10% of fuel rods release to cask cavity.

S3:

- Large distortions
- Seal leakage likely
- Lead slump likely
- 100% fuel rods release to cask cavity.

As stated above, limited lead slumping may occur at damage level S2, but is likely to occur at damage level S3. The respective strain levels associated with damage levels S2 and S3 were applied to the results from NUREG/CR-6672 (Ref. D4.1.65) to establish a threshold impact speed for the onset of LOS.

### **D3.2 SEVERITY OF DAMAGE VERSUS IMPACT VELOCITY**

The FEA results given in Table 5.3 of NUREG/CR-6672 (Ref. D4.1.65) are summarized in Table D3.2-1. The strain in the inner shell of the SLS casks are shown in Table D3.2-1 and illustrated in Figure D3.2-1. These data were plotted (Figures D3.2-2 and D3.2-3). The data points start at the lowest speed range of 30 to 60 mph. The data were plotted as points using the

lower boundary of each of the four speed ranges on the abscissa. The strain plots were extended to the origin by including the point (0, 0) with the Table D3.2-1 data.

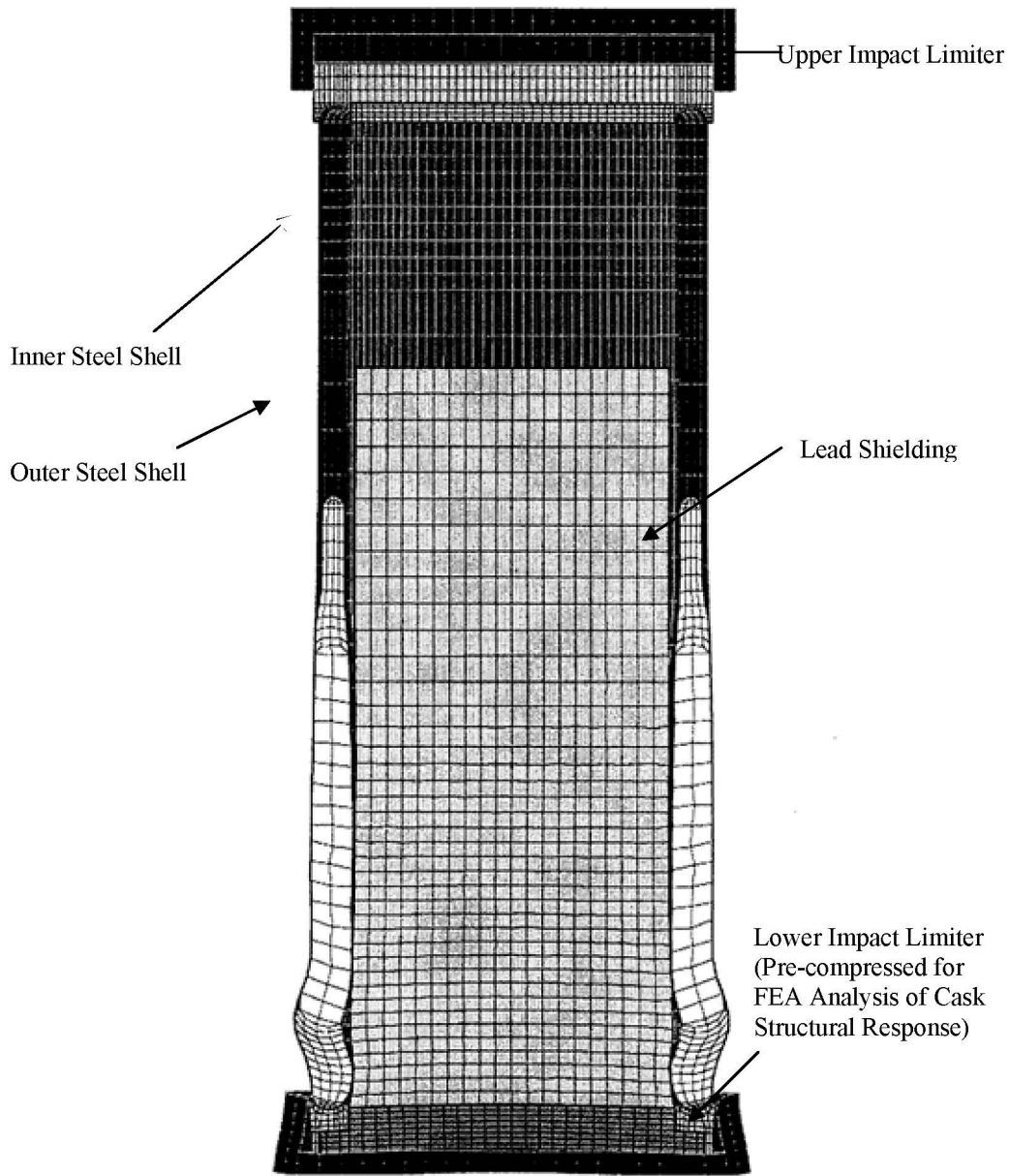
Two horizontal lines were superimposed on Figures D3.2-2 and D3.2-3 to plot the 0.2% and 2.0% strain to represent the respective S2 and S3 thresholds for inner shell strain. The intersections of the strain curves with the respective threshold values indicate the minimum impact speed at which the respective S2 and S3 strain thresholds appear to be exceeded.

Table D3.2-1. Maximum Plastic Strain in Inner Shell of Sandwich Wall Casks

Cask Type	Orientation: Speed, mph	Corner Impact Strain, %	End Impact Strain, %	Side Impact Strain, %
SLS Truck	30	12	3.9	N/A
	60	29	12	16
	90	33	18	24
	120	47	27	27
SDUS Truck	30	11	1.8	6
	60	27	4.8	13
	90	43	8.3	21
	120	55	13	30
SLS Rail	30	21	1.9	5.9
	60	34	5.5	11
	90	58	13	15
	120	70	28	N/A

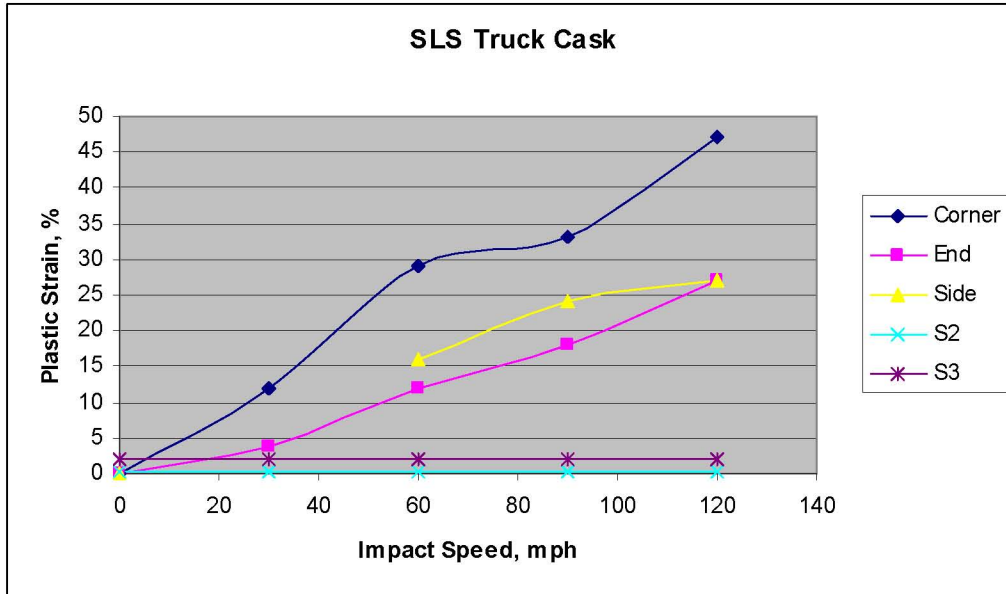
NOTE: SDUS = steel-depleted uranium-steel; SLS = steel-lead-steel.

Source: From Ref. D4.1.65, Table 5.3.



Source: From Ref. D4.1.65, Figure 5.9

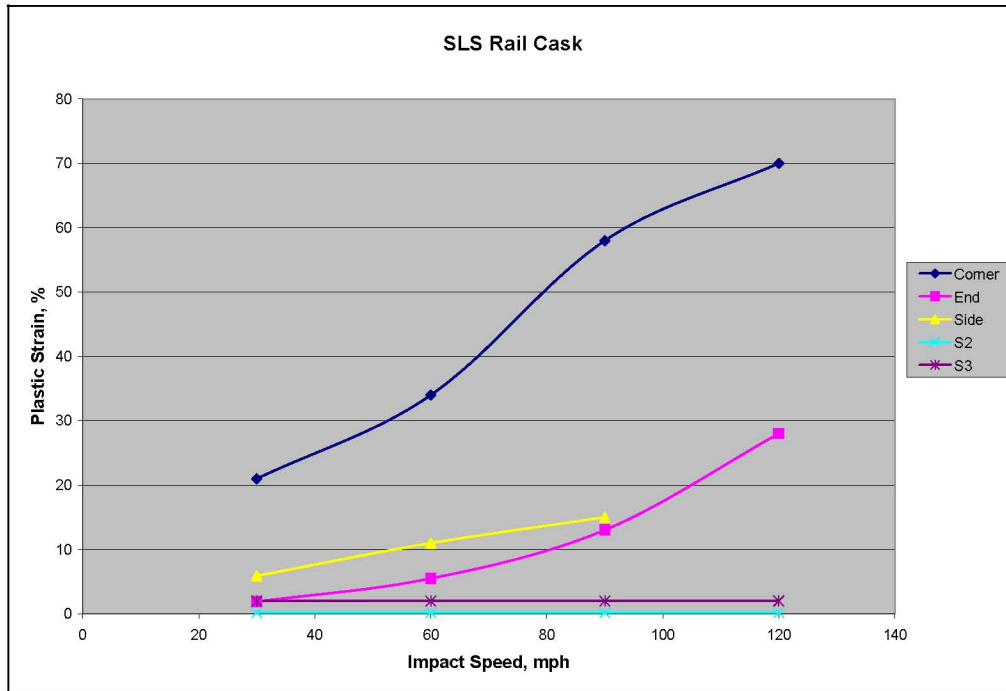
Figure D3.2-1. Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph



NOTE: <sup>1</sup> Data points for strain versus speeds greater than 30 mph taken directly from NUREG/CR-6672, Table 5.3: plots extended to origin (0,0) to determine crossover for S2 and S3 threshold strains.  
<sup>2</sup> S2 and S3 threshold strains based on information in *A Railroad Industry Critique of the Model Study* (Ref. D4.1.30). mph = miles per hour; SLS = steel-lead-steel.

Source: Original

Figure D3.2-2. Truck Steel/Lead/Steel Inner Shell Strain versus Impact Speed



NOTE: <sup>1</sup> Data points for strain versus speeds greater than 30 mph taken directly from NUREG/CR-6672 (Ref. D4.1.65, Table 5.3): plots extended to origin (0,0) to determine crossover for S2 and S3 threshold strains.  
<sup>2</sup> S2 and S3 threshold strains based on information in *A Railroad Industry Critique of the Model Study* (Ref. D4.1.30). mph = miles per hour; SLS = steel-lead-steel.

Source: Original

Figure D3.2-3. Rail Steel/Lead/Steel Strain versus Impact Speed

### D3.3 ESTIMATE OF THRESHOLD SPEEDS FOR LOSS OF SHIELDING DUE TO IMPACTS

The plots in Figures D3.2-2 and D3.2-3, and Table D3.2-1 illustrate that the S2 threshold is exceeded for both the truck and rail SLS casks for all four speed ranges and all orientations. Since NUREG/CR-6672 (Ref. D4.1.65) does not report LOS conditions for low impact speeds, it is concluded that the S2 criterion is not a valid threshold for LOS in SLS casks. Therefore, the remainder of this analysis applies the S3 criterion (2% shell strain) as a basis for estimating LOS threshold impact speeds.

Figures D3.2-2 and D3.2-3, and Table D3.2-1 indicate that the S3 threshold is exceeded for both truck and rail SLS casks for all orientations. The intersections of the strain curves and the 2% strain line in Figures D3.2-2 and D3.2-3 illustrate the impact speed at where the S3 threshold is reached for each case. A small exception being the end drop of a SLS rail cask in the 30-60 mph range for which the shell strain of 1.9% is just below the lower bound for S3 damage. However, this margin is too small to exclude that case. Although the strains for the side drop cases exceed the threshold for lead slumping, NUREG/CR-6672 (Ref. D4.1.65) states that lead slumping does not occur in side drops. Therefore, LOS for side drops is excluded from the remainder of this report.

Using the 2% shell strain condition as the threshold for LOS in SLS casks, the following is observed:

- LOS for the truck SLS cask would occur at impact speeds of about 5 mph for corner impact and about 18 mph for end impact
- LOS for the rail SLS cask would occur at about 3 mph for corner impact and about 30 mph for end impact.

It is observed that the corner drop cases give the largest shell strain at a given impact speed but the finite element analyses indicate that the extent of lead slumping is less in corner drops than for end impacts.

Table D3.3-1 shows the drop height equivalents for impact speed onto a horizontal unyielding surface. Thus, to exceed 5 mph, for example, a drop height greater than 0.8 ft is required; to exceed 30 mph impact, a drop height greater than 30 ft is required. Using the results cited above:

- LOS for the truck SLS cask would occur at impact speeds of about 0.8 ft (5 mph) for corner impact and about 10 ft (18 mph) for end impact
- LOS for the rail SLS cask would occur at about 0.5 ft (3 mph) for corner impact and about 30 ft (30 mph) for end impact.

Such drop heights could occur in some GROA handling operations.

However, when the effect of the energy absorption by real targets is considered, much greater impact speeds are required to impose the damage equivalent to impacts on unyielding targets. NUREG/CR-6672 (Ref. D4.1.65) provides a correlation of impact speeds for real versus unyielding target, but provides only bounding values for a large number of cases as presented in Table D3.3-2. Therefore, if LOS occurs at 30 mph for an end drop of a SLS train cask on unyielding surface, a speed of greater than 150 mph is required for an impact on concrete. This impact speed would require a drop of over 500 ft. Such drop heights cannot be achieved in repository handling.

Some of the LOS cases, including corner drops of truck and rail SLS casks, appear to result in LOS for impact speeds less than 10 mph. If the corner drops are onto concrete, a speed of 2 to 3 times the threshold speed for LOS for impact on an unyielding target. This implies a threshold impact speed of 20 to 30 mph for a corner drop onto concrete. The corresponding drop height is 13 feet to 30 feet. Such drops could occur in event sequences for repository handling.

Table D3.3-1. Drop Height to Reach a Given Impact Speed

Impact Speed, mph	Equivalent Drop Height, ft
2	0.1
5	0.8
10	3.3
20	13.4
30	30.1
40	53.4
50	83.5
60	120.2
70	163.7
80	213.8
90	270.6
100	334.0
110	404.2
120	481.0

Source: Original

Table D3.3-2. Impact Speeds on Real Target for Equivalent Damage for Unyielding Targets

Cask Type	Real Target type	Impact Type\Orientation w/o Impact Limiters	Impact Speed , mph			
			30	60	90	120
Rail SLS	Soil	End	>>150	>>150	>>150	>>150
		Side	72	>150	>>150	>>150
		Corner	68	133	>150	>150
	Concrete slab	End	>150	>>150	>>150	>>150
		Side	85	>150	>>150	>>150
		Corner	>>150	>>150	>>150	>>150
Truck SLS	Soil	End	>150	>>150	>>150	>>150
		Side	70	>150	>>150	>>150
		Corner	61	>150	>>150	>>150
	Concrete slab	End	123	180	>>150	>>150
		Side	35	86	135	>150
		Corner	56	123	>150	>>150

NOTE: mph = miles per hour; SLS = steel-lead-steel.

Source: Based on NUREG/CR-6672 (Ref. D4.1.65, Tables 5.10 and 5.12)

### D3.4 PROBABILITY OF LOSS OF SHIELDING

NUREG/CR-6672 (Ref. D4.1.65) develops probabilities for LOS in transportation accidents. The probability of LOS uses event tree analysis with split fractions for various types of transportation accidents and frequencies based on accident rates per mile of travel for



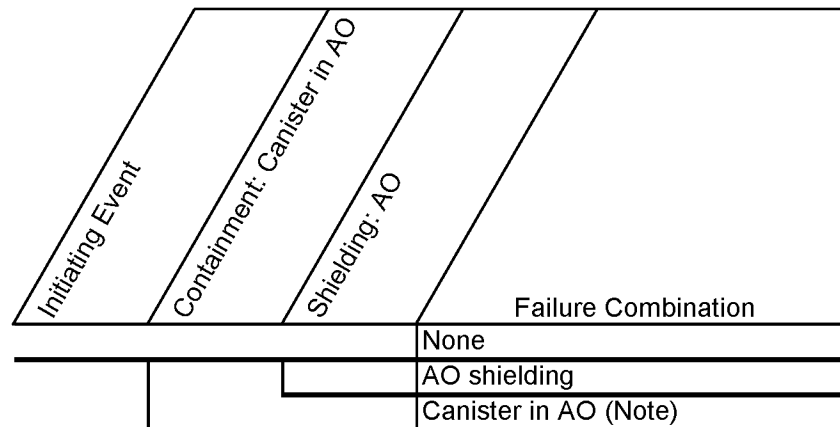
cask-bearing truck trailers or rail cars. The results of probability analyses of LOS as derived in NUREG/CR-6672 (Ref. D4.1.65) do not have any direct relevance to event sequences for waste handling operations. However, the basic approach that breaks down the overall probability of an event sequence involving LOS into conditional probabilities for occurrence of various physical conditions that lead to LOS can be adapted for PCSA.

The vulnerability to LOS for repository event sequences varies with the container type:

1. Concrete overpack with no containment boundary (aging overpack)
2. Sandwich type with steel containment boundary and lead in the annulus between the steel shells (transportation cask).
3. All other casks including monolithic steel casks or casks with layers of steel or steel and depleted uranium (transportation cask, shielded transfer cask (STC)).

**Concrete Overpacks**

Aging overpacks provide shielding but not containment. They are used within the GROA to transport DPCs and TAD canisters between buildings and to and from the aging pads. The event sequences that involve both are of the form shown in Figure D3.4-1 below.



Note: Implies shielding is ineffective because of radionuclide release

NOTE: AO = aging overpack

Source: Original

Figure D3.4-1. Summary Event Tree Showing Model Logic for Canisters and Aging Overpacks

A site transporter transports aging overpacks with canisters within the GROA. The transporter is designed for a maximum speed of 2.5 mph (Ref. D4.1.18, Sections 3.2.1 and 3.2.4) and will elevate the aging overpack no more than 3 feet from the ground (equipment limit is 12 inches (Ref. D4.1.18, Section 2.2, item 9)), additional two feet is allowed for potential drop off edge of aging pad). Expanding the probability of success (no breach) of a canister within an aging overpack yields:

$$p_{AO}(C) = p_{AO}(C|O)p_{AO}(O) + p_{AO}(C|\bar{O})p_{AO}(\bar{O}), \quad (\text{Eq. D-26})$$

where

$p_{AO}(C)$  = probability of canister success within an AO.

$p_{AO}(C|O)$  = probability of canister success given AO shielding does not fail.

$p_{AO}(O)$  = probability that AO shielding does not fail.

$p_{AO}(C|\bar{O})$  = probability of canister success given AO shielding fails.

$p_{AO}(\bar{O})$  = probability that AO shielding fails.

The inner and outer steel lined 3 foot concrete aging overpack is much more robust against impact loads than a DPC. Therefore, if the overpack fails, it is much more likely that the canister will breach. This yields:  $p_{AO}(C|O) \gg p_{AO}(C|\bar{O})$ . Furthermore, the probability of aging overpack breach is much less than probability of aging overpack success at the above drop and speed conditions. Therefore:  $p_{AO}(O) \gg p_{AO}(\bar{O})$ . The second term on the right hand side of Equation D-26 is much less than the first term and need not be considered further in this analysis.

This leaves

$$p_{AO}(C) \cong p_{AO}(C|O)p_{AO}(O) \quad (\text{Eq. D-27})$$

Note that

$$p_{AO}(C) = 1 - p_{AO}(\bar{C}) \quad \text{and} \quad p_{AO}(O) = 1 - p_{AO}(\bar{O}) \quad \text{and}$$

$$p_{AO}(C|O) = 1 - p_{AO}(\bar{C}|O) \quad (\text{Eq. D-28})$$

Substituting Equations D-28 into D-27 and rearranging yields:

$$p_{AO}(\bar{O}) \cong 1 - \frac{1 - p_{AO}(\bar{C})}{1 - p_{AO}(\bar{C}|O)} \quad (\text{Eq. D-29})$$

LLNL has developed a mean probability of failure for a canister within an aging overpack,  $p_{AO}(\bar{C})$ , for a 3-foot drop onto a rigid surface with an initial velocity of 2.5 mph (Ref. D4.1.27).

This analysis uses a conservative value of 1E-05 relative to the 1E-08 value in the referenced LLNL report. The probability of canister failure given the aging overpack does not fail,  $p_{AO}(\bar{C} | O)$ , must be less than the overall probability of canister failure within an aging overpack,  $p_{AO}(\bar{C})$ . It is, therefore, reasonable to use a range of values of 1E-06 to 1E-05 for this, both of which are conservative relative to the value in the reference. The LLNL (Ref. D4.1.27) value, itself, has a conservative element in that it analyzes impact onto a rigid surface. The more realistic concrete surface would have a lower canister failure probability. Using the average between 1E-06 and 1E-05 of 5E-06 for  $p_{AO}(\bar{C} | O)$  and also substituting the aforementioned value for  $p_{AO}(\bar{C})$  into Equation D-29, there obtains:

$$p_{AO}(\bar{O}) \cong 1 - \frac{1 - p_{AO}(\bar{C})}{1 - p_{AO}(\bar{C} | O)} = 1 - \frac{1 - 10^{-5}}{1 - 5 \times 10^{-6}} = 5 \times 10^{-6} \quad (\text{Eq. D-30})$$

### ***Steel/Lead/Steel Sandwich-Type Casks***

For these sandwich-type casks, the probability of LOS due to lead slumping can be estimated from results of transportation cask studies that can be coupled to event sequence probability analysis and insights from the passive failure analyses. Since the speed of transport of transportation casks to, and within, the processing facilities is limited to a few mph, it is judged that LOS of SLS casks (and the other types) may be screened out from collision scenarios. However, LOS for SLS casks due to drops cannot be ruled out, if SLS casks are processed in the repository.

For SLS casks, the probability of LOS is derived from the probability that the drop height or impact speed exceeds the threshold at which lead shielding may slump. For all cask types, the probability of LOS is derived from the probability that the drop height or impact speed exceeds the threshold at which cask closure and/or seals fail in such a way to permit to permit direct streaming. A simplified conservative approach to estimating the probability of LOS due to lead slumping resulting from a drop of an SLS cask is summarized in the next section.

The PCSA considers drop and collision event sequences of transportation casks. Should a canister rupture occur, the analysis conservatively models the shielding as also lost. In such event sequences the probability of loss of shielding is taken to be 1.0 given canister rupture. This applies to all types of casks.

Event sequences also include LOS without canister rupture. That is, the drop or collision was not severe enough to cause a rupture but a LOS is possible in some casks. Such an event sequence can not occur in the steel/depleted uranium truck casks. The loss of shielding associated with streaming through the head of steel monolith rail casks is due to structural failure of the casks. The probability of this is estimated by taking the breach/rupture probability of a steel monolith transportation cask at the weakest location and applying it as a head rupture probability.

Collisions of casks will occur at less than 5 mph. Drops can occur as high as 30 feet. Drops may be at any orientation: side, bottom, and end. A conservative approach to estimation of the probability of SLS LOS is to use the information associated with end drops, which can cause bulging of the steel containment that allows the lead to collect towards one end. Although the corner impact can cause greater strain in the steel containment, it does not cause the spreading that increases collection of the lead at one end. All surfaces in the repository upon which a transportation cask can be dropped (concrete or soil) are concrete or softer. Therefore, the concrete related drop height vs. LOS information may be accurately used.

An impact of at least 123 mph against a real surface such as concrete or soil is required in order to cause the same damage as an impact of 30 mph against an unyielding surface (Table D3.3-2). The vast majority of casks are to be delivered to the repository by rail. The maximum strain due to an end impact of 30 mph against an unyielding surface, or 123 mph against a real surface, is about 3.9% for a truck cask (greater than the 1.9% strain for a rail cask) (Table D3.2-1). Noting in Figure D3.2-3 that the amount of strain is roughly linear with the impact velocity, a velocity of 63 mph is estimated to correspond to the strain of 2% indicative of S3 damage and lead slumping. A 63 mph collision, equivalent to a 133-foot drop, is the threshold for causing enough damage to indicate potential loss of shielding due to lead slumping.

In order to develop fragility over height, the available information described herein indicates that an estimate of a median threshold for a failure drop height is 133 feet. This would yield 2% strain. A coefficient variation (the ratio of standard deviation to the median) is 0.1. This is an estimate derived from the distribution of capacity associated with the tensile strength elongation data described in Section D1.1. The probability of LOS due to lead slumping resulting from a 15-foot vertical drop would be less than  $1 \times 10^{-8}$ , given the drop event. For a 30-foot drop resulting from a 2-blocking event, the computed failure probability based on the 133-foot median drop height is also less than  $1 \times 10^{-8}$ . LOS due to lead slumping applies only to those casks using lead for shielding but the PCSA applied this analysis to all casks. A conservative value of  $1 \times 10^{-5}$  is used to be consistent with the probabilities based on the LLNL (Ref. D4.1.27) results.

Results are shown in Tables D3.4-1.

Table D3.4-1. Probabilities of Degradation or Loss of Shielding

	Probability	Note
Sealed transportation cask and shielded transfer casks shielding degradation after structural challenge	$1 \times 10^{-5}$	Section D3.4
Aging overpack shielding loss after structural challenge	$5 \times 10^{-6}$	Section D3.4
CTM shielding loss after structural challenge	0	Structural challenge sufficiently mild to leave the shielding function intact <sup>a</sup>
WPTT shielding loss after structural challenge	0	Structural challenge sufficiently mild to leave the shielding function intact <sup>a</sup>
TEV shielding loss (shield end)	0	Structural challenge sufficiently mild to leave the shielding function intact <sup>a</sup>
Shielding loss by fire for waste forms in transportation casks or shielded transfer casks	1	Lead shielding could potentially expand and degrade. This probability is conservatively applied to transportation casks and STCs that do not use lead for shielding
Shielding loss by fire of aging overpacks, CTM shield bell, and WPTT shielding	0	Type of concrete used for aging overpacks is not sensitive to spallation; Uranium used in CTM shield bell and WPTT shielding does not lose its shielding function as a result of fire

NOTE: <sup>a</sup>In the event sequence diagrams of the PCSA, the shielding function for the CTM, WPTT and TEV is queried for the challenges that do not lead to a radioactive release. Such challenges, which were not sufficiently severe to cause a breach of containment of the waste form container, are also deemed mild enough to leave the shielding function of the CTM, WPTT and TEV intact.

CTM = canister transfer machine; STC = shielded transfer cask; TEV=transport and emplacement vehicle; WPTT = waste package transfer trolley.

Source: Original

### ***All Other Cask Types***

For all other cask types, the results of the transportation cask study indicate that the only mechanism for LOS is streaming via closure failures and closure geometry changes. Therefore, the probability of LOS can be equated to the probability of rupture/breach of such casks.

## D4 REFERENCES

### D4.1 DESIGN INPUTS

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

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

- D4.1.1\* Allegheny Ludlum 2006. "Technical Data Blue Sheet, Stainless Steels Chromium-Nickel-Molybdenum, Types 316 (S31600), 316L (S31603), 317 (S31700), 317L (S31703)." Technical Data Blue Sheet. Brackenridge, Pennsylvania: Allegheny Ludlum. TIC: 259471. LC Call Number: TA 486 .A4 2006.
- D4.1.2\* A.M. Birk Engineering 2005. *Tank Car Thermal Protection Defect Assessment: Updated Thermal Modelling with Results of Fire Testing*. TP 14367E. Ontario, Canada: Transportation Development Centre of Transport Canada. ACC: MOL.20071113.0095.
- D4.1.3\* ASM (American Society for Metals) 1961. "Properties and Selection of Metals." Volume 1 of *Metals Handbook*. 8th Edition. Lyman, T.; ed. Metals Park, Ohio: American Society for Metals. TIC: 257281. LC Call Number: TA459 .M43 1961 Vol.1.
- D4.1.4\* ASM 1976. *Source Book on Stainless Steels*. Metals Park, Ohio: American Society for Metals. TIC: 259927. LC Call Number: TA479 .S7 S64 1976.
- D4.1.5\* ASME (American Society of Mechanical Engineers) 2001. *2001 ASME Boiler and Pressure Vessel Code (includes 2002 addenda)*. New York, New York: American Society of Mechanical Engineers. TIC: 251425.
- D4.1.6\* ASME 2004. *2004 ASME Boiler and Pressure Vessel Code*. 2004 Edition. New York, New York: American Society of Mechanical Engineers. TIC: 256479.
- D4.1.7\* ASTM (American Society for Testing and Materials) G 1-03. 2003. *Standard Practice for Preparing, Cleaning, and Evaluating Corrosion Test Specimens*. West Conshohocken, Pennsylvania: American Society for Testing and Materials. TIC: 259413.
- D4.1.8\* Avallone, E.A. and Baumeister, T., III, eds. 1987. *Marks' Standard Handbook for Mechanical Engineers*. 9th Edition. New York, New York: McGraw-Hill. TIC: 206891. ISBN: 0-07-004127-X.

- D4.1.9\* BNFL Fuel Solutions 2003. *FuelSolutions™ TSI25 Transportation Cask Safety Analysis Report, Revision 5*. Document No. WSNF-120. Docket No. 71-9276. Campbell, California: BNFL Fuel Solutions. TIC: 257634.
- D4.1.10 Not Used.
- D4.1.11 BSC 2006. *CRCF, IHF, RF, and WHF Canister Transfer Machine Mechanical Equipment Envelope*. 000-MJ0-HTC0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20061120.0011.
- D4.1.12 BSC 2007. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle*. 000-30R-HE00-00200-000 REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0002.
- D4.1.13 BSC 2007. *5-DHLW/DOE SNF - Long Co-Disposal Waste Package Configuration*. 000-MW0-DS00-00203-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070719.0007.
- D4.1.14 BSC 2007. *Aging Facility Vertical DPC Aging Overpack Mechanical Equipment Envelope Sheet 1 of 2*. 170-MJ0-HAC0-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070928.0032.
- D4.1.15 BSC 2007. *Basis of Design for the TAD Canister-Based Repository Design Concept*. 000-3DR-MGR0-00300-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0042.
- D4.1.16\* BSC 2007. *Discipline Design Guide and Standards for Surface Facilities HVAC Systems*. 000-3DG-GEHV-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070514.0007.
- D4.1.17 BSC 2007. *Leak Path Factors for Radionuclide Releases from Breached Confinement Barriers and Confinement Areas*. 000-00C-MGR0-01500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071018.0002.
- D4.1.18 BSC 2007. *Mechanical Handling Design Report - Site Transporter*. 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.
- D4.1.19 BSC 2007. *Naval Long Oblique Impact Inside TEV*. 000-00C-DNF0-01200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070806.0016.
- D4.1.20 BSC 2007. *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert*. 000-00C-DNF0-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071017.0001.
- D4.1.21 BSC 2007. *Probabilistic Characterization of Preclosure Rockfalls in Emplacement Drifts*. 800-00C-MGR0-00300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070329.0009.

- D4.1.22 BSC 2007. *TAD Waste Package Configuration*. 000-MW0-DSC0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0010.
- D4.1.23 BSC 2007. *TAD Waste Package Configuration*. 000-MW0-DSC0-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0011.
- D4.1.24 BSC 2007. *TAD Waste Package Configuration*. 000-MW0-DSC0-00103-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0012.
- D4.1.25 BSC 2007. *Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident*. 000-00C-WIS0-02900-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070220.0008.
- D4.1.26 BSC 2007. *Waste Package Capability Analysis for Nonlithophysal Rock Impacts*. 000-00C-MGR0-04500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071113.0017.
- D4.1.27 BSC 2008. *Seismic and Structural Container Analyses for the PCSA*. 000-PSA-MGR0-02100-000-00A. Rev. 00A. Las Vegas, NV: Bechtel SAIC Company. ACC: ENG.20080220.0003.
- D4.1.28 DOE (U.S. Department of Energy) 2007. *Transportation, Aging and Disposal Canister System Performance Specification*. WMO-TADCS-000001, Rev. 0. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070614.0007. (DIRS 181403)
- D4.1.29 DOE 2007. *Quality Assurance Requirements and Description*. DOE/RW-0333P, Rev. 19. Washington, D. C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: DOC.20070717.0006. (DIRS 182051)
- D4.1.30\* English, G.W.; Moynihan, T.W.; Worswick, M.J.; Birk, A.M. 1999. *A Railroad Industry Critique of the Model Study*. 96-025-TSD. Kingston, Ontario, Canada: Association of American Railroads Safety & Operations. TIC: 260032. LC Call Number: TK9152.17 .T73 1999.
- D4.1.31\* Evans, D.D. 1993. "Sprinkler Fire Suppression Algorithm for HAZARD." *Fire Research and Safety, 12th Joint Panel Meeting, October 27-November 2, 1992, Tsukuba, Japan*. Pages 114-120. Tsukuba, Japan: Building Research Institute and Fire Research Institute. ACC: MOL.20071114.0163.
- D4.1.32\* Fischer, L.E.; Chou, C.K.; Gerhard, M.A.; Kimura, C.Y.; Martin, R.W.; Mensing, R.W.; Mount, M.E.; and Witte, M.C. 1987. *Shipping Container Response to Severe Highway and Railway Accident Conditions*. NUREG/CR-4829. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: NNA.19900827.0230; NNA.19900827.0231.



- D4.1.33\* Friedrich, T. and Schellhaas, H. 1998. *Computation of the percentage points and the power for the two-sided Kolmogorov-Smirnov one sample test*. Statistical Papers 39:361-75. TIC: 260013.
- D4.1.34\* General Atomics. 1995. *GA-9 Legal Weight Truck From-Reactor Spent Fuel Shipping Cask, Final Design Report (FDR)*. 910354 N/C. San Diego, California: General Atomic. ACC: MOV.20000106.0003.
- D4.1.35\* Haynes International 1990. Reliability and Longevity of Furnace Components as Influenced by Alloy of Construction. H-3124. Kokomo, Indiana: Haynes International. TIC: 256362.
- D4.1.36\* Haynes International 1997. Hastelloy C-22 Alloy. Kokomo, Indiana: Haynes International. TIC: 238121.
- D4.1.37\* Hertz, K.D. 2003. "Limits of Spalling of Fire-Exposed Concrete." *Fire Safety Journal*, 38, 103-116. [New York, New York]: Elsevier. TIC: 259993.
- D4.1.38\* Holtec International 2003. *Storage, Transport, and Repository Cask Systems, (Hi-Star Cask System) Safety Analysis Report, 10 CFR 71, Docket 71-9261*. HI-951251, Rev. 10. [Marlton, New Jersey]: Holtec International. ACC: MOL.20050119.0271.
- D4.1.39\* Holtec International 2005. *Final Safety Analysis Report for the HI-STORM 100 Cask System*. USNRC Docket No.: 72-1014. Holtec Report No.: HI-2002444. Marlton, New Jersey: Holtec International. TIC: 258829.
- D4.1.40\* Hubbell, J.H. and Seltzer, S.M., *Tables of X-Ray Mass Attenuation Coefficients and Mass Energy-Absorption Coefficients* (version 1.4). National Institute of Standards and Technology, Gaithersburg, MD, 2004. (Originally published as NISTIR 5632, National Institute of Standards and Technology, Gaithersburg, MD, 1995) (Available online at: <http://physics.nist.gov/PhysRefData/XrayMassCoef/tab4.html>) ACC: MOL.20080303.0046.
- D4.1.41\* Incropera, F.P. and DeWitt, D.P. 1996. *Introduction to Heat Transfer*. 3<sup>rd</sup> Edition. New York, New York: John Wiley and Sons. TIC: 241057. ISBN: 0-471-30458-1.
- D4.1.42 Not used.
- D4.1.43\* Kodur, V.K.R.; Wang, T.C.; and Cheng, F.P. 2004. "Predicting the Fire Resistance Behaviour of High Strength Concrete Columns." *Cement & Concrete Composites*, 26, 141-153. [New York, New York]: Elsevier. TIC: 259996.
- D4.1.44\* Larson, F.R. and Miller, J. 1952. "A Time-Temperature Relationship for Rupture and Creep Stresses." *Transactions of the American Society of Mechanical Engineers*, 74, 765-775. New York, New York: American Society of Mechanical Engineers. TIC: 259911.

- D4.1.45 Lide, D.R., ed. 1995. *CRC Handbook of Chemistry and Physics*. 76th Edition. Boca Raton, Florida: CRC Press. TIC: 216194. ISBN: 0-84930476-8.
- D4.1.46\* Majumdar, S.; Shack, W.J.; Diercks, D.R.; Mruk, K.; Franklin, J.; and Knoblich, L. 1998. *Failure Behavior of Internally Pressurized Flawed and Unflawed Steam Generator Tubing at High Temperatures – Experiments and Comparisons with Model Predictions*. NUREG/CR-6575. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071106.0053.
- D4.1.47\* Mason, M. 2001. “NUHOMS-MP197 Transport Packaging Safety Analysis Report.” Letter from M. Mason (Transnuclear) to E.W. Brach (NRC), May 2, 2001, E-21135, with enclosures. TIC: 255258.
- D4.1.48\* Morris Material Handling 2008. *Mechanical Handling Design Report - Canister Transfer Machine*. Morris Material Handling. V0-CY05-QHC4-00459-00018-001-004; ACC: ENG.20080121.0010.
- D4.1.49\* NAC (Nuclear Assurance Corporation) 2000. *Safety Analysis Report for the NAC Legal Weight Truck Cask*. Revision 29. Docket No. 71-9225. T-88004. [Norcross, Georgia]: Nuclear Assurance Corporation International. ACC: MOL.20070927.0003.
- D4.1.50\* NAC (Nuclear Assurance Corporation) 2004. "NAC-STC NAC Storage Transport Cask, Revision 15." Volume 1 of *Safety Analysis Report*. Docket No. 71-9235. Norcross, Georgia: NAC International. TIC: 257644.
- D4.1.51\* Nakos, J.T. 2005. *Uncertainty Analysis of Steady State Incident Heat Flux Measurements in Hydrocarbon Fuel Fires*. SAND2005-7144. Albuquerque, New Mexico: Sandia National Laboratories. ACC: MOL.20071106.0054.
- D4.1.52\* Nowlen, S.P. 1986. *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report*. NUREG/CR-4680. SAND86-0312. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0099.
- D4.1.53\* Nowlen, S.P. 1987. *Quantitative Data on the Fire Behavior of Combustible Materials Found in Nuclear Power Plants: A Literature Review*. NUREG/CR-4679. SAND86-0311. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071113.0100.
- D4.1.54\* NRC (U.S. Nuclear Regulatory Commission) 1997. *Standard Review Plan for Dry Cask Storage Systems*. NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.
- D4.1.55\* NRC 2003. *Interim Staff Guidance - 18. The Design/Qualification of Final Closure Welds on Austenitic Stainless Steel Canisters as Confinement Boundary for Spent Fuel Storage and Containment Boundary for Spent Fuel Transportation*. ISG-18. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 254660.

- D4.1.56\* NRC 2007. *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis - Level of Information and Reliability Estimation*. HLWRS-ISG-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.
- D4.1.57\* Quintiere, J.G. 1998. *Principles of Fire Behavior*. Albany, New York: Delmar Publishers. TIC: 251255. ISBN: 0-8273-7732-0.
- D4.1.58\* Rieth, M.; Falkenstein, A.; Graf, P.; Heger, S.; Jäntschi, U.; Klimiankou, M.; Materna-Morris, E.; and Zimmermann, H. 2004. *Creep of the Austenitic Steel AISI 316L(N), Experiments and Models*. FZKA 7065. Karlsruhe, Germany: Forschungszentrum Karlsruhe GmbH. TIC: 259943.
- D4.1.59\* Sasikala, G.; Mathew, M.D.; Bhanu Sankara Rao, K.; and Mannan, S.L. 1997. "Assessment of Creep Behaviour of Austenitic Stainless Steel Welds." *Creep-Fatigue Damage Rules for Advanced Fast Reactor Design, Proceedings of a Technical Committee Meeting, Manchester, United Kingdom, 11-13 June 1996*. IAEA-TECDOC-993. Pages 219-227. Vienna, Austria: International Atomic Energy Agency. TIC: 259880.
- D4.1.60\* Savolainen, K.; Mononen, J.; Ilola, R.; Hanninen, H. 2005. *Materials Selection for High Temperature Applications [TKK-MTR-4/05]*. TKK-MTR-4/05. Helsinki, Finland, Espoo, Finland: Helsinki University of Technology, Laboratory of Engineering Materials; Otamedia Oy. TIC: 259896. ISBN: 951-22-7892-8.
- D4.1.61\* Society of Fire Protection Engineering (SFPE) 1988. *The SFPE Handbook of Fire Protection Engineering, Society of Fire Protection Engineers*. Edition 1. Boston, MA: Society of Fire Protection Engineering (SFPE). TIC: 101351. ISBN: 0-87765-353-4 .
- D4.1.62\* Shapiro, S. S. and Wilk, M. B. 1965. "An analysis of variance test for normality (complete samples)", *Biometrika*, 52 (3 - 4), pages 591-611. TIC: 259992.
- D4.1.63\* Siegel, R. and Howell, J.R. 1992. *Thermal Radiation Heat Transfer*. 3rd Edition. Washington, D.C.: Taylor & Francis. TIC: 236759. ISBN: 0-89116-271-2. (Radiation view factors also available online at: <http://www.me.utexas.edu/~howell/index.html>.)
- D4.1.64\* Snow, S.D. 2007, *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-Foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations*, EDF-NSNF-085, Rev. 0. [Idaho Falls, Idaho: Idaho National Laboratory]. ACC: MOL.20080206.0062.
- D4.1.65\* Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; and Yoshimura, H.R. 2000. *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20001010.0217.
- D4.1.66\* Transnuclear 2001. *TN-68 Transport Packaging Safety Analysis Report, Revision 4*. Hawthorne, New York: Transnuclear. TIC: 254025.

## **D4.2 DESIGN CONSTRAINTS**

- D4.2.1 10 CFR 20. 2007. Energy: Standards for Protection Against Radiation. Internet Accessible
- D4.2.2 10 CFR 71. 2007. Energy: Packaging and Transportation of Radioactive Material. ACC: MOL.20070829.0114.

**ATTACHMENT E**  
**HUMAN RELIABILITY ANALYSIS**

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	E-6
E1 INTRODUCTION .....	E-8
E1.1 SUMMARY .....	E-8
E2 SCOPE AND BOUNDARY CONDITIONS .....	E-10
E2.1 SCOPE .....	E-10
E2.2 BOUNDARY CONDITIONS .....	E-11
E3 METHODOLOGY .....	E-12
E3.1 METHODOLOGY BASES .....	E-12
E3.2 GENERAL APPROACH .....	E-12
E3.2.1 Step 1: Define the Scope of the Analysis .....	E-12
E3.2.2 Step 2: Describe Base Case Scenarios .....	E-13
E3.2.3 Step 3: Identify and Define HFEs of Concern .....	E-13
E3.2.3.1 Identifying Pre-initiator HFEs .....	E-14
E3.2.3.2 Identifying Human-Induced Initiator HFEs .....	E-14
E3.2.3.3 Identifying Non-recovery Post-initiator HFEs .....	E-14
E3.2.3.4 Identifying Recovery Post-initiator HFEs .....	E-15
E3.2.4 Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis .....	E-15
E3.2.5 Step 5: Identify Potential Vulnerabilities .....	E-16
E3.2.6 Step 6: Search for HFE Scenarios .....	E-17
E3.2.7 Step 7: Quantify Probabilities of HFEs .....	E-17
E3.2.8 Step 8: Incorporate HFEs into PCSA .....	E-18
E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design .....	E-19
E3.3 DEPENDENCY .....	E-19
E3.3.1 Capturing Dependency .....	E-19
E3.3.2 Sources of Dependency .....	E-20
E3.4 UNCERTAINTY .....	E-20
E3.5 DOCUMENTATION OF RESULTS .....	E-22
E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT .....	E-22
E4.1 FACILITY FAMILIARIZATION AND INFORMATION COLLECTION .....	E-23
E4.1.1 General Information Sources .....	E-23
E4.1.2 Industry Data Reviewed by the HRA Team .....	E-24
E4.2 USE OF EXPERTS AND ENGINEERING JUDGMENT IN THE HRA .....	E-25
E4.2.1 Role of HRA Team Judgment .....	E-25
E4.2.1.1 HRA Team .....	E-26
E4.2.2 Role of Subject Matter Expert Judgment .....	E-27
E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES .....	E-29
E5.1 TERMINOLOGY .....	E-29

**CONTENTS (Continued)**

	<b>Page</b>
E5.1.1 Classification of HFEs .....	E-29
E5.1.1.1 Temporal Phases of HFEs .....	E-30
E5.1.1.2 Error Modes .....	E-31
E5.1.1.3 Human Failure Type .....	E-31
E5.1.1.4 Informational Processing Failures .....	E-31
E5.1.2 Personnel Involved in ISO Operations .....	E-32
E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES .....	E-33
E6 ANALYSIS .....	E-34
E6.0 OVERVIEW OF THE HRA ANALYSIS .....	E-34
E6.1 DESCRIPTION OF INTRA-SITE OPERATIONS BASE CASE SCENARIOS .....	E-37
E6.1.1 Site Transportation Activities .....	E-37
E6.1.1.1 Railcar with Transportation Cask .....	E-38
E6.1.1.2 Truck Trailer with Transportation Cask .....	E-39
E6.1.2 Aging Facility Operations .....	E-39
E6.1.2.1 Site Transporter Movement of an Aging Overpack (TAD canisters and DPCs) .....	E-41
E6.1.2.2 Transportation and Positioning of the HTC or HSTC .....	E-42
E6.1.2.3 Canister Operations at the HAM .....	E-42
E6.1.3 Low-Level Waste Facility Activities .....	E-44
E6.1.4 Balance of Plant Facility Activities .....	E-44
E6.2 ANALYSIS OF INTRA-SITE HUMAN FAILURE EVENTS .....	E-45
E6.2.1 HFES Common to Multiple Operations .....	E-45
E6.2.2 HFE Descriptions and Preliminary Analysis .....	E-46
E6.3 HUMAN FAILURE EVENTS REQUIRING DETAILED ANALYSIS .....	E-51
E7 RESULTS: HUMAN RELIABILITY ANALYSIS DATABASE .....	E-51
E8 REFERENCES .....	E-53
E8.1 DESIGN INPUTS .....	E-53
E8.2 DESIGN CONSTRAINTS .....	E-55
APPENDIX E.I RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA .....	E-56
APPENDIX E.II GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS .....	E-57
APPENDIX E.III PRELIMINARY (SCREENING) QUANTIFICATION PROCESS FOR HUMAN FAILURE EVENTS .....	E-58
APPENDIX E.IV SELECTION OF METHODS FOR DETAILED QUANTIFICATION .....	E-63
APPENDIX E.V HUMAN FAILURE EVENTS NAMING CONVENTION .....	E-68

## FIGURES

	<b>Page</b>
E6.0-1. Movement of Waste Forms through the GROA.....	E-36
E.I-1. Incorporation of Human Reliability Analysis within the PCSA.....	E-56
E.II-1 Post Initiator Operator Action Event Tree.....	E-57
E.V-1. Basic Event Naming Convention.....	E-68



**TABLES**

	<b>Page</b>
E3.3-1. Formulae for Addressing HFE Dependencies .....	E-20
E3.4-1. Lognormal Error Factor Values .....	E-21
E6.0-1. Correlation of Intra-Site Operations to ESDs and HAZOP Evaluation (PFD) Nodes .....	E-35
E6.2-1. Descriptions and Preliminary Analysis for Intra-Site HFEs.....	E-47
E6.2-2. Vendor Vehicle Collision Data.....	E-49
E6.2-3. Vendor Vehicle Crash Factors Mitigated by Escorting .....	E-50
E7-1. HFE Data Summary .....	E-51
E.III-1. Examples of Information Useful to HFE Quantification.....	E-58
E.III-2. Types of HFEs .....	E-61
E.IV-1. Comparison between NPP and YMP Operations .....	E-64
E.V-1. Human Failure Event Type Codes and Failure Mode Codes .....	E-69

## ACRONYMS AND ABBREVIATIONS

### Acronyms

ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event Analysis
BOP	balance of plant
CBDT	Cause-Based Decision Tree
CRCF	Canister Receipt and Closure Facility
CREAM	Cognitive Reliability and Error Analysis Method
CSNF	commercial spent nuclear fuel
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EFC	error forcing context
EOC	error of commission
EOO	error of omission
EPC	error-producing condition
EPRI	Electric Power Research Institute
ESD	event sequence diagram
GROA	geologic repository operations area
HAM	horizontal aging module
HAZOP	hazard and operability
HCR	Human Cognitive Reliability
HCTT	cask tractor and cask transfer trailer
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HSTC	horizontal shielded transfer cask
HTC	a transportation cask that is upended using a tilt frame
INPO	Institute of Nuclear Power Operations
ISFSI	independent spent fuel storage installation
LIS	Licensing Information Service
LLW	low-level radioactive waste
LLWF	Low-Level Waste Facility
MLD	master logic diagram

---

**ACRONYMS AND ABBREVIATIONS (Continued)**

MAUD	Multi-Attribute Utility Decomposition
MERMOS	Methode d'Evaluation de la Relisation des Missions Operateur pour la Surete
NARA	Nuclear Action Reliability Assessment
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
PCSA	preclosure safety analysis
PFD	process flow diagram
PRA	probabilistic risk assessment
PSF	performance-shaping factor
RF	Receipt Facility
SHARP	Systematic Human Action Reliability Procedure
SLIM	Success Likelihood Index Method
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SPM	site prime mover
TAD	transportation, aging, and disposal
THERP	Technique for Human Error Rate Prediction
TRC	Time-Reliability Correlation
TTC	transportation casks that are upended using a tilt frame
VTC	a transportation cask that is upended on a railcar
YMP	Yucca Mountain Project

## **E1 INTRODUCTION**

This document describes the work scope, definitions, terms, methods, and analysis for the human reliability analysis (HRA) task of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA) reliability assessment.

The HRA task identifies, models, and quantifies human failure events (HFEs) postulated in the PCSA to assess the impact of human actions on event sequences modeled in the PCSA. The HFEs evaluated and quantified by this task are identified during the following activities:

- Initiating event identification and grouping
- Event sequence development and categorization
- System analysis
- Sequence quantification and uncertainty analysis.

The HRA task ensures that the HFEs identified by the other tasks (e.g., hazard and operability (HAZOP) evaluation, event sequence diagram (ESD) development, event tree analysis, fault tree analysis) are quantified with HRA techniques. The ESD finding is that the human-induced initiating events dominate the HRA. No post-initiator human actions have been credited in this analysis. The HRA task also ensures that modeled HFEs are appropriately incorporated into the PCSA and provides appropriate human error probabilities (HEPs) for all modeled HFEs. It is important to note that YMP operations differ from those of traditional nuclear power plants (NPPs), and the HRA analysis reflects these differences; Appendix E.IV of this analysis provides further discussion on these differences and how they influenced the choice of methodology.

### **E1.1 SUMMARY**

The HRA was carried out using a nine-step process that is derived from A Technique for Human Event Analysis (ATHEANA) (Ref. E8.1.23):

1. Define the scope of the analysis.
2. Describe the base case progression of actions and responses that constitute successful completion of the operations being evaluated (base case scenarios).
3. Identify and define HFEs of concern.
4. Perform preliminary (screening) analysis and identify HFEs requiring detailed analysis.
5. Identify potential vulnerabilities for the HFEs requiring detailed analysis.
6. Search for HFE scenarios (i.e., scenarios of concern).
7. Quantify probabilities of HFEs.

8. Incorporate HFEs into the PCSA.
9. Evaluate HRA/PCSA results and iterate with design.

After the scope was defined, the activities within the Intra-Site Operations scope were identified and base case scenarios were defined that described in detail the normal operations for each activity. Once the operations were defined and the base cases were documented, HFEs were identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and Engineering and Operations personnel, met and discussed the design and operations in order to appropriately model the human interface. This process consisted of the HAZOP evaluation, master logic diagram (MLD) and event sequence development, fault tree and event tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the model. The iteration with the event sequence and system reliability analysis also identified HFEs of potential concern. HFEs identified include both errors of omission (EOOs) and errors of commission (EOCs).

Included in this process was an extensive information collection process where the human reliability analysts reviewed industry data and interviewed subject matter experts to identify potential vulnerabilities and HFE scenarios.

The result of this identification process was a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then became the error forcing context (EFC) for a specific HFE. Additions and refinements to these initial EFCs were made during the preliminary and detailed analyses.

A preliminary, or screening-type, analysis was then performed to preserve HRA resources so that detailed analyses can be focused on only the most risk-significant HFEs. The preliminary analysis included verification of the validity of HFEs included in the initial PCSA model, assignment of a conservative screening value to each HFE, and verification of preliminary values. The actual quantification of preliminary values was a six-step process that is described in detail in Appendix E.III of this analysis. Once the preliminary values were assigned, the PCSA model was quantified (initial quantification), and HFEs were identified for detailed analysis if: (1) the HFE was a risk-driver for a dominant sequence, and (2) using the preliminary values, that event sequence was above Category 1 or 2 according to the 10 CFR 63.111 (Ref. E8.2.1) performance objectives. The remaining HFEs retained their preliminary values. While most of the activities associated with preliminary analysis were tedious and time-consuming, extra care was taken to perform these tasks conscientiously since the results of the initial quantification were used to identify which HFEs require detailed analysis. For this analysis, preliminary values proved to be sufficient to demonstrate compliance with the performance objectives of 10 CFR 63.111; therefore, no detailed analyses were required for this HRA.

For the preliminary analysis, HFEs were modeled at a high level in order to reduce dependencies that arise from modeling detailed actions. In addition, uncertainties were accounted for by assigning a lognormal distribution and applying an error factor of 3, 5, or 10 to the distribution, depending on the mean value of the final HEP.

To aid the reader in linking the HRA with other parts of the PCSA, Section E6.0.1 provides an overview of the Intra-Site Operations and provides a map which links this analysis back to the MLD, the event sequence diagram (ESD), and the HAZOP evaluation.

## **E2 SCOPE AND BOUNDARY CONDITIONS**

### **E2.1 SCOPE**

The scope of the HRA is established in order to focus the analysis on the issues pertinent to the goals of the overall PCSA. Thus, the scope is as follows:

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers.
2. Pursuant to the above, the following types of HFEs are excluded:
  - A. HFEs resulting in standard industrial injuries (e.g., falls)
  - B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount
  - C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.
3. The identification of HFEs is restricted to those areas of the site or facility that handle waste forms and only during the times that waste forms are being handled (e.g., HFEs are not identified for site transportation activities during the movement of empty transportation casks).
4. The exception to #3 is that system-level HFEs are considered for support systems when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.
5. Recovery post-initiator actions (as defined in Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.
6. In accordance with Section 1 (boundary conditions of the PCSA), initiating events associated with conditions introduced in structures, systems, and components (SSCs) before they reach the site are not, by definition of 10 CFR 63.2 (Ref. E8.2.1), within the scope of the PCSA nor, by extension, within the scope of the HRA.

## E2.2 BOUNDARY CONDITIONS

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

- Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior (i.e., deliberate acts of sabotage and the like) are not considered in this task.
- Facility personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard operating procedures is made because employees believe their actions to be more efficient or because they believe the action as stated in the procedure to be unnecessary.
- Since the YMP is currently in the design phase, facility-specific information and operating experience is generally not available. Instead, similar operations involving similar hazards and equipment are reviewed to establish surrogate operating experience to use in the qualitative analysis. Examples of reviewed information would include spent nuclear fuel (SNF) handling at reactor sites having independent spent fuel storage installations (ISFSIs), chemical munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the geologic repository operations area facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.
- The facility is initially operating under normal conditions and is designed to the highest quality human factors specifications. The level of operator stress is optimal unless otherwise noted in the analysis.
- In performing the operations, the operator does not need to wear protective clothing unless the operation is similar to those performed in other comparable facilities where protective clothing is required.
- The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are experienced and have functioned in their present positions for a sufficient amount of time to be proficient.
- The environment inside each facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made

regarding optimal weather and road conditions. YMP personnel are required to stop work if conditions are perceived to be unsafe.

- Personnel involved with the facility operations are expected to have the proper training commensurate with nuclear industry standards. As appropriate, this training is followed by a period of observation until the operator is proficient.
- While all personnel are trained to procedures, and procedures exist for all work required, the direct presence and use of procedures (including checklists) during operation is generally restricted to actions performed in the control room. Workers performing skill-of-craft operations do not carry written procedures on their person while performing their activities.

These factors are evaluated qualitatively for each situation being analyzed.

## **E3 METHODOLOGY**

### **E3.1 METHODOLOGY BASES**

The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in the American Society of Mechanical Engineers (ASME RA-S-2002, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. E8.1.3)) and incorporates the guidance provided by the U.S. Nuclear Regulatory Commission (NRC) in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. E8.1.24).

### **E3.2 GENERAL APPROACH**

The HRA consists of several steps, that follow the intent of ASME RA-S-2002 (Ref. E8.1.3) and the process guidance provided in *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.23). Detailed descriptions of each HRA step are provided in the following subsections to summarize the processes used by the analysts. The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt the material based on NPPs to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. E8.1.23). Further discussion on information collection and use of expert judgment in this process can be found in Section E4.

HFE probabilities produced in this analysis are mean values. The HEPs are modeled as a lognormal distribution, where the error factors are defined based on the method presented in Section E3.4.

#### **E3.2.1 Step 1: Define the Scope of the Analysis**

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



### **E3.2.2 Step 2: Describe Base Case Scenarios**

In this step, the base case scenarios are defined and characterized for the operations being evaluated. In general, there is one base case scenario for each operation included in the model. The base case scenario:

- Represents the most realistic description of expected facility, equipment, and operator behavior for the selected operation.
- Provides a basis from which to identify and define deviations from such expectations (Step 6).

In the ideal situation (which is seldom achieved), the base case scenario:

- Has a consensus operator model<sup>1</sup>
- Is well-defined operationally
- Has well-defined physics
- Is well-documented in public or proprietary references
- Is realistic.

Since operators and “as built, as operated” information are not currently available for YMP, this information is sought from comparable facilities with comparable operations. Documented reference analyses (e.g., engineering analyses) can assist in defining the scenario from the standpoint of physics and operations. The reference analyses may need to be modified to be more realistic. Expert judgment, engineering documents and applicable industry experience are the keys to defining realistic base case scenarios for YMP operations; Section E4 provides greater detail on how information was collected and the role of subject matter experts in this process.

### **E3.2.3 Step 3: Identify and Define HFEs of Concern**

Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken, or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The classification process is described further in Section E5.1.1. The analyses performed in later steps (i.e., Steps 4 through 7) may identify the need to define an HFE or unsafe action not previously identified in Step 3.

Human errors were identified based upon the three temporal parts generally analyzed by probabilistic risk assessment (PRA) and are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs

---

<sup>1</sup>ATHEANA (Ref. E8.1.23), Section 9.3.1 defines a consensus operator model in the following manner: “Operators develop mental models of plant responses to various PRA initiating events through training and experience. If a scenario is well defined and consistently understood among all operators (i.e., there is a consensus among the operators), then there is a consensus operator model.”

- Post-initiator HFEs<sup>2</sup>:
  - Non-recovery
  - Recovery.

Each of these types of HFEs is defined in Section E5.1.1.1; identification of the HFEs for each temporal phase is described in the following sections.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., PSFs). This combination of conditions and human factor concerns then becomes the EFC for a specific HFE. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses.

### **E3.2.3.1 Identifying Pre-initiator HFEs**

Pre-initiators are identified by the system analysts when modeling fault trees, while performing the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human common-cause failure.

### **E3.2.3.2 Identifying Human-Induced Initiator HFEs**

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the site, facility and SSCs in order to appropriately model the human interface. This iterative process begins with the HAZOP evaluation and MLD development, described and documented in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8), followed by a second iteration during the initial fault tree and event tree modeling, and ending with a third iteration through the preliminary analysis and incorporation of HFEs into the model. Included in this process is an extensive information collection process where industry data was reviewed (Section E4.1) and subject matter experts were interviewed (Section E4.2) to identify potential vulnerabilities and HFE scenarios. HFEs identified include both EOOs and EOCs.

### **E3.2.3.3 Identifying Non-recovery Post-initiator HFEs**

Non-recovery post-initiator HFEs are identified by examining the human contribution to pivotal events in the event tree analysis. The event sequence analysts, with support from the human reliability analysts, identify HFEs that represent the operator's failure to perform the proper action to mitigate the initiating event and/or the unavailability of automatic mitigation functions as called for in the emergency operating procedures or in accordance with their emergency response training. This identification includes all actions required, whether in a control room or locally. Post-initiator EOCs and EOOs are also considered. It should be emphasized that this section presents the methodology that is used to identify non-recovery post-initiator events. However, as shown in Section E6, none of these types of errors have been identified for the

---

<sup>2</sup>Terminology common to NPPs refer to non-recovery post-initiator events as Type C events and recovery events as Type CR events.

Intra-Site operations event sequence and categorization analysis. During the qualitative evaluation, non-recovery post-initiator events were considered and ruled out because it was unnecessary to credit non-recovery actions to demonstrate compliance with the performance objectives stated in 10 CFR 63.111 (Ref. E8.2.1).

#### **E3.2.3.4 Identifying Recovery Post-initiator HFEs**

Recovery actions are of limited relevance to YMP operations and, for conservatism, were not credited in this analysis. Recovery post-initiator HFEs are outside the scope of this analysis (Section E2.1).

#### **E3.2.4 Step 4: Perform Preliminary Analysis and Identify HFEs for Detailed Analysis**

The preliminary analysis is a type of screening analysis used to identify HFEs of concern. A screening analysis is commonly performed in HRA to conserve resources and focus the effort on the subsequent detailed analysis of those HFEs that are involved in the important event sequences. Preliminary values are assigned for the probabilities of HFEs based upon predetermined characteristics of each HFE. This analysis involves the following steps:

- Verification of the validity of HFEs included in the initial PCSA model
- Assignment of conservative preliminary values to all HFEs included in the initial PCSA model
- Verification of assigned preliminary probabilities to all HFEs in the PCSA
- Quantification of the initial PCSA model using preliminary values (i.e., the “initial quantification”)
- Identification of HFEs for detailed analysis.

The human reliability analyst performs the first three of these steps with the assistance of the PCSA quantification task leader, who also performs the last two steps. While most of the activities associated with this preliminary analysis are tedious and time-consuming, it is important to perform these tasks conscientiously since the results of the initial quantification are used to identify those HFEs requiring detailed analysis.

Analysts must strike a balance between conservatism and too much conservatism. Using too conservative a value for an HEP can overemphasize the importance of an HFE in the sequence quantification, perhaps masking a significant component failure event. By contrast, using a less conservative preliminary HEP may lead to inappropriately screening out a potentially significant event sequence. Instead of the usual screening process used in PRA, where relatively high screening values of 1.0 or 0.1 for an HEP are often inserted in initial fault tree and event sequence quantification, the PCSA applies an intermediate process where conservative preliminary values are assigned based on the context and failure modes of the HFE. Appendix E.III of this analysis provides specific details on guidelines for preliminary quantification.

Depending on the results obtained with the preliminary quantification, the event sequence and human reliability analysts may conclude that the preliminary results are sufficient for event sequence quantification and that a detailed analysis would not provide a better basis for event sequence categorization or more insights into the human factors issue for a particular waste handling operation. The preliminary quantification process is based on a characterization of each human action with respect to complexity and operational context using a judgment-based approach consisting of the following subtasks:

1. Complete the “lead-in” initial conditions required for quantification.
2. Identify the key or driving factors of the scenario context.
3. Generalize the context by matching it with generic, contextually anchored rankings or ratings.
4. Discuss and justify the judgments made in subtask 3.
5. Refine HFEs, associated contexts, and assigned HEPs.
6. Determine final preliminary HEPs for each HFE and associated context. These HEPs are then entered into the PRA logic structure to see which HFEs call for more detailed evaluation. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a given sequence, and (2) using the preliminary values, that sequence falls in a category (i.e., a Category 1 or Category 2) such that it does not meet 10 CFR 63.111 performance objectives (Ref. E8.2.1).

Appendix E.III of this analysis defines and provides technical bases for the HEP preliminary values recommended to be used in the YMP PRA for different categories of HFEs, depending on the general HFE characteristics. Section E4.2 provides a list of experts used in this process.

### **E3.2.5 Step 5: Identify Potential Vulnerabilities**

This information collection step defines the context for Step 6 in which scenarios that deviate from the base case are identified. In particular, analysts search for potential vulnerabilities in the operators’ knowledge and information base for the initiating event or base case scenario(s) under study that might result in the HFEs and/or unsafe actions identified in Step 4. Potential traps<sup>3</sup> inherent in the ways operators may respond to the initiating event or base case scenario are identified through the following:

- Investigation of potential vulnerabilities in operator expectations for the scenario
- Understanding of the base case scenario time line and any inherent difficulties associated with the required response
- Identification of operator action tendencies and informal rules

---

<sup>3</sup>A “trap” is a human failure that is encouraged or enabled by the existence of a specific vulnerability. That is, vulnerabilities influence operators to fall into particular traps.

- Evaluation of formal rules and operating procedures expected to be used in the scenario.

The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). Section E4 provides a description of the information types that comprise this knowledge base.

### **E3.2.6 Step 6: Search for HFE Scenarios**

In this step, the analyst must identify deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). These deviations are referred to as HFE scenarios. In serious accidents, these HFE scenarios are usually combinations of various types of unexpected conditions (which form the EFC).

The principal method for identifying HFE scenarios is a HAZOP evaluation-like search scheme, coupled with a means for relating scenario characteristics with error mechanisms for each stage in the information processing model (Ref. E8.1.1). The result of such a search is a description of the HFE scenarios, including system and equipment conditions, along with any resident or triggered human factor concerns (e.g., PSFs). Again, this combination of conditions and human factor concerns then becomes the EFC for a specific HFE. As defined by the ATHEANA document (Ref. E8.1.23), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. (Additions and refinements to this initial EFC are likely in later steps of the process).

### **E3.2.7 Step 7: Quantify Probabilities of HFEs**

As shown in Section E6, no HFEs requiring detailed analysis have been identified for the Intra-Site Operations event sequence and categorization analysis. Therefore, only a general summary of the methodology associated with detailed quantification is presented here.

Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 (Ref. E8.2.1) after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9, Section E3.2.9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CFR 63.111 (Ref. E8.2.1). The qualitative analysis in steps 3, 5, and 6 sets the stage for the detailed quantification by providing the accident progression(s) for a given HFE and its context. Specifically, the qualitative analysis provides a list of unsafe actions, along with their context, characteristics, and classification (i.e., EOO or EOC). For each unsafe action, the following steps are performed:

1. Qualitative analysis (e.g., identification of PSFs, definitions of important characteristics of the given unsafe action, assessment of dependencies)
2. Selection of a quantification model

3. Quantification
4. Verification that HFE probabilities are appropriately updated in the PCSA database.

There are four HRA methods that have been selected for this quantification:

1. CREAM (Basic and Extended)—*Cognitive Reliability and Error Analysis Method, CREAM* (Ref. E8.1.19)<sup>4</sup>
2. HEART/NARA - “HEART - A Proposed Method for Assessing and Reducing Human Error” (Ref. E8.1.28) and *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.9)
3. THERP (with some modifications)—*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Ref. E8.1.27).

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

4. ATHEANA’s expert elicitation approach—*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.23).

Appendix E.IV of this analysis provides a discussion why these specific methods were selected for quantification, as well as a discussion of why some methods, deemed appropriate for HRA of NPPs, are not suitable for application in the PCSA. This discussion summarizes the main differences between NPPs and repository operations with respect to contexts and failure modes that affect potential HFEs. It also gives some background about when a given method is applicable based on the focus and characteristic of the method.

### **E3.2.8 Step 8: Incorporate HFEs into PCSA**

After HFEs are identified, defined, and quantified, they must be incorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. E8.1.23) provides an overview of the state-of-the-art method for performing this step in PRAs. This process is done in conjunction with the PCSA analysts. Appendix E.I of this analysis provides the recommended approach for incorporation of human errors in the YMP PCSA, and Appendix E.V of this analysis provides the recommended naming conventions for HFEs incorporated in the fault tree models.

HFEs are incorporated, in the form of basic events, into the fault trees that support the initiating event and pivotal events of event trees. The HEP that is entered in a basic event is modeled as a lognormal distribution, whose mean value is the nominal value of the HEP, to which an error factor is assigned (Section E3.4) to reflect the uncertainty in the probability estimate. In many cases, the equipment failures and the associated HFEs are calculated as part of an integrated

---

<sup>4</sup>Extended CREAM (Ref. E8.1.19) creates a link between CREAM and HEART (Ref. E8.1.28), and enhances the ability of CREAM to quantify skill-based HFEs.

HRA. The resulting probability of both equipment and human failures is then placed in the fault tree as a single basic event. Because preliminary values were sufficient to demonstrate compliance, this iteration was unnecessary for Intra-Site operations.

### **E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design**

This last step in HRA is performed each time the PCSA is quantified. The primary results are the HFEs in dominant cut sets and the associated qualitative inputs to such HFEs. Potential “fixes” to the design or operational environment can be supported by these results.

Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is noncompliant with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1) because the probability of a given HFE dominates the probability of the event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or to completely eliminate the HFE. In such cases, the modification is analyzed for potential new HFEs, and the applicable HFEs are requantified, along with the event sequences.

## **E3.3 DEPENDENCY**

Dependency between human actions is defined to exist when the outcome of a particular human action is related to the outcome of a prior human action or actions. According to THERP (Ref. E8.1.27), the joint probability of human error for a set of dependent human actions is higher than if they were independent.

The possibility of dependencies between human actions and defined HFEs is recognized throughout the HRA task. The concern with respect to dependencies is that the joint probabilities separately assigned to a set of dependent HFEs treated as independent actions can result in a lower event sequence frequency than would result if dependencies among the HFEs were appropriately recognized and treated. This situation is especially important in the HRA activities leading up to and including preliminary analysis where an inappropriately low HEP might lead to an inappropriate screening out of a potentially significant cut set or event sequence. If dependence were properly identified and treated, the resulting HEP might then appear in dominant cut sets and, therefore, be identified for detailed analysis.

### **E3.3.1 Capturing Dependency**

Dependencies between defined HFEs can exist for two reasons:

- Due to the characteristics of the event sequence in which the HFEs are modeled
- Due to the modeling style, especially the degree of decomposition, in HFE definition.

In the first case, dependencies are unavoidable due to the inherent characteristics of the initiator type or event sequence. In the second case, dependencies can be avoided by redefining dependent HFEs into a single HFE. In either case, dependencies can be treated by using a structured method for adjusting probabilities to account for dependencies. However, some HRA quantification methods (e.g., ATHEANA (Ref. E8.1.23)) account for certain types of

dependencies within their formulation by combining dependent events as part of the normal process of addressing the accident scenario as a whole. These methods do not require additional treatment.

All event sequences that contain multiple HFEs are examined for possible dependencies. For the preliminary analysis, HFEs are modeled at a high level where several subtasks are combined into a single task so that explicit consideration of dependencies between subtasks is eliminated. For a detailed assessment, where the various actions that constitute an HFE are explicitly quantified, dependencies are explicitly addressed using the formulae in Table E3.3-1 from THERP (Ref. E8.1.27), where N is the independently derived HEP. The THERP dependency model was selected for its formalism and reproducibility. The model itself is not dependent on what the source of the baseline (i.e., independent) HEP is; it can be obtained from any existing model or from expert elicitation. None of the other “objective” quantification approaches used (i.e., HEART (Ref. E8.1.28)/NARA (Ref. E8.1.9) or CREAM (Ref. E8.1.19) has its own dependency model, and NARA (Ref. E8.1.9) specifically endorses the use of the THERP (Ref. E8.1.27) approach.

Table E3.3-1. Formulae for Addressing HFE Dependencies

Level of Dependence	Zero	Low	Medium	High	Complete
Conditional Probability	N	$\frac{1 + 19N}{20}$	$\frac{1 + 6N}{7}$	$\frac{1 + N}{2}$	1.0

Source: Modified from Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278 (Ref. E8.1.27, Table 20-17, p. 20-33).

### E3.3.2 Sources of Dependency

The determination of the level of dependence between HFEs is left to the judgment of the HRA analyst. Certain factors typically are recognized as indicators of dependency. Examples of such factors are:

- Common time constraints for task performance
- Common cues or indicators for task performance
- Common diagnosis of situation
- Common facility function or system operation involved in task performance
- Common procedure steps for task performance
- Common personnel and location for task performance
- Common PSFs.

In addition, any human-induced failures of equipment that can directly or indirectly cause other equipment to fail through equipment dependencies are also identified as human dependencies.

### E3.4 UNCERTAINTY

As with the values of failure probabilities used for active and passive components used in other parts of the PCSA, it is important that HFE quantification accounts for uncertainty. The HRA quantification, therefore, provides a mean HEP and an expression of the uncertainty. There are a



number of ways to approach this task, as each of the HRA methods discussed in Section E3.2.7.2 provides recommendations on uncertainty parameters or bounds for HEPs. These recommendations run from the specific to the general and are often inconsistent. After a review of various recommendations, the HRA team has determined that to use any of them in their specific applications is both impractical and questionable. Rather, it was decided to develop a simple set of generic error factors developed through the use of the judgment by the HRA team, based on a holistic overview of the various recommendations presented in the following sources:

- Section 6 of NARA (Ref. E8.1.9)
- HEART (Ref. E8.1.28)
- Chapter 9 of CREAM (Ref. E8.1.19)
- Chapter 20 of THERP (Ref. E8.1.27).

Although ATHEANA (Ref. E8.1.23) does not provide specific recommendations regarding uncertainty estimation, it stresses that it is important to consider uncertainty in HRAs and that one way to approach it is through the use of expert judgment. To this extent, it can be said that the approach follows the guidance established in ATHEANA.

After review and due consideration of the uncertainty recommendations, the HRA team determined that for the purposes of this study it would be both reasonable and acceptable to establish a generic set of uncertainty parameters based on the calculated (total) HEP for any given HFE. The HRA team reached a consensus on the following error factor values to be applied to a lognormal distribution based on the mean HEP, as shown in Table E3.4-1. For each HEP range, the error factor reflects the HRA team's degree of confidence in the probability estimate.

Table E3.4-1. Lognormal Error Factor Values

Calculated Mean HEP	Lognormal Error Factor
≥ 0.05	3
>0.0005–<0.05	5
≤0.0005	10

NOTE: HEP = human error probability.

Source: Original

The same error factors are applied to both preliminary values and results of detailed HRAs. Therefore, after the HRA team has decided on an appropriate mean value, the corresponding generic error factor is assigned unless there is a basis from the detailed analysis to do otherwise.

### **E3.5 DOCUMENTATION OF RESULTS**

The following information is included in the documentation of the results for the YMP PCSA HRA:

- General discussion of the overall set of PSFs (e.g., error-producing conditions (EPCs), common performance conditions) on human performance that are applicable to or especially important for the YMP PCSA and how they apply to the operations of the facility in question
- A list of all HFEs (by basic event name and category, along with a brief description of the HFE) included in the PCSA model, with their final assigned HFE probabilities
- Identification of preliminary values used for these HFEs
- Identification of all expected pertinent procedures or, if no procedures are expected to exist, alternative evidence that supports the identification and quantification of HFEs and recoveries or substantiates the likelihood of human actions (e.g., normal operating practices, formal training)
- References to sources of input information (e.g., thermal-hydraulic calculations) used in detailed quantification
- Results of qualitative and preliminary analysis

The following information is generally included in the documentation of the results for the YMP PCSA HRA, but it is not applicable to the Intra-Site Operations HRA:

- Identification of the HFEs analyzed in detail
- A more detailed description of each HFE analyzed in detail
- For each HFE analyzed in detail, identification of the quantification method, associated input parameters (e.g., PSFs), and any approximations or required procedural controls used to determine probabilities for that HFE
- Results of detailed quantitative analysis.

### **E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT**

This section addresses how and what information was collected to support the HRA analysis and how expert judgment was used in the identification and quantification of HFEs.

## **E4.1 FACILITY FAMILIARIZATION AND INFORMATION COLLECTION**

### **E4.1.1 General Information Sources**

As with all of the tasks in the PCSA, facility information is required to support the HRA steps. In addition to the information that is gathered to support the other modeling tasks (e.g., initiating events, systems), the analysts obtain specific additional information that is needed to support the HRA task.

Since the YMP is in the design phase, there are limits on facility-specific information available to support the HRA. Sources utilized in this analysis include the following:

- Design drawings and design studies
- Concept of operations documents
- Engineering calculations
- Discussions of event sequences with knowledgeable individuals
- Event trees and supporting documentation
- Fault trees and supporting documentation.

Information from similar facilities is used, including NPPs (particularly those with ISFSIs), chemical agent disposal facilities, and any other facilities whose primary function includes handling and disposal of very large containers of hazardous material. This was conducted primarily for ISFSI activities at NPPs. The use of this information in place of YMP plant-specific information is pursuant to the third analytical boundary condition specified in Section E2.2. The following are sources of information from ISFSI that are applied to support the YMP PCSA:

- Interviews with plant operators, operations personnel, and/or other ISFSI knowledgeable personnel
- Pertinent ISFSI procedures (e.g., operating procedures, test and maintenance procedures)
- Plant walk-downs (e.g., at locations where operations similar to those at repository may be performed) and operations reviews
- Studies, including PRAs and HRAs, conducted at these facilities that would substitute for the previously mentioned sources.

This information was acquired from two sources. First, information was obtained by the HRA team from outside sources specifically for use on the YMP, such as from NPPs, industry organizations, and governmental sources. Some of this information may have been obtained directly by the HRA team or may have been provided to the HRA team by members of the Licensing and Nuclear Safety, Engineering, or Operations departments who had obtained the information as a part of their regular duties on the YMP (Section E4.2.2). Second, information was obtained by the HRA team directly from internal sources, including members of the aforementioned departments who had past experience and information on ISFSIs from prior employment and projects before joining the YMP (Section E4.2.1).

Initially, information is gathered to support the identification of pre-initiator, human-induced initiator, and non-recovery post-initiator HFEs. This information is needed to:

- Identify test and maintenance activities performed for equipment included in the PCSA model
- Determine the frequency of test and maintenance activities
- Identify the procedures used to perform test and maintenance activities
- Determine what equipment is impacted by test and maintenance activities.

For human-induced initiator and post-initiator HFEs, such information is needed to:

- Identify important operator tasks
- Identify the specific actions required for each operator task
- Identify the procedures (e.g., normal operating and emergency operating procedures) and procedure steps associated with each operator task
- Identify the cues (e.g., procedure steps, alarms) for operator tasks
- Assess the procedures that support operator tasks as PSFs
- Assess the training that supports operator tasks as PSF.

#### **E4.1.2 Industry Data Reviewed by the HRA Team**

The following sources of industry data were reviewed by the HRA team for potential vulnerabilities and HFE scenarios applicable to the YMP:

- "Summary Tables." *Large Truck Crash Causation Study*. (Ref. E8.1.14)
- "Speeding Counts...on All Roads!" (Ref. E8.1.11)
- *Traffic Safety Facts 2002: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System* (Ref. E8.1.13)
- *Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report* (Ref. E8.1.12)
- *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*, NUREG-1774 (Ref. E8.1.20)
- *Control of Heavy Loads at Nuclear Power Plants*, NUREG-0612 (Ref. E8.1.21)

- Navy Crane Center, Naval Facilities Engineering Command Internet Web Site. The database includes the following information:
  - Navy Crane Center Quarterly Reports (“Crane Corner”) 2001 through 2007
  - Fiscal Year 06 Crane Safety Report (covers fiscal years 2001 through 2006)
  - Fiscal Year 06 Audit Report
- U.S. Department of Energy (DOE) Operational Experience Summary (2002 through 2007) (<http://www.hss.energy.gov/CSA/analysis/orps/orps.html>).
- Institute of Nuclear Power Operations (INPO) database (<https://www.inpo.org>). The INPO database contains the following information:
  - Licensee Event Reports
  - Equipment Performance and Information Exchange System
  - Nuclear Plant Reliability Data System.
- *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)* (Ref. E8.1.4)
- All Scientech/Licensing Information Service data on ISFSI events (1994 through 2007) Scientech LIS Database and Dry Storage Information Forum (New Orleans, LA, May 2-3, 2001). This database includes the following information:
  - Inspection reports
  - Trip reports
  - Letters, etc.

## **E4.2 USE OF EXPERTS AND ENGINEERING JUDGMENT IN THE HRA**

Subject matter experts were employed in the identification, verification, preliminary analysis, and detailed analysis of HFEs. Identification of HFEs, of which a HAZOP evaluation was a part, was performed as a combined effort by experts from a wide range of areas. This identification was not specifically a part of the HRA task, but it was used by the HRA team in the process of identifying HFEs. A description of the HAZOP evaluation process and a list of experts who specifically participated in the HAZOP evaluation is provided in the *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8).

### **E4.2.1 Role of HRA Team Judgment**

Preliminary and detailed analyses were primarily performed by the HRA team in a consensus-based process. For the preliminary analysis, the judgment process can be summarized in the following fashion:

- Each HFE that was identified during the HAZOP evaluation and the operational experience review was characterized with input from the Engineering and Operations departments, including the context under which the HFE would occur.

- Once the individual members of the HRA team were confident that they understood the HFE and the context, they each independently assigned an HEP to the HFE and briefly documented the rationale relative to a set of anchor points established for the HRA (the basic anchor points can be found in Appendix E.III of this analysis).
- The values and rationales were combined into a single spreadsheet, and the team then met to discuss their values.
- The HRA team used their knowledge of the preclosure process and design to develop a consensus on the factors affecting the HFE and a resulting conservative estimate of the HEP. In most cases, the HRA team ultimately reached a consensus on a value and a rationale. In a few cases a consensus could not be reached, and the most conservative value and rationale from that HRA team member was used. The value and rationale applied was then documented.

This process is explained in much greater detail in Appendix E.III of this analysis.

As shown in Section E6, no HFEs requiring detailed analysis have been identified for Intra-Site Operations event sequence and categorization analysis. Therefore, the judgment process associated with detailed quantification is not relevant in this case.

#### **E4.2.1.1 HRA Team**

**Paul J. Amico**—Mr. Amico is a nuclear engineer with 30 years of experience in risk, safety, regulation, and operation of NPPs, nuclear material production reactors, nuclear weapons research, production and storage facilities, nuclear fuel cycle facilities, chemical demilitarization facilities, and industrial chemical plants. He has been involved in the conduct and review of HRA since 1979. His experience includes the use of THERP, Time-Reliability Correlation (TRC), Systematic Human Action Reliability Procedure (SHARP), Human Cognitive Reliability (HCR), HEART, ATHEANA, CREAM and NARA, and he has been involved in projects related to methodology enhancements to some of these techniques. Prior to joining the YMP, he was involved in HRA for a number of NPP PRAs in the United States and overseas; for chemical process plants; and for SNF handling and storage at NPPs, including the development of project procedures for HRA. He developed a phased approach to the use of HRA during the design process of advanced NPPs and supported a project to expand HRA techniques for SNF handling operations.

**Erin P. Collins**—Ms. Collins is a risk analyst with over 20 years of experience in safety, reliability, and risk analysis for the U.S. Army chemical weapons destruction program, National Aeronautics and Space Administration, the Federal Aviation Administration, NPPs, and the chemical process industry. Her specialties are equipment reliability database development and HRA. Ms. Collins was a prime participant in a safety hazard analysis of an acrylic fiber spinning facility in northeastern Italy. This analysis evaluated worker risk in various areas of the facility through the use of hazard analysis techniques, including a HAZOP evaluation, and resulted in the recommendation of economical risk reduction measures. Her project experience in Spain includes technical review and support of the HRAs for the Ascó and the Santa Maria de Garoña nuclear plant PRAs. She also supported the review of the Kola and Novovoronesh Russian

nuclear reactor HRAs for the DOE. In the United States, Ms. Collins has participated in PRA-related HRAs of the Hanford N Reactor and the Robinson (using simulator exercises), Crystal River 3, and Catawba NPPs. Throughout these efforts, she has applied the HEART, CREAM, THERP, and TRC methods of quantification.

**Douglas D. Orvis, Ph.D.**—Dr. Orvis is a registered professional engineer (California, Nuclear No. 0925) with over 35 years of experience in nuclear engineering, regulation, and risk analysis of NPPs, alternative concepts for interim storage of SNF, and aerospace applications. Dr. Orvis has participated in the development of HRA techniques (e.g., SHARP for Electric Power Research Institute (EPRI), effects of organizational factors for the NRC) and has measured and analyzed data for evaluating the reliability of NPP control room operators during simulated accidents. These data-based analyses included the EPRI-sponsored Operator Reliability Experiments (ORE) (e.g., measurements performed at the Diablo Canyon, Kewaunee, and LaSalle simulators) and the follow-on programs performed at the Maanshan (Taiwan) simulator. Data collection and analysis included observing operator behavior, variability between crews, developing time-response correlations for key operator actions, and evaluating the numbers and kinds of errors and deviations committed. Postsimulation interviews with crew members and trainers were conducted to elicit information on conditions and factors that contributed to crew performance. The data analysis included comparisons of data to the HCR model and a statistical evaluation of the types and causes of errors and deviations. A similar data collection evaluated the efficacy of an expert system called the Emergency Operating Procedures Tracking System.

Dr. Orvis participated in a comprehensive review of HRA methods for a Swiss agency and was a consultant to the International Atomic Energy Agency to incorporate concepts of HRA and organizational factors into (Assessment of the Safety Culture in Organizations Team) guidelines for plant self-assessment of safety culture. Dr. Orvis has performed event tree and fault tree analyses of hazardous systems for both internal events and seismic initiators that included consideration of HRA. Dr. Orvis has participated in HAZOP evaluation sessions for repository operations.

**Mary R. Presley**—Ms. Presley is an engineer with 3 years of experience in risk analysis for NPPs, specializing in human reliability. Ms. Presley graduated in 2006 from the Massachusetts Institute of Technology with her M.S. in nuclear engineering, where she wrote her thesis *On the Assessment of Human Error Probabilities for Post Initiating Events*, which included an extensive review of current HRA methods. While her work focused on the EPRI HRA calculator and the NRC ATHEANA framework, she is also familiar with other HRA methods, including THERP, Accident Sequence Evaluation Program (ASEP), HEART, NARA, Failure Likelihood Index Methodology (FLIM), Success Likelihood Index Method/Multi-Attribute Utility Decomposition (SLIM/MAUD), Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H), CREAM, Methode d’Evaluation de la Relisation des Missions Operateur pour la Surete (MERMOS), Cause-Based Decision Tree (CBDT), and HCR/ORE.

#### **E4.2.2 Role of Subject Matter Expert Judgment**

Subject matter experts were also consulted during the compilation of the base case scenarios. The outline of the base case scenarios came from the mechanical handling block flow diagram. The details of human interaction with the mechanical systems were derived from expected

operations inferred directly from the design by the subject matter experts. Where a detailed design was not available, the experts extrapolated these details from common industry practice for similar operations. These experts come from the YMP engineering, operations, and PCSA groups, as well as from outside the YMP project.

In addition to the development of base case scenarios, subject matter experts were regularly consulted during the analysis to provide clarification of design, clarification of expected operations, and insight into expected operating conditions and failure modes. These experts provided details about the design of systems that were relevant to human performance, such as the presence of job aids and interlocks and the intended design of control system interfaces. They also provided details regarding the concept of operations for the processes, such as the role of the humans versus the use of automatic systems, the operational controls, and the use of procedures. These experts would also review specific parts of the analysis for technical accuracy.

Below is a list of some areas where subject matter experts were consulted during the HRA for their expertise:

- PCSA models (i.e., facility or system fault trees)
- Site prime mover (SPM), railcar, truck trailer, cask tractor and cask transfer trailer (HCTT), and site transporter design and operation
- Crane design—No-single failure proof cranes (i.e., jib cranes designed to NUM-1 Type 1B (Ref. E8.1.2))
- Gas sampling process
- Radiation protection (e.g., cask shielding/shield rings; locks, interlocks, and procedural controls for entering high radiation areas)
- General facility (including aging pad and drifts) layout and time line of operations
- Interlocks (general)
- Design and handling of the following: aging overpacks, horizontal shielded transfer casks (HSTC), transportation casks that are never upended (HTCs), transportation casks that are upended using a tilt frame (TTC) and transportation casks that are upended on a railcar (VTC).
- Horizontal aging module (HAM) design and operation
- Ventilation and inspection of cask on the aging pads
- Other systems



## **E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES**

Over the history of performance of HRAs, certain terminology has become commonplace and different classification schemes for human error has been developed. This section provides a background of this terminology and associates it to the YMP PCSA HRA. In addition, the description of operations includes references to different types of personnel. The functions of each classification of personnel are described in this section. Finally, a discussion is provided of the specific issues that relate to human performance at the YMP.

### **E5.1 TERMINOLOGY**

#### **E5.1.1 Classification of HFEs**

As noted in the methodology (Section E3.2), HFEs are classified to support the HRA preliminary analysis, selection of HRA quantification methods, and detailed quantification. A combination of four classification schemes is used in the YMP HRA. The first three schemes are familiar standards in HRA. The fourth scheme has its basis in behavioral science and has been used in some second-generation HRA methods.<sup>5</sup>

The four classification schemes are based on the following:

1. The three temporal phases used in PRA modeling:
  - A. Pre-initiator
  - B. Human-induced initiator
  - C. Post-initiator
2. Error modes:
  - A. EOOs
  - B. EOCs
3. Human failure types:
  - A. Slips/lapses
  - B. Mistakes
4. Informational processing failures:
  - A. Monitoring and detection
  - B. Situation awareness

---

<sup>5</sup>There is another classification not included here that has been often used in nuclear power plant PRAs: the behavior type taxonomy. This category classifies HFEs into skill-, rule-, or knowledge-type behavior. While this taxonomy has limited usefulness in addressing HFEs that take place in an NPP control room under time constraints, this distinction is not particularly useful for other types of actions. As a result, it is generally not used for HRAs in such applications as chemical process facilities, chemical demilitarization facilities, or National Aeronautics and Space Administration manned-mission risk assessments. Given the type of human actions and HFEs that are important at the YMP, use of this approach for the YMP PCSA HRA is not recommended.

- C. Response planning
- D. Response implementation.

The following sections define these classification methods.

#### **E5.1.1.1 Temporal Phases of HFEs**

There are three temporal phases of HFEs:

- Pre-initiator HFE—An HFE that represents actions taken before the initiating event that causes systems or equipment to be unavailable. Examples of such HFEs are miscalibration of equipment or failure to restore equipment to an operable state after testing or maintenance activities.
- Human-Induced Initiator—An HFE that represents actions that cause or lead to an initiating event.
- Post-initiator HFE<sup>6</sup>—A post-initiator HFE represents those operator failures to manually actuate or manipulate systems or equipment, as required for accident response. Post-initiator HFEs can be further divided into recovery and non-recovery events.
  - A non-recovery post-initiator HFE (i.e., failure during response to an initiator) is when an operator does not operate frontline equipment in accordance with required procedural actions due to errors in diagnosis or implementation. For quantification purposes, these HFEs are usually decomposed into cognitive and implementation parts, as shown in Appendix E.II of this analysis. In general, post-initiator HFEs associated with such actions are incorporated directly in the model prior to initial PRA quantification using preliminary values. The results of the initial event sequence quantification are used to determine if detailed modeling of these HFEs is needed.
  - A recovery post-initiator HFE represents operator failure to manually actuate or manipulate frontline equipment (or alternatives to frontline equipment<sup>7</sup>) that has failed to automatically actuate as required. In general, post-initiator HFEs associated with correction or recovery of failed frontline systems from either equipment or human failures are not modeled until after initial PRA quantification. The results of initial event sequence quantification are used to determine if modeling of such recovery HFEs is needed.

The HRA did not take credit for post-initiator human actions, and no post-initiator HFEs were identified.

---

<sup>6</sup> The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

<sup>7</sup> Alternatives to frontline equipment, include equipment that operators can use for performing the functions of frontline equipment in case of an impossibility to recover the failed frontline equipment in a timely manner.

### **E5.1.1.2 Error Modes**

HFEs can be classified by error mode as either an EOO or EOC. EOOs and EOCs can occur in any temporal phase (i.e., pre-initiator, initiator, or post-initiator). This classification is highly dependent upon the specific event tree or fault tree model. In other words, the same operator action could be modeled as either an EOO (e.g., failed to actuate system x) or an EOC (e.g., actuated system y instead of x). The error mode model is chosen based on consistency with the PCSA model and at the discretion of the HRA analyst. In early PRAs, EOCs were often excluded. Current PRAs, however, address both EOOs and EOCs, although there are still few methods for identifying and quantifying EOCs. In the current analysis, EOO and EOC are defined as follows:

- EOO—An HFE that represents the failure to perform one or more actions that should have been taken and that then leads to an unchanged or inappropriately changed configuration with the consequences of a degraded state. Examples include the failure of a radiation protection worker to perform the radiologic survey before a cask is released from the facility.
- EOC—An HFE that represents one or more actions that are performed incorrectly or some other action(s) that is performed instead. It results from an overt, unsafe action that, when taken, leads to a change in configuration with the consequence of a degraded state. Examples include commanding a crane to lift when it should be lowered.

### **E5.1.1.3 Human Failure Type**

Human failure types include the following:

- Slip/lapses—An action performed where the outcome of the action was not as intended due to some failure in execution. Slips are errors that result from attention failures, while lapses are errors that result from failures in memory recall.
- Mistake—An action performed as intended, but the intention is wrong. Mistakes are typically failures associated with monitoring (especially deciding what to monitor and how frequently to monitor), situation awareness, and response planning. Section E5.1.1.4 provides definitions of these terms.

### **E5.1.1.4 Informational Processing Failures**

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Several such models have been proposed and used in discussing pilot performance for aviation. The model that is recommended for the YMP HRA is based on the discussion in Chapter 4 of ATHEANA (Ref. E8.1.23) and consists of the following elements:

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring.

Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.

- **Situation awareness**—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents operators' understanding of the present situation and their expectations for future conditions and consequences.
- **Response planning**—This term is defined as the process operators use to decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.
- **Response implementation**—This term is defined as the activities involved with physically carrying out the actions identified in response planning.

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

### **E5.1.2 Personnel Involved in Intra-Site Operations**

A list of personnel involved in Intra-Site operations with a brief description of their duties is provided below:

**HCTT operator**—The person who is designated to operate the cask tractor with cask transfer trailer for HCTT cask transfer activities.

**Crane operator**—The person who is designated to operate the crane for a given operation (i.e., mobile crane).

**Crew member**—A generic term for personnel (not including crane operators, radiation protection workers, or supervisors) involved in the facility operations.

**Forklift operator**—The person who is designated to operate the forklift for transferring drums of low-level radioactive waste (LLW).

**Quality control**—The certified crew member in charge of quality control. This person is involved in supervising critical operations and tracking the appropriate documentation (i.e., tracking the location of casks which come into the GROA).

**Radiation protection worker**—The certified health physics technician, whose job is to monitor radiation during certain cask-related activities. This person is responsible for stopping operations if high radiation levels are detected.

**Signaling crew member**—The person who is designated to provide signals to the crane operator. This person is predesignated and is distinguished from the verification crew member (most likely through an orange hard hat, orange gloves, or an orange vest as per the high-level radioactive waste (HLW) *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)* (Ref. E8.1.10)).

**SPM operator**—The person who is designated to operate the SPM to bring a railcar or truck trailer into the facility.

**Site Transporter operator**—The person who is designated to operate the site transporter to move an aging overpack into and around the facility.

**Supervisor**—The person who is in charge of the given operation and who supervises and checks off critical operations in a given step. For steps requiring independent verification, this analysis uses the term “supervisor” as the personnel who will provide the independent check. This analysis does not rely upon the fact that this check will be performed by the actual supervisor, only that an independent check is done by someone with the appropriate training and qualifications (i.e., the supervisor).

**Vendor vehicle operator**—The person who operates a vehicle of an authorized vendor transporting materials or personnel into the facility.

**Vendor vehicle escort vehicle operator**—The person who is designated to operate the vehicle (e.g., golf cart) that escorts a vehicle of an authorized vendor transporting materials or personnel into the facility.

**Verification crew member**—The person who is designated to assist with crane operations that require a second spotter. This person can only give the stop signal to the crane operator.

## **E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES**

This section discusses the general human performance issues that characterize the human interaction with the YMP facilities.

**Limited Automation (Significant Human Interaction)**—The types of operations being performed in the Intra-Site operations are not always conducive to automation. In particular, crane and transport operations are generally performed both manually and locally. Even those that are performed remotely require significant interaction by the operators. The dependence on human performance is quite high, and that dependence provides many opportunities for unsafe actions.

**Limited Nature of Procedures**—Other than those operations that are performed remotely from a control room, YMP operations are not highly proceduralized, but rather they depend primarily on skills learned and training. That is, while written procedures exist for all activities and training of all personnel is thorough, the actual use of procedures and checklists during operation (i.e., the step-by-step following of written procedures) generally occurs only during operations in a control room. The vast majority of local operations (e.g., skill-of-craft activities performed outside the control room) does not use written procedures at all during the actual performance of

the tasks and does not have formal checklists or verbal confirmation requirements spelled out in procedures physically in the possession of the crew performing the operation. This circumstance is consistent with observations of activities at NPPs during ISFSI operations.

**Communication Difficulties**—There are significant challenges in communication between the team members performing certain Intra-Site operations. The environment in the entrance and exit vestibules of a facility contains a not insignificant amount of background noise, predominantly machine noise. Although headsets may be used by key participants for communication, they do not eliminate the potential for misunderstanding. Garbled communication (due to system interference or background noise) is clearly possible, and in some cases it may not even be possible to clearly determine who is speaking. A belief that a particular individual is speaking, even if they are not, can bias the listeners into hearing what they expect to hear.

**Visual Challenges**—For most of the remote operations, successful completion of the operation requires a certain amount of visual acuity both for the performance of the operation and the confirmation of the status. For example, local crane operations can create visual challenges. The crane operator can only be at one given distance and orientation with relation to the operation, and therefore cannot be viewed on all three axes. In addition, views may be obstructed, such as by the load being moved or some other structure or equipment. Thus, the operator is often put in the position of being the hands for someone else's eyes, which make the operations vulnerable to the communication vulnerabilities discussed previously.

**Unchallenging Activities**—The activities involved in Intra-Site operations are, in general, quite simple in nature. In addition, the speed of the movements is quite slow, so each action takes a long time to complete. Basically, this is mostly boring work, with a significant amount of downtime between actions for some individuals. There is ample opportunity for diversion and distraction, and an air of informality and complacency can easily exist within and amongst the crew members. From a psychological perspective, there is insufficient dynamic activity to generate an optimum stress level for performance.

## **E6 ANALYSIS**

### **E6.0 OVERVIEW OF THE HRA ANALYSIS**

Intra-Site Operations cover the following four high-level operational activities:

1. Site transportation of SNF and HLW (rail car and truck trailer)
2. Aging Facility operations (i.e., aging overpack transit, placement, and retrieval from the aging pads)
3. Low Level Waste Facility (LLWF) operations
4. Balance of plant (BOP) facilities that directly or indirectly establish or support the repository infrastructure and operating services systems.

This section documents the qualitative and quantitative analysis of HFEs associated with the Intra-Site operations. Since the activities involving site transportation of SNF and HLW, Aging Facility, LLWF, and BOP were treated as separate nodes of the same ESD, the discussion of the relevant HFEs will be discussed sequentially for these facilities rather than as separate groups. Note that no HFEs were identified for BOP activities and the one LLW HFE involving forklift operation was quantified using industry data (Attachment C).

Each high-level operational activity is described in Section E6.1 and Section E6.2 provides a description and quantification for the corresponding HFEs. Table E6.0-1 provides a link between the high-level operational activities described in Section E6.1 and the ESD and the HAZOP nodes. Figure E6.0-1 provides an illustration of the movement of waste forms through the GROA. The link between the HFEs and the rest of the PCSA is provided through the ESD cross references for each HFE in Table E6.2-1.

Table E6.0-1. Correlation of Intra-Site Operations to ESDs and HAZOP Evaluation (PFD) Nodes

Activity	HAZOP Evaluation (PFD) Node	ESD
<b>Site Transportation of SNF and HLW (Section E6.1.1)</b>		
Site transportation – Railcar with Transportation Cask (Section E6.1.1.1)	1, 3-6	1, 9
Site transportation – Truck with Trailer with Transportation Cask (Section E6.1.1.2)	1, 2, 4-6	
<b>Aging Facility Operations (Section E6.1.2)</b>		
Aging Facility Operations – Aging Overpack (Section E6.1.2.1)	7-8	2, 9
Aging Facility Operations – Transport of HTC or HSTC (Section E6.1.2.2)	10	3, 9
Aging Facility Operations – HAM Activities (Section E6.1.2.3)	11-13	4, 9
<b>Low-Level Waste Facility Operations (Section E6.1.3)</b>		
Low-Level Waste Facility Process (Section E6.1.3)	14-15	5-8
<b>Balance of Plant (Section E6.1.4)</b>		
Balance of Plant Facility Process (Section E6.1.4)	N/A	N/A

NOTE: ESD = event sequence diagram; HAM = horizontal aging module; HAZOP = hazard and operability; HLW = high-level radioactive waste; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; N/A = not applicable; PFD = process flow diagram; SNF = spent nuclear fuel.

Source: Original

**ABBREVIATIONS:**

**WASTE FORMS (CASKS AND/OR CANISTERS)**

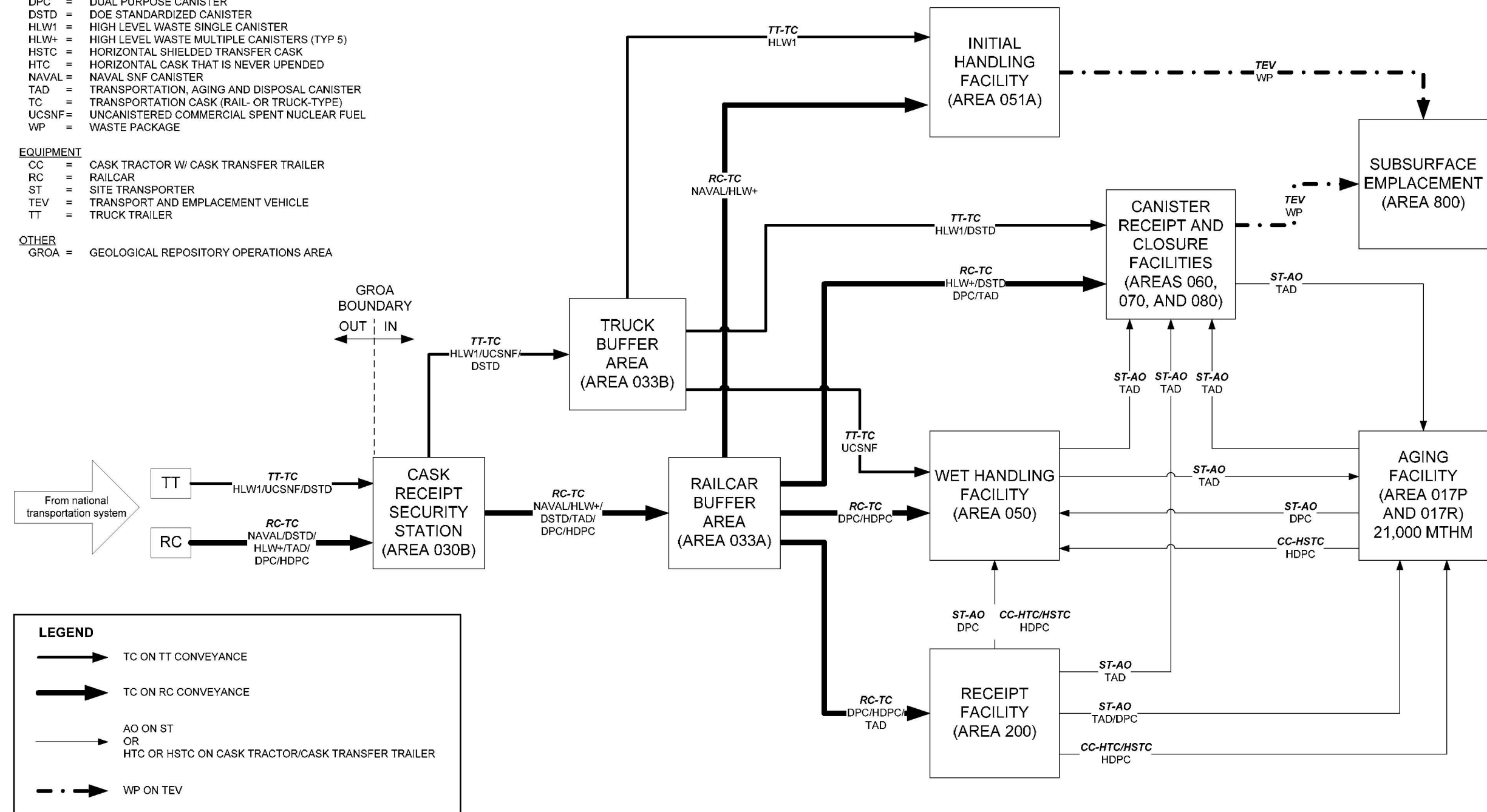
- AO = AGING OVERPACK
- DPC = DUAL PURPOSE CANISTER
- DSTD = DOE STANDARDIZED CANISTER
- HLW1 = HIGH LEVEL WASTE SINGLE CANISTER
- HLW+ = HIGH LEVEL WASTE MULTIPLE CANISTERS (TYP 5)
- HSTC = HORIZONTAL SHIELDED TRANSFER CASK
- HTC = HORIZONTAL CASK THAT IS NEVER UPENDED
- NAVAL = NAVAL SNF CANISTER
- TAD = TRANSPORTATION, AGING AND DISPOSAL CANISTER
- TC = TRANSPORTATION CASK (RAIL- OR TRUCK-TYPE)
- UCSNF = UNCANISTERED COMMERCIAL SPENT NUCLEAR FUEL
- WP = WASTE PACKAGE

**EQUIPMENT**

- CC = CASK TRACTOR W/ CASK TRANSFER TRAILER
- RC = RAILCAR
- ST = SITE TRANSPORTER
- TEV = TRANSPORT AND EMPLACEMENT VEHICLE
- TT = TRUCK TRAILER

**OTHER**

- GROA = GEOLOGICAL REPOSITORY OPERATIONS AREA



Source: Modified from *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. E8.1.8, Figure 15).

Figure E6.0-1. Movement of Waste Forms through the GROA



## **E6.1 DESCRIPTION OF INTRA-SITE OPERATIONS BASE CASE SCENARIOS**

### **E6.1.1 Site Transportation Activities**

The national transportation system delivers transportation casks containing the various waste forms to the site via either rail or truck. Once the conveyance is accepted, the SPM is connected to the conveyance to move it from the security gate to other surface facilities. The SPM, a multi-wheel, tractor-tired and rail-guided vehicle, is used to tow or push railcars, trailers, and other heavy load conveyances.

Movement between repository facilities is accomplished using a site transporter for TAD canisters and DPCs, and a cask tractor and cask transfer trailer (HCTT) for horizontal DPCs. Figure E6.0-1 provides an illustration of this movement. TAD canisters and DPCs are transferred between facilities in aging overpacks (Section E6.1.2). The boundary of Intra-Site operations for site transportation activities begins at the entrance to the GROA and ends at the entrance to the preparation area of a facility (i.e., Intra-Site operations includes the entrance vestibule of a facility).

The primary mode of human failure was considered to be the potential for collisions of other site vehicles with waste forms. These other site vehicles could include site owner-and-operated vehicles (e.g., fork lifts, equipment and supply trucks, etc) as well as externally owned and operated vehicles (e.g., welding gas delivery, LLW pick-up, etc.). The following conditions were anticipated regarding the operation of these vehicles:

- Although speed limits have not yet been established, it is anticipated that they will be established based on imparting less kinetic energy to the potential target than the current PEFA calculations being performed (e.g., less energy than an aging overpack at 2.5 mph, less energy than a 12-ft drop of a transportation cask, etc.). This allows, as a first approximation, the conditional failure probability of the waste form that is calculated for these cases to be used as the conditional failure probability for the collision event.
- All site owned-and operated vehicles are equipped with speed governors or the equivalent set at or below these speeds.
- All externally-owned vehicles are escorted by a member of the security force using a site-owned escort vehicle (e.g., a "golf cart") that is equipped with a speed governor. The externally owned vehicle is required to follow the escort vehicle at all times.
- Whenever a waste form is being moved on site, the security force erects and mans barriers at each road crossing where a site road crosses the path of the waste form.

This sets up a system of multiple, independent actions that would have to be violated in order for a "high-speed" collision to occur.

In similar fashion, vehicles that operate within the facilities, such as forklifts moving supplies, are also be equipped with speed governors.

The general procedure for entering a facility with a SPM attached to a railcar or truck trailer is as follows:

Two crew members are at the facility entrance vestibule. The railcar or truck trailer is pushed by a SPM (a diesel/electric vehicle with on board controls), and is driven by the SPM operator who is located in the cab of the SPM. When the railcar or truck trailer approaches the facility, the conveyance is visually inspected and one crew member opens the outside overhead door and the other crew member uses hand signals to direct the railcar/truck trailer into the facility entrance vestibule, ensuring there are no vehicles/obstructions in the path. The crew members follow all relevant restrictions and procedures regarding railcar/truck trailer speed and direction of travel. Once the railcar/truck trailer has cleared the door, the first crew member closes the outside door then opens the inside overhead door so the railcar can proceed to the facility cask preparation area where it will stop. A crew member then sets the railcar/truck trailer brakes and chocks the wheels. The SPM detaches from the railcar/truck trailer and proceeds back through the facility entrance vestibule to the outside.

#### **E6.1.1.1 Railcar with Transportation Cask**

When a cask shipment arrives by commercial rail at the repository site security gate, the conveyance is moved through the outer security gate by the commercial rail locomotive. The locomotive is disconnected and exits the area through the outer security gate. Once the conveyance is released by YMP security, the inner security gate is opened and the SPM is connected to the railcar. Railcars loaded with transportation casks are moved either directly to the various surface facilities or stored in the Railcar Buffer Area. The following is a general description of railcar/personnel interactions:

1. The railcar is pulled by the SPM which runs on a rail, so it cannot be steered.
2. The operator can control the speed of the SPM, but there is a speed limiter (~5 mph) on the SPM.
3. The operator can abruptly stop the railcar.
4. After parking, the operator must set the brakes and chock the wheels of the railcar.
5. In the rail yard, the operators can switch the railcars. Switching the railcars involves engaging or disengaging the connector and air hoses for the braking system of the SPM.
6. There is an interlock that, if the air hoses for the braking system fail, sever, or disconnect, then the mechanical brakes automatically engage. Therefore, if the railcar separates from the SPM, then the railcar automatically stops.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

### **E6.1.1.2 Truck Trailer with Transportation Cask**

When a cask shipment arrives by commercial trailer at the repository site security gate, the conveyance is moved through the outer security gate by the commercial truck. The commercial truck is disconnected and exits the area through the outer security gate. Once the conveyance is released by YMP security, the inner security gate is opened and the SPM is connected to the truck trailer. Truck trailers loaded with transportation casks are moved either directly to the various surface facilities or stored in the Truck Buffer Area. The following is a general description of truck trailer/personnel interactions:

1. The truck trailer is pulled by the SPM and runs on a paved road, so the truck trailer can be steered.
2. The operator can control speed of the SPM, but there is a speed limiter (~5 mph) on the SPM .
3. The operator can abruptly stop the truck trailer.
4. After parking, the operator must set the brakes and turn off the truck ignition.
5. In the truck yard, the operators can switch the truck trailers. Switching the trailers involves engaging or disengaging the connector and air hoses for the braking system of the truck.
6. There is an interlock that, if the air hoses for the braking system fail, sever, or disconnect, then the mechanical brakes automatically engage. Therefore, if the trailer separates from the SPM, the trailer automatically stops.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

### **E6.1.2 Aging Facility Operations**

The Aging Facility consists of a series of concrete pads whose purpose is to provide an area for the safe cooling of TAD canisters and DPCs containing commercial spent nuclear fuel (CSNF). The TAD canisters and DPCs requiring cooling are placed into an aging overpack for cooling at one of the two aging pads. DPCs, which arrive in HTCs, do not get placed in aging overpacks, but are placed into a horizontal aging module (HAM) on the southern aging pad. The TAD canisters and DPCs are aged until the thermal heat load of the TAD canister or waste content of the DPCs has decayed to a level low enough to be accepted by a waste package for underground emplacement. The Aging Facility is located north of the North Portal Pad. Figure E6.0-1 provides an illustration of the movement of waste forms between the waste handling facilities and the Aging Facility.

Aging cask and cask transfer equipment support the aging of the CSNF at the Aging Facility. Aging casks consist of aging overpacks and HAMs. The aging casks are either oriented vertically (i.e., aging overpacks, Section E6.1.2.1), or oriented horizontally (i.e., HAMs, Section

E6.1.2.3). Cask transfer equipment consists of cask tractors, cask transfer trailers, and crawler-type site transporters. The cask transfer trailers and the site transporters are used to move the aging overpacks and the HAMs containing canisters of CSNF between the various waste handling facilities of the repository to the aging pads.

Generally, transportation casks arriving at the geologic repository operations area (GROA) containing CSNF that require aging in TAD canisters or in DPCs are unloaded in the Receipt Facility (RF) and then transferred to aging overpacks. Site transporters are used to move the aging overpacks to one of the concrete aging pads for long-term thermal management. Once the thermal heat output declines to an acceptable level, the aging overpacks are moved to an appropriate waste handling facility for packaging. The Canister Receipt and Closure Facility (CRCF) can provide the receipt and transfer functions of the RF during the first few years of GROA operations before the RF has been constructed and brought on-line. The boundary of Intra-Site operations includes and ends at the entrance vestibule of a facility.

DPCs that contain CSNF are moved to the Wet Handling Facility (WHF) where the DPCs are opened and the CSNF contents are transferred to TAD canisters. TAD canisters with heat output low enough to be placed into a waste package are moved to the CRCF for processing and subsequent emplacement. TAD canisters and vertically-handled DPCs that require aging are placed into aging overpacks and transported to an aging pad by a site transporter for long-term cool-down.

The Aging Facility provides the capability to:

- Age up to 21,000 metric tons of heavy metal at the repository
- Store nuclear waste in canisters with high thermal power in a location where they can cool to appropriate levels
- Move waste in canisters between the aging pads and waste handling facilities
- Decouple the receipt of waste from the subsurface emplacement of the waste by creating a location to house and cool waste canisters by natural convection until the handling facilities can accommodate it.

The Aging Facility consists of three basic systems:

- Aging pads
- Aging casks (i.e., aging overpacks and HAMs)
- Cask transfer equipment (crawler type site transporters and HCTTs).

There are two basic variations of Aging Facility Operations, as follows:

1. Aging waste forms in a vertical orientation (Section E6.1.2.1), including the following activities:
  - A. Transit to an aging pad in aging overpacks via a site transporter.
  - B. Placement of aging overpacks on the aging pads.
  - C. Retrieval of aging overpacks and transit to a waste handling facility via a site transporter.
2. Aging horizontal DPCs in HAMs, including the following activities:
  - A. Transit of a horizontal DPC in an HTC to the Aging Facility; retrieval of the horizontal DPC in an HSTC from the Aging Facility and transport to the WHF (Section E6.1.2.2).
  - B. Placement or retrieval of horizontal DPC from HAMs (Section E6.1.2.3).

#### **E6.1.2.1 Site Transporter Movement of an Aging Overpack (TAD canisters and DPCs)**

The site transporter is used to transfer aging overpacks between the waste handling facilities and the aging pads. Loaded vertical aging overpacks containing canistered CSNF are lifted and moved to and from the aging pads using a site transporter. The following is a general description of site transporter/personnel interactions:

1. The site transporter runs on a (dirt) road, and can be steered.
2. The site transporter operator can control the speed of the site transporter; however, it is equipped with a speed limiter. In addition, the speed is limited by the power of the motor.
3. The operator can abruptly stop the site transporter.
4. When parking, the operator sets the brakes and turns off the site transporter.
5. Crew members strap the aging overpack in the site transporter.
6. The site transporter does not lift the aging overpack more than ~6 in.
7. Construction activities are not conducted in the vicinity of normal waste handling operations. Construction operations and waste handling operations are divided by double fences, each with a separate road system.

The following activities are associated with site transporter movement of aging overpacks containing TAD canisters and DPCs:

- The loaded aging overpack is moved to the Aging Facility. The operator uses the site transporter to transfer a loaded aging overpack with a TAD canister from the WHF, or a loaded aging overpack with either a TAD canister or DPC from the CRCF or RF, to the Aging Facility.
- The loaded aging overpack is placed in the assigned aging pad location. At the Aging Facility, the aging overpack is lowered into place, the lifting mechanism is disengaged and the site transporter is moved away.
- The aging temperature sensors are installed on the aging overpack (if required) to monitor the age of the loaded aging overpack.
- Temperature sensors are disconnected upon conclusion of the aging process.
- The loaded aging overpack is moved with the site transporter to the CRCF or WHF once the aging process is complete.

#### **E6.1.2.2 Transportation and Positioning of the HTC or HSTC**

The transportation of horizontal DPCs in HTCs or HSTC is conducted utilizing a specially designed cask transfer trailer that is towed by a separate cask tractor. The boundary of Intra-Site operations for moving an HCTT unit into or out of a facility includes and ends at the entrance vestibule of that facility. The following actions are associated with this activity:

- The horizontal DPC in an HTC is moved via the HCTT to the designated HAM on Aging Facility.
- Once aged, the horizontal DPC is unloaded from the HAM. The HCTT is aligned with the HAM access port, the horizontal DPC is loaded into an HSTC, and the loaded HSTC is transported to the appropriate waste handling facility.

#### **E6.1.2.3 Canister Operations at the HAM**

Using the cask transfer trailer, the cask is transported from the RF to the Aging Facility. A portable commercial mobile crane capable of lifting the HAMs concrete closure ports and the end cover lids of the transportation casks (and HSTCs) is used to support DPC insertion and retrieval operations to and from the HAM. The casks and HAM are capable of protecting the canister from credible accidents or operator errors associated with lid removal and installation on the casks or HAMs such as a drop of a lid onto the cask or HAMs.

The cask transfer trailer is positioned within a few feet of the HAM. The position of the trailer is checked to ensure that the centerline of the HAM and cask approximately coincide. If the trailer is not properly oriented, the trailer is repositioned as necessary.

Outriggers and jacks are used to stabilize the cask and the cask transfer trailer during the transfer of a DPC into the HAM. A hydraulic ram and hydraulic power unit are set up behind the cask and aligned to engage the hydraulic ram to the DPC ram grapple rings. The hydraulic ram cylinder is actuated to insert the DPC into the HAM. The transfer is facilitated using the support guide rails inside the HAM.

Operations begin, with a DPC loaded in an HTC on the cask transfer trailer (from the RF). The following steps are performed as part of HAM loading and unloading operations:

#### **E6.1.2.3.1 Movement of a DPC from an HTC into a HAM**

The following steps are performed to move a DPC from an HTC into a HAM:

1. The loaded HTC is aligned with the access port of the designated HAM. The HCTT operator visually aligns the HCTT with the HAM with the help of a crew member who watches and directs the HCTT operator.
2. The closure door on the HAM and the closure lid on loaded HTC are removed.
3. The DPC inside the HTC is aligned with the DPC cradle inside HAM.
4. The loaded HTC is docked and restrained to the HAM access port. The operators install struts to tie the skid to the HAM.
5. The hydraulic ram access cover is removed from the loaded HTC.
6. The hydraulic ram on the cask transfer trailer is raised.
7. The ram grapple with DPC is engaged and the DPC is inserted from the HTC into the HAM.
8. The hydraulic ram and grapple are retracted from the DPC and undocked from the HAM.
9. DPC restraints are installed, as required.
10. The closure door is installed on the HAM.

#### **E6.1.2.3.2 Age and Monitor DPC in HAM**

Aging temperature sensors are installed and the condition of air inlet/outlet ports is verified.

### **E6.1.2.3.3 Retrieve DPC from HAM and Insert into HSTC**

The following steps are performed to retrieve a DPC from a HAM and insert the DPC into an HSTC:

1. The closure door on the HAM and the closure lid on unloaded HSTC are removed.
2. DPC restraints are removed as required.
3. The unloaded HSTC is aligned with the DPC inside of the HAM.
4. The HSTC is docked and restrained to the HAM access port.
5. The hydraulic ram access cover on the HSTC is removed and the hydraulic ram on the cask transfer trailer is raised.
6. The ram grapple is engaged with the DPC and the DPC is moved from the HAM into the HSTC.
7. The loaded HSTC is undocked from the HAM and the hydraulic ram is lowered.
8. The HSTC closure lid and ram access cover are installed and the closure door is placed on the HAM
9. The loaded HSTC is moved to the WHF.

### **E6.1.3 Low-Level Waste Facility Activities**

The LLWF is designed for the collection, processing, and disposal of LLW streams generated during the handling of HLW and SNF.

The LLWF is designed as a commercially-available structure with a steel frame. Four separate shielded storage bays, with partial-height-walls, are located inside the building on the side of the facility opposite the truck bay. These four bays provide for interim storage of boxes, drums, high integrity containers, filters, and empty DPCs. A concrete storage pad is located outside the facility adjacent to the four storage bays.

A pull-through truck bay is located on one end of the building. This area has hatches through which waste containers are moved. An open process area is located adjacent to the Receipt Area, which contains a scale and areas for the storage of supplies and tools. Other areas that are entered from the open process area include the Cold Support Area, Decontamination Room, Glove Box Area, and two sorting rooms.

### **E6.1.4 Balance of Plant Facility Activities**

The BOP facilities provide the space, layout, and embedded facilities that directly or indirectly establish or support the repository infrastructure and operating services systems.



The BOP facilities extend beyond the GROA to provide infrastructure and to interface with offsite services and functions (i.e., the primary site access road, service roads, South Portal, North Construction Portal, and utility structures).

The BOP facilities provide operational infrastructure and services for waste handling operations and waste emplacement facilities but do not directly perform waste handling or waste emplacement operations or processes.

## **E6.2 ANALYSIS OF INTRA-SITE HUMAN FAILURE EVENTS**

This section documents the qualitative analysis of HFES associated with the operations described in Section E6.1. The qualitative analysis includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis.

### **E6.2.1 HFES Common to Multiple Operations**

Before beginning the analysis of the individual failure events, there are a number of generic HFES that were evaluated across operations and determined to be conducive to establishing ground rules for use throughout the analysis. These HFES are discussed in this section.

**Interlocks**—For the HRA, interlocks were generally modeled explicitly in the fault tree instead of being embedded in the HRA for the preliminary analysis. The approach chose by the HRA team to assign preliminary HEPs when interlocks were present was simplified. Since the interlock would prevent the operator from completing an unsafe action (even if the operator tried to) it was conservatively analyzed as if the operator would always take the unsafe action (i.e., the HEP for the HFE containing the unsafe action was conservatively set to 1.0 as a first approximation of the HEP). Unless otherwise specified, this was done for all cases where the human cannot easily defeat the interlock that protects against the associated unsafe action and HFE. Therefore, the analysis is relying entirely upon the interlock to prevent the failure. The interlock failure probability is taken from the active component failure database, which gives a value of  $2.7E-5$  per demand (approximately  $3E-5$ /demand). It is recognized in using this approach that, despite the interlock not being easy to defeat, there is always a possibility that it could be defeated (either by the operator or by the maintenance crew and then not restored). However, if this were the case then it would still be necessary for the operator to erroneously conduct the unsafe action. The HRA team considered that it was very unlikely that the screening combination of the bypass error and the unsafe action would approach or exceed the  $3E-5$  value for the random failure of the interlock. The HRA team judged that this preliminary value would implicitly account for the failure to restore an interlock after maintenance if that interlock is difficult to bypass and is not bypassed during normal maintenance. If this conservative approach was not adequate to demonstrate compliance with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1), a more realistic preliminary value was applied and justified. That is, the HRA team went back and took a further look at the unsafe action and its associated interlock, and determined whether a lower preliminary HEP for the unsafe action could be justified. If so, this is clearly discussed and documented in the preliminary analysis. Interlocks that humans can reasonably defeat were generally not explicitly modeled in the fault tree, but rather included in the HEP for the HFE since they are not independent of operator actions. Regardless of this approach, in any case where the preliminary HEP was not sufficient to demonstrate compliance

with 10 CFR Part 63 (Ref. E8.2.1) and a detailed analysis was needed, all interlocks and other mechanical failures or physical phenomena that contribute to the overall HFE were integrated into the HRA along with the contributing unsafe actions and evaluated within the overall HFE quantification as part of the context of the HFE and fully discussed and documented in the detailed analysis. In all cases, interlocks that rely on programmable logic controllers were not credited in this analysis since they won't be declared important to safety.

**Crane Drops (Drop of Object onto Cask)**—There are several lifts of heavy objects in the Intra-Site Operations involving mobile cranes (considered as jib cranes) which can potentially result in a drop. Crane drop related HFEs were not explicitly quantified because the probability of a crane drop due to human failure is incorporated in the historical data used to provide general failure probabilities for drops involving various crane and rigging types. Documentation for this failure can be found in Attachment C.

### **E6.2.2 HFE Descriptions and Preliminary Analysis**

This section defines and screens the HFEs that are identified for the base case scenarios, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during Intra-Site Operations are summarized in Table E6.1-1. Tables E6.1-2 and E6.1-3 provide additional data to support the analysis in Table E6.1-1. The analysis presented here includes the assignment of preliminary HEPs in accordance with the methodology described in Section E3.2 and Appendix E.III of this analysis. Section E4.2 provides details on the use of expert judgment in this preliminary analysis.

Table E6.2-1. Descriptions and Preliminary Analysis for Intra-Site Operation HFEs

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
ISO-OPRCOLLIDE1-HFI-NOD	<i>Operator Causes Prime Mover Railcar (PMRC) Collision:</i> Operator causes the collision of a railcar with a facility structure, piece of equipment, or another vehicle while moving through the Entrance Vestibule of a facility.	1	3E-03	<p>The SPM moves the railcar into a facility vestibule. There are three observers with clear visibility, the operation is simple, the railcar speed is low, the distance is short, and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a railcar are limited, and include:</p> <ul style="list-style-type: none"> <li>• Backward motion beyond the limit could result in collision with the end stops, wall, or vestibule doors.</li> <li>• Improperly attached railcar could continue moving when SPM stops, resulting in collision with the end stops, wall, or vestibule doors.</li> <li>• Forklift or other auxiliary vehicle could collide into the conveyance.</li> </ul> <p>The preliminary value was chosen based on the determination that this failure is "highly unlikely" (one in a thousand or 0.001) and was adjusted because there are several ways for a collision to occur, and there are potentially multiple other vehicles (forklifts) that can collide into the conveyance (×3).</p>
ISO-OPRCINTCOL01-HFI-NOD	<i>Operator Initiates PMRC Runaway:</i> Operator causes a collision of the railcar at a speed higher than design requirements. If the speed governor of the SPM fails, the operator could collide the railcar into an SSC.	1	1	<p>The operator can cause the SPM to over speed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event are assigned an HEP of 1.0.</p>
ISO-OPSTCOLLIDE2-HFI-NOD	<i>Operator Error Causes Site Transporter Collision:</i> Operator causes a collision of the site transporter with a facility structure, piece of equipment, or another vehicle while entering or exiting a facility.	2	3E-03	<p>In this step, the site transporter, loaded with an aging overpack, enters or exits a facility. There are three observers with clear visibility, the operation is simple, the conveyance speed is low, the distance is short and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a site transporter are limited, and include:</p> <ul style="list-style-type: none"> <li>• Backward motion beyond the limit could result in collision with the end stops, wall, or vestibule doors.</li> <li>• Forklift or other auxiliary vehicle could collide into the conveyance.</li> </ul> <p>The preliminary value was chosen based on the determination that this failure is "Highly Unlikely" (0.001) and was adjusted (×3) consistent with other collision events.</p>
ISO-OPTTCOLLIDE1-HFI-NOD	<i>Operator Causes Truck Trailer Collision:</i> Operator causes a collision of the truck trailer with a facility structure, piece of equipment, or another vehicle while moving through the Entrance Vestibule of a facility.	1	3E-03	<p>In this step, the SPM with truck trailer moves into a facility vestibule. There are three observers with clear visibility, the operation is simple, the truck trailer speed is low, the distance is short and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a truck trailer are limited, and include:</p> <ul style="list-style-type: none"> <li>• Improper (i.e., backward or lateral) motion could result in collision with the end stops, wall, or vestibule doors.</li> <li>• Improperly attached trailer could continue moving when truck stops, resulting in collision with the end stops, wall, or vestibule doors.</li> <li>• Forklift or other auxiliary vehicle could collide into the conveyance.</li> </ul> <p>The preliminary value was chosen based on the determination that this failure is "Highly Unlikely" (0.001) and was adjusted (×3) consistent with other collision events.</p>
ISO-OPTTINTCOL01-HFI-NOD	<i>Operator Initiates Truck Trailer Runaway:</i> Operator causes a collision of the truck trailer at a speed higher than design requirements. If the speed governor of the SPM fails, the operator could collide the truck trailer into an SSC.	1	1	<p>The SPM can over speed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.</p>

Table E6.2-1. Descriptions and Preliminary Analysis for Intra-Site HFEs (Continued)

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
ISO-OPHTCOLLIDE1-HFI-NOD	<i>Operator Causes Collision of HCTT while Leaving the Facility:</i> Operator causes a collision of the HCTT unit with a facility structure, piece of equipment, or an auxiliary vehicle while moving through the Entrance Vestibule of a facility.	3	3E-03	In this step, the HCTT enters the WHF with a loaded HSTC or exits the RF with a loaded HTC. There are three observers with clear visibility, the operation is simple, the conveyance speed is low, the distance is short and the operators are expected to perform this operation on a very regular (almost daily) basis. There are no interlocks, and it would be normal for an obstruction (e.g., door) to be in place during movement. The possibilities for collision involving a cask transfer trailer are limited, and include: <ul style="list-style-type: none"> <li>• Improper (i.e., backward or lateral) motion could result in collision with the end stops, wall, or vestibule doors.</li> <li>• Improperly attached cask transfer trailer could continue moving when cask tractor stops, resulting in collision with the end stops, wall, or vestibule doors.</li> <li>• Forklift or other auxiliary vehicle could collide into the conveyance.</li> </ul> The preliminary value was chosen based on the determination that this failure is "Highly Unlikely" (0.001) and was adjusted (×3) consistent with other collision events.
ISO-OPHTINTCOL01-HFI-NOD	<i>Operator Causes Collision of HCTT due to Overspeed:</i> Operator causes a collision of the HCTT unit at a speed higher than design requirements. If the cask tractor speed limiter fails, the operator could collide the cask transfer trailer into an SSC.	3	1	The cask tractor can over speed, resulting in collision. In order to accomplish this, the speed governor must fail. To be conservative, unsafe actions that require an equipment failure to cause an initiating event have generally been assigned an HEP of 1.0.
ISO-OP-HAMIMPACT-HFI-NOD	<i>Operator Causes HAM Impact with Crane:</i> Operator impacts HAM with door removed using the mobile crane.	4	3E-03	In this HFE, the operator impacts the HAM with the door that has already been removed using a mobile crane. Crane operations are performed frequently by this team and is a very simple task. A preliminary value based on the determination that this failure is "Highly Unlikely" (0.001) has been used, but adjusted (×3) because there are several ways for this impact to occur, including: <ul style="list-style-type: none"> <li>- Crane moved outside its safe load path (e.g., operators cut corners)</li> <li>- Crane moved in wrong direction</li> <li>- Operator failed to maintain proper vertical and horizontal distance between cask and SSCs during crane operations.</li> </ul>
ISO-OP-HAMINSERT-HFI-NOD	<i>Operator Misaligns Transport and HAM Opening:</i> Cask transfer trailer is not properly oriented by operator to ensure that the centerline of the HAM and the HTC coincide.	4	1E-03	The cask transfer trailer is supposed to be positioned to within a few feet of the HAM and the position of the trailer checked to ensure that the centerline of the HAM and cask approximately coincide. If the trailer is not properly oriented, the trailer is supposed to be repositioned as necessary. The preliminary value was chosen based on the determination that this failure is "Highly Unlikely" (0.001) since the operator can take the time needed to properly align the cask transfer trailer and the HAM opening, with assistance from other personnel watching the operation.
ISO-VEH-COLISION-COL-RAT	<i>Vendor Vehicle Collision:</i> RC, TT, HCTT or ST collides with auxiliary vehicle or SSC during transit across the GROA (non-facility related).	8	7E-07 <sup>a</sup>	A separate analysis using historical data was performed to evaluate the likelihood of a collision occurring on intra-site roadways that would involve the transport of waste forms or used HEPA filters, and therefore could potentially result in a radioactive release. Considerations were that the nature of the materials transported would be considered hazardous (hazmat), the speed at which the vehicle would be traveling would be very slow, and that vehicle escorts would be provided on-site, further monitoring and restricting the vehicle speed. The data and the sources used for this portion of the analysis are summarized in Tables E6.2-2 and 6.2-3.
ISO-OPSICOMPDROP-HFI-NOD	<i>Operator Drops Object onto Transportation Cask</i>	1	N/A <sup>a</sup>	This Intra-Site operation involves a drop of an object from a mobile crane onto a transportation cask. A human-induced drop HFE was not explicitly quantified because the probability of crane drop due to human failure is incorporated in the historical data used to provide a general failure probability for jib crane drops (CRJ-DRP). Documentation for this failure can be found in Attachment C.
ISO-PMRC-DERAIL-PER-MILE	<i>Railcar Derailment</i>	1	N/A <sup>a</sup>	This event deals with the derailment of the prime mover railcar. An HFE was not explicitly quantified because historical data was used to provide a general failure probability for railcar derailments (DER-FOM). Documentation for this failure can be found in Attachment C.
ISO-HEPA-XFER-L-FORKLIFT	<i>Operator Punctures Drum of LLW with Forklift</i>	5	N/A <sup>a</sup>	This Intra-Site operation involves a drum of low level waste being punctured by an improper operation of a forklift during transfer of HEPA filters. A human-induced forklift HFE was not explicitly quantified because historical data was used to provide a general failure probability for forklift punctures (FRK-PUN). Documentation for this failure can be found in Attachment C.

NOTE: <sup>a</sup> HRA preliminary value replaced by use of historic data See Attachment C on active component reliability data for more information.

ESD = event sequence diagram; GROA = geologic repository operations area; HAM = horizontal aging module; HCTT = cask tractor and cask transfer trailer; HEP = human error probability; HEPA = high efficiency particulate air; HFE = human failure event; HSTC = horizontal shielded transfer cask; HTC = a transportation cask that is never upended; ID = identification; LLW = low-level radioactive waste; N/A = not applicable; PMRC = prime mover railcar; RC = railcar; RF = Receipt Facility; SPM = site prime mover; SSC = structure, system, or component; SSCs = structures, systems, and components; ST = site transporter; TT = truck trailer; WHF = Wet Handling Facility.

Source: Original

Table E6.2-2. Vendor Vehicle Collision Data

Source	Description	Value
<i>Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report.</i> (Ref. E8.1.12, Table 9, p. 4-1).	Annual en route release accidents for HM Category 7 vehicles (Radioactive materials)	6
<i>Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report.</i> (Ref. E8.1.12, Table 9, p. 4-1).	Annual en route leaks for HM Category 7 vehicles (Radioactive materials)	4
Original: sum of en route release accidents and leaks for HM Category 7 (Radioactive materials) [6 + 4 = 10]	<b>Total en route incidents</b>	<b>10</b>
<i>Traffic Safety Facts 2002: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System.</i> (Ref. E8.1.13, Table 29, p. 51).	Percent of all single and multiple vehicle crashes at 40 mph or less	0.57
Original: product of total en route incidents and percent of crashes at 40 mph or less. [0.57 × 10 = 5.7]	Total estimated en route incidents at 40 mph or less	5.7
<i>Large Truck Crash Causation Study</i> (Ref. E8.1.14, Table 14).	Percent of truck crash factors <u>not</u> mitigated by use of escorting vehicle [See separate table]	48%
Original: total estimated en route incidents at 40 mph or less, adjusted by the percent of crash factors not mitigated by use of escort vehicle. [5.7 × 0.48 = 2.7]	<b>Total estimated en route incidents at 40 mph or less not mitigated by use of escorting vehicle</b>	<b>2.7</b>
<i>Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report.</i> (Ref. E8.1.12, Table 24, p. 4-13).	Hazmat miles traveled for 1996 for HM Category 7 vehicles (Radioactive materials)	3.00E+07
"Speeding Counts...on All Roads!" (Ref. E8.1.11).	Percent of annual vehicle-miles traveled on local roads, with posted speed limits usually between 20 and 45 mph	0.134
Original: Hazmat miles adjusted by percentage of miles traveled between 20 and 45 mph. [3.00E+07 × 0.134 = 4.02E+06]	<b>Estimated annual vehicle-miles traveled on local roads between 20 - 45 mph</b>	<b>4.02E+06</b>
Original: total en route incidents at 40 mph or less divided by the total vehicle-miles traveled at between 20 and 45 mph for Hazmat Category 7 vehicles (Radioactive materials). [2.7 / 4.02E+06 = 7.E-07]	<b>Estimated radioactive hazmat vehicle crashes per vehicle mile traveled below ~40 mph per year</b>	<b>7.E-07</b>

Source: Original

Table E6.2-3. Vendor Vehicle Crash Factors Mitigated by Escorting

Truck Crash Factors	Amt in 1000's	Percent	Addressed by Escorting
<b>Driver Factors</b>			
Prescription drug use	37	8.0%	
Traveling too fast for conditions	33	7.2%	7.2%
Unfamiliar with roadway	31	6.7%	
Over-the-counter drug use	25	5.4%	
Inadequate surveillance	20	4.3%	4.3%
Fatigue	18	3.9%	
Illegal maneuver	13	2.8%	2.8%
Inattention	12	2.6%	
Exterior distraction	11	2.4%	
Inadequate evasive action	9	2.0%	2.0%
Aggressive driving behavior	9	2.0%	2.0%
Unfamiliar with vehicle	9	2.0%	
Following too closely	7	1.5%	1.5%
False assumption of others' actions	7	1.5%	1.5%
Under pressure to accept additional loads	6	1.3%	1.3%
Conversation	5	1.1%	
Under pressure to operate even if fatigued	4	0.9%	
Misjudgment of gap distance	4	0.9%	0.9%
In a hurry prior to crash	4	0.9%	0.9%
Illness	4	0.9%	
Interior distraction	3	0.7%	
Illegal drug use	3	0.7%	
Uncomfortable with some aspect of vehicle or load	4	0.9%	
Self induced legal work pressure	3	0.7%	
Required to accept short notice trips	3	0.7%	0.7%
Work schedule pressure	3	0.7%	
Upset prior to crash	3	0.7%	
Alcohol use	1	0.2%	
Other decision factors – includes proceeding with obstructed view, stopping when not required to, failing to yield, and others	13	2.8%	2.8%
Other physical factors – includes hearing problems, prosthesis, paraplegia, strenuous activities, sleep apnea, as well as others	11	2.4%	
Other motor carrier work pressure	9	2.0%	
Other recognition factors – includes impending problem masked by traffic flow pattern, driver focused on extraneous issues	4	0.9%	0.9%
<b>Environment Factors</b>			
Traffic flow interruption – includes work zones, roadway immersion, prior crash, and traffic congestion	40	8.7%	8.7%
Roadway related factors	29	6.3%	6.3%

Table E6.2-3. Vendor Vehicle Crash Factors Mitigated by Escorting (Continued)

Truck Crash Factors	Amt in 1000's	Percent	Addressed by Escorting
<b>Driver Factors</b>			
Stop required prior to crash—includes stop required for traffic control device, and yield right of way requirement	28	6.1%	6.1%
Weather related factors	20	4.3%	
Sight obstructed by road/other vehicle	6	1.3%	1.3%
Other traffic/vehicle factors— includes any factors not listed causing the driver to feel uncomfortable with surrounding traffic or the vehicle	7	1.5%	1.5%
Other vehicle obscured (by glare/headlights, etc)	2	0.4%	
Other environmental factors	1	0.2%	
Total	461	100%	52%
<b>Percent of truck crash factors not mitigated by use of escorting vehicle</b>			<b>48%</b>

Source: "Summary Tables." *Large Truck Crash Causation Study*. (Ref. E8.1.14, Table 14).

### E6.3 DETAILED ANALYSIS

There are no HFEs in this group that require detailed analysis; the preliminary values in the facility model do not result in any Category 1 or Category 2 event sequences that fail to comply with the 10 CFR 63.111 performance objectives, therefore, the preliminary values were sufficient to demonstrate compliance with 10 CFR Part 63 (Ref. E8.2.1).

### E7 RESULTS: HUMAN RELIABILITY ANALYSIS DATABASE

Table E7-1 presents a summary of all of the human failures identified in this analysis, and provides a link between the HFE and the ESD in which the human failure is modeled.

Table E7-1. HFE Data Summary

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
ISO-OPSIKOMPDRP-HFI-NOD	Operator drops object onto transportation cask	1	N/A <sup>a</sup>	N/A	Historic Data
ISO-HEPA-XFER-L-FORKLIFT	Operator punctures drum of LLW with forklift	5	N/A <sup>a</sup>	N/A	Historic Data
ISO-OPHTCOLLIDE1-HFI-NOD	Operator causes collision of HCTT in the facility	3	3.00E-03	5	Preliminary
ISO-OPHTINTCOL01-HFI-NOD	Operator causes collision of HCTT due to cask tractor overspeed	3	1.0	N/A	Preliminary
ISO-OP-HAMIMPACT-HFI-NOD	Operator causes HAM impact with crane	4	3.00E-03	5	Preliminary
ISO-OP-HAMINSERT-HFI-NOD	Operator misaligns transport and HAM opening	4	1.00E-03	5	Preliminary

Table E7-1. HFE Data Summary (Continued)

Basic Event Name	HFE Description	ESD	Basic Event Mean Probability	Error Factor	Type of Analysis
ISO-OPRCCOLLIDE1-HFI-NOD	Operator causes SPM/railcar collision in the facility	1	3.00E-03	5	Preliminary
ISO-OPRCINTCOL01-HFI-NOD	Operator initiates PMRC runaway	1	1.0	N/A	Preliminary
ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes site transporter collision in the facility	2	3.00E-03	5	Preliminary
ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes SPM/truck trailer collision in the facility	1	3.00E-03	5	Preliminary
ISO-OPTTINTCOL01-HFI-NOD	Operator initiates truck trailer runaway	1	1.0	N/A	Preliminary
ISO-PMRC-DERAIL-PER-MILE	PMRC derailment	1	N/A <sup>a</sup>	N/A	Historic Data
ISO-VEH-COLISION-COL-RAT	Collision of RC, TT, ST or HCTT with SSC during transport across the GROA	8	7.00E-07	10	Historic Data

NOTE: <sup>a</sup> Historical data was used to produce a probability of crane drops; this historical data is not included as part of the HRA, but is addressed in Attachment C.

ESD = event sequence diagram; GROA = geologic repository operations area; HAM = horizontal aging module; HCTT = cask tractor and cask transfer trailer; HFE = human failure event; LLW = low-level radioactive waste; N/A = not applicable; PMRC = prime mover railcar; RC = railcar; SPM = site prime mover; SSC = structure, system, or component; ST = site transporter; TT = truck trailer.

Source: Original



## E8 REFERENCES

### E8.1 DESIGN INPUTS

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

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

- E8.1.1\* AIChE (American Institute of Chemical Engineers) 1992. *Guidelines for Hazard Evaluation Procedures*. 2nd Edition with Worked Examples. New York, New York: American Institute of Chemical Engineers. TIC: 239050. ISBN: 0-8169-0491-X.
- E8.1.2\* ASME NUM-1-2004. 2005. *Rules for Construction of Cranes, Monorails, and Hoists (with Bridge or Trolley or Hoist of the Underhung Type)*. New York, New York: American Society of Mechanical Engineers. TIC: 259317. ISBN: 0-7918-2938-3.
- E8.1.3\* ASME RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.
- E8.1.4\* Benhardt, H.C.; Eide, S.A.; Held, J.E.; Olsen, L.M.; and Vail, R.E. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)*. WSRC-TR-93-581. Aiken, South Carolina: Westinghouse Savannah River Company, Savannah River Site. ACC: MOL.20061201.0160.
- E8.1.5\* BSC 2006. *Engineering Standard for Repository Component Function Identifiers*. 000-30X-MGR0-00900-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20060816.0001.
- E8.1.6\* BSC 2007. *Engineering Standard for Repository Area Codes*. 000-3DS-MGR0-00400-000 REV 004. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070911.0015.
- E8.1.7\* BSC 2007. *Repository System Codes*. 000-30X-MGR0-01200-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071101.0022.
- E8.1.8 BSC (Bechtel SAIC Company) 2008. *Intra-Site Operations and BOP Event Sequence Development Analysis*. 000-PSA-MGR0-00800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0004.
- E8.1.9\* CRA (Corporate Risk Associates) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique*.

- CRA-BEGL-POW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.
- E8.1.10 DOE-STD-1090-2004. 2004. *Hoisting and Rigging (Formerly Hoisting and Rigging Manual)*. 800-30R-SS00-00400-000-000. Washington, D.C.: U.S. Department of Energy. ACC: ENG.20060407.0002.
- E8.1.11\* DOT (U.S. Department of Transportation). 2000. "Speeding Counts...on All Roads!" Washington, D.C.: U.S. Department of Transportation, Federal Highway Administration. ACC: MOL.20080228.0001.
- E8.1.12\* DOT 2001. *Comparative Risks of Hazardous Materials and Non-Hazardous Materials Truck Shipment Accidents/Incidents, Final Report*. Washington, D.C.: U.S. Department of Transportation. ACC: MOL.20080228.0002.
- E8.1.13\* DOT 2004. *Traffic Safety Facts 2002: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System*. DOT HS 809 620. Washington, D.C.: U.S. Department of Transportation, National Highway Traffic Safety Administration. ACC: MOL.20080228.0003.
- E8.1.14\* DOT [n.d.]. "Summary Tables." *Large Truck Crash Causation Study*. [Washington, D.C.]: U.S. Department of Transportation. ACC: MOL.20080227.0020.
- E8.1.15\* Dougherty, E.M., Jr. and Fragola, J.R. 1988. *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. New York, New York: John Wiley & Sons. TIC: 3986. ISBN: 0-471-60614-6.
- E8.1.16\* Gertman, D.; Blackman, H.; Marble, J.; Byers, J.; and Smith, C. 2005. *The SPAR-H Human Reliability Analysis Method*. NUREG/CR-6883. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0009.
- E8.1.17\* Hall, R.E.; Fragola, J.R.; and Wreathall, J. 1982. *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlations*. NUREG/CR-3010. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0211.
- E8.1.18\* Hannaman, G.W. and Spurgin, A.J. 1984. *Systematic Human Action Reliability Procedure (SHARP)*. EPRI-NP-3583. Palo Alto, California: Electric Power Research Institute. TIC: 252015.
- E8.1.19\* Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.
- E8.1.20\* Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

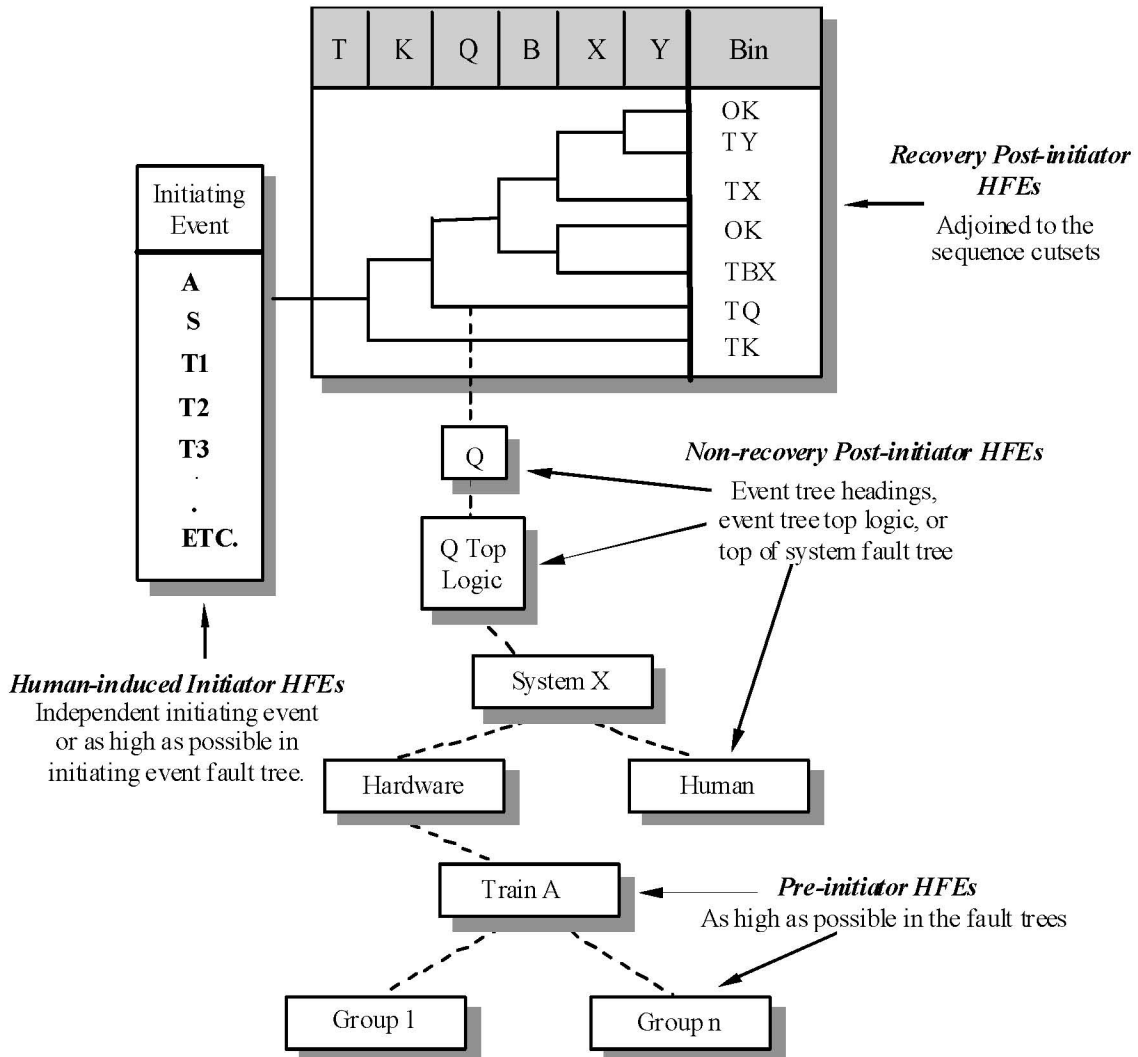
- E8.1.21 NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.
- E8.1.22 NRC 1983. *PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.
- E8.1.23 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.
- E8.1.24 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071211.0230.
- E8.1.25\* Rasmussen, J. 1983. "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models." *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13*, (3), 257–266. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259863.
- E8.1.26\* Swain, A.D. 1987. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. NUREG/CR-4772. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20061103.0026.
- E8.1.27\* Swain, A.D. and Guttman, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*. NUREG/CR-1278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.
- E8.1.28\* Williams, J.C. 1986. "HEART - A Proposed Method for Assessing and Reducing Human Error." *9th Advances in Reliability Technology Symposium - 1986*. Bradford, England: University of Bradford. TIC: 259862.
- E8.1.29\* Williams, J.C. 1988. "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance." *[Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants]*. Pages 436–450. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259864.

## **E8.2 DESIGN CONSTRAINTS**

- E8.2.1 10 CFR (Code of Federal Regulations) Part 63. 2007. Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada. U.S. Nuclear Regulatory Commission.

### APPENDIX E.I RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA

Figure E.I-1 provides a graphical illustration of how HFEs are incorporated into the PCSA.

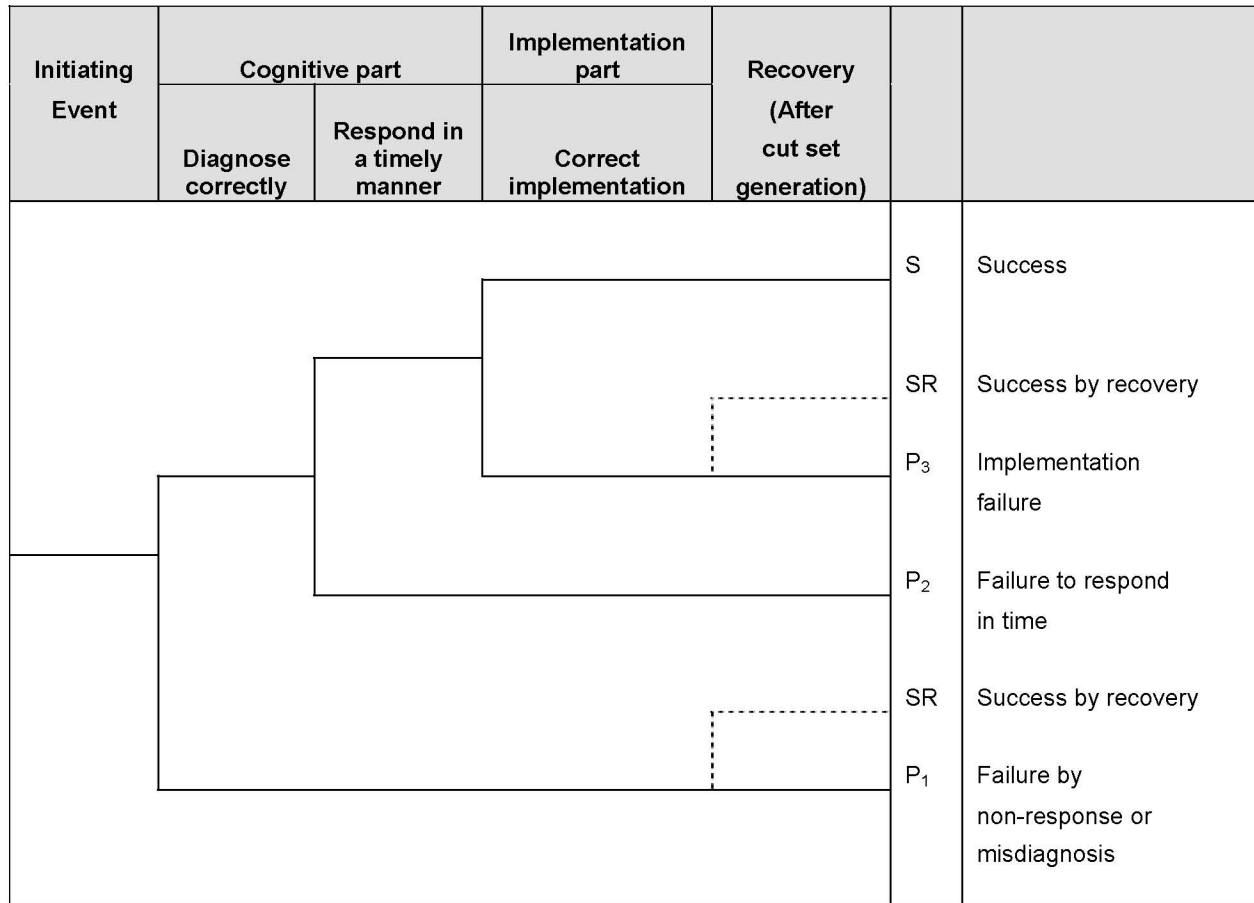


NOTE: HFE = human failure event.

Source: Original

Figure E.I-1. Incorporation of Human Reliability Analysis within the PCSA

**APPENDIX E.II  
GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS**



Source: Original

Figure E.II-1 Post Initiator Operator Action Event Tree

The representation in Figure E.II-1 consists of two elements, corresponding to a cognitive part (detection, diagnosis, and decision making) and an implementation (i.e., action) part.

P<sub>1</sub> represents the probability that operators make an incorrect diagnosis and decision and do not realize that they have done so. Some of the reasons for such mistakes are: incorrect interpretation of the procedures, incorrect knowledge of the plant state owing to communication difficulties, and instrumentation problems.

Given that the crew decides what to do correctly, there is still a possibility of failure to respond in time (represented by P<sub>2</sub>) or making an error in implementation (represented by P<sub>3</sub>).

However, it may be probable in certain scenarios that a recovery action can be taken. This consideration is taken into account after the initial quantification is completed and is applied as appropriate to the dominant cut sets.

**APPENDIX E.III  
PRELIMINARY (SCREENING) QUANTIFICATION  
PROCESS FOR HUMAN FAILURE EVENTS**

The preliminary quantification process consists of the following:

**Step 1—Complete the Initial Conditions Required for Quantification.**

The preliminary quantification process requires the following:

- The baseline scenarios are available.
- The HFEs and their associated context have been defined.
  - Collect any additional information that is not already collected and that is needed to describe and define the HFEs (and associated contexts).
  - Review all information for clarity, completeness, etc.
  - Interpret and prioritize all information with respect to relevance, credibility, and significance.

Table E.III-1 provides examples of information normally identified using the ATHEANA method (*Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis* (Ref. E8.1.23) that serve as inputs to the quantification process. The HFE/context descriptions in Table E.III-1 touch briefly on the information that is relevant to the screening-level quantification of the HFE. Since the baseline scenario generally touches on much of this information, the point of including the HFE/context descriptions is to summarize the information that pertains to the specific HFE to minimize the need for the analysts to refer back to the baseline scenario, except to obtain additional detail.

Table E.III-1. Examples of Information Useful to HFE Quantification

Information Type	Examples
Facility, conditions, and behavior for possible deviations of the scenarios	Reasonably possible unusual plant behavior and failures of systems; equipment, and indications, especially those that may be unexpected or difficult to detect by operators. Includes presence of interlocks that would have to fail to promote the deviation.
Operating crew characteristics (i.e., crew characterization)	Crew structure, communication style, emphasis on crew discussion of the “big picture.”
Features of procedures	Structure, how implemented by operating crews, opportunities for “big picture” assessment and monitoring of critical safety functions, emphasis on relevant issue, priorities, any potential mismatches with deviation scenarios.
Relevant informal rules	Experience, training, practice, ways of doing things—especially those that may conflict with informal rules or otherwise lead operators to take inappropriate actions.
Timing	Plant behavior and requirements for operator intervention versus expected timing of operator response in performing procedure steps, etc.

Table E.III-1. Examples of Information Useful to HFE Quantification (Continued)

Information Type	Examples
Relevant vulnerabilities	Any potential mismatches between the scenarios and expected operator performance with respect to timing, formal and informal rules, biases from operator experience, and training, etc.
Error mechanisms	Any that may be particularly relevant by plant context or implied by vulnerabilities; applicable mechanisms depend upon whether HFE is a slip or mistake. Examples include: failures of attention, possible tunnel vision, conflicts in priorities, biases, missing or misleading indications, complex situations, lack of technical knowledge, timing mismatches and delays, workload, and human-machine interface concerns.
Performance-shaping factors	Those deemed associated with, or triggered by, the relevant plant conditions and error mechanisms.

NOTE: HFE = human failure event.

Source: Original

In Step 1, interpreting and prioritizing all information with respect to relevance, credibility, and significance is especially important if:

- Some information is applicable only to certain scenarios, HFEs, or contexts
- There are conflicts among information sources
- Information is ambiguous, confusing, or incomplete
- Information must be extrapolated, interpolated, etc.

Completion of the initial conditions is primarily performed by a single individual, using the results of the YMP HAZOP evaluation process and reviews of other relevant information sources. Discussions are also held with the Operations Department to augment that information, and the resulting write-ups are reviewed by the PCSA facility leads and the HRA team. The initial conditions are refined as part of an open discussion among the experts (in this case, the HRA team for the study) involved in the expert opinion elicitation process. The goal of this discussion is not to achieve a consensus but, rather, to advance the understanding of all the experts through the sharing of distributed knowledge and expertise. In each case, the scenario (or group of similar scenarios) and the HFE in question are described and the vulnerabilities and strong points associated with taking the right action are discussed openly among the HRA team.

**Step 2—Identify the Key or Driving Factors of the Scenario Context.**

The purpose of Step 2 is to identify the key or driving factors on operator behavior/performance for each HFE and associated context. Each expert participating in the elicitation process individually identifies these factors based on the expert’s own judgment. Usually, these factors are not formally documented until Step 4.

Typically, there are multiple factors deemed most important to assessing the probability for the HFE in question. This is due to the focus of the ATHEANA search process on combinations of factors that are more likely to result in an integrated context (Ref. E8.1.23). When there is only a single driving factor, it is usually one that is so overwhelming that it alone can easily drive the estimated probability. For example, if the time available is shorter than the time required to

perform the actions associated with the HFE, quantification becomes much simpler and other factors need not be considered.

**Step 3—Generalize the Context by Matching it With Generic, Contextually Anchored Rankings, or Ratings.**

In Step 3, each expert participating in the elicitation process must answer the following question for each HFE: based upon the factors identified in Step 2, how difficult or challenging is this context relative to the HFE being analyzed?

Answering this question involves independent assessments by each expert. In order to perform this assessment, the specifics of the context defined for an HFE must be generalized or characterized. These characterizations or generalizations then must be matched to general categories of failures and associated failure probabilities.

To assist the experts in making their judgments regarding the probability of events, some basic guidance is provided. In thinking about what a particular HEP associated with an HFE may be, they are encouraged to think about similar situations or experiences and use that to help estimate how many times out of 10, 100, 1,000, etc., would they expect crews to commit the HFE, given the identified conditions. The following examples of what different probabilities mean are provided to the experts to help them scale their judgments:

“Likely” to fail (extremely difficult/challenging)	~0.5	(5 out of 10 would fail)
“Infrequently” fails (highly difficult/challenging) <sup>8</sup>	~0.1	(1 out of 10 would fail)
“Unlikely” to fail (somewhat difficult/challenging)	~0.01	(1 out of 100 would fail)
“Highly unlikely” to fail (not difficult/challenging)	~0.001	(1 out of 1000 would fail)

The experts are allowed to select any value to represent the probability of the HFE. That is, other values (e.g., 3E-2, 5E-3) can be used. The qualitative descriptions above are provided initially to give analysts a simple notion of what a particular probability means. For exceptional cases, the quantification approach allows an HEP of 1.0 to be used when failure was deemed essentially certain. The following general guidance in Table E.III-2 is also provided to help calibrate the assessment by providing specific examples that fall into each of the above bins, and is based on the elicited judgment and consensus of the HRA team based on their past experience. This guidance applies to contexts where generally optimal conditions exist during performance of the action. Therefore, the experts should modify these values if they believe that the action may be performed under non-optimal conditions or under extremely favorable conditions. Values may also be adjusted to take credit for design features, controls and interlocks, or procedural safety controls<sup>9,10</sup>. Examples of such adjustments are also provided below; however

<sup>8</sup> The default value is 0.1. This value is used if no preliminary assessment is performed.

<sup>9</sup> As an initial preliminary value, unsafe actions that are backed up by interlocks are assigned a human error probability of 1.0 such that no credit for human performance is taken (i.e., only the interlocks are relied upon to demonstrate 10 CFR Part 63 (Ref. E8.2.1) compliance). If this proves insufficient, a more reasonable preliminary value is assigned to the unsafe action in accordance with this Appendix.



these values are not taken to be firm in any sense of the word, but rather simply as examples of where in general terms HEPs may fall and how they may relate to each other. Types of HFEs not listed here can be given values based on being “similar to” HFEs that are listed. Whatever value is selected, the basis is briefly documented.

Table E.III-2. Types of HFEs

<b>PRE-INITIATOR HFEs</b>	
Fail to properly restore a standby system to service	0.1
Failure to properly restore an operating system to service when the degraded state is not easily detectable	0.01
Failure to properly restore an operating system to service when the degraded state is easily detectable	0.001
Calibration error	0.01
<b>HUMAN-INDUCED INITIATOR HFEs</b>	
Failure to properly conduct an operation performed on a daily basis	0.001
Failure to properly conduct an operation performed on a very regular basis (on the order of once/week)	0.01
Failure to properly conduct an operation performed only very infrequently (once/month or less)	0.1
Operation is extremely complex OR conducted under environmental or ergonomic stress	×3
Operation is extremely complex AND conducted under environmental or ergonomic stress	×10
<b>NON-RECOVERY POST-INITIATOR HFEs</b>	
Not trained or proceduralized, time pressure	0.5
Not trained or proceduralized, no time pressure	0.1
Trained and/or proceduralized, time pressure	0.1
Trained and/or proceduralized, no time pressure	0.01

Source: Original

#### Step 4—Discuss and Justify the Judgments Made in Step 3

In Step 3, each expert independently provides an estimate for each HFE. Once all the expert estimates are recorded, each expert describes the reasons why they chose a particular failure probability. In describing their reasons, each expert identifies what factors (positive and negative) are thought to be key to characterizing the context and how this characterization fit the failure category description and the associated HEP estimate.

After the original elicited estimates are provided, a discussion is held that addresses not only the individual expert estimates but also differences and similarities among the context characterizations, key factors, and failure probability assignments made by all of the experts. This discussion allows the identification of any differences in the technical understanding or interpretation of the HFE versus differences in judgment regarding the assignment of failure probabilities. Examples of factors important to HFE quantification that might be revealed in the discussion include:

<sup>10</sup>Note that if such credit is taken, then it may be necessary (based on the PCSA results) to include these items in the nuclear safety design basis or the procedural safety controls for the YMP facilities.

- Differences in key factors and their significance, relevance, etc., based upon expert-specific expertise and perspective.
- Differences in interpretations of context descriptions.
- Simplifications made in defining the context.
- Ambiguities and uncertainties in context definitions.

A consensus opinion is not required following the discussion.

#### **Step 5—Refinement of HFEs, associated contexts, and assigned HEPs (if needed)**

Based upon the discussion in Step 4, the experts form a consensus on whether or not the HFE definition must be refined or modified, based upon its associated context. If the HFE must be refined or redefined, this is done in Step 5. If such modifications are necessary, the experts “reestimate” based upon the newly defined context for the HFE (or new HFEs, each with an associated context).

The experts participating in the elicitation process are also allowed to change their estimate after the discussion in Step 4 based on the discussions during that step, whether or not the HFE definition and context are changed. Once again, a consensus is not required.

#### **Step 6—Determine final preliminary HEP for HFE and associated context**

The final preliminary value to be incorporated into the PCSA for each HFE is determined in Step 6.

The failure probabilities assigned in the preliminary HRA quantification are based on the context outlined in the base case scenarios and deemed to be “realistically conservative.” To help ensure this conservatism, if a consensus value could not be reached, the final failure probability that was assigned to each HFE was determined by choosing the highest assigned probability among the final estimates of the experts participating in the expert elicitation process.

## **APPENDIX E.IV SELECTION OF METHODS FOR DETAILED QUANTIFICATION**

There are a number of methods available for the detailed quantification of HFEs (preliminary quantification is discussed in Appendix E.III of this analysis). Some are more suited for use for the YMP PCSA than others. A number of methods were considered, but many were rejected as inapplicable or insufficient for use in quantification. Several sources were examined as part of the background analysis for selecting a method for detailed quantification (Ref. E8.1.18; Ref. E8.1.15; Ref. E8.1.25; and Ref. E8.1.22). As discussed in Section E3.2 the following four were chosen:

- ATHEANA expert judgment (Ref. E8.1.23).
- CREAM (Ref. E8.1.19)
- HEART (Ref. E8.1.28)/NARA (Ref. E8.1.9)
- THERP (Ref. E8.1.27)

This appendix discusses the selection process.

**Basis for Selection**—The selection process was conducted with due consideration of the HRA quantification requirements set forth in the ASME Level 1 PRA standard (Ref. E8.1.3) to the extent that those requirements, which were written for application to NPP PRA, apply to the types of operations conducted at the YMP. Certainly, all of the high level HRA quantification requirements were considered to be applicable. Further, all of the supporting requirements to these high level requirements were considered applicable, at least in regards to their intent. In some cases, the specifics of the supporting requirements are only applicable to NPP HRA and some judgment is needed on how to apply them. This was particularly true of those supporting requirements that judged certain specific quantification methods acceptable. This appendix lays out the specific case for the methods selected for use at the YMP (or, more to the point, the exclusion of certain methods that would normally be considered acceptable under the standard, but are deemed inappropriate for use for the YMP PCSA).

**Differences between NPP and the YMP Relevant to HRA Quantification**—There are a number of contrasts between the operations at the YMP and the operations at a NPP that affect the selection of approaches to performing detailed HRA quantification (Table E.IV-1).

Table E.IV-1. Comparison between NPP and YMP Operations

NPP	YMP
Central control of operations maintained in control room.	Decentralized (local), hands on control for most operations.
Most important human actions are in response to accidents.	Most important human actions are initiating events.
Post-accident response is important and occurs in minutes to hours. Short time response important to model in HRA.	Post-accident response evolves more slowly (hours to days). Short time response not important to model.
Multiple standby systems are susceptible to pre-initiator failures.	Standby systems do not play major role in the YMP safeguards, therefore few opportunities for pre-initiator failures.
Auxiliary operators sent by central control room operators to where needed in the plant.	Local control reduces time to respond.
Most actions are controlled by automatic systems.	Most actions are controlled by operators.
Reliance on instrumentation /gauges as operators' "eyes".	Most actions are local, either hands on or televised. Less reliance on man-machine interface.
High complexity of systems, interactions, and phenomena. Actions may be skill, rule, or knowledge based.	Relatively simple process with simple actions. Actions are largely skill based.
Many in operation for decades; HRA may include walk-downs and consultation with operators.	First of a kind; HRA performed for construction application, therefore walk-downs and consultation with operators not feasible.

NOTE: HRA = human reliability analysis; NPP = nuclear power plant; YMP = Yucca Mountain Project.

Source: Original

**Assessment of Available Methods**—There are essentially four general types of quantification approaches available:

1. Procedure focused methods:
  - A. Basis: These methods concentrate on failures that occur during step-by-step tasks (i.e., during the use of written procedures). They are generally based on observations of human performance in the completion of manipulations without much consideration of the root causes or motivations for the performance (e.g., how often does an operator turn a switch to the left instead of to the right).
  - B. Methods considered: THERP (Ref. E8.1.27).
  - C. Applicability: This method is of limited use for the YMP because important actions are not procedure driven. Many operations are skill-based and/or semi-automated (e.g., crane operation, trolley operation, CTM operation, TEV operation). However, there are some instances where such an approach would be applicable to certain unsafe actions within an HFE. In addition, the THERP dependency model is adopted by NARA as being appropriate to use within a context-based quantification approach.

- D. Assessment: THERP is retained as an option in the detailed quantification for its dependency model and for limited use when simple, procedure-driven unsafe actions are present within an HFE.
2. Time-response focused methods:
- A. Basis: These methods focus on the time available to perform a task, versus the time required, as the most dominant factor in the probability of failure. They are, for the most part, based on NPP control room observations, studies, and simulator exercises. They also tend to be correlated with short duration simulator exercises (i.e., where there is a clear time pressure in the range of a few minutes to an hour to complete a task in response to a given situation).
  - B. As discussed in *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications* (Ref. E8.1.15), examples of time-response methods include: HCR (Ref. E8.1.15) and TRCs (Ref. E8.1.17).
  - C. Applicability: These methods are not applicable to the YMP because most actions do not occur in a control room and, in addition, are generally not subject to time pressure. This is particularly true of the most important HFEs, those that are human-induced initiators. Other than a desire to complete an action in a timely fashion to maintain production schedules, time is irrelevant to these actions, especially in the context of the type of time pressure considered by these methods. Even those actions at the YMP that may take place in a control room in response to an event sequence and have time as a factor would only require response in the range of hours or days, which is outside the credible range for these methods.
  - D. Assessment: No use can be identified for these methods within the YMP PCSA. None of them are retained.
3. Context and/or cognition driven methods:
- A. Basis: These methods focus on the context and motivations behind human performance rather than the specifics of the actions, and as such are independent of the specific facility and process. To the extent that some of the methods are data-driven (i.e., they collect and use observations of human performance) the data utilized is categorized by generic task type rather than by the type of facility or equipment where the human failure occurred. This makes them more broadly applicable to various industries, tasks, and situations, in large part because they allow context-specific PSFs to be considered. This allows for them to support a variety of contexts, individual performance factors (e.g., via PSFs) and human factor approaches.
  - B. Methods considered: HEART (Ref. E8.1.28 and Ref. E8.1.29)/NARA (Ref. E8.1.9), CREAM (Ref. E8.1.19), and ATHEANA (Ref. E8.1.23) expert judgment.

- C. **Applicability:** The broad applicability of these methods and their flexibility of application make them most suited for application at the YMP. The use of information from a broad range of facilities and other performance regimes (e.g., driving, flying) support their use as facility-independent methods. The generic tasks considered can be applied to the types of actions of most concern to the YMP (i.e., human-induced initiators) as opposed to the more narrow definitions used in other approaches that make it difficult to use them for other than post-initiator or pre-initiator actions.
- D. **Assessment:** Optimally it would be convenient to use only one of the three methods of this type for all the detailed quantification. However, HEART (Ref. E8.1.28)/NARA (Ref. E8.1.9) and CREAM (Ref. E8.1.19) approach their generic task types slightly differently and also use different PSFs and adjustment factors. There are unsafe actions within the YMP HFEs that would best fit the HEART (Ref. E8.1.28)/NARA (Ref. E8.1.9) approach and others that would best fit the CREAM (Ref. E8.1.19) approach. In addition, the union of the two approaches still has some gaps that would not cover a small subset of unsafe actions for the YMP (primarily in the area of unusual acts of commission). One gap relates to dependencies between actions, but in this case NARA (Ref. E8.1.9) specifically endorses the THERP (Ref. E8.1.27) approach and so this is used. However, other gaps exist. For these cases, the ATHEANA (Ref. E8.1.23) expert judgment approach provides a viable and structured framework for the use of judgment to establish the appropriate HEP values in a manner that would meet the requirements of the ASME RA-S-2002 (Ref. E8.1.3) standard. Therefore, all three of these methods are retained for use and the selection of one versus the other is made based on the specific unsafe action being quantified. This is documented as appropriate in the actual detailed quantification of each HFE.

#### 4. Simplified methods:

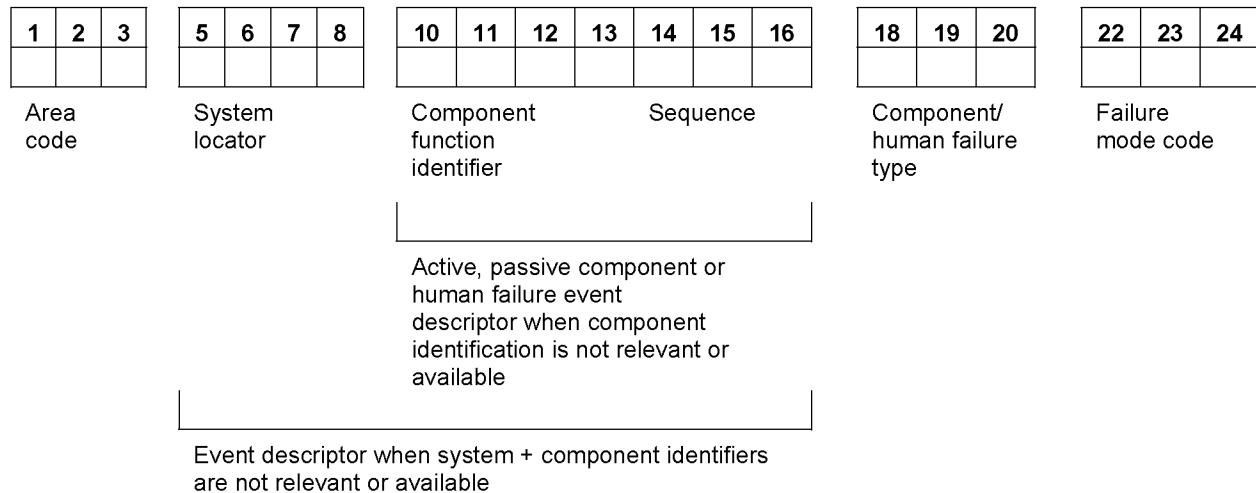
- A. **Basis:** These methods use the results of past PRAs to focus attention on those HFEs that have dominated risk. These are essentially PRA results from NPPs. As such, they presuppose NPP situations and actions, and define important PSFs based on these past NPP PRAs. They have very limited (if any) ability to investigate context, individual and human factors that are beyond NPP experience. The HEPs that result from applying these methods are calibrated to other NPP methods.
- B. **Methods considered:** ASEP (Ref. E8.1.26), SPAR-H (Ref. E8.1.16).
- C. **Applicability:** These methods are clearly biased by their very close dependence on the results of past NPP PRAs. They are too limited for application beyond the NPP environment. They are not simply inappropriate for this application, but it would be extremely difficult to make a sound technical case regarding technical validity.

- D. Assessment: No use can be identified for these methods within the YMP PCSA or any technical case made supporting them for a non-NPP application. None of them are retained.

## APPENDIX E.V HUMAN FAILURE EVENTS NAMING CONVENTION

Event names for HFEs in the YMP PCSA model follow the general structure of the naming convention for fault tree basic events. This is true whether the HFE is modeled in a fault tree, directly on an event tree, or as an initiating event. The convention, as adapted for HFEs, is as follows:

This basic event naming convention in Figure E.V-1 below is provided to ensure consistency with project standards and to permit this information to fit into a 24-character SAPHIRE field such that each basic event can be correlated to a unique component or human failure.



Source: Original

Figure E.V-1. Basic Event Naming Convention

The area code defines the physical design or construction areas where a component would be installed. Area codes are listed in *Engineering Standard for Repository Area Codes*, (Ref. E8.1.6). These codes are used rather than the facility acronyms to maintain consistency with Engineering. In this system, the CRCF is designated by area code 060, the WHF is 050, the RF is 200, the Initial Handling Facility is 51A, and Subsurface is 800. Intra-Site Operations could fall under one of several repository area codes and therefore the most appropriate code to use was the repository general area code. However, this code was insufficient for the purposes of this analysis, and a designator of ISO was substituted instead. For the majority of cases, the area coding of HFEs in Attachment E reflects the location of the operations being evaluated, such as ISO for Intra-Site Operations. However, for certain HFEs, the coding corresponds to the location of the systems impacted by the human failure, such as HVAC, which is specific to the CRCF and therefore retains the 060 coding, and AC power, which retains the 26x and 27x coding. For these specific instances, such coding provides better traceability of the HFE back to the affected equipment.



The system locator code identifies operational systems and processes. System locator codes (four characters) are listed in Table 1 of *Repository System Codes* (Ref. E8.1.7). These are generally three or four characters long, such as VCT for tertiary confinement HVAC.

The component function identifiers identify the component function and are listed in the *Engineering Standard for Repository Component Function Identifiers* (Ref. E8.1.5). These are generally three or four characters long. Some BSC component function identifiers for typical components are shown in Table E.V-1, but in cases where there is not an equivalent match, the most appropriate PCSA type code should be used (also given in Table E.V-1).

The sequence code is a numeric sequence and train assignment (suffix), if appropriate, that uniquely identifies components within the same area, system, and component function.

If an HFE is related to the failure of an individual component with an existing component function identifier and sequence code, the naming scheme should utilize these codes in the event name. If an HFE is such that these codes do not apply, the basic event name can be a free form field for describing the nature of the event, such as HCSKSCF for operator topples cask during scaffold movement or HFCANLIDAJAR for operator leaves canister lid ajar, utilizing either seven characters when there is a relevant system locator code, or 12 characters when no system codes are applicable.

The human failure type and failure mode codes are three characters each, consistent with the coding provided in Table E.V-1 below.

For HFEs, the type code always begins with HF and continues with a one letter designator for the HFE temporal phase: P for pre-initiator, I for human-induced initiator, N for non-recovery post-initiator, R for recovery post-initiator (this latter code is not used during preliminary analysis).

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes

<b>PRE-INITIATOR HFEs; TYP=HFP</b>		<b>FMC=</b>
Fail to properly restore a standby system to service		RSS
Failure to properly restore an operating system to service when the degraded state is not easily detectable		ROH
Failure to properly restore an operating system to service when the degraded state is easily detectable		ROE
Calibration error		CAL
<b>HUMAN-INDUCED INITIATOR HFEs; TYP=HFI</b>		
Failure to properly conduct an operation	Operation is performed on a daily basis.	NOD
	Operation is performed on a very regular basis (on the order of once per week)	NOW
	Operation is performed only very infrequently (once per month or less)	NOM
Operation is extremely complex OR conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	COD
	Operation is performed on a very regular basis (on the order of once per week)	COW
	Operation is performed only very infrequently (once per month or less)	COM

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes (Continued)

Operation is extremely complex AND conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	CSD
	Operation is performed on a very regular basis (on the order of once per week)	CSW
	Operation is performed only very infrequently (once per month or less)	CSM
<b>NON-RECOVERY POST-INITIATOR HFEs; TYP=HFN</b>		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN
<b>RECOVERY POST-INITIATOR HFEs; TYP=HFR</b>		
Not trained or proceduralized, time pressure		NPT
Not trained or proceduralized, no time pressure		NPN
Trained and/or proceduralized, time pressure		TPT
Trained and/or proceduralized, no time pressure		TPN

NOTE: FMC = failure mode code; HFE = human failure event; HFI = human-induced initiator HFE; HFN = human failure non-recovery post-initiator HFE; HFP = pre-initiator HFE; HFR = human failure recovery post-initiator HFE; TYP = type.

Source: Original

**ATTACHMENT F  
FIRE ANALYSIS**

## CONTENTS

	<b>Page</b>
ACRONYMS .....	F-5
F1 INTRODUCTION .....	F-6
F2 REFERENCES .....	F-7
F3 BOUNDARY CONDITIONS .....	F-9
F3.1 PLANT OPERATIONAL STATE .....	F-9
F3.2 NUMBER OF FIRE EVENTS TO OCCUR .....	F-9
F3.3 RELATIONSHIP TO PROCESS BUILDINGS.....	F-9
F3.4 IRRELEVANCY OF INDUSTRIAL FACILITY TYPE TO OUTSIDE FIRE FREQUENCY.....	F-9
F3.5 NO OTHER SIMULTANEOUS INITIATING EVENTS .....	F-9
F3.6 COMPONENT FAILURE MODES.....	F-10
F3.7 COMPONENT FAILURE PROBABILITY .....	F-10
F3.8 INTERNAL EVENTS PCSA MODEL .....	F-10
F4 ANALYSIS METHODOLOGY.....	F-11
F4.1 INTRODUCTION .....	F-11
F4.2 IDENTIFICATION OF OUTSIDE FIRE INITIATING EVENTS.....	F-11
F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY.....	F-12
F5 ANALYSIS.....	F-17
F5.1 INTRODUCTION .....	F-17
F5.2 INITIATING EVENT FREQUENCIES.....	F-17
F5.3 RESULTS .....	F-20
F6 SPECIAL STUDY – FIRE THREATENS LOW-LEVEL RADIOACTIVE WASTE IN THE LOW-LEVEL WASTE FACILITY .....	F-21
APPENDIX F.I DERIVATION OF IGNITION FREQUENCY DISTRIBUTION .....	F-24

## FIGURES

	<b>Page</b>
F.I-1. Ignition Frequency Observations.....	F-24
F.I-2. Data Point Determination .....	F-25
F.I-3. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area).....	F-26
F.I-4. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area) Divided into Two Floor Area Ranges.....	F-27
F.I-5. Plot of the Ignition Frequency Data, the Predicted Ignition Frequency, and Confidence Limits for the Predicted Value .....	F-28

**TABLES**

	<b>Page</b>
F4.2-1. Outside Fire Area Categories.....	F-12
F4.3-1. Types of Facilities: Cross Reference Between NFPA and NAICS .....	F-14
F4.3-2. Fraction of Fires and Fire Frequency for Outside Areas of a Facility .....	F-15
F5.3-1. Outside Fire Initiating Event Frequencies and Associated Distributions .....	F-20
F6-1. LLW Fire Initiating Event Frequencies with Associated Distributions.....	F-22
F6-2. Room Areas and Total Ignition Frequency.....	F-23
F.I-1. Ignition Frequency Data from Figure F.I-1 and Equation F.I-1 .....	F-25
F.I-2. Calculated Mean and Confidence Limits for the YMP LLWF Ignition Frequency.....	F-29

## ACRONYMS

CRCF	Canister Receipt and Closure Facility
FEMA	Federal Emergency Management Agency
IHF	Initial Handling Facility
LLW	low-level radioactive waste
LLWF	Low-Level Waste Facility
NAICS	North American Industry Classification System
NFIRS	National Fire Incident Reporting System
NFPA	National Fire Protection Association
PCSA	preclosure safety analysis
RF	Receipt Facility
SPM	site prime mover
TEV	transport and emplacement vehicle
WHF	Wet Handling Facility
YMP	Yucca Mountain Project

## **F1 INTRODUCTION**

This document describes the work scope, definitions and terms, methodology, and results for the fire analysis performed as part of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA). Fire analysis is divided into four major areas:

1. Initiating event identification
2. Initiating event quantification (including both ignition frequency and propagation probability)
3. Fragility analysis (including convolution of fragility and hazard curves)
4. Fire analysis model development and quantification.

Within the task, the internal events PCSA model is evaluated with respect to fire initiating events, and modified as necessary to address fire-induced failures that lead to exposures. The lists of fire-induced failures that are included in the model are evaluated as to fire vulnerability, and fragility analyses are conducted as needed.



## F2 REFERENCES

This PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design input in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents, as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.A, Section 3.2.2.F), that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

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

### Design Inputs

- F2.1 \*Amico, P.J. 2007. "Re: NFPA Correspondence." E-mail from P.J. Amico to J. Lorenz, December 3, 2007, with attachment. ACC: MOL.20071211.0227; MOL.20071211.0228.
- F2.2 \*ANSI/ANS (American National Standards Institute/American Nuclear Society) 58.23-2007. 2007. *Fire PRA Methodology Standard*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.
- F2.3 \*ASME RA-S-2002. 2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.
- F2.4 \*BSC (Bechtel SAIC Company) 2007. *Low-Level Waste Facility General Arrangement Ground Floor Plan*. 160-P10-LW00-00102-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070924.0026.
- F2.5 \*BSC 2007. *Low-Level Waste Facility General Arrangement Second Floor & Mezzanine Plan*. 160-P10-LW00-00103-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070924.0027.
- F2.6 BSC 2007. *Waste Form Throughputs for Preclosure Safety Analysis*. 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.
- F2.7 \*EPRI (Electric Power Research Institute) and NRC (U.S. Nuclear Regulatory Commission) 2005. *Detailed Methodology*. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI TR-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0062.
- F2.8 \*EPRI and NRC (2005. *Summary & Overview*. Volume 1 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0061.

- F2.9 \*Ahrens, M. 2000. *Fires in or at Industrial Chemical, Hazardous Chemical and Plastic Manufacturing Facilities, 1988 - 1997 Unallocated Annual Averages and Narratives*. Quincy, Massachusetts: National Fire Protection Association. TIC: 259997.
- F2.10 \*SAIC (Science Applications International Corporation) 2002. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*. SAIC-01/2650. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20080115.0138.
- F2.11 \*Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. Ph.D. Dissertation. Espoo, Finland: VTT Technical Research Centre of Finland. TIC: 259928. ISBN: 951-38-6392-1.
- F2.12 \*U.S. Census Bureau 3/21/2000. "1997 Economic Census: Summary Statistics for the United States 1997 NAICS Basis." Washington, DC: U.S. Census Bureau. Accessed 12/11/2007. URL: <http://www.census.gov/epcd/ec97/ustotals.htm>. ACC: MOL.20080310.0082.
- F2.13 \*Winkler, R. L. and Hays, W. L. 1975. *Statistics: Probability, Inference, and Decision*. Series in Quantitative Methods for Decision Making. 2nd Edition. Winkler, R.L., ed., New York, New York: Holt, Rinehart, and Winston. TIC: 259976. ISBN: 0-03-014011-0.
- F2.14 BSC 2008. *Intra-Site Operations and BOP Event Sequence Development Analysis*. 000-PSA-MGR0-00800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0004.
- F2.15 \*Benhardt, H.C. 1994. *Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities (U)*, WSRC-TR-93-581, Westinghouse Savannah River Company, Aiken SC, ACC: MOL.20061201.0160.

### **F3 BOUNDARY CONDITIONS**

The general boundary conditions used during the analysis of fire vulnerabilities and fire model development are clearly stated and documented. In general, the conditions are compatible with those usually applied to internal events due to fire events. The principal boundary conditions for the fire analysis are listed in the following sections.

#### **F3.1 PLANT OPERATIONAL STATE**

The initial state of the facility is normal with each system operating within its limiting condition of operation limits.

#### **F3.2 NUMBER OF FIRE EVENTS TO OCCUR**

The facility is analyzed to respond to one fire event at a given time. Additional fire events, as a result of independent causes or of reignition once a fire is extinguished, are not considered.

#### **F3.3 RELATIONSHIP TO PROCESS BUILDINGS**

Fires that occur during Intra-Site Operation activities take place outside of the main process buildings. With regard to the frequency of such fires, based on historical fire ignition frequencies from other facilities, the fire frequency across the site is proportional to the number of main process buildings on the site. That is, the number of opportunities for fires outside buildings is affected by the number of main process buildings being serviced. The number of main waste handling buildings at YMP is six (Initial Handling Facility (IHF), Receipt Facility (RF), Wet Handling Facility (WHF) and three Canister Receipt and Closure Facilities (CRCFs)).

#### **F3.4 IRRELEVANCY OF INDUSTRIAL FACILITY TYPE TO OUTSIDE FIRE FREQUENCY**

The frequency of outside fires at YMP is expected to be similar to those from other industrial facilities. The specific type of facility, the type of construction of the buildings and other features, are not considered relevant to the frequency of outside fires since the ignition sources that exist outside of the buildings are considered to be generic to any industrial facility. This does not extend to the assessment of fire severity, since the type of facility could affect the type and availability of combustibles. Fire severity is addressed in Attachment D and, as such, is not relevant here.

#### **F3.5 NO OTHER SIMULTANEOUS INITIATING EVENTS**

It is standard practice to not consider the occurrence of other initiating events (human-induced and naturally occurring) during the time span of an event sequence because: (1) the probability of two simultaneous initiating events within the time span is small, and (2) each initiating event causes operations of the waste handling facility to cease, which further reduces the conditional probability of the occurrence of a second initiating event, given the first has occurred.

### **F3.6 COMPONENT FAILURE MODES**

The failure mode of a structure, system, or component affected by a fire is the most severe, with respect to consequences. For example, the failure mode for a canister could be the overpressurization of a reduced-strength canister.

### **F3.7 COMPONENT FAILURE PROBABILITY**

Fires large enough to fail waste containment components are large enough to fail all active components in the immediate vicinity. Active components fail in a de-energized state for such fires.

### **F3.8 INTERNAL EVENTS PCSA MODEL**

To implement the systems analysis guidance contained herein, the fire PCSA team uses the internal events PCSA model, which is developed concurrently with the fire PCSA. This internal events PCSA is used as the basis for the fire PCSA. The internal events PCSA is in general conformance with the ASME PRA *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. F2.3).

## **F4 ANALYSIS METHODOLOGY**

### **F4.1 INTRODUCTION**

The general methodological basis of this analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. F2.10). Chemical agent disposal facilities are similar to those in the geologic repository operations area in that these facilities are handling and disposal facilities for highly hazardous materials, and so the analysis of fires in those facilities has similar issues and needs. This is a “data based” approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the YMP waste handling facilities. To the extent applicable to a non-reactor facility, NUREG/CR-6850, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*, Volumes 1 (Ref. F2.8) and 2 (Ref. F2.7) are also considered in the development of this analysis method. The method complies with the applicable requirements of the American Nuclear Society fire probabilistic risk assessment standard (Ref. F2.2) that are relevant to a non-reactor facility. Many of the definitions, modeling approximations, and requirements of these documents were used to develop this analysis.

### **F4.2 IDENTIFICATION OF OUTSIDE FIRE INITIATING EVENTS**

Outside fire initiating events at YMP are considered for the potential for a fire to directly affect the waste containers and cause a breach that would result in a release. The fire analysis, therefore, focused on the potential for a fire to directly affect the waste containers and cause a breach that would result in a release. The initiating events for Intra-Site Operations were identified in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. F2.14). The steps of this process are as provided in the following sections.

#### **F4.2.1 Identify Areas Onsite Where Waste Containers Can Be Present**

The processes for the movement of waste containers onsite but outside of buildings are evaluated, and the areas where the waste containers either sit or traverse are identified. Each area where waste can be present, even if only for a brief time, is listed.

#### **F4.2.2 Correlate These Areas with National Fire Protection Association Historical Data for Outside Fires**

The National Fire Protection Association (NFPA) historical data identifies the areas outside buildings where fires have occurred (Ref. F2.9). These have been grouped into broader categories for use in this study. These groupings are as follows in Table F4.2-1:

Table F4.2-1. Outside Fire Area Categories

Area
Storage areas <sup>a</sup> —To include all areas where products are held while awaiting process, shipment, or use.
Receiving areas <sup>b</sup> —To include all areas where products are moved into or out of a building while onsite, but are still outside the building.
Trash/rubbish areas
Areas containing equipment <sup>c</sup> —To include all areas outside the building that contain operating process, HVAC, maintenance, or other machinery and equipment.
Open areas <sup>d</sup> —To include fields, roads, and right of ways.
Vehicles <sup>e</sup>
Other —Primarily applies to exterior structural areas of buildings.

NOTE: <sup>a</sup> The sum of the following NFPA areas are 1) product storage area, tank, or bin, 2) unclassified storage area, and 3) supply storage room or area.

<sup>b</sup> The sum of the following NFPA areas are 1) shipping, receiving, or loading area, 2) court, terrace, or patio, and 3) conveyor.

<sup>c</sup> The sum of the following NFPA areas are 1) process or manufacturing area, 2) unclassified service or equipment area, 3) heating equipment room or area, 4) incinerator room or area, 5) unclassified service facility, 6) machinery room or area, and 7) maintenance shop or area.

<sup>d</sup> The sum of the following NFPA areas are 1) lawn, field, or open areas, 2) railroad right of way or embankment, and 3) highway, public right of way, or street.

<sup>e</sup> The sum of the following NFPA areas are 1) engine, wheel, or running area of vehicle, 2) exterior surface of vehicle, 3) truck or load-carrying area of vehicle, and 4) unclassified vehicle area.

HVAC = heating, ventilation, and air conditioning; NFPA = National Fire Protection Association.

Source: Original

### F4.2.3 Define Initiating Events

Fire ignition occurrences are identified for each outside area where a waste container can be present.

### F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY

In order to assess the total fire frequency, two pieces of information are required: the number of facilities, and the number of fires at these facilities. The first piece of data is maintained by the U.S. Census Bureau, which conducts an economic census (Ref. F2.12, Codes 324, 325, and 3261). The second piece of data is tracked by NFPA. This approach uses historical data over a 10-year period (1988 to 1998) from these databases. Specifically, the fire data used in this report were taken from a report authored by the NFPA Division of Fire Analysis and Research: *Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Plants, 1988 - 1997 Unallocated Annual Averages and Narratives*<sup>1</sup> (Ref. F2.9). These data are used to develop estimates for the total frequency of fires and the distribution of fires on the grounds of the facility.

<sup>1</sup> As stated in the boundary conditions, the type of facility is considered to be irrelevant to the frequency of ignition of outside fires.

The primary source of data on the number of fires is the National Fire Incident Reporting System (NFIRS), which is jointly administered by the Federal Emergency Management Agency (FEMA) and NFPA. NFIRS provides annual computerized databases of fire incidents. It is a voluntary program wherein individual fire departments fill out data forms and submit them through their state NFIRS coordinator to FEMA/NFPA. Because it is a voluntary program, it is recognized that the NFIRS database only captures about one third to one half of all U.S. fires each year. Projecting NFIRS results develops NFPA's national fire estimates. To project NFIRS results, at least an estimate of the NFIRS fires as a fraction of the total, is needed. However, the NFIRS data does not provide any information on the total population from which the data is collected, nor do they address the nonuniformity of the data due to the voluntary collection methods used. To address the limitations of the NFIRS data, and to extend the NFIRS data to provide a more complete analysis of the U.S. fire problem, the NFPA conducts an additional annual survey to augment the FEMA NFIRS program.

The NFPA survey is based on a stratified random sample of roughly 3,000 (of 30,000) U.S. fire departments. The survey is stratified by the population size (i.e., the number of people protected by the department) to reduce the uncertainty of the final estimates. Small rural communities protect fewer people and are less likely to respond, so a large number are surveyed to obtain an adequate sample. Large city fire departments are few in number, so all are surveyed and have a high response rate so that an excellent estimate is obtained. A variety of data is collected during the NFPA survey process, which allows the NFIRS data to be projected on a nationwide basis with some accuracy. The NFPA survey also allows individual component parts of the NFIRS data to be projected on a national basis. This multiple calibration approach makes use of the NFPA survey where its statistics design advantages are the strongest and yields scaling ratios to extend the fractional NFIRS data to a true nationwide estimate of the U.S. fire problem.

Data on the number and type of facilities is maintained by the U.S. Census Bureau, which conducts an economic census (Ref. F2.12). The U.S. Census Bureau performs a count of all businesses in the United States and categorizes them in accordance with the North American Industry Classification System (NAICS) (Ref. F2.12). As this program is not voluntary, these data are believed to be accurate as reported.

The NFPA does not use the NAICS to categorize the type of facility, so there is a need to correlate the two systems in order to ensure that both the number of facilities and the number of fires represent counts from the same population. This is relatively straightforward at the level of the major categories of facilities. Table F4.3-1 gives a cross-reference between the two systems at that level. Some of the cross reference matching of categories shown in the table may not seem obvious from the titles, but a review of the definitions used by NFPA/FEMA (Ref. F2.9) and NAICS (Ref. F2.12) clearly leads to the classifications shown in Table F4.3-1.

Table F4.3-1. Types of Facilities: Cross Reference Between NFPA and NAICS

NFPA Facility Categories	NAICS Facility Categories
Food Products	Food Products
Beverage, Tobacco, or Related Oil Products	Beverage and Tobacco Products
Textiles	Textile Mills Textile Product Mills
Wearing Apparel, Leather, Rubber Products	Apparel Products Leather and Allied Products Plastics and Rubber (Rubber subgroup)
Wood, Furniture, Paper, or Printing Products	Wood Products Paper Products Printing and Related Support Activities Furniture and Related Products
Chemical, Plastic, or Petroleum Products	Petroleum and Coal Products Chemical Products (Except photographic) Plastics and Rubber (Plastics subgroup)
Metal or Metal Products	Primary Metal Products Fabricated Metal Products Machinery Computer and Electronic Products Electrical Equipment, Appliances, and Components
Vehicle Assembly or Manufacturing	Transportation Equipment
Other	Miscellaneous Chemical Products (photographic)
Unclassified or Unknown	Nonmetallic Mineral Products

NOTE: NFPA = National Fire Protection Association; NAICS = North American Industry Classification System.

Source: *Fires in or at Industrial Chemical, Hazardous Chemical and Plastic Manufacturing Facilities, 1988 - 1997 Unallocated Annual Averages and Narratives* (Ref. F2.9) and "1997 Economic Census: Summary Statistics for the United States 1997 NAICS Basis." (Ref. F2.12).

Two different calculations are performed on two different sub-populations in order to test the sensitivity of the overall fire frequency to the type of process facility. The first calculation uses facilities classified by NFPA under, "Chemical, Plastic, or Petroleum Products." According to NFPA data (Ref. F2.1), there are approximately 287 outside fires involving property of value annually (2,870 total fires in the ten year period) in such facilities. Ref. F2.1 contains an e-mail that was sent from the author of Ref. F2.9 (M. Ahrens) to the originator of this Attachment, Paul Amico. The information from this correspondence is being used to provide information based on the NFIRS and NFPA survey to supplement the information from Ref. F2.9.

According to NAICS (Ref. F2.12, Codes 324, 325, and 3261), the total number of facilities of this type is 29,303. Therefore, the frequency of potentially significant fires in these facilities is:

$$F = \frac{287 \text{ fires/yr}}{(29,303 \text{ facilities})} = 9.8\text{E-}03 \text{ fires/facility-yr} \quad (\text{Eq. F-1})$$

The second calculation uses subcategories within the classification systems to determine whether a particular subcategory of, "Chemical, Plastic, or Petroleum Products" would yield a different result (i.e., whether the answer was significantly related to facility type).



According to NFPA data (Ref. F2.1), each year there are approximately 62 outside fires involving property of value per year (620 total fires in the ten year period) in the subcategory, “Industrial Chemical, Hazardous Chemical, and Plastics Facilities.” According to NAICS (Ref. F2.12), the total number of facilities in the corresponding subcategories is 5,870. Therefore, the frequency of potentially significant fires in these facilities is:

$$F = \frac{62 \text{ fires/yr}}{(5,870 \text{ facilities})} = 1.1\text{E-}02 \text{ fires/facility-yr} \quad (\text{Eq. F-2})$$

Thus, the two estimates of the outside fire frequency are virtually the same. Overall, the use of a total mean outside fire frequency of 1E-02 fires per facility, per facility-year is deemed to be appropriate.

The next refinement is to determine where these outside fires start. One analysis performed by the NFPA was in terms of this distribution (Ref. F2.9, Section 5). With some interpretation, these data can be used to estimate the fraction of the total fire frequency that should be assigned to the various onsite areas outside the building. The results of this assessment are provided in Table F4.3-2.

Table F4.3-2. Fraction of Fires and Fire Frequency for Outside Areas of a Facility

Area	# of Fires <sup>a</sup>	Fraction	Fire Frequency per Facility-year
Storage areas – To include all areas where products are held while awaiting process, shipment, or use	125	0.20	2.0E-03
Receiving areas – To include all areas where products are moved into or out of a building while onsite but are still outside the building	57	0.092	9.2E-04
Trash/rubbish areas	84	0.135	1.4E-03
Areas containing equipment – To include all areas outside the building that contain operating process, HVAC, maintenance, or other machinery and equipment	121	0.195	2.0E-03
Open areas – To include fields, roads, and right of ways	84	0.135	1.4E-03
Vehicles	16	0.025	2.5E-04
Other	136	0.22	2.2E-03

NOTE: <sup>a</sup> Does not total 620 due to rounding after weighted allocation of fires coded in database as starting in unknown location (6.2% of fires).  
HVAC = heating, ventilation, and air conditioning.

Source: Derived from (Ref. F2.9, Section 5).

As shown in Table F4.3-2, the frequency is expressed in terms of facility-year (since the number of NFPA fires is divided by the number of NAICS facilities). There is some uncertainty as to what is meant by a “facility” in this context. The NAICS does not make clear whether multiple process buildings can be considered a single facility, although, noting in this context, that the purpose of the NAICS is an economic census, implies that the number of main process buildings (i.e., the throughput of a given site) is more important than the number of sites. Because of this, in order to avoid potentially non-conservative probabilistic results, a boundary condition has been established that each main process building at the YMP constitutes a facility, and the

outside fire frequency pertains to each of them (i.e., each of these buildings generates the necessary conditions to contribute a full measure of potential fire ignitions). The aging pads, buffer areas and subsurface are not considered as separate facilities, but rather as support areas for the process buildings (i.e., they are an integral part of a typical facility in that they supply the “raw materials” to the process and take the “product” from the process). In addition, the other support buildings are also not considered facilities for the purpose of determining the overall frequency of outside fires, for a similar reason. Therefore, the overall frequency of outside fires for the geologic repository operations area is the frequency per facility-year, times the number of main process buildings (six: IHF, WHF, RF, and three CRCFs).

A suitable uncertainty distribution is applied to the results of the initiating event frequency analysis to represent the significant uncertainty that results from the application of this methodology. The distribution is selected to reflect that, in particular recognition of the discussion above, it is likely that the calculated mean is conservative.

## F5 ANALYSIS

### F5.1 INTRODUCTION

Fire initiating event frequencies have been calculated for each initiating event identified for Intra-Site Operations. This section details the analysis performed to determine these frequencies, using the methodology documented in section F4. The discussion of the analysis below presupposes that the reader has developed a thorough understanding of the details of that methodology, as those details are not repeated in this section.

### F5.2 INITIATING EVENT FREQUENCIES

There were three initiating events identified for Intra-Site Operations:

1. Fire threatens a waste container during onsite transport (site transporter, cask tractor/cask transfer trailer, or site prime mover (SPM))
2. Fire threatens a waste container in buffer area
3. Fire threatens a waste container on aging pad.

The selection of these events is documented in *Intra-Site Operations and BOP Event Sequence Development Analysis* (Ref. F2.14). This section addresses the quantification of these events.

#### F5.2.1 Fire Threatens a Waste Container during Transport (Site Transporter, Cask Tractor/Cask Transfer Trailer, or Site Prime Mover)

This represents fires that ignite on/in the transportation vehicles used to move containerized waste forms around the site. Transportation vehicles include the site transporter, cask tractor, the SPM, and the transport and emplacement vehicle (TEV) (the TEV is not included as part of Intra-Site Operations, but rather is included as part of Subsurface Operations). While it could be argued that a vehicle fire can occur at any time, it is more likely that it occurs while the vehicle is in use. For that reason, the fire frequency per year is converted to a frequency per vehicle operation by dividing by the total average number of operations of all such vehicles (both when loaded with a waste container and when not) per year. This allows initiating event frequencies over the preclosure period to be determined for each vehicle, and waste container to be quantified by multiplying by the total number of operations for each vehicle and waste container when the waste container is present.

The outside area that is relevant to this event, from Table F4.3-2, is “vehicles.” That is, the waste container is vulnerable to a vehicle fire during transport. The total frequency per facility-year of such fires is, from the same table, 2.5E-04 per facility-year. As discussed in the methodology, this value is multiplied by six to determine the overall frequency of vehicle fires on the site.

$$\begin{aligned}\text{Site vehicle fire frequency/year} &= 2.5\text{E-}04 \text{ fires/facility-year} \times 6 \text{ facilities} \\ &= 1.5\text{E-}03 \text{ fires/year}\end{aligned}$$

This is then converted to the total expected number of vehicle fires over the 50-year preclosure period.

$$\begin{aligned} \text{Site vehicle fire frequency (preclosure period)} &= 1.5\text{E-}03 \text{ fires/year} \times 50 \text{ years} \\ &= 7.5\text{E-}02 \text{ fires} \end{aligned}$$

This needs to be converted into a frequency per vehicle operation, which is the final form of the initiating event frequency. In actuality, a vehicle fire can start in any type of vehicle (e.g., service vehicle, delivery vehicle, etc.), not just in a vehicle that transports waste. There is no estimate available for the number of onsite vehicle movements; however, the number of waste container movements is estimated since this is integral to the throughput of the site (Ref. F2.6). Therefore, the potential for fires in other types of vehicles is ignored, which adds a level of conservatism to the results.

The PCSA throughput analysis (Ref. F2.6, Table 4) estimates that there are approximately 40,000 waste container movements outside of the process buildings during the preclosure period. This includes operations of the site transporter, cask tractor, SPM, and TEV.<sup>2</sup> For each waste container movement, there is another movement of the vehicle when a waste container is not present. Thus, the total number of operations of the transport vehicles is approximately 80,000. The fire initiating event frequency per operation is therefore:

$$\begin{aligned} \text{Fire threatens a waste container during onsite transport} \\ &= 7.5\text{E-}02 \text{ fires}/80,000 \text{ operations} \\ &= 9\text{E-}07 \text{ fires}/\text{operation}^3 \end{aligned}$$

### **F5.2.2 Fire Threatens a Waste Container in Buffer Area**

The outside area that is relevant to this event, from Table F4.3-2, is “receiving areas.” That is, the waste container is vulnerable to a fire in an outside receiving area for a short term while awaiting processing. The total frequency per facility-year of such fires is, from the same table, 9.2E-04 per facility-year. As discussed in the methodology, this value is multiplied by six to determine the overall frequency of storage area fires on the site.

$$\begin{aligned} \text{Site receiving fire frequency/year} &= 9.2\text{E-}04 \text{ fires/facility-year} \times 6 \text{ facilities} \\ &= 5.5\text{E-}03 \text{ fires/year} \end{aligned}$$

This is then converted to the total expected number of buffer area fires over the 50-year preclosure period.

---

<sup>2</sup> When determining the fire ignition rate per operation on the site, the operation of all site vehicles needs to be considered in the allocation, not just those involved in Intra-Site Operations. When assembling the risk model for Intra-Site Operations, the resultant rate is used as the initiating event frequency and is multiplied only by the number of Intra-Site vehicle operations involving waste movements.

<sup>3</sup> Given the broad range of the approximations used in this analysis, there is no justification for using a mean to more than one significant digit.

$$\begin{aligned}\text{Site receiving fire frequency (preclosure period)} &= 5.5\text{E-}03 \text{ fires/year} \times 50 \text{ years} \\ &= 3\text{E-}01 \text{ fires}\end{aligned}$$

This is the final form of the initiating event frequency. This event is not conducive to converting into a frequency per operation, since individual operations do not affect whether a waste container is present in a storage area (only how much is present, which is not important to the analysis since a release from even a single waste container has unacceptable consequences).

$$\text{Fire threatens a waste container in buffer area} = 0.3 \text{ fires}$$

### **F5.2.3 Fire Threatens a Waste Container on Aging Pad**

The outside area that is relevant to this event, from Table F4.3-2, is “storage areas.” That is, the waste container is vulnerable to a fire in an outside storage area over a longer term while awaiting handling. The total frequency per facility-year of such fires is, from the same table, 2E-03 per facility-year. As discussed in the methodology, this value is multiplied by six to determine the overall frequency of storage area fires on the site.

$$\begin{aligned}\text{Site storage fire frequency/year} &= 2\text{E-}03 \text{ fires/facility-year} \times 6 \text{ facilities} \\ &= 1.2\text{E-}02 \text{ fires/year}\end{aligned}$$

This is then converted to the total expected number of aging pad fires over the 50-year preclosure period.

$$\begin{aligned}\text{Site storage fire frequency (preclosure period)} &= 1.2\text{E-}02 \text{ fires/year} \times 50 \text{ years} \\ &= 6\text{E-}01 \text{ fires}\end{aligned}$$

This is the final form of the initiating event frequency. This event is not conducive to converting into a frequency per operation, since individual operations do not affect whether a waste container is present in a storage area (only how much is present, which is not important to the analysis since a release from even a single waste container has unacceptable consequences).

$$\text{Fire threatens a waste container on aging pad} = 0.6 \text{ fires}^4$$

### **F5.2.4 Uncertainty**

Formal analysis of the uncertainties in this estimate is not appropriate given the sources of information used. It was decided that the use of analyst judgment was most appropriate. A team of three individuals held a discussion of the sources of uncertainty and their potential effects on the calculated mean value.

First, the uncertainties are expected to be large. The use of two different data bases for the numerator and denominator offer the opportunity for a mismatch in the populations covered. The accuracy of the databases is also unclear. The NFPA data on fires is based on voluntary

---

<sup>4</sup> Given the broad range of the approximations used in this analysis, there is no justification for using a mean to more than one significant digit.

compliance by fire departments, and while NFPA adjusts the data for this and has a substantial past history of this type of analysis, the level of uncertainty is still greater than for a more rigorous system of data collection. Further, the data collectors (the individuals assigned to collect the data by each fire department) are not subject to a single consistent training course.

The census bureau data is likely to be more accurate, however there is still a potential for error in determining the number of actual buildings that constitute a facility for counting purposes. The methodology states that “A company operating at more than one location is required to file a separate report for each store, factory, shop, or other location.” This is clear in regards to physical locations, but not clear in regards to multiple operations at one location. The approach used in this analysis to consider each of the six main waste handling buildings as a facility for counting purposes is conservative, but it increases uncertainty and also skews the distribution towards the high side (i.e., there is more room for the actual value to be lower than higher).

Taking all of this into consideration, the team selected a lognormal distribution (to address the issue of the conservative mean) with an error factor of 15 (to address the nature of the uncertainties).

### F5.3 RESULTS

The results of the analysis are the fire initiating event frequencies and their associated distributions. The initiating event frequencies represent the probability, over the length of the preclosure period, that a fire threatens the stated waste container during the stated vulnerability. The results are summarized in Table F5.3-1.

Table F5.3-1. Outside Fire Initiating Event Frequencies and Associated Distributions

Initiating Event	Mean frequency (per 50 years)	Error Factor	Distribution
Fire threatens a waste container during transportation	9E-07 fires/operation	15	lognormal
Fire threatens a waste container in buffer area	0.3 fires	15	lognormal
Fire threatens a waste container on aging pad	0.6 fires	15	lognormal

Source: Original

## F6 SPECIAL STUDY – FIRE THREATENS LOW-LEVEL RADIOACTIVE WASTE IN THE LOW-LEVEL WASTE FACILITY

In addition to outside fires, Intra-Site Operations analysis also considers fires that affect the Low-Level Waste Facility (LLWF). The methodology used for the analysis of outside fires is not applicable to a fire in this facility. Instead, the fire ignition frequency for the LLWF was developed from the approach to fire ignition frequencies by building type that was used for the other surface facilities (Ref. F2.11). This methodology provides Equation F-3 (Ref. F2.11, Section 5.3.3.1):

$$f_m(A) = c_1 A^r + c_2 A^s \quad (\text{Eq. F-3})$$

where  $f_m$  is the fire ignition frequency per  $\text{m}^2\text{-yr}$ ,  $A$  is the floor area (in  $\text{m}^2$ ) and  $c_1$ ,  $c_2$ ,  $r$ , and  $s$  are coefficients that were determined from historical data observations for different types of facilities. It was determined that the facility type ‘warehouse’ best suits the LLWF. The coefficients for a warehouse are 3.82, 2.0E-06, -2.08, and -0.05 for  $c_1$ ,  $c_2$ ,  $r$ , and  $s$  respectively (Ref. F2.11, Section 5.3.3.2). Utilizing general layout drawings *Low-Level Waste Facility General Arrangement Ground Floor* (Ref. F2.4) and *Low-Level Waste Facility General Arrangement Second Floor & Mezzanine Plan* (Ref. F2.5), the total area (in  $\text{m}^2$ ) was determined to be 5,514, yielding an ignition frequency of 1.36E-06 (per  $\text{m}^2/\text{year}$ ). This frequency is then multiplied by the area of the facility and the preclosure period to determine the overall frequency of LLWF fires on the site.

$$\begin{aligned} &\text{Low-level radioactive waste (LLW) fire frequency}/\text{m}^2/\text{year} \\ &= 1.4\text{E-}06 \text{ fires}/\text{facility-year} \times 5,514 \text{ m}^2 \\ &= 7.52\text{E-}03 \text{ fires}/\text{year} \end{aligned}$$

This is then converted to the total expected number of LLWF fires over the 50-year preclosure period.

$$\begin{aligned} \text{LLW fire frequency (preclosure period)} &= 7.5\text{E-}03 \text{ fires}/\text{year} \times 50 \text{ years} \\ &= 3.8\text{E-}01 \text{ fires} \end{aligned}$$

An uncertainty distribution was estimated for the LLWF based on the distribution derived in Appendix F.I. The approach to determining the distribution is the same as was developed for the industrial facility-type analysis that was used for other YMP facilities. It was determined that the effort required to perform a specific uncertainty assessment for warehouse-type facilities for the purpose of developing an uncertainty value for the LLWF was not required. Although the two different facility types have different coefficients for Equation F-1, it is not expected that the error factors on the final frequency values would be sufficiently different to merit a special analysis.

The estimated error factor obtained from Appendix F.I (Ref. F2.15) is utilized in Equation F-4 to convert the median LLW fire frequency to the mean LLW fire frequency (4.1E-01).

$$mean = Median \times e^{\frac{\left(\frac{\ln EF}{1.645}\right)^2}{2}} \quad (\text{Eq. F-4})$$

where

*EF* = error factor

This mean LLW fire frequency is then converted to the total expected number of large (fires which consume the building) LLWF fires over the 50-year preclosure period.

LLW fire frequency (preclosure period)  
 = 4.1E-01 fires/year × 0.165 large fire propagation probability  
 = 6.8E-02 large fires

The results of the analysis are the fire initiating event mean frequency, the large fire initiating event mean frequency, and their associated distributions shown below in Table F6-1. The initiating event frequency represents the probability, over the length of the preclosure period, that a fire could threaten a LLW container during the stated vulnerability.

Table F6-1. LLW Fire Initiating Event Frequencies with Associated Distributions

Initiating Event	Mean frequency (per 50 years)	Error Factor	Distribution
Fire threatens LLW in the LLWF	4.1E-01 fires	2.0	Lognormal
Large fire threatens LLW in the LLWF	6.8E-02 fires	2.0	Lognormal

NOTE: LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility.

Source: Original

Table F6-2 shows the calculations that were performed to identify individual room areas, total ignition frequency, and uncertainty distributions.



Table F6-2. Room Areas and Total Ignition Frequency

Room	Length (ft)	Width (ft)	Area (sq-ft)	Area (sq-m)	NOTES
1001	42	102	4,284	398	
1002	108	81	13,292	1,235	Area multiplied by 2 - room extends two floors
1002A	12	9	216	20	Area multiplied by 2 - room extends two floors
1002B	9	9	162	15	Area multiplied by 2 - room extends two floors
1003	24	32	1,536	143	Area multiplied by 2 - room extends two floors
1004	23	25	1,150	107	Area multiplied by 2 - room extends two floors
1005	15	25	750	70	Area multiplied by 2 - room extends two floors
1006	15	25	750	70	Area multiplied by 2 - room extends two floors
1007	105	9	1,890	176	Area multiplied by 2 - room extends two floors
1008	49	29	2,842	264	Area multiplied by 2 - room extends two floors
1009	49	29	2,842	264	Area multiplied by 2 - room extends two floors
1010	49	29	2,842	264	Area multiplied by 2 - room extends two floors
1011	49	29	2,842	264	Area multiplied by 2 - room extends two floors
1012	113	68	7,684	714	
1013	26	47	1,222	114	
1014	26	9	234	22	
1200-1223	81	68	5,508	512	
M001	42	95	3,990	371	
2001	80	66	5,280	491	

<b>Total Area (sq-m)</b>	<b>5,514</b>
<b>Ignition Frequency (per sq-m/yr)</b>	<b>1.36E-06</b>
<b>Ignition Frequency (per yr)</b>	<b>7.52E-03</b>
<b>Ignition Frequency (50 years - preclosure period)</b>	<b>3.76E-01</b>
<b>Large Fire Propagation Probability</b>	<b>1.65E-01</b>
<b>Large Fire Frequency</b>	<b>6.20E-02</b>

EF	Mean
<b>2.00E+00</b>	<b>4.11E-01</b>
	<b>1.65E-01</b>
	<b>6.78E-02</b>

NOTE: EF = error factor; ft = feet; m = meter; yr = year.

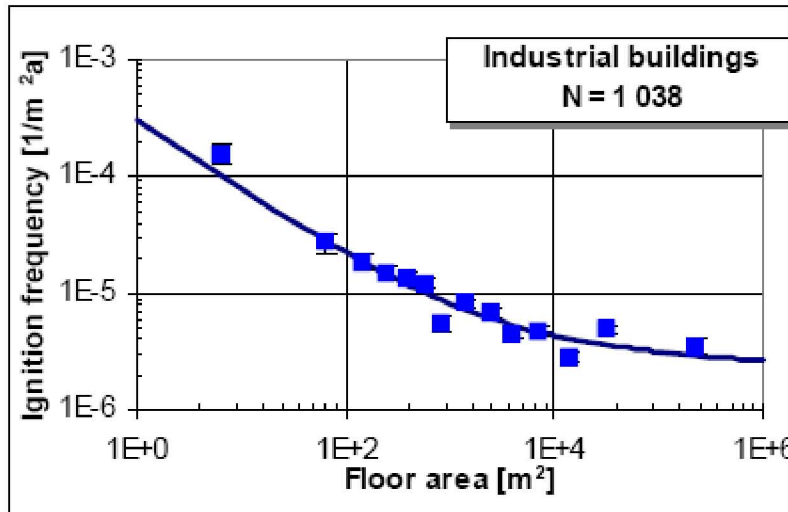
Source: Original

### APPENDIX F.I DERIVATION OF IGNITION FREQUENCY DISTRIBUTION

For proper consideration of the fire frequency analysis of the CRCF, WHF, IHF, and RF, it was necessary to develop an uncertainty distribution for the industrial building fire frequency. The *Utilisation of Statistics to Assess Fire Risks in Buildings* study (Ref. F2.11) used to develop these frequencies presents an equation with floor area as an input to determine frequency. Equation F.I-1 is developed based on sample data collected:

$$f_m''(A) = c_1 A^r + c_2 A^s \quad (\text{Eq. F.I-1})$$

where  $f_m''$  is the annual fire frequency per square meter of floor area,  $A$  is the floor area, and the values  $c_1$ ,  $c_2$ ,  $r$ , and  $s$  are constants determined by the line of best fit derived from the data. For industrial buildings, the values for the constants are as follows:  $c_1 = 3E-04$ ,  $c_2 = 5E-06$ ,  $r = -0.61$ , and  $s = -0.05$ . The data for industrial buildings and the resulting line of best fit are presented in Figure F.I-1.



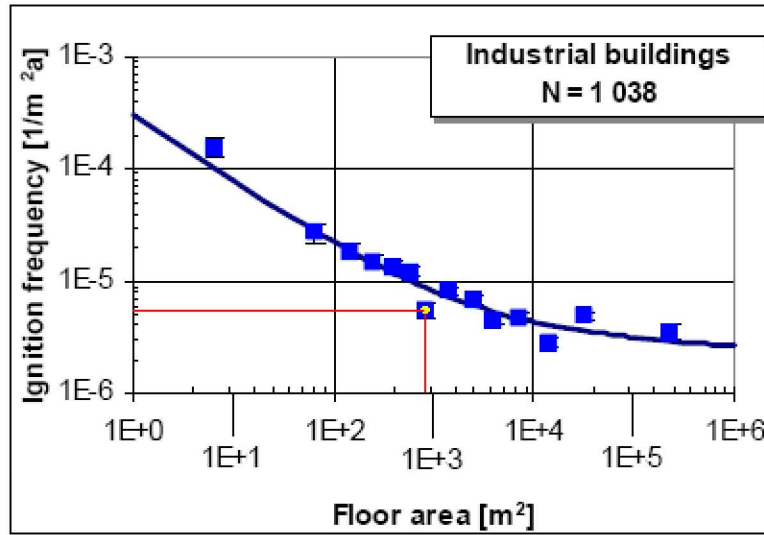
NOTE: a = area; m = meter; n = data sample size.

Source: (Ref. F2.11).

Figure F.I-1. Ignition Frequency Observations

Each data point in the graph represents the average of many data points. The individual data points and the average values were not provided. Because the data is only presented graphically, it is necessary to estimate the data for the purposes of this analysis. To accomplish this, the center of each data point is found, and x axis values are added such that the powers increase by a unit of one. Horizontal and vertical lines are drawn from each data point to the x and y axes. The ignition frequency and floor area are then estimated based on the relative distances between these lines and the major axis values. For the example shown in Figure F.I-2, the distance from the 1E+2 label to the red vertical line is divided by the distance from the 1E+2 to 1E+3 labels. In this case, the result is 0.925. Thus, the floor area for the data point is  $10^{2.925}$ . The ignition frequency is determined in an identical manner. The ignition frequency and floor area obtained

in this manner are displayed in Table F.I-1. The ignition frequency predicted based on Equation F.I-1 is also provided in the table.



NOTE: a = area; m = meter; n = data sample size.

Source: Original

Figure F.I-2. Data Point Determination

Table F.I-1. Ignition Frequency Data from Figure F.I-1 and Equation F.I-1

Graphically Determined Data Points	From Equation 1	
	Ignition Frequency (1/yr m <sup>2</sup> )	Predicted Frequency (1/yr m <sup>2</sup> )
Floor Area (m <sup>2</sup> )		
7	1.6E-04	9.6E-05
65	2.8E-05	2.8E-05
150	1.9E-05	1.8E-05
240	1.5E-05	1.4E-05
380	1.4E-05	1.2E-05
570	1.2E-05	9.9E-06
840	5.6E-06	8.5E-06
1,400	8.9E-06	7.1E-06
2,500	7.0E-06	5.9E-06
4,100	4.6E-06	5.2E-06
7,100	4.8E-06	4.5E-06
14,000	2.9E-06	4.0E-06
33,000	5.1E-06	3.5E-06
230,000	3.6E-06	2.9E-06

NOTE: m = meter; yr = year.

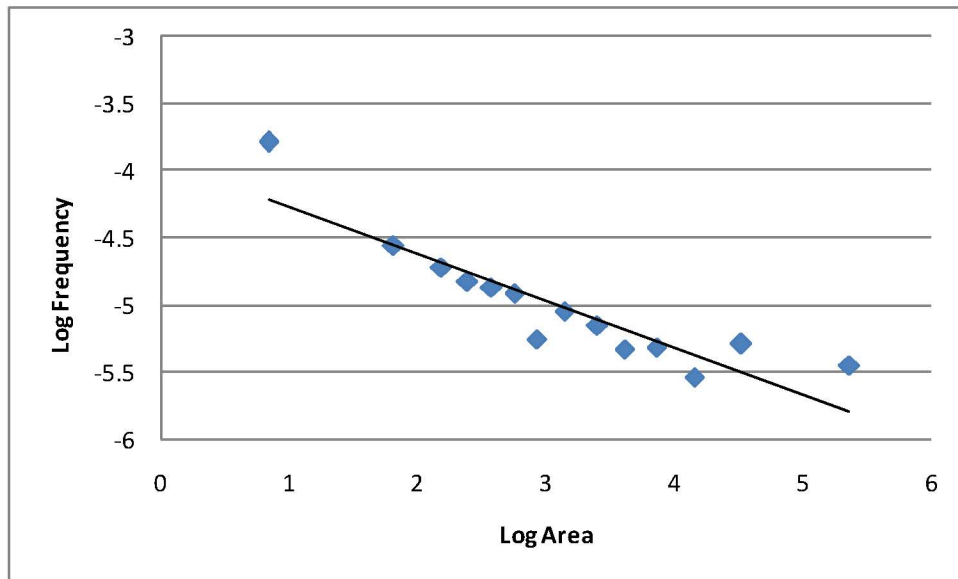
Source: Original

Because the ignition frequency is determined based on the line of best fit, the uncertainty distribution for the calculated ignition frequency can be determined by estimating the uncertainty

in the ability of the best fit equation to predict the ignition frequency of any industrial building not included in the database. This is accomplished using the methodology presented below.

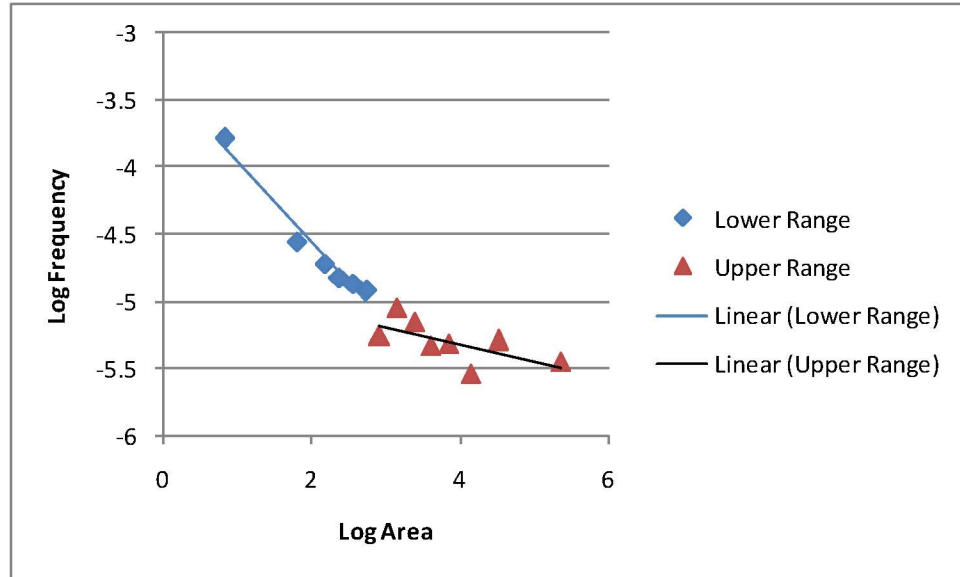
*Statistics: Probability, Inference, and Decision* (Ref. F2.13) outlines a procedure to determine the confidence limits for a value predicted, based on a linear regression equation. Though the ignition frequency and floor area are not linearly related, as illustrated by the figure and by Equation F.I-1, the relationship between the log of the ignition frequency and the log of the floor area are approximately linear. This is illustrated in Figure F.I-3.

As shown in Figures F.I-1 and F.I-3, the portion of the curve for buildings less than 1,000 m<sup>2</sup> has a steeper slope than the portion of the curve for buildings larger than 1,000 m<sup>2</sup>. For that reason, the data was divided into two ranges as shown in Figure F.I-4. Because all of the YMP facilities have floor areas larger than 1,000 m<sup>2</sup>, the remaining analysis focused on the upper end of the floor area range.



Source: Original

Figure F.I-3. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area)



Source: Original

Figure F.I-4. Plot of Log (Ignition Frequency) as a Function of Log (Floor Area) Divided into Two Floor Area Ranges

To arrive at the confidence interval for the log of the ignition frequency, Equations F.I-2, F.I-3, F.I-4 are used (Ref. F2.13):

$$\hat{y} \pm a \frac{s_{xy}}{\sqrt{n-2}} \sqrt{n+1 + \frac{(x - m_x)^2}{s_x^2}} \tag{Eq. F.I-2}$$

$$s_{xy} = \sqrt{s_y^2(1 - r_{xy}^2)} \tag{Eq. F.I-3}$$

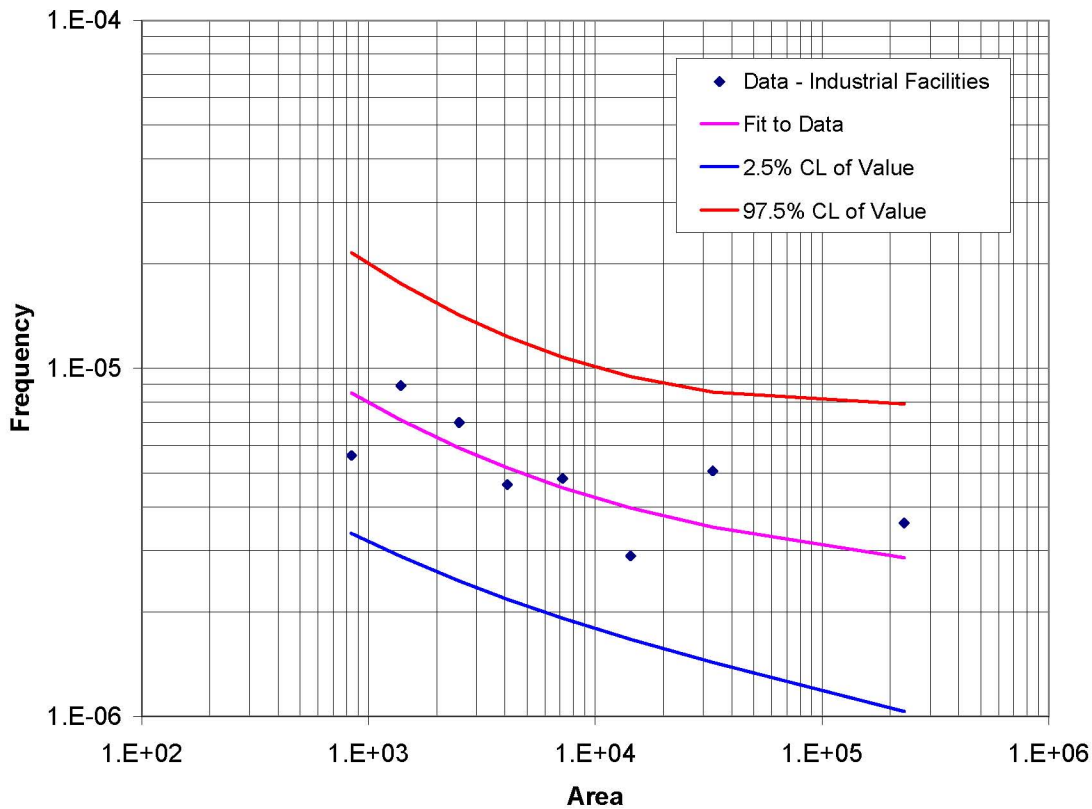
$$r_{xy} = \frac{\sum_{i=0}^{i=n} (x_i - m_x)(y - m_y)}{n s_x s_y} \tag{Eq. F.I-4}$$

where

- $\hat{y}$  = the predicted value for the log of the ignition frequency using Equation F-I.1
- $x$  = the log of the corresponding floor area value
- $n$  = number of data points used in the linear regression analysis (8 for the upper floor area range)
- $a$  = the  $1-(\alpha/2)$  fractile of the t-distribution with  $n-2$  degrees of freedom (for a 95% confidence interval,  $\alpha$  is 5% and the value for  $a$  is 2.447)
- $x_i$  = the  $x$  data values (log of floor area)

- $y_i$  = the y data values (log of ignition frequency)
- $m_x$  = the mean of the x data values
- $m_y$  = the mean of the y data values
- $s_x$  = the standard deviation of the x data values
- $s_y$  = the standard deviation of the y data values

The upper and lower confidence limits (i.e., the 97.5% and 2.5% values) for any predicted value of the ignition frequency can be determined from Equations F.I-2 through F.I-4 using the x-y data for the upper end of the floor area range. The upper and lower confidence limits for the ignition frequency were then determined by taking the anti-log of the predicted y values. Figure F.I-5 is a plot showing the original data, the predicted values using Equation F.I-1, and the upper and lower confidence limits for the predicted values. The same approach can be used to determine the upper and lower confidence limits for the ignition frequency calculated for each of the YMP facilities. Those results are provided in Table F.I-2.



NOTE: CL = confidence limit.

Source: Original

Figure F.I-5. Plot of the Ignition Frequency Data, the Predicted Ignition Frequency, and Confidence Limits for the Predicted Value

The median and 97.5% values are utilized as input into Crystal Ball to obtain an output from the software which includes the mean and median (Table F.I-2). Using this output and Equation F.I-5 (which is Equation F-4 reorganized), the error factor can be calculated for use as an estimated error factor for warehouse buildings.

$$EF = e^{\left(1.645 \sqrt{2 \ln \frac{mean}{median}}\right)} \quad (\text{Eq. F.I-5})$$

where

$EF$  = error factor

Table F.I-2. Calculated Mean and Confidence Limits for the YMP LLWF Ignition Frequency

Facility	Ignition Frequency (Ignitions per sq-m per year)		
	Mean	Median	EF
LLWF	5.30E-06	4.83E-06	2.0

NOTE: This calculation is performed **only** for the purpose of determining an error factor to be applied to the LLW fire frequency distribution. The mean and median above are not the actual values, since the parameters for c1, c2, r, and s are for industrial buildings. Section F6 provides the actual calculation of the median fire frequency for the LLWF, to which the 2.0 error factor is applied.

EF = error factor; LLW = low-level radioactive waste; LLWF = Low-Level Waste Facility; YMP = Yucca Mountain Project.

Source: Original

**ATTACHMENT G**  
**EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES**



**ATTACHMENT G**  
**EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES**

Table G-1. Event Sequence Quantification

Table G-2. Final Event Sequences Summary

Table G-3. Beyond Category 2 Final Event Sequences Summary

Table G-4. Important to Criticality Final Event Sequences Summary

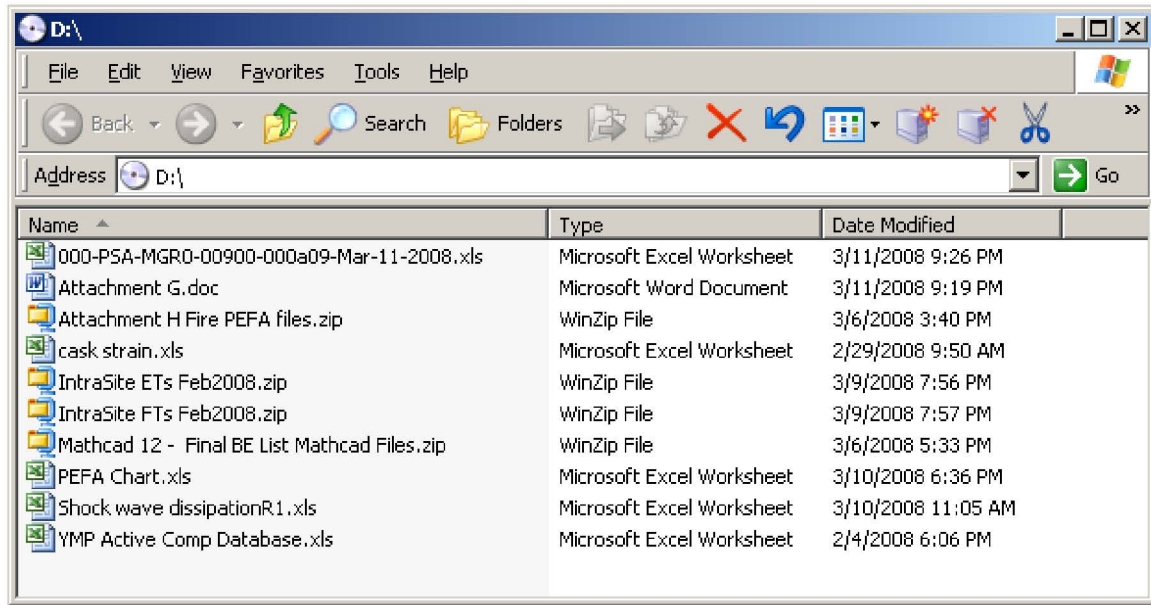
NOTE: Cells in these tables with a value of 0.00E+00 indicate that the value is <1E-12.

This attachment can be found on the CD in Attachment H, in a file named *Attachment G.doc*.

**ATTACHMENT H**  
**SAPPHIRE MODEL AND SUPPORTING FILES**

## ATTACHMENT H EXCEL SPREADSHEET, SAPHIRE MODEL, AND SUPPORTING FILES

This attachment is the CD containing the Excel Spreadsheet and SAPHIRE model and supporting files. The electronic files contained on the CD are identified below.



OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT  
SPECIAL INSTRUCTION SHEET

1. QA: QA  
Page 1 of 1

This is a placeholder page for records that cannot be scanned.

2. Record Date 03/11/2008	3. Accession Number Att. To: ENG.20080312.0032
4. Author Name(s) Martin-Miller, D	5. Authorization Organization BSC/PCSA
6. Title/Description Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis	
7. Document Number(s) 000-PSA-MGR0-00900-000	8. Version Designator 00A
9. Document Type Data	10. Medium 2 CD's
11. Access Control Code PUB	
12. Traceability Designator 000-PSA-MGR0-00900-000-00A	
13. Comments 2 CD's: 1 Original, 1 Copy  Validation of complete file transferred. All files copied. Software used: SAPHIRE Version 7.26; Visio Professional 2003; Word 2003; Excel 2003; Crystal Ball Version 7.3.1 and WinZip 9.0.	
14. RPC Electronic Media Verification	

XREF

MOL.20080317.0030

MAR 17 2008

*T Church / BSC*

MD5 Validation

THIS IS AN ELECTRONIC  
ATTACHMENT

dir.txt

Volume in drive D is 080311\_2128  
Volume Serial Number is F397-334C

Directory of D:\

03/11/2008	09:26 PM	1,904,640	000-PSA-MGR0-00900-000a09-Mar-11-2008.xls
03/11/2008	09:19 PM	1,044,480	Attachment G.doc
03/06/2008	03:40 PM	3,930,232	Attachment H Fire PEFA files.zip
02/29/2008	09:50 AM	130,560	cask strain.xls
03/09/2008	07:56 PM	844,476	IntraSite ETs Feb2008.zip
03/09/2008	07:57 PM	797,210	IntraSite FTs Feb2008.zip
03/06/2008	05:33 PM	6,157,289	Mathcad 12 - Final BE List Mathcad Files.zip
03/10/2008	06:36 PM	62,464	PEFA Chart.xls
03/10/2008	11:05 AM	76,288	Shock wave dissipationR1.xls
02/04/2008	06:06 PM	347,648	YMP Active Comp Database.xls
	10 File(s)	15,295,287	bytes
Total Files Listed:			
	10 File(s)	15,295,287	bytes
	0 Dir(s)	0	bytes free