

**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-MGR0-00500-000-00A
5. Title Subsurface Operations 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 Cancelled/Superseded	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	22
Attachment B. System/Pivotal Event Analysis – Fault Trees	243
Attachment C. Active Component Reliability Data Analysis	51
Attachment D. Passive Equipment Failure Analysis	91
Attachment E. Human Reliability Analysis	63
Attachment F. Fire Analysis	14
Attachment G. Event Sequence Quantification Summary Tables	2
Attachment H. SAPHIRE Model and Supporting Files	2 + CD

**RECORD OF REVISIONS**

9. No.	10. Reason For Revision	11. Total # of Pgs.	12. Last Pg. #	13. Originator (Print/Sign/Date)	14. Checker (Print/Sign/Date)	15. EGS (Print/Sign/Date)	16. Approved/Accepted (Print/Sign/Date)
00A	Initial Issue	682	H-2	Phouc Le/Sec Page 2	See Page 3	Mike Frank <i>Mike Frank</i> 3/12/08	Mark Wisenbegg <i>Mark Wisenbegg</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.

Section	Section Name	Originator	Signature/Date
1	Purpose	Phuoc Le	<i>[Signature]</i> 3/12/08
2	References	Phuoc Le	<i>[Signature]</i> 3/12/08
3	Assumptions	Phuoc Le	<i>[Signature]</i> 3/12/08
4	Methodology	Phuoc Le	<i>[Signature]</i> 3/12/08
4.1	Quality Assurance	Phuoc Le	<i>[Signature]</i> 3/12/08
4.2	Use of Software	Phuoc Le	<i>[Signature]</i> 3/12/08
4.3	Description of Analysis Methods	Doug Orvis Erin Collins & Pierre Macheret Dan Christman David Bradley Paul Amico Mary Presley Joe Minarick	<i>[Signatures]</i> 3/12/08 P. Macheret 03/12/08
5	List of Attachments	Phuoc Le	<i>[Signature]</i> 3/12/08
6	Body of Calculation	NA	
6.0	Initiating Event Screening	Phuoc Le	<i>[Signature]</i> 3/12/08
6.1	Event Tree Analysis	Phuoc Le	<i>[Signature]</i> 3/12/08
6.2	Initiating and Pivotal Event Analysis	Phuoc Le	<i>[Signature]</i> 3/12/08
6.3	Data Utilization	Erin Collins Dan Christman (Sections 6.3.2.1, 6.3.2.2, and 6.3.2.5) David Bradley (Sections 6.3.2.3 and 6.3.2.4)	<i>[Signatures]</i> 3/12/08
6.4	Human Reliability Analysis	Paul Amico Mary Presley Erin Collins Doug Orvis	<i>[Signatures]</i> 3/12/08
6.5	Fire Analysis	Paul Amico & Laura Plumb under supervision of Paul Amico	<i>[Signatures]</i> 3/12/08
6.6	(Not used)		
6.7	Event Sequence Frequency Results	Phuoc Le	<i>[Signature]</i> 3/12/08
6.8	Event Sequence Grouping And Categorization	Phuoc Le	<i>[Signature]</i> 3/12/08
6.9	Defined ITS SSCs and Procedural Safety Controls Requirements	Phuoc Le	<i>[Signature]</i> 3/12/08
7	Results and Conclusions	Phuoc Le	<i>[Signature]</i> 3/12/08
Att A	Event Tree Analysis	Phuoc Le	<i>[Signature]</i> 3/12/08
Att B	System/Pivotal Event - FT	DAN GALLAGHER	<i>[Signature]</i> 3/12/08

Suzanne Loyd *[Signature]* March 2008

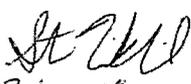
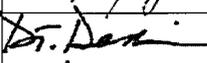
Section	Section Name	Originator	Signature/Date
Att C	ACTIVE COMPONENT RELIABILITY DATA ANALYSIS	Erin Collins	<i>[Signature]</i> 3/12/08
Att D	PASSIVE EQUIPMENT FAILURE ANALYSIS	Dan Christman (Sections D1 and D3) & David Bradley (Section D2)	<i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08
Att E	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> 3/24/08
Att F	FIRE ANALYSIS	Paul Amico and 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 TABLE	Phuoc Le	<i>[Signature]</i> 3/12/08
Att H	EXCEL AND SAPHIRE MODEL AND SUPPORTING FILES (CD)	Phuoc Le	<i>[Signature]</i> 3/12/08

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

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Andrew Burningham	<i>[Signature]</i> 3/12/08	Section 1-7, + Att's A, C, F, G + H 3/12/08	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 A, B, C, D, E, F, G, H B, D, + E only 3/12/08		
Shyang-Fenn (Alex) Deng	<i>[Signature]</i> 03/14/08	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.
Douglas Orvis	<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 the correct ESD and values for Tables 6.9-1 and 6.9-2.
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

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Laura Plumb	<i>[Signature]</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
Kenneth Draper	<i>[Signature]</i> 3/12/08	Attachment B-1 Transport and Emplacement Vehicle (TEV) Fault Tree Analysis	Design Concurrency	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
Nasser Dehkordi For Ajit Hiranandani	<i>Nasser H. Dehkordi</i> 3/12/08	Attachment B-2 Heating Ventilating and Air Conditioning- Fault Tree Analysis	Design Concurrency	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
Nohemi Brewer	PARTIAL CHECK (SEE EMAIL) <i>[Signature]</i> 3/12/08 <i>[Signature]</i> 3/12/08	Attachment B 3 – Important to Safety AC Power Fault Tree Analysis	Design Concurrency	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
Leo Gatchalian	<i>[Signature]</i> 3/12/08	Attachment B-4 Drip Shield Emplacement Gantry Fault Tree Analysis	Design Concurrency	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

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Mary Jane Rubano For Ekachai Danupatampa	<i>Mary Jane Rubano</i> 3.12.08	Attachment B 5 Shield Door Fault Tree Analysis	Design concurrency	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
Leo Gatchalian	<i>L. Gatchalian</i> 3/12/08	Attachment B-6 Emplacement Drift Access Door 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
Daniel Christman	<i>D. Christman</i> 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
Oliver (Doug) Smith Stephen Skochko For Karim Vekhsheeri Stephen Skochko	<i>Doug Smith</i> 3-12-08 <i>Stephen Skochko</i> For Karim Vekhsheeri 3/12/08 <i>Stephen Skochko</i> 3/12/08	Inputs to 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	<i>D. Christman</i> 3/12/08	Attachment D Passive Equipment Failure Analysis	Specialty Check	Check Sections D 2, 6.3.2.3 and 6.3.2.4.
David Bradley	<i>D. Bradley</i> 3/12/08	Attachment D Passive Equipment Failure Analysis	Specialty Check	Check Sections D 1, D 3, 6.3.2.1, 6.3.2.2, and 6.3.2.5
Anthony Spurgin	<i>A. Spurgin</i> 3/12/08	Attachment E- Human Reliability Analysis	Specialty Check	Section 6.4 and Attachment E
Clarence Smith	<i>C. Smith</i> 3/12/08	Attachment E - Human Reliability Analysis	Design concurrency	Check that the Basic Scenarios in Attachment E are consistent with the concept of operations.
Dan Christman	<i>D. Christman</i> 3/12/08	Attachment F Fire Analysis	Specialty check	Check the fire analysis calculation
Sandra Castro	<i>Sandra Castro</i> 3/12/08	Section 2 of main body of Analysis	References	Check that all references to engineering document are correct and up to date

Checker	Signature/Date	Section	Type of Check	Detailed Scope of Check
Steve Mikhail	 3/12/08	All Section of Main Body and Attachments	Detailed References and Numerical Inputs	Check that all references in the main body and attachments E and F are references to the appropriate document
Wesley Wu For Elliot Bedrosian	 3/12/08	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	 3/12/08	Section 6.8	Specialty Check	Check consistency with Preclosure Consequence Analysis

## CONTENTS

	<b>Page</b>
ACRONYMS AND ABBREVIATIONS .....	10
1. PURPOSE .....	13
2. REFERENCES .....	17
2.1 PROCEDURES/DIRECTIVES .....	17
2.2 DESIGN INPUTS .....	17
2.3 DESIGN CONSTRAINTS .....	25
2.4 DESIGN OUTPUTS .....	25
2.5 ATTACHMENT REFERENCES .....	25
3. ASSUMPTIONS .....	27
3.1 ASSUMPTIONS REQUIRING VERIFICATION .....	27
3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION .....	27
4. METHODOLOGY .....	28
4.1 QUALITY ASSURANCE .....	28
4.2 USE OF SOFTWARE .....	29
4.3 DESCRIPTION OF ANALYSIS METHODS .....	30
5. LIST OF ATTACHMENTS .....	92
6. BODY OF ANALYSIS .....	93
6.0 INITIATING EVENT SCREENING .....	93
6.1 EVENT TREE ANALYSIS .....	102
6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS .....	106
6.3 DATA UTILIZATION .....	128
6.4 HUMAN RELIABILITY ANALYSIS .....	166
6.5 FIRE INITIATING EVENTS .....	171
6.6 NOT USED .....	172
6.7 EVENT SEQUENCE FREQUENCY RESULTS .....	172
6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION .....	177
6.9 IMPORTANT TO SAFETY STRUCTURES, SYSTEMS, AND COMPONENTS AND PROCEDURAL SAFETY CONTROL REQUIREMENTS .....	185
7. RESULTS AND CONCLUSIONS .....	191
ATTACHMENT A   EVENT TREES .....	A-1
ATTACHMENT B   SYSTEM/PIVOTAL EVENT ANALYSIS–FAULT TREES .....	B-1
ATTACHMENT C   ACTIVE COMPONENT RELIABILITY DATA ANALYSIS .....	C-1
ATTACHMENT D   PASSIVE EQUIPMENT FAILURE ANALYSIS .....	D-1
ATTACHMENT E   HUMAN RELIABILITY ANALYSIS .....	E-1
ATTACHMENT F   FIRE ANALYSIS .....	F-1
ATTACHMENT G   EVENT SEQUENCE QUANTIFICATION SUMMARY TABLE .....	G-1
ATTACHMENT H   EXCEL SPREADSHEET, SAPHIRE MODEL, AND SUPPORTING FILES .....	H-1

**FIGURES**

	<b>Page</b>
4.3-1. Event Sequence Analysis Process.....	31
4.3-2. Preclosure Safety Assessment Process .....	36
4.3-3. Simplified Process Flow Diagram for Example with Node 4 Emphasized for Further Discussion .....	38
4.3-4. Event Sequence Diagram–Event Tree Relationship .....	40
4.3-5. Example Excel Spreadsheet.....	44
4.3-6. Example Grouped Event Sequences .....	47
4.3-7. Example Fault Tree.....	48
4.3-8. Concept of Uncertainty in Load and Resistance.....	51
4.3-9. Point Estimate Load Approximation Used in PCSA .....	53
4.3-10. Component Failure Rate “Bathtub Curve” Model.....	59
4.3-11. Incorporation of Human Reliability Analysis within the PCSA.....	69
6.3-1. Likelihood Functions from Data Sources (Dashed Lines) and Population- Variability Probability Density Function (Solid Line) .....	131
6.4-1. Subsurface Operations .....	167

**TABLES**

	<b>Page</b>
4.3-1. Criticality Control Parameter Summary .....	87
6.0-1. Retention Decisions from External Events Screening Analysis.....	97
6.0-2. Bases for Screening Internal Initiating Events.....	99
6.0-3. Flood Height Estimation .....	102
6.1-2. Figure Locations for Initiating Event Trees and Response Trees.....	106
6.2-1 Summary of Top Event Quantification for the TEV .....	113
6.2-2 Top Level and Linking Fault Trees .....	123
6.2-3 Probability of Spurious Sprinkler Actuation.....	125
6.3-1. Active Component Reliability Data Summary .....	134
6.3-2. Failure Probabilities Due to Drops and Other Impacts.....	148
6.3-3. Failure Probabilities Due to Miscellaneous Events .....	148
6.3-4. Failure Probabilities for Collision Events and Two-Blocking.....	151
6.3-5. Summary of Canister Failure Probabilities in Fire .....	153
6.3-6. Probabilities of Degradation or Loss of Shielding.....	157
6.3-7. Summary of Passive Event Failure Probabilities.....	158
6.3-8. Passive Failure Basic Events used in Event Sequence Analysis .....	159
6.3-9. Miscellaneous Data Used In the Reliability Analysis.....	162
6.4-1. Human Failure Event Probability Summary.....	169
6.5-1 Fire Initiating Event Frequency Distributions .....	172
6.7-1. Event Sequence Quantification Example.....	174
6.8-1. Bounding Category 2 Event Sequences.....	178
6.8-2. Event Sequence Grouping and Quantification Example .....	180
6.8-3. Category 1 Final Event Sequences Summary .....	183
6.8-3. Category 2 Final Event Sequences Summary .....	184
7-1. Key to Results.....	191
7-2. Summary of Category 2 Event Sequences.....	192

## ACRONYMS AND ABBREVIATIONS

### Acronyms

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

## ACRONYMS AND ABBREVIATIONS (CONTINUED)

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

---

**ACRONYMS AND ABBREVIATIONS (CONTINUED)**

YMP            Yucca Mountain Project

**Abbreviations**

AC            alternating current

°C            degrees Celsius

DC            direct current

ft            foot, feet

gpm          gallons per minute

hp            horsepower

hr, hrs      hour, hours

K            Kelvin

kV            kilovolt

min          minute, minutes

mph          miles per hour

V            volt

yr,yrs      year, years

## 1. PURPOSE

This document on the Subsurface operations and its companion document entitled *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) constitute a portion of the preclosure safety analysis (PCSA) that is described in its entirety in the safety analysis report that will be submitted to the U.S. Nuclear Regulatory Commission (NRC) as part of the Yucca Mountain Project (YMP) license application. These documents are part of a collection of analysis reports that encompass all waste handling activities and facilities of the geologic repository operations area (GROA) from the beginning of operations to the end of the preclosure period. The *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) 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* (Ref. 2.2.71). The PCSA, however, limits the use of PRA technology to identification and development of event sequences that might lead to the direct exposure of workers or onsite members of the public; radiological releases that may affect the workers or public (onsite and offsite), and criticality.

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

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

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

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

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

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

In order to determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity to variations in each of the parameters important to criticality during the preclosure period. The parameters are waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor ( $k_{\text{eff}}$ ) 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.

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

10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4) and associated quality assurance (QA) programs. As a result of compliance to such regulations, the SSCs are deemed to pose no undue risk to health and safety. Although the analyses do not address quantitative probabilities to the aforementioned excluded precursors, it is clear that the use of conservative design criteria and the implementation of QA controls result in unlikely exposures to radiation.

Other boundary conditions used in the PCSA include:

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

As stated, the scope of the preclosure safety analysis is limited to internal initiating events originating within the GROA boundary and external initiating events that have their origin outside the GROA boundary, but can affect buildings and/or equipment within the GROA. External event analyses are documented in *External Events Hazards Screening Analysis* (Ref. 2.2.34) and *Frequency Analysis of Aircraft Hazards for License Application* (Ref. 2.2.21). Internal event identification (using a master logic diagram and hazard and operability evaluation), event sequence development and grouping, and related facility details are provided in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40), which also documents the methodology and process employed and initiates the analysis that is completed here.

This document uses event trees from *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) to quantify the event sequences for each waste form. Quantification refers to the process of obtaining the mean frequency of each event sequence for the purpose of categorization. This document shows the categorization of each event sequence based on:

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

Other PCSA documents which are not referenced here cover the reliability and categorization of external events and summarize procedural safety controls and nuclear safety design bases. The main documents that will emanate from Volume I (Ref. 2.2.40) and the current analyses are:

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

## 2. REFERENCES

### 2.1 PROCEDURES/DIRECTIVES

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

### 2.2 DESIGN INPUTS

The PCSA is a safety analysis 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), paragraph 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 \*A.M. Birk Engineering 2005. *Tank-Car Thermal Protection Defect Assessment: Updated Thermal Modelling with Results of Fire-Testing: Summary Report*. TP 14367E. Ontario, Canada: Transportation Development Centre of Transport Canada. ACC: MOL.20071113.0095.
- 2.2.3 \*ANSI/ANS (American National Standards Institute/American Institute of Steel Construction)-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 (American Society of Civil Engineers/Structural Engineering Institute) 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) 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.
- 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. ISBN: 0-7918-2899-9.
- 2.2.8 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.
- 2.2.9 \*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.
- 2.2.10 \*Brereton, S.J.; Alesso, H.P.; Altenbach, T.J.; Bennett, C.T.; and Ma, C. 1998. *AVLIS Criticality Risk Assessment*. UCRL-JC-130693. Livermore, California: Lawrence Livermore National Laboratory. ACC: MOL.20080102.0002.
- 2.2.11 BSC (Bechtel SAIC Company) 2003. *Underground Layout Configuration*. 800-P0C-MGR0-00100-000-00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20031002.0007.
- 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. *Conceptual Shielding Study for Transport Emplacement Vehicle*. 000-30R-HE00-00100-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20060911.0001.
- 2.2.14 \*BSC 2007. *Access Mains 25' Diameter Isolation Bulkhead & Airlock Door Elevation & Notes*. 800-S00-SSD0-00701-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070628.0010.
- 2.2.15 BSC 2007. *Basis of Design for the TAD Canister-Based Repository Design Concept*. 000-3DR-MGR0-00300-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071002.0042.

- 2.2.16 \*BSC 2007. *Canister Receipt and Closure Facility 1 Fire Hazard Analysis*. 060-M0A-FP00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0032.
- 2.2.17 \*BSC (Bechtel SAIC Company) 2007. *Subsurface Construction Strategy*. 800-30R-MGR0-00100-000-002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070426.0025.
- 2.2.18 BSC 2007. *CRCF-1 and IHF WP Transfer Trolley Mechanical Equipment Envelope Plan & Elevations-Sh 1 of 2*. 000-MJ0-HL00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0015.
- 2.2.19 BSC 2007. *Drift Cross Section Showing Emplaced Waste Package and Drip Shield*. 800-M00-WIS0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070412.0003.
- 2.2.20 BSC 2007. *Emplacement and Retrieval Transport and Emplacement Vehicle Mechanical Equipment Envelope*. 800-MJ0-HE00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070918.0041.
- 2.2.21 BSC 2007. *Frequency Analysis of Aircraft Hazards for License Application*. 000-00C-WHS0-00200-000-00F. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070925.0012.
- 2.2.22 BSC 2007. *GROA External Dose Rate Calculation*. 000-PSA-MGR0-01300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071023.0003.
- 2.2.23 \*BSC 2007. *Liquid Low-Level Waste Collection Calculation (C2 and C3 Contamination Zones)*. Las Vegas, Nevada: Bechtel SAIC Company. 000-M0C-MWL0-00100-000-00A. ENG.20071101.0013.
- 2.2.24 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.
- 2.2.25 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.
- 2.2.26 BSC 2007. *Receipt Facility Fire Hazard Analysis*. 200-M0A-FP00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070823.0001.
- 2.2.27 \*BSC 2007. *Repository Subsurface Transport and Emplacement Vehicle (TEV) Routes, General Arrangement*. 800-KM0-SS00-00401-000 REV 00A, Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0041.

- 2.2.28 \*BSC 2007. *Repository Subsurface Transport and Emplacement Vehicle (TEV) Routes Details*. 800-KM0-SS00-00402-000 REV 00A, Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0042.
- 2.2.29 \*BSC 2007. *Repository Subsurface Turnout, Invert & Rails Plan and Elevation*. 800-D00-SSD0-00701-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070529.0025.
- 2.2.30 BSC 2007. *Straight Wind Hazard Curve Analysis*. 000-00A-MGR0-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071023.0002.
- 2.2.31 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.
- 2.2.32 \*BSC 2008. *Geologic Repository Operations Area North Portal Site Plan*. 100-C00-MGR0-00501-000-00F. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080125.0007.
- 2.2.33 BSC 2008. *Canister Receipt and Closure Facility Event Sequence Development Analysis*. 060-PSA-CR00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080221.0008.
- 2.2.34 BSC 2008. *External Events Hazards Screening Analysis*. 000-00C-MGR0-00500-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080219.0001
- 2.2.35 \*BSC 2008. *Initial Handling Facility Fire Hazard Analysis*. 51A-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0007.
- 2.2.36 BSC 2008. *Preclosure Consequence Analyses*. 000-00C-MGR0-00900-000-00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080129.0006.
- 2.2.37 BSC 2008. *Preclosure Criticality Analysis Process Report*. TDR-DS0-NU-000001 REV 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080220.0001.
- 2.2.38 BSC 2008. *Preclosure Criticality Safety Analysis*. TDR-MGR-NU-000002 REV 01. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0007.
- 2.2.39 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.
- 2.2.40 BSC 2008. *Subsurface Operations Event Sequence Development Analysis*. 000-PSA-MGR0-00400-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080214.0004.
- 2.2.41 BSC 2008. *Waste Package Misplacement Probability*. 000-PSA-MGR0-02500-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080124.0006.

- 2.2.42 \*BSC 2008. *Wet Handling Facility Fire Hazard Analysis*. 050-M0A-FP00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080213.0001.
- 2.2.43 \*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.
- 2.2.44 \*Crowell, W.; Denson, W.; Jawoski, P.; and Mahar, D. 1997. *Failure Mode/Mechanism Distributions 1997*. FMD-97. Rome, New York: U.S. Department of Defense, Reliability Analysis Center. TIC: 260074.
- 2.2.45 \*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, Griffin Air Force Base. TIC: 259757.
- 2.2.46 DOE (U.S. Department of Energy) 2007. *Software Independent Verification and Validation Report, Change in Operating System Version Report for SAPHIRE v7.26*. STN: 10325-7.26-01. Las Vegas, NV: U.S. Department of Energy, Office of Repository Development. ACC: MOL.20070607.0263. (DIRS 184933)
- 2.2.47 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. (DIRS 181403)
- 2.2.48 \*Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Loss of Offsite Power Events: 1986-2004*. Volume 1 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants*. NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0164.
- 2.2.49 \*Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; and Rasmuson, D.M. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*. NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.
- 2.2.50 \*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.
- 2.2.51 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.

- 2.2.52 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.
- 2.2.53 \*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.
- 2.2.54 \*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.
- 2.2.55 \*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.
- 2.2.56 \*Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.
- 2.2.57 \*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.
- 2.2.58 \*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.
- 2.2.59 \*Martz, H.F. and Waller, R.A. 1991. *Bayesian Reliability Analysis*. Malabar, Florida: Krieger Publishing Company. TIC: 252996. ISBN: 0-89464-395-9.
- 2.2.60 \*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.
- 2.2.61 \*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.
- 2.2.62 \*Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1988. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106.
- 2.2.63 NFPA (National Fire Protection Association) 13. 2006. *Standard for the Installation of Sprinkler Systems*. 2007 Edition. NFPA 13-2007. Quincy, Massachusetts: National Fire Protection Association. TIC: 258713.

- 2.2.64 \*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.
- 2.2.65 \*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.
- 2.2.66 \*NRC (U.S. Nuclear Regulatory Commission) 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.
- 2.2.67 NRC 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. LWR Edition. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.
- 2.2.68 NRC 1997. *Standard Review Plan for Dry Cask Storage Systems*. NUREG-1536. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20010724.0307.
- 2.2.69 NRC 2000. *Standard Review Plan for Transportation Packages for Spent Nuclear Fuel*. NUREG-1617. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 249470.
- 2.2.70 NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.
- 2.2.71 NRC 2003. *Yucca Mountain Review Plan, Final Report*. NUREG-1804, Rev. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards. TIC: 254568.
- 2.2.72 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, DC. U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0230.
- 2.2.73 NRC 2007. *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation*. HLWRS-ISG-02. Washington, DC: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.
- 2.2.74 \*Owen, A.B. 1992. *A Central Limit Theorem for Latin Hypercube Sampling*. Journal of the Royal Statistical Society: Series B, Statistical Methodology, 54, (2), 541-551. London, England: Royal Statistical Society. TIC: 253131.
- 2.2.75 Regulatory Guide 1.174, Rev. 1. 2002. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington, D.C.: U. S. Nuclear Regulatory Commission. ACC: MOL.20080215.0049.

- 2.2.76 \*SAIC (Science Applications International Corporation) 2002. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*. SAIC-01/2650. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20080115.0138.
- 2.2.77 SAPHIRE V. 7.26. 2007. VMware/WINDOWS XP. STN: 10325-7.26-01. (DIRS 183846)
- 2.2.78 SFPE (Society of Fire Protection Engineers) 2002. *SFPE Handbook of Fire Protection Engineering*. 3rd Edition. Quincy, Massachusetts: National Fire Protection Association. TIC: 255463. ISBN: 087765-451-4.
- 2.2.79 \*Siu, N.O. and Kelly, D.L. 1998. *Bayesian Parameter Estimation in Probabilistic Risk Assessment*. Reliability Engineering and System Safety, 62, 89-116. New York, New York: Elsevier. TIC: 258633.
- 2.2.80 \*Smith, C. 2007. *Master Logic Diagram*. Bethesda, Maryland: Futron Corporation. ACC: MOL.20071105.0153; MOL.20071105.0154.
- 2.2.81 \*Snow, S.D. and Morton, D.K. 2007. *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository*. EDF-NSNF-087, Rev. 0. [Idaho Falls, Idaho: Idaho National Laboratory]. ACC: MOL.20080206.0063.
- 2.2.82 \*Snow, S.D. 2007. *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-Foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations*. EDF-NSNF-085, Rev. 0. [Idaho Falls, Idaho: Idaho National Laboratory]. ACC: MOL.20080206.0062.
- 2.2.83 \*Sprung, J.L.; Ammerman, D.J.; Breivik, N.L.; Dukart, R.J.; Kanipe, F.L.; Koski, J.A.; Mills, G.S.; Neuhauser, K.S.; Radloff, H.D.; Weiner, R.F.; and Yoshimura, H.R. 2000. *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672; SAND2000-0234. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20001010.0217. .
- 2.2.84 \*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.
- 2.2.85 \*Tillander, K. 2004. *Utilisation of Statistics to Assess Fire Risks in Buildings*. VTT Technical Research Centre of Finland. Ph.D. Dissertation. Espoo, Finland, TIC: 259928. ISBN: 951-38-6392-1.
- 2.2.86 \*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. ACC: MOL.20080310.0082. URL: <http://www.census.gov/epcd/ec97/ustotals.htm>

- 2.2.87 Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook*. NUREG-0492. Washington, D.C. U.S. Nuclear Regulatory Commission. TIC: 208328.
- 2.2.88 \*Williams, J.C. 1986. HEART - A Proposed Method for Assessing and Reducing Human Error. In: *Proceedings of the 9th Advances in Reliability Technology Symposium – 1986* Bradford, England: University of Bradford. TIC: 259862.
- 2.2.89 NRC 2007. *Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program*. HLWRS-ISG-03. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20070918.0096.

### 2.3 DESIGN CONSTRAINTS

- 2.3.1 10 CFR (Code of Federal Regulations) 50. 2007. *Energy: Domestic Licensing of Production and Utilization Facilities*.
- 2.3.2 10 CFR 63. *Energy: Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada*. U.S. Nuclear Regulatory Commission.
- 2.3.3 10 CFR 71. *Energy: Packaging and Transportation of Radioactive Material*. U.S. Nuclear Regulatory Commission. ACC: MOL.20070829.0114.
- 2.3.4 10 CFR 72. *Energy: Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste*. U.S. Nuclear Regulatory Commission.

### 2.4 DESIGN OUTPUTS

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

### 2.5 ATTACHMENT REFERENCES

- 2.5.1 Attachment A: Design Input references are listed in Section 2.2 of the main report.
- 2.5.2 Attachment B: Design Input references are listed in Sections B1.1, B2.1, B3.1, B4.1, B5.1, B6.1
- 2.5.3 Attachment C: Design Input references are listed in Section C5.

- 2.5.4 Attachment D: Design Input references are listed in Section D4.1.
- 2.5.5 Attachment E: Design Input references are listed in Section E8.1.
- 2.5.6 Attachment F: Design Input references are listed in Section F2.
- 2.5.7 Attachment G: This attachment does not contain Design Input references.
- 2.5.8 Attachment H: This attachment does not contain Design Input references.

### 3. ASSUMPTIONS

#### 3.1 ASSUMPTIONS REQUIRING VERIFICATION

There are no assumptions requiring verification.

#### 3.2 ASSUMPTIONS NOT REQUIRING VERIFICATION

##### 3.2.1 General Analysis Assumptions

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

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

## 4. METHODOLOGY

### 4.1 QUALITY ASSURANCE

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

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

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

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

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

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

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

**Documentation of suitability for intended use of BSC Interoffice 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. 2.2.77) is used in this analysis for PRA simulation and analyses. The SAPHIRE software is used on a personal computer running Windows XP inside a VMware virtual machine; it is also listed in the

current *Qualified and Controlled Software Report*, and was obtained from Software Configuration Management. The SAPHIRE software is specifically designed for PRA simulation and analyses, and has been verified to show that this software produces precise solutions for encoded mathematical models within the defined limits for each parameter employed (Ref. 2.2.46). Therefore, SAPHIRE version 7.26 is suitable for use in this analysis.

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

#### 4.2.2 Level 2 Software

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

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

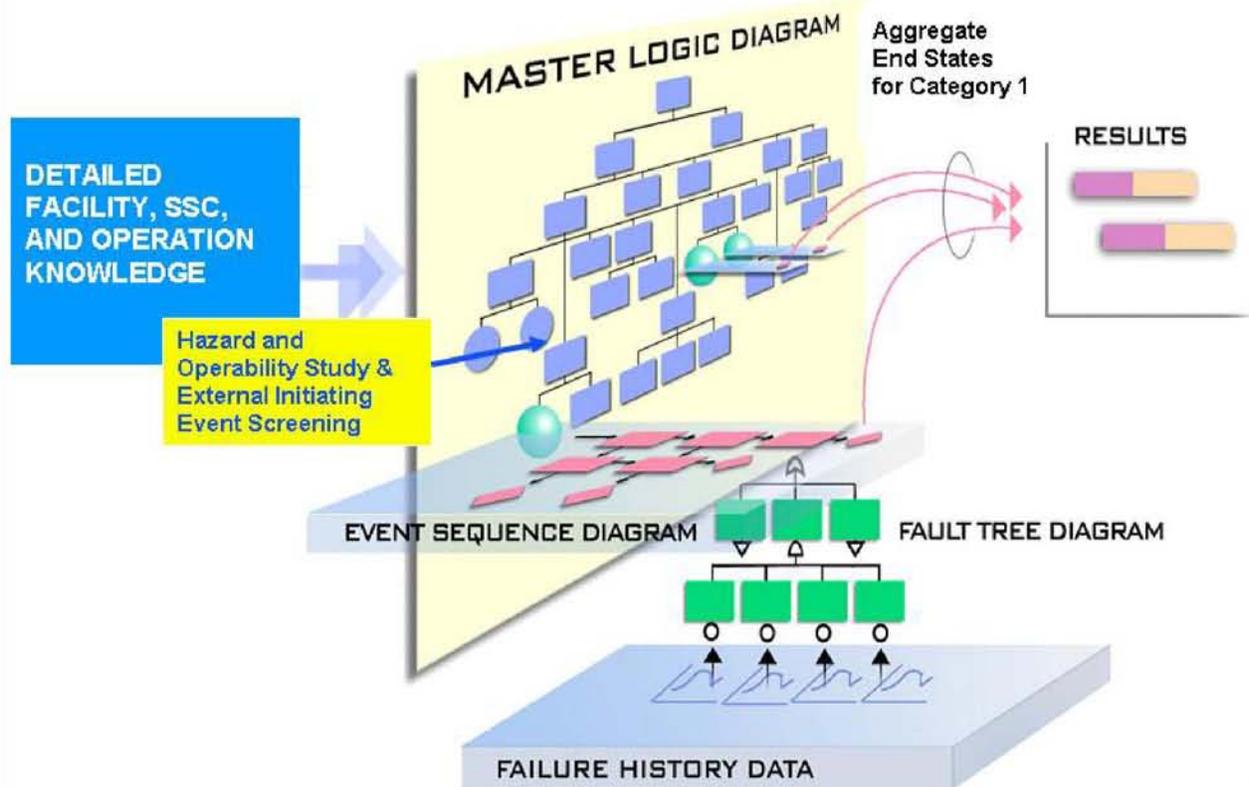
### 4.3 DESCRIPTION OF ANALYSIS METHODS

This section presents the PCSA approach and analysis methods in the context of overall repository operations. As such, it includes a discussion of operations that may not apply to the Subsurface Operations. Specific features of the IHF and its operations are not discussed until

Section 6, where the methods described here are applied to the Subsurface Operations. The PCSA uses the technology of PRA as described in references such as *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6). The PRA answers three questions:

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

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



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

Figure 4.3-1. Event Sequence Analysis Process

The PCSA starts with analysts obtaining sufficient knowledge of facility design and operation, and equipment and SSC design and operation to understand how the YMP waste handling is conducted. This is largely performed and documented as part of the *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40). An understanding of how a facility operates is a prerequisite for developing event sequences that depict how it would fail. An important additional set of information is called *success criterion*. *Success criteria* are important

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

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

1. “OK”–Indicates the absence of radiation exposure and potential for criticality.
2. Direct Exposure, Degraded Shielding–Applies to event sequences where an SSC providing shielding is not breached, but its shielding function is jeopardized. An example is a lead-shielded transportation cask that is dropped from a height great enough for the lead to slump toward the bottom of the cask at impact, leaving a partially shielded path for radiation to stream. This end state excludes radionuclide release.
3. Direct Exposure, Loss of Shielding–Applies to event sequences where an SSC providing shielding fails, leaving a direct path for radiation to stream. For example, this end state applies to a breached transportation cask, with a canister inside maintaining its containment function. In another example, this end state applies to shield doors inadvertently opened. This end state excludes radionuclide release.
4. Radionuclide Release, Filtered–Indicates a release of radioactive material from its confinement, through a filtered path, to the environment. The release is filtered when it is confined and filtered through the successful operation of the HVAC system over its mission time. This end state excludes moderator intrusion.
5. Radionuclide Release, Unfiltered–Indicates a release of radioactive material from its confinement, through the pool of the Wet Handling Facility or through an unfiltered path, to the environment. This end state excludes moderator intrusion.
6. Radionuclide Release, Filtered, Also Important to Criticality–This end state refers to a situation in which a filtered radionuclide release occurs and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.

7. Radionuclide Release, Unfiltered, Also Important to Criticality—This end state refers to a situation in which an unfiltered radionuclide release occurs and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.
8. Important to Criticality—This end state refers to a situation in which there has been no radionuclide release and (unless the associated event sequence is Beyond Category 2) for which a criticality investigation is indicated.

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

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

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

The third question, “How likely is it?” is answered by the estimation of event sequence frequencies. The PCSA uses *failure history* records (for example, *Nonelectronic Parts Reliability Data* (Ref. 2.2.45) and *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations*. NUREG/CR-4639 (Ref. 2.2.55), structural reliability analysis, thermal stress analysis, and engineering and scientific knowledge about the design is the basis for estimation of probabilities and frequencies. These sources coupled with the techniques of probability and statistics, for example, *Handbook of Parameter Estimation for Probabilistic Risk Assessment* (Ref. 2.2.9), are used to estimate frequencies of initiating events and event sequences and the conditional probabilities of pivotal events.

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

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

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

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

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

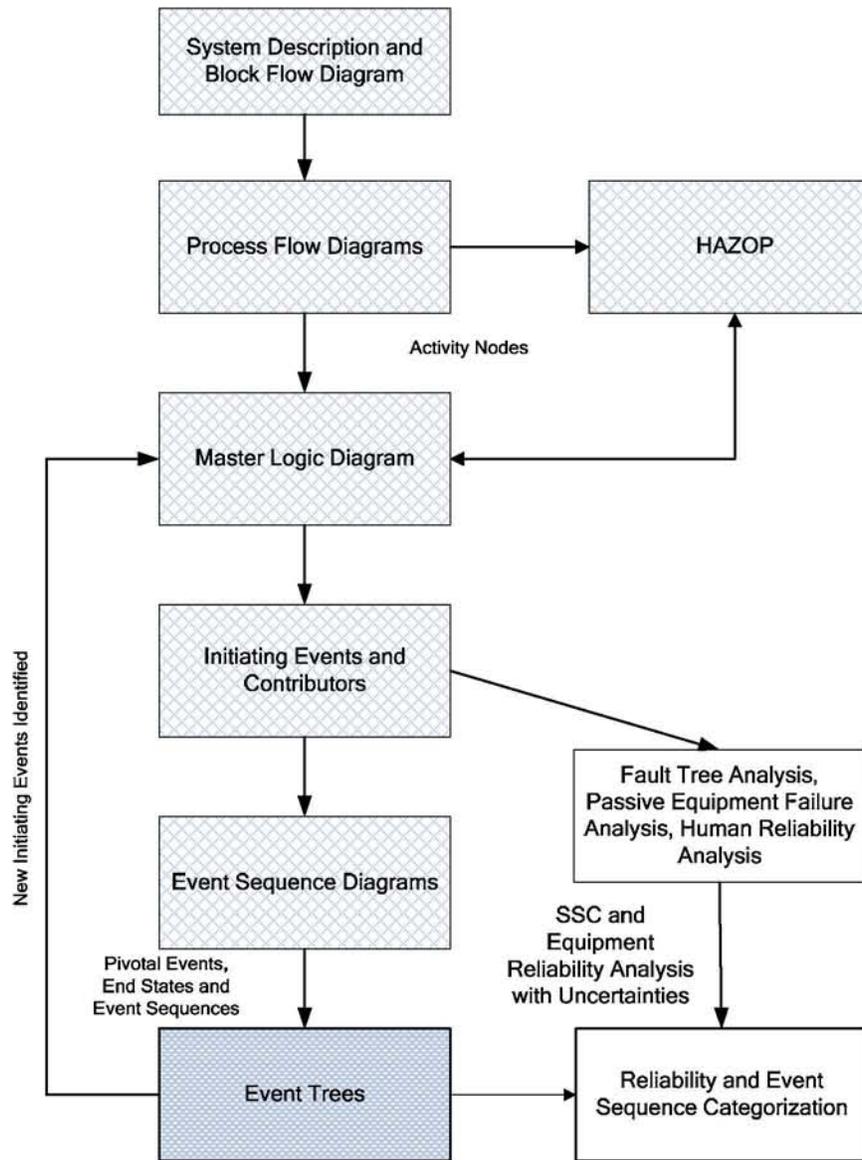
As required by the performance objectives for the GROA through permanent closure in 10 CFR 63.111 (Ref. 2.3.2), each aggregated event sequence is categorized based on its frequency. Therefore, the focus of the analysis in this document is to:

1. Quantify the frequency of each initiating event that is identified in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40).
2. Quantify the conditional probability of the pivotal events in each event sequence.

3. Calculate the frequency of each event sequence (i.e., calculate the product of the initiating event frequency and pivotal event conditional probabilities).
4. Calculate the frequencies of the aggregated event sequences.
5. Categorize the aggregated event sequences for further analysis.

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

The cross-hatched boxes in Figure 4.3-2 serve as a review of the analysis performed for the *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) and the interface between the event sequence development analysis and the present categorization analysis is the set of event trees, as represented by the darkly shaded box. The event trees from the prerequisite analysis are passed as input into the current analysis. The unshaded boxes represent the analysis performed in this study, the methods of which are described in Section 4.



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

Source: Modified from (Ref. 2.2.40, Figure 2)

Figure 4.3-2. Preclosure Safety Assessment Process

The event sequences that are categorized in the present analysis can be more fully understood by consulting the event sequence development analysis (Ref. 2.2.40). The remainder of this subsection presents a refresher of the event sequence development process.

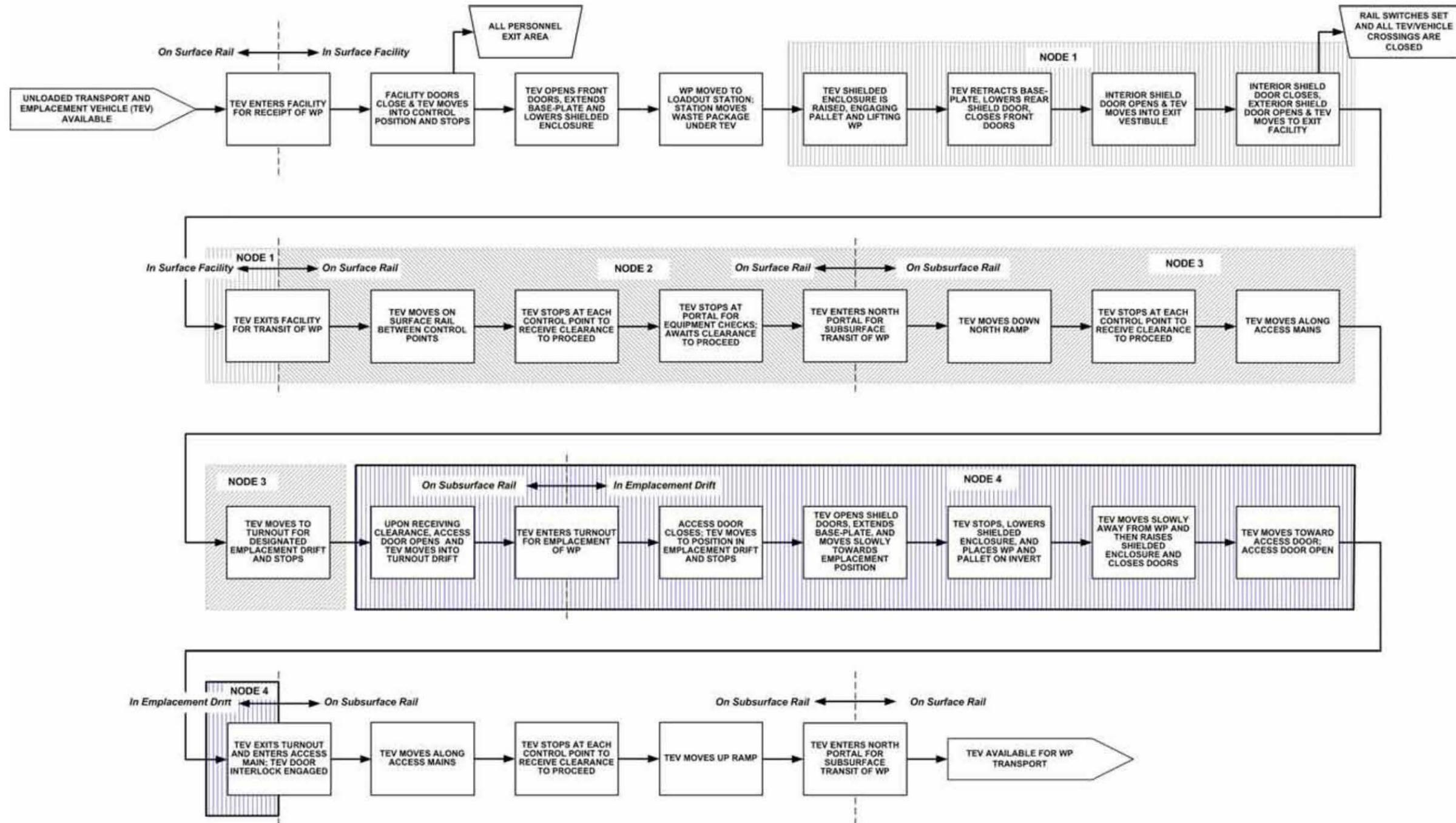
A simplified process flow diagram (PFD) is developed to clearly delineate the process and sequence of operations to be considered within the analysis of the facility. An excerpt from an example PFD is shown in Figure 4.3-3. The PFD guides development of the MLD and the conduct of the HAZOP evaluation.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

processes and operations that are evaluated with both a MLD and HAZOP evaluation to identify potential initiators.

Development of the MLD is accomplished by deriving specific failures from a generalized statement of the undesired state. As a “top-down” analysis, the MLD starts with a top event, which represents a generalized undesired state. The top event includes direct exposure to radiation and exposure as result of a release of radioactive material. The basic question answered by the MLD is “How can the top event occur?” Each successively lower level in the MLD hierarchy divides the identified ways in which the top event can occur with the aim of eventually identifying specific initiating events that may cause the top event. In the MLD, the initiating events are shown at the next-to-lowest level. The lowest level provides an example of contributors to the initiating event. This process for the PCSA is detailed in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40, Section 4.3.1.2).

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

The MLD and HAZOP evaluation are strongly interrelated. The MLD is cross-checked to the HAZOP evaluation. That is, the MLD is modified to include any initiators and contributors that are identified in the HAZOP evaluation but not already included in the MLD. The entire process is iterative in nature (Figure 4.3-2 (does not show iteration)) with insights from succeeding steps often feeding back to predecessors. The top-down MLD and the bottom-up HAZOP evaluation provide a diversity of viewpoints that adds confidence that no important initiating events have been omitted. Details on implementation of the HAZOP evaluation are presented in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40, Section 4.3.1.3).

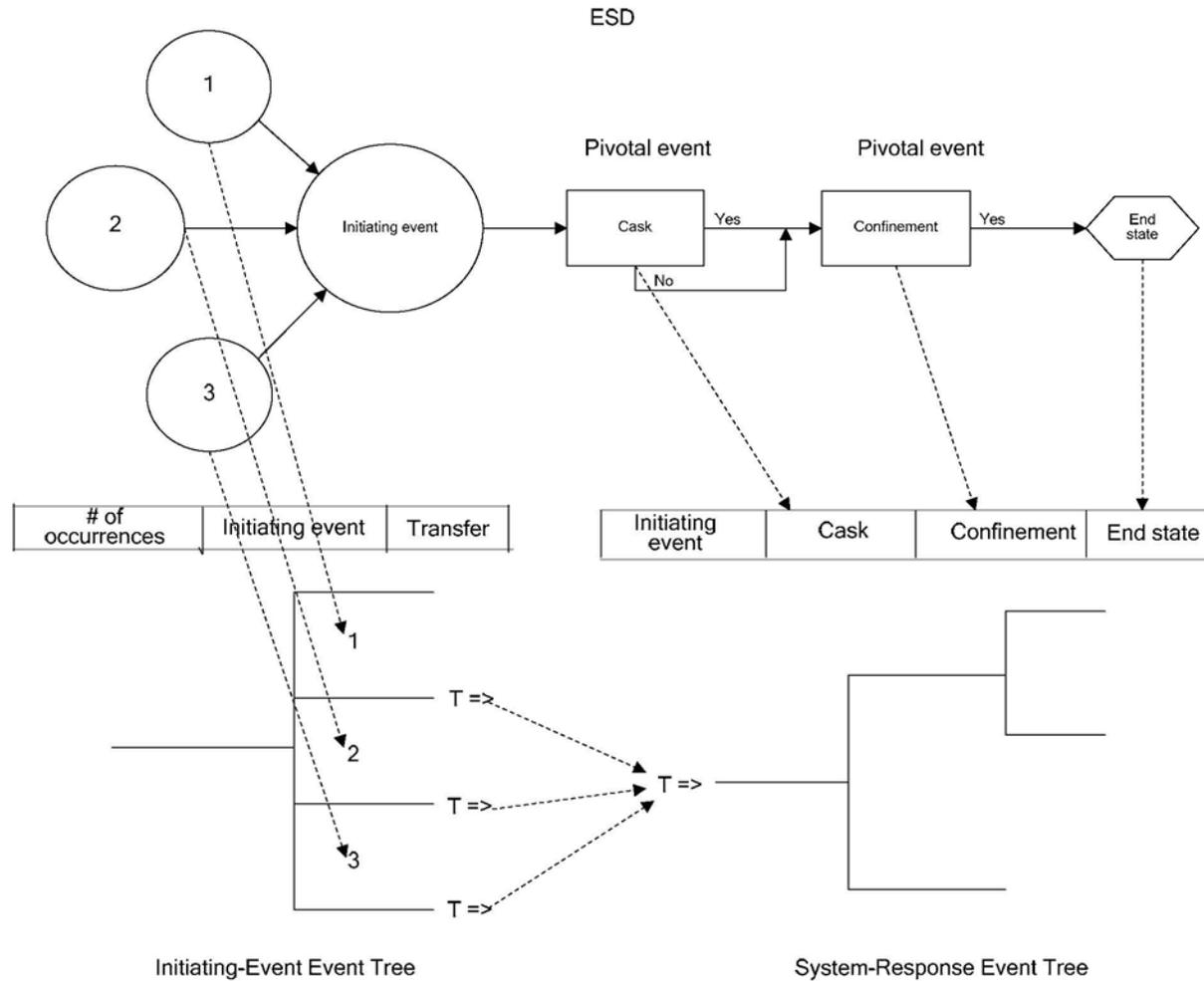


NOTE: CTT = cask transfer trolley; CTM = canister transfer machine; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Excerpt from (Ref. 2.2.40)

Figure 4.3-3. Simplified Process Flow Diagram for Example with Node 4 Emphasized for Further Discussion

An overview of the pertinent human and SSC responses to an initiating event is depicted in an ESD. As shown in Figure 4.3-4, an ESD represents event sequences in terms of initiating events, pivotal events, and end states. The boxes (pivotal events) represent events that have binary outcomes: success (yes) or failure (no). Because the future is uncertain, the analyst does not know which of the alternative scenarios might occur. The ESD depicts the alternative scenarios as paths that can be traced through the diagram. Each alternative path from 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., heating, ventilation, and air conditioning (HVAC)) become pivotal events in the ESD.



Source: Original

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

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

For example, all initiating events that challenge the containment function of a canister would include pivotal events that question the containment integrity of the canister and the availability of HVAC confinement. The knowledge to develop such ESDs and appropriately group the initiating events comes from a detailed knowledge of the SSCs and operations derived from developing the PFD, MLD, and HAZOP evaluation. The pivotal event conditional probabilities are the same for all initiating events in a little bubble. All initiating events represented by the big

bubble have the same human and SSC responses and, therefore, may be represented by the same event sequences. However, the conditional probability for each pivotal event is not necessarily the same for each little bubble.

#### 4.3.1 Event Tree Analysis and Categorization

Also illustrated in Figure 4.3-4, is the relationship of the YMP ESDs to their equivalent event trees. Event trees contain the same information as ESDs but in a form suitable to be used by software such as SAPHIRE (Ref. 2.2.46), which ultimately stores event trees, fault trees, and reliability data, and can be used to quantify complex event sequences. (SAPHIRE was not used for quantifying event sequences for Intra-Site Operations or 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. 2.2.66, Section 3.4.4.2). Any path from left to right that begins with the initiating event and terminates with an end state is an event sequence. Every path must be associated with an end state. As illustrated in the event tree portion of Figure 4.3-4, each intersection of a horizontal and vertical line is referred to as a node (or branch point). Each node is associated with a conditional probability of following the vertical downward branch. By convention, the description of each branch is stated as a success, and the downward branch indicates a failure. The complement is the probability of taking the vertical upward branch, that is, the probability of success. To quantify the event sequence, the initiating event frequency (or expected number of occurrences) is multiplied by the conditional probability of each subsequent pivotal event node in the event sequence until an end state is reached.

The YMP PCSA uses the concept of linked event trees (Ref. 2.2.66). Each facility has its own set of event trees. The first event tree simply represents the little bubbles, one horizontal line per little bubble. This is called the initiator event tree (IET). The second event tree contains the pivotal events and end states. This is called the system response event tree (SRET). An event sequence would start with each of the horizontal lines as if it were the initiating event on the SRET, as indicated in Figure 4.3-4. Each set of IET and SRET is quantified for each waste container type (e.g., dual-purpose canisters (DPCs), transportation, aging, and disposal (TAD) canisters, DOE SNF that is handled in a facility). The event in the IET labeled “# of occurrences” represents the number of handlings (i.e., demands) for that initiating event. For example, each lift of a transportation cask provides an opportunity for a drop. An event sequence quantification includes the frequency (or number of occurrences) of each end state (e.g., radionuclide release), associated with a single lift, and multiplies it by the number of lifts to obtain the expected number of drops over the preclosure period. This approach is consistent with a binomial model of reliability.

Categorization of event sequences is based on the aggregated “big bubble” initiating event. Each line on the IET coupled with the SRET is quantified separately. Using Figure 4.3-4, this would mean three quantifications, corresponding to the three initiating event frequencies and three corresponding sets of pivotal event probabilities. (By SAPHIRE convention, the top line is a dummy initiating event.) Each event sequence, therefore, would have three values. In order to obtain the total frequency of an event sequence for purposes of categorization, per 10 CFR

63.111 (Ref. 2.3.2), the three frequencies are probabilistically summed. Doing this summation is equivalent to basing categorization on the big bubble. If an event sequence has only one little bubble, then only the SRET needs to be used with the initiating event in the place so denoted, in the second event tree. In this case, summation of event sequences is not necessary and not performed.

Because each event sequence is associated with a mean number of occurrences over the preclosure period, categorization is straightforward. Those event sequences that are expected to occur one or more times before permanent closure of the GROA are Category 1 event sequences. Other event sequences that have at least one chance in 10,000 of occurring but less than one occurrence before permanent closure are Category 2 event sequences. Sequences that have less than one chance in 10,000 of occurring before permanent closure are identified as Beyond Category 2. As described in Section 4.3.6, event sequence quantification considers uncertainties and categorization is performed on the basis of an event sequence mean value of the underlying probability distribution. The preclosure period lasts 100 years but actual emplacement operations occupy 50% of this time (Ref. 2.2.15, Section 2.2.2.7).

Although event trees were developed for the subsurface operations in the *Subsurface Operations Event Sequence Development Analysis* report (Ref. 2.2.40), detailed event tree analysis using SAPHIRE software was not carried out. Instead, the event sequence logic was developed directly from the set of IET and SRET established for each ESD and input into an Excel spreadsheet. Subsequently, data for initiating event frequencies and pivotal event conditional probabilities obtained via fault tree analysis or derived from empirical data are incorporated into the spreadsheet. When the spreadsheet is fully populated, event sequence quantification begins, followed by event sequence grouping and categorization. The method for obtaining initiating and pivotal event data is described in the following sections.

#### **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 system response event tree for each ESD): The conditional probabilities used in this analysis are point values that represent a passive failure (refer to 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) follows a transfer to a system response event tree, 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 provided in Section 6.3.) The initiator event trees and the system response event trees developed in SAPHIRE for the event sequence development analysis (Section 4.2) 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.													
		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 Std Dev	End State
	ISO-ESD02-TAD													
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-UNFILTR	ISO02-TAD-SEQ3-RRU	8.2E-07	3.3E-07	1.6E-07
RR-UNFILTR	ISO02-TAD-SEQ4-RUC	0.0E+00	0.0E+00	0.0E+00

Initial Categ.
Cat2
BC2
BC2

Source: Original

Figure 4.3-5. Example Excel Spreadsheet

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 important to criticality (RRU), starts with an initiator event tree 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. 2.2.31, Table 4), there are 16,286 such movements (i.e., 8,143 waste forms x 2 trips each). The branch on the initiator event tree 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-05. The next pivotal event is “MODERATOR”, which has a probability value of “0”, 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 to 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 and median values can be directly summed, as described below.

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,  $\sigma$ , 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.

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

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

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

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 is calculated from the mean and standard deviation according to Equation 4:

$$\text{Median} = \frac{\mu^2}{\sqrt{\mu^2 + \sigma^2}} \quad (\text{Eq. 4})$$

where

$\mu$  is the mean for the lognormal distribution (i.e.,  $\mu_{X+Y}$  for the summed distributions)

$\sigma^2$  is the variance for the lognormal distribution (i.e.,  $\sigma_{X+Y}^2$  for the summed distributions)

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 important to criticality (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	<u>Initial Categ.</u>
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

Source: Original

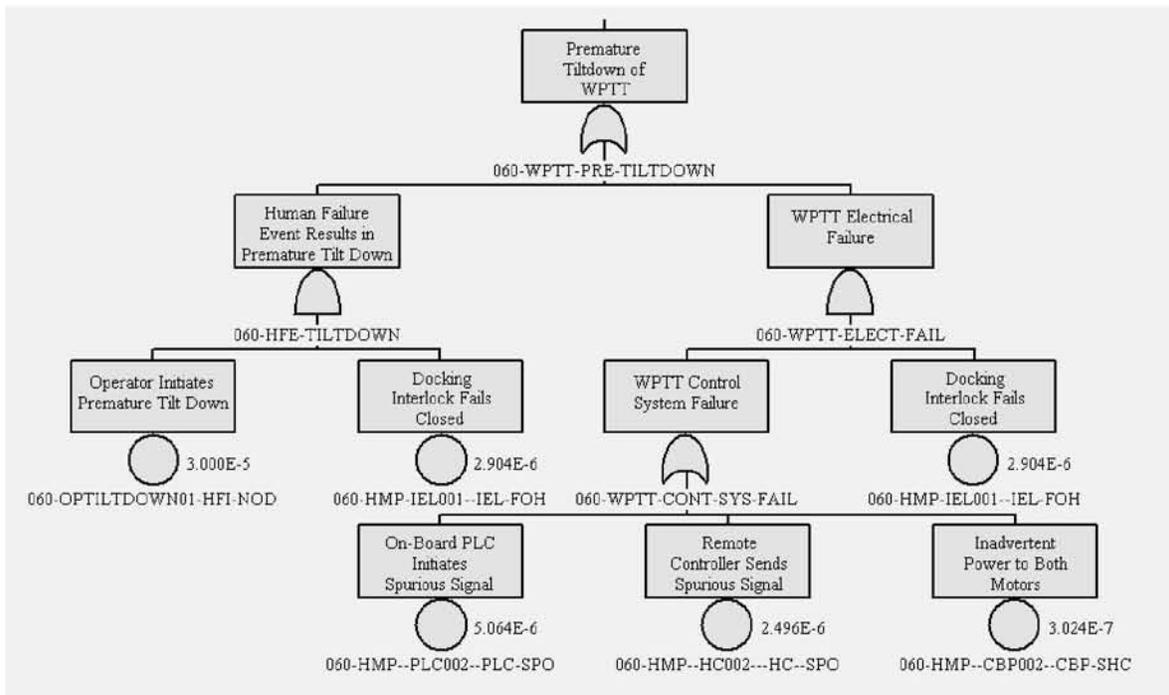
Figure 4.3-6. Example Grouped Event Sequences

### 4.3.2 Initiating and Pivotal Event Analysis

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

### 4.3.2.1 Fault Tree Analysis

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



NOTE: This fault tree is presented for illustrative purposes only and is not intended to represent results for 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 usually failures or faults. Fault trees use logic or Boolean gates. Figure 4.3-7 shows two types of gates: the AND gate (mound shaped symbol with a flat bottom) and the OR gate (mound shaped symbol with a concave bottom). An AND gate passes an output up the tree if all events immediately attached to it occur. An OR gate passes an output up the tree if one or more events immediately attached to it take place. An AND gate often implies components or system features that back each other up, if one fails, the other continues to perform the function adequately. The success criterion of the SSC or equipment being analyzed is important in determining the appropriate use of gates.

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

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

As illustrated in Figure 4.3-7, the organization of the fault trees in the PCSA is developed to emphasize two primary elements, which together result in the occurrence of the top event: (1) human failure events, and (2) equipment failures. The human failure events include postulated unintended crew actions and omissions of crew actions. Identification and quantification of human failure events (HFEs) are performed in phases. Initial identification of HFEs led to design changes to either eliminate them or reduce the probability that they would cause the fault tree top event. For example, Figure 4.3-7 shows an HFE logically intersected with an electro-mechanical interlock such that both a crew error of commission and failure of the interlock must occur for premature WPTT tiltdown to occur.

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

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

Passive equipment (e.g., transportation casks, storage canisters, waste packages) may fail from manufacturing defects, material variability, defects introduced by handling, long-term effects such as corrosion, and normal and abnormal use. Industry codes, such as *Minimum Design Loads for Buildings and Other Structures* (Ref. 2.2.5) and Section III, Subsection NCA of *ASME Boiler and Pressure Vessel Code* (Ref. 2.2.7) 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 Section III, Subsection NCA of the *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).

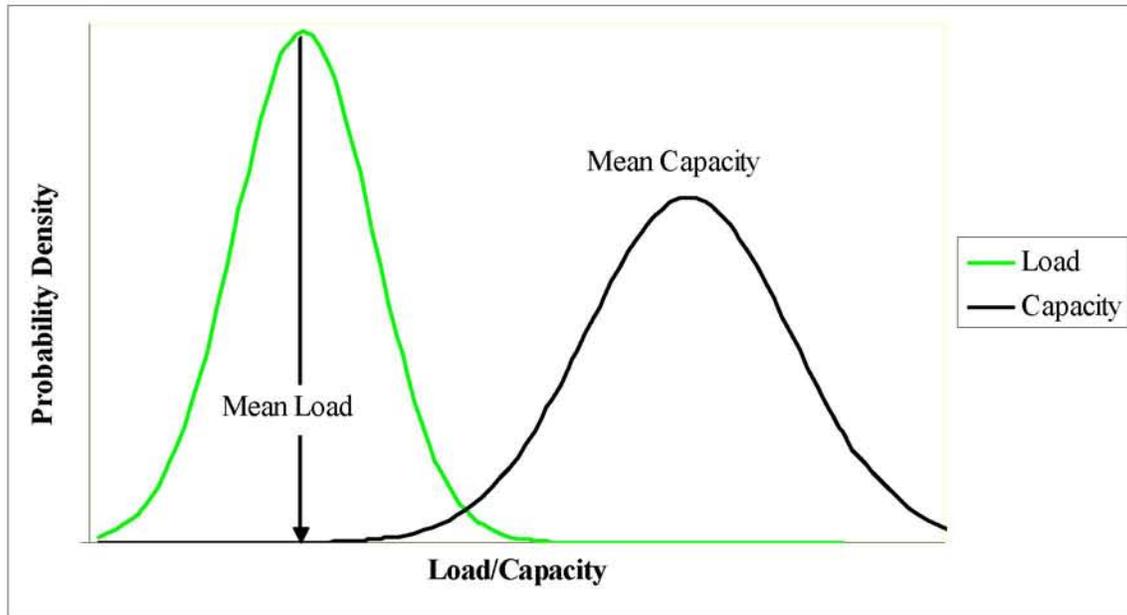
The development of code requirements for minimum design loads in buildings and other structures in the late 1970s considered multiple loads. A probabilistic basis for structural reliability was developed as part of the development of *Development of a Probability Based Load Criterion for American National Standard A58, Building Code Requirements for Minimum Design Loads in Buildings and Other Structures* (Ref. 2.2.50). 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 4:

$$g(x_1, x_2, \dots, x_i, \dots, x_n) = 0 \quad (\text{Eq. 4})$$

In Equation 4,  $g$  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 5:

$$P_f = \int \dots \int f_x(x_1, x_2, \dots, x_i, \dots, x_n) dx_1 dx_2 \dots dx_n \quad (\text{Eq. 5})$$

Where  $f_x$  is the joint probability density function of  $x_i$  and the integral is over the region in which  $g < 0$ . The fact that these variables are represented by probability distributions implies that absolutely precise values are not known. In other words, the variable values are uncertain. This concept is illustrated in Figure 4.3-8. 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 margin, often called a factor of safety, between the load and capacity. The factor of safety is established in recognition that quantities, methods used to evaluate them, and tests used to ascertain material strength give rise to uncertainty. A heuristic measure of the factor of safety is the distance between the mean values of the two curves.



Source: Original

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

In the case in which Equations 4 and 5 are approximated by one variable representing resistance 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 6.

$$P_f = \int F(y)h(y)dy \quad (\text{Eq. 6})$$

$P_f$  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 6,  $F(y)$  represents the cumulative density function (CDF) of structural capacity and  $h(y)$  represents the probability density function (PDF) of the load. The former is sometimes called the fragility function and the later is sometimes called the hazard function.

To analyze the probability of breach of a dropped canister,  $y$  is typically in units of strain,  $F$  is typically a fragility function, which provides the conditional probability of breach given a strain; and  $h$  is the probability density function of the strain that would emerge from the drop. For seismic risk analysis,  $h$  represents the seismic motion input,  $y$  is in units of peak ground acceleration, and  $F$  is the seismic fragility. The seismic analysis of the YMP structures is documented separately in *Seismic Event Sequence Quantification and Categorization* (Ref. 2.4.4). Degradation of shielding owing to impact loads uses a strain to failure criterion within the simplified approach of Equation 7, described below. For analysis of the conditional probability of breach owing to fires,  $y$  is temperature,  $F$  is developed from fire data for non-combustible structures, and  $h$  is developed using probabilistic heat transfer calculations. Analysis for heating up casks, canisters, and waste packages associated with loss of building forced convection cooling was similarly accomplished, but Equation 7 was used.

If load and capacity are known, then Equations 5 and 6 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,  $\bar{L}$  and  $\bar{R}$ , and a measure of the uncertainty, generally the standard deviation, usually denoted by  $\sigma_L$  and  $\sigma_R$  for  $L$  and  $R$ , respectively. The spread of the functions may be expressed, alternatively, by the corresponding coefficient of variation (V) given by the ratio of standard deviation to mean, or  $V_L = \sigma_L/\bar{L}$  and  $V_R = \sigma_R/\bar{R}$  for load and resistance, respectively. The coefficient of variation may be thought of as a measure of dispersion expressed in terms of the number of means.

In the PCSA, the capacity curve for developing the fragility of casks and canisters against drops was constructed by a statistical fit to tensile elongation to failure tests (Ref. 2.2.39). The load curve may be constructed by varying drop height. A cumulative distribution function may be fit to a locus of points each of which is the product of drop height frequency and strain given drop height.

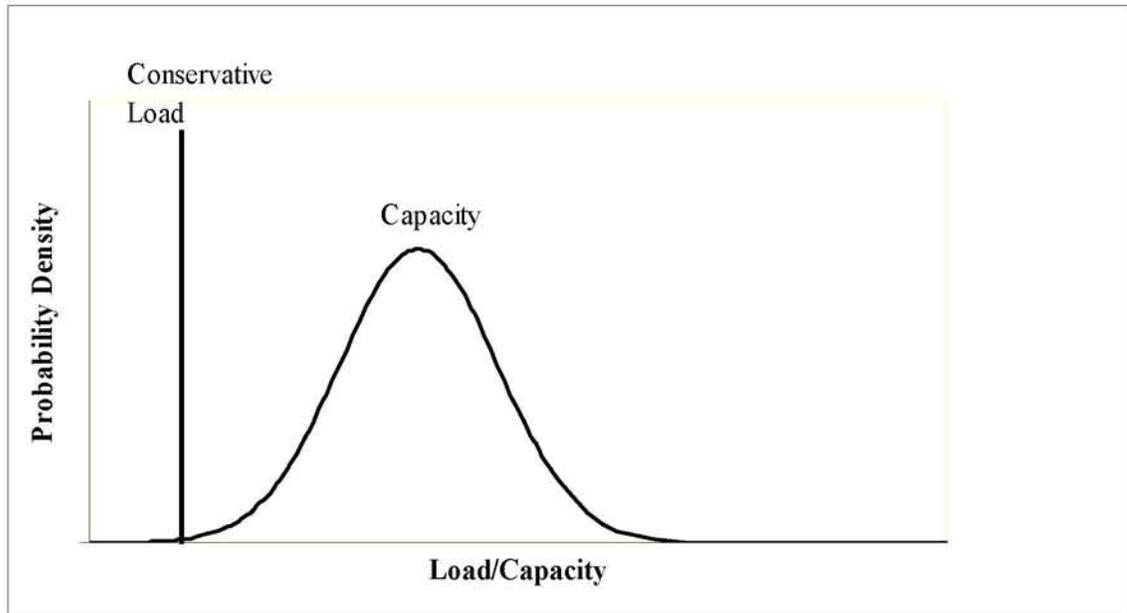
### Impact Events Associated with Containment Breach

A simplification of Equation 6, consistent with *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73), and shown in Equation 7 is used in the PCSA. It is illustrated in Figure 4.3-9.

$$P_f = \int_0^h F(y)dy \quad (\text{Eq. 7})$$

In Equation 7,  $h$  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 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 the TEV. The conditional probability of breach is an increasing function of drop height. Strain resulting from drops is calculated by dynamic finite element analysis using Livermore Software–Dynamic Finite Element Program (LS-DYNA) for canisters and transportation cask drops (Ref. 2.2.39). 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 PEFA's to a wide variety of event sequences including those associated with:

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

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

### Shielding Degradation Events

Impact loads (such as drops) may not be severe enough to breach a transportation cask, but might lead to degradation of shielding such that onsite personnel are exposed. The waste package does not provide shielding; worker protection from direct radiation is provided by the TEV. In this analysis, the TEV is considered to function as a transportation cask in providing shielding protection, and thus, all discussions regarding transportation cask shielding is applicable to the TEV shielding function. According to *Conceptual Shielding Study for Transport Emplacement Vehicle* (Ref. 2.2.13, Table 1, Configuration B), the TEV shielding consists of a steel shell with a sandwich of depleted uranium and polymer. This shielding is similar to the steel/depleted uranium truck cask noted below.

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

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

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

Principal insights reported in (Ref. 2.2.83) are the following:

- Monolithic steel rail casks do not exhibit any shielding degradation, but there may be some radiation streaming through gaps in closures in any of the impact scenarios. This result can be applied to both transportation casks.

- 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.

Since the TEV shielding construction is similar to the steel/depleted uranium truck cask, no shielding degradation would occur following an impact to the TEV under similar conditions listed in the study.

### **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 6 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 fire suppression, which leads to an assessment that significantly overstates the risk of fires.

#### **4.3.2.2.1 Uncertainty in Fire Duration**

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

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

Uncertainty in fire duration was developed from:

- *Utilisation of Statistics to Assess Fire Risks in Buildings* (Ref. 2.2.85)
- *Heat and Mass Release for Some Transient Fuel Source Fires: A Test Report. NUREG/CR-4680* (Ref. 2.2.64)
- *Quantitative Data on the Fire Behavior of Combustible Material in Nuclear Power Plants: A Literature Review. NUREG/CR-4679* (Ref. 2.2.65).

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

The fire temperature used in this calculation is the effective blackbody temperature of the fire. This temperature implicitly accounts for the effective emissivity of the fire, which for large fires approaches a value of 1.0 (Ref. 2.2.78, p. 2-56). Fires within 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. 2.2.78, Section 2, Chapter 2) with information about liquid hydrocarbon pool fires (Ref. 2.2.2) and (Ref. 2.2.78, p. 2-56). The derivation of this distribution is described in Attachment D, Section D2.1.2. The fire temperature is normally distributed with a mean of 1,072 K (799°C) and a standard deviation of 172 K. The mean of this distribution is approximately equal to the transportation cask design basis fire temperature of 800°C specified in 10 CFR 71.73, Hypothetical Accident Conditions (Ref. 2.3.3).

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

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

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

The total radiant energy deposited in the container can be roughly estimated using Equation 8:

$$Q_{rad} = \varepsilon F_{cf} \sigma (T_{fire})^4 A t \quad (\text{Eq. 8})$$

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 ( $\text{W}/\text{m}^2 \text{K}^4$ )
$T_{fire}$	=	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 spent fuel or high-level radioactive waste.

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

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

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

Equation 6, along with the heat transfer equations, are solved using Monte Carlo simulation (described in Section 4.3.7) with the above described fragility and target fire severity probability distributions, and distributions for the uncertain heat transfer factors. For each Monte Carlo trial, the calculated maximum canister temperature is compared to the sampled target failure temperature. If the maximum temperature of the target exceeds the sampled failure temperature, then target failure is counted. The failure probability in this method is equal to the fraction of the samples for which failure is calculated.

Uncertainty in the calculated canister failure probability is given by a calculated mean and standard deviation, where the mean is simply the number of failures divided by the total number of samples and the standard deviation is given by Equation 9 for the standard deviation of a binomial distribution:

$$\sigma = \sqrt{\frac{\frac{n_{fail}}{N} \left( \frac{N - n_{fail}}{N} \right)}{N}} \quad (\text{Eq. 9})$$

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

### Fire Event Associated with Shielding Degradation

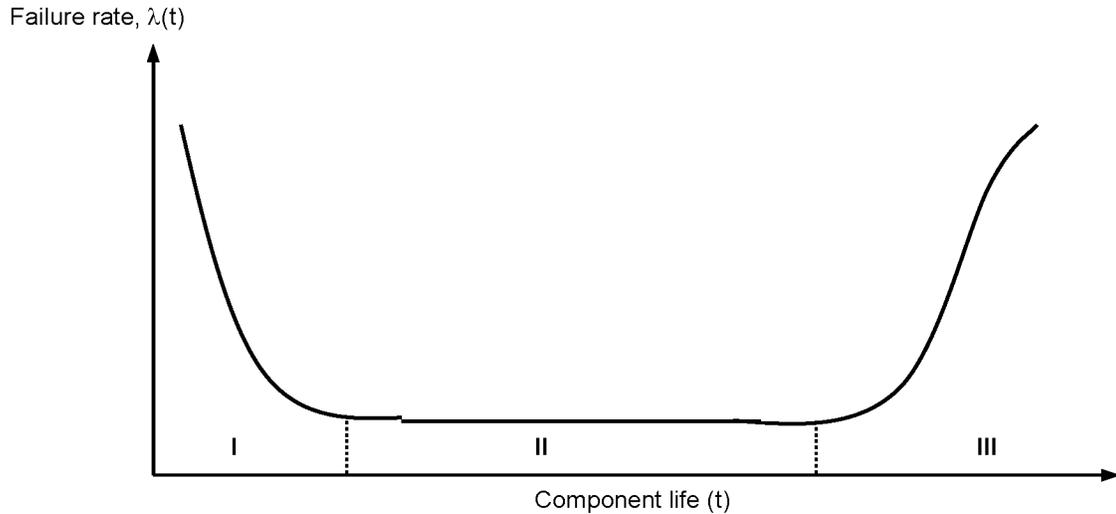
The thermal analyses in *Reexamination of Spent Fuel Shipment Risk Estimates*. NUREG/CR-6672 (Ref. 2.2.83) indicates that the probability of shielding degradation in a fire scenario should be based on the probability of having a fire that is equivalent to a 1,000°C engulfing fire that lasts for more than a half-hour. However, TEV shielding degradation does not occur unless the depleted uranium layer is broken into pieces and drops out of the steel shell. Although TEV gamma radiation shielding provided by depleted uranium layer is expected to remain in place, the neutron shielding provided by the polymer layer would be destroyed and considered a loss under fire scenario. As a result, it is conservatively considered that TEV shielding function would be a loss under fire scenarios.

### 4.3.3 Utilization of Industry-Wide Reliability Data

#### 4.3.3.1 Use of Population Variability Data

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

As presented in *Fault Tree Handbook* (Ref. 2.2.87, Figure X-8, p. X-23), the typical model of failure probability for a component is depicted as a “bathtub curve” illustrated in Figure 4.3-10. 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, which is represented by Phase III of the curve; the probability of failure increases.



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

Figure 4.3-10. 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 10:

$$P_F(\lambda, t_m) = 1 - \exp(-\lambda t_m) \quad (\text{Eq. 10})$$

When the product  $\lambda t_m$  is small ( $<0.1$ ), the failure probability may be calculated by the following Equation 11 approximation, which introduces less than a 10% error:

$$P_F(\lambda, t_m) \cong \lambda t_m \quad (\text{Eq. 11})$$

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. Reliability theory assumes that after each test the component or system is "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 12:

$$q_d(\lambda, \tau) = \frac{1}{2}(\lambda \tau) \quad (\text{Eq. 12})$$

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

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

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

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

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

The lack of actual operating experience, the use of industry-wide data, and the consideration of uncertainties (Ref. 2.2.73) suggested that a Bayesian approach was appropriate for the PCSA. A Bayesian approach and the use of judgment in expressing the state-of-knowledge of basic event unreliability is a well-recognized and accepted practice (Ref. 2.2.59, Ref. 2.2.9, and Ref. 2.2.66). Furthermore, *Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis – Level of Information and Reliability Estimation* includes the use of engineering judgment, supported by sufficient technical basis, as a means of justifying reliability estimates for certain SSCs (Ref. 2.2.73).

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 13:

$$P(\lambda_j / E) = \frac{P(\lambda_j)L(E / \lambda_j)}{\sum_j P(\lambda_j)P(E / \lambda_j)} \quad (\text{Eq. 13})$$

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 13 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 13 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 13 will await actual test and operations. The following summarizes the methods used to develop the Bayesian prior distributions.

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution,  $g$ , representing the source-to-source variability, also called population variability, of the component reliability (Ref. 2.2.9, Section 8.1). In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. The population-variability distributions developed in this analysis attempt to encompass the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the PCSA. As indicated in *Bayesian Parameter Estimation in Probabilistic Risk Assessment* (Ref. 2.2.79, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

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

For each data source, the reliability information about a component's failure rate 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. 2.2.79, Section 4.2). When no exposure data is available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution (Ref. 2.2.79, Section 4.4) and (Ref. 2.2.57, 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. 2.2.9, 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. 2.2.57, 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. 2.2.79, 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 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 in Equation 14:

$$L_i(\nu, \tau) = \int_0^1 \text{Binom}(x, r, n) \times g(x, \nu, \tau) dx \quad (\text{Eq. 14})$$

where  $\text{Binom}(x, r, n)$  represents the binomial distribution evaluated for  $r$  failures out of  $n$  demands, given a failure probability equal to  $x$ , and  $g(x, \nu, \tau)$  is defined as previously indicated. This equation is similar to that shown in *Bayesian Parameter Estimation in Probabilistic Risk Assessment* (Ref. 2.2.79, Equation 37). If the component reliability is expressed in terms of a failure rate and the data source provides exposure data, the binomial distribution in Equation 14 would be replaced by a Poisson distribution. If the data source provides expert opinion only (no exposure data), the binomial distribution in Equation 14 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine  $\nu$  and  $\tau$  (Ref. 2.2.79, 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. 2.2.57, 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 *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.9, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to  $\exp(\nu + \tau^2/2)$  and the error factor is equal to  $\exp(1.645 \times \tau)$ . A discussion of the adequacy of the empirical Bayes method for the YMP analysis is found in Attachment C.

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, *External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom* (Ref. 2.2.54, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between  $2 \times 10^{-8}/\text{hr}$  (5th percentile) and  $6 \times 10^{-5}/\text{hr}$  (95th percentile), using the definition of the error factor given in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823 (Ref. 2.2.9, Section A.7.3), this corresponds to an error factor of  $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$ . Therefore, in the PCSA, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55, are too diffuse to adequately represent the population-variability distribution of a component. In such instances (i.e., the two cases in the entire PCSA database when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution, and therefore is unaffected by the value taken by the error factor. Based on the NUREG/CR-6823 (Ref. 2.2.9, 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. 2.2.9, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution, and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not

approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using the data source that yields the most diffuse likelihood using one of the two methods described in the next paragraph.

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean, and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data, i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities, the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffreys' noninformative prior distribution as indicated in NUREG/CR-6823 (Ref. 2.2.9, Section 6.2.2.5.2). This noninformative prior conveys little prior belief or information, thus allowing the data to speak for itself.

#### 4.3.3.2 Dependent Events

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

1. **Functional dependence** is present when one component or system relies on another to supply vital functions. An example of a functional dependence in this analysis is electric power supply to HVAC. Functional dependence is explicitly modeled in the event tree and fault tree logic.
2. **Environmental dependence** is in play when system functionality relies on maintaining an environment within designed or qualified limits. Here, an example is material property change as a result of temperature change. Environmental effects are modeled in the system reliability analyses as modifications (e.g., multiplying factors) to system- and component-failure probabilities and are also included in the passive equipment failure analyses. External events such as earthquakes, lightning strikes, and high winds that can degrade multiple SSCs are modeled explicitly as initiating events and are discussed in other documents (Ref. 2.2.34 and Ref. 2.4.4).
3. **Spatial dependence** is at work when one SSC fails by virtue of close proximity to another. For example, during an earthquake one SSC may impact another because of close proximity. Another example is inadvertent fire suppression actuation which wets SSCs below it. Spatial dependences are identified by explicitly looking for them in the facility layout drawings. Inadvertent fire suppression is modeled explicitly in the event trees and fault trees.

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

#### 4.3.3.3 Common-Cause Failures

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

Because CCFs are relatively uncommon, it is difficult to develop a statistically significant sample from monitoring only one system or facility, or even several systems. The development of CCF techniques and data, therefore, rely on a national data collection effort that monitors a large number of nuclear power systems. Typically, the fraction of component failures associated with common causes leading to multiple failures ranges between 1% and 10% (Ref. 2.2.53), (Ref. 2.2.62), and (Ref. 2.2.58). 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. 2.2.53), the Multiple Greek Letter method (Ref. 2.2.61), and the Alpha Factor method (Ref. 2.2.62). These methods do not require an explicit knowledge of the dependence failure mode.

The PCSA uses the Alpha Factor method (Ref. 2.2.62), which is summarized below. After identifying potential CCF events from the fault trees, appropriate alpha factors are identified according to the procedure described in *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis* NUREG/CR-5801 (Ref. 2.2.60). The general equations for estimating the probability of a CCF event in which  $k$  of  $m$  components fail are as follows in Equation 15, Equation 16, and Equation 17:

$$Q(k, m) = \frac{k}{\binom{m-1}{k-1}} \alpha_k Q_i \quad \text{for staggered test} \quad (\text{Eq. 15})$$

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

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

$$\alpha_t = \sum_{k=1}^m k \alpha_k \quad (\text{Eq. 17})$$

Generic alpha factors used in the PCSA are taken from NUREG/CR-5801 (Ref. 2.2.60). The process of applying these alpha factors is explained further in Attachment C, Section C3.

#### 4.3.4 Human Reliability Analysis

Human interactions that are typically associated with the operation, test, calibration, or maintenance of an SSC (e.g., drops from a crane when using slings) are implicit in the empirical data. If this is the case, empirical data may be used, provided human errors that cause the SSC failures are explicitly enumerated and determined to be applicable to YMP operations. When this was the case in the PCSA, the appropriate method of Section 4.3.3.1 was applied. Otherwise, an HRA was performed, the methodology of which is summarized in this section. The HRA task is performed in a manner that implements the intent of the high-level requirements for HRA in *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6) and incorporates the guidance in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. 2.2.72). It emphasizes a comprehensive qualitative analysis and uses applicable quantitative models.

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

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

#### 4.3.4.1 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:

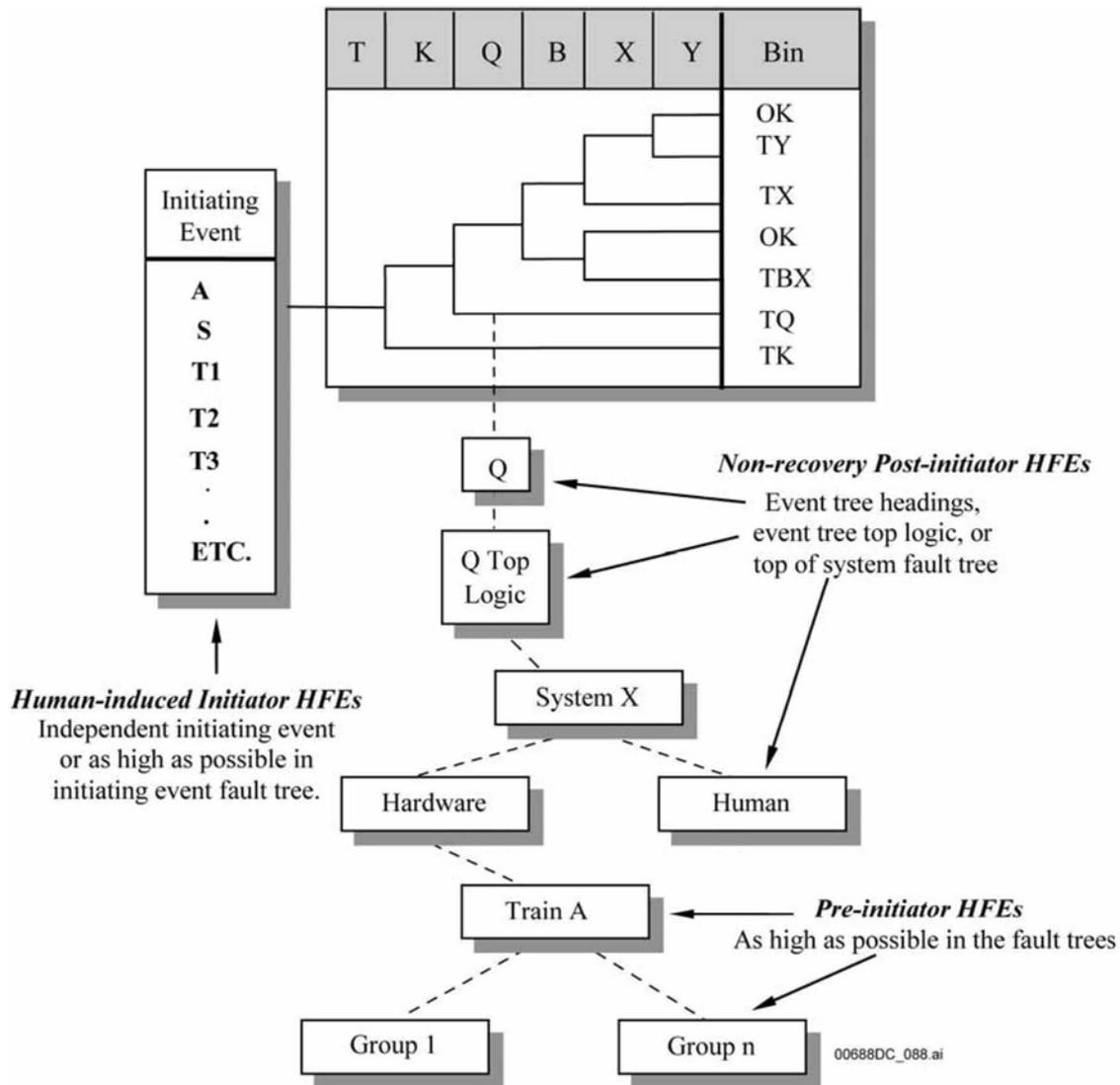
1. Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior, deliberate acts of sabotage, and the like are not considered in this task.
2. All personnel act in a manner they believe to be in the best interests of operation and safety. Any intentional deviation from standard 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 spent fuel storages, chemical munitions handling at U.S. Army chemical demilitarization facilities, and any other facilities whose primary function includes handling and disposal of very large containers of extremely hazardous material. Equipment design and operational characteristics at the GROA facilities, once they are built and operating (including crew structures, training, and interactions), are adequately represented by these currently operating facilities.
4. The YMP is initially operating under normal conditions and is designed to the highest quality human factor specifications. The level of operator stress is optimal unless the analyst determines that the human action in question cannot be accommodated in such a manner as to achieve optimal stress.
5. In performing the operations, the operator does not need to wear protective clothing unless it is an operation similar to those performed in comparable facilities where protective clothing is required.
6. The tasks are performed by qualified personnel, such as operators, maintenance workers, or technicians. All personnel are certified in accordance with the training and certification program stipulated in the license. They are to be experienced and have functioned in their present positions for a sufficient amount of time to be proficient.
7. The environment inside each YMP facility is not adverse. The levels of illumination and sound and the provisions for physical comfort are optimal. Judgment is required to determine what constitutes optimal environmental conditions. The analyst makes this determination, and documents, as part of the assessment of performance influencing factors, when there is a belief that the action is likely to take place in a suboptimal environment. Regarding outdoor operations onsite, similar judgments must be made regarding optimal weather conditions.

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

These factors are evaluated qualitatively for each situation being analyzed.

#### **4.3.4.2 HRA Methodology**

The HRA consists of several steps that follow the intent of ASME RA-S-2002, *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. 2.2.6) and the process guidance provided in *Technical Basis and Implementation Guidelines for Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. 2.2.70). The step descriptions are based on the ATHEANA documentation, with some passages taken essentially verbatim and others paraphrased to adapt material that is based on nuclear power plants to the YMP facilities. Additional information is available in the ATHEANA documentation (Ref. 2.2.70). Section 10.3 of *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. NUREG-1624 (Ref. 2.2.70) provides an overview of the method for incorporating HFEs into a PRA. Figure 4.3-11 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 the description of expected facility, equipment, and operator behavior for the selected operation.

**Step 3: Identify and Define HFEs of Concern**—Possible HFEs and/or unsafe actions (i.e., actions inappropriately taken or actions not taken when needed) that result in a degraded state are generally identified and defined in this step. After HFEs are identified they must be classified to support subsequent steps in the process. The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then becomes the error-forcing context (EFC) for a specific HFE. As defined by ATHEANA (Ref. 2.2. 70), an EFC is the situation that arises when particular combinations of PSFs and plant conditions create an environment in which unsafe actions are more likely to occur. Additions to and refinements of these initial EFCs are made during the preliminary and detailed analyses. The analyses performed in later steps (e.g., Steps 6 and 7) may identify the need to define additional HFEs or unsafe actions.

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

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

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

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

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

**Step 7: Quantify Probabilities of HFEs**—Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with 10 CFR 63.111 performance objectives (Ref. 2.3.2) 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 CRF 63.111 performance objectives (Ref. 2.3.2). The activities of a detailed HRA are as follows:

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

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

1. Cognitive Reliability and Error Analysis Method (CREAM) (Ref. 2.2.56)
2. Human Error Assessment and Reduction Technique (HEART) (Ref. 2.2.88)/  
*Nuclear Action Reliability Assessment (NARA)* (Ref. 2.2.43)
3. Technique for Human Error Rate Prediction (THERP) with some modifications (Ref. 2.2.84).

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

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

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

**Step 8: Incorporate HFEs into PCSA**—After HFEs are identified, defined, and quantified, they must be reincorporated into the PCSA. Section 10.3 of NUREG-1624 (Ref. 2.2.70) provides an overview of the state-of-the-art method for performing this step in PRAs. The term “reincorporated” is used because some HFEs are identified within the fault tree and event tree analysis. All event sequences that contain multiple HFEs are examined for possible dependencies. Figure 4.3-11 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 procedural safety control could be added to reduce the probability or completely eliminate the HFE. An example of such iteration includes the interlocks that ensure that cask lids are securely grappled 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 (EOOs)
  - B. Errors of commission (EOCs).
3. Human failure types:
  - A. Slips/lapses
  - B. Mistakes.

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

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

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

- Monitoring and detection—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring initiated by a person's knowledge or expectations is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.
- Situation awareness—This term is defined as the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents the operator's understanding of the present situation and their expectations for future conditions and consequences.
- Response planning—This term is defined as the process by which operators decide on a course of action, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.
- Response implementation—This term is defined as the activities involved with physically carrying out the actions identified in response planning.
- When there are short time frames for response and the possibility of severely challenging operating conditions (e.g., environmental conditions) exists, then failures in all information processing stages must be considered. Also, slips/lapses and mistakes are considered for each information processing stage. Response implementation failures are expected to dominate the pre-initiator failures that are modeled. Post-initiator failures and failures that initiate event sequences can occur for all information processing stages, although detection failures are likely to be important only for events requiring response in very short time frames.

### 4.3.5 Fire Analysis

Fire event sequence analysis consists of four parts:

1. Development of fire ignition frequencies for each location in the facility or operations area. These are all called fire initiating event frequencies.
2. Development of the fire severity in terms of both temperature and durations. This was discussed in Section 4.3.2.
3. Development of the conditional probability of fire damaging a cask, canister, or waste package target. This was also discussed in Section 4.3.2.
4. Development of and quantification of fire event sequence diagrams and event trees. Development of the ESDs and event trees was discussed in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40). Quantification of fire event trees is conducted exactly like quantification of any other event tree and is described in Section 4.3, Section 4.3.1, and Section 4.3.7.

This section summarizes the method for the fire initiating event analysis performed as a part of the PCSA. The analysis was performed as part of an integrated analysis of internal fires in the subsurface facilities. This section only discusses those aspects of the fire analysis methodology that apply directly to the analysis for 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

The general boundary conditions used during this 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 of operation limits.
- 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 re-ignition 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 Subsurface Fire Frequency. The frequency of subsurface fires at YMP is expected to be similar to 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 over pressurization of a reduced strength canister.

#### 4.3.5.2 Analysis Method

Nuclear power plant fire risk assessment techniques have limited applicability to repository operations in the GROA. The general methodological basis of the PCSA fire analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76). Chemical agent disposal facilities are similar to those in the GROA in that these facilities are handling and disposal facilities for highly hazardous materials. This is a “data based” approach in that it utilizes actual historical experience on fire ignition and fire propagation to determine fire initiating event frequencies. That approach has been adapted to utilize data applicable to the YMP waste handling facilities. To the extent applicable to a non-reactor facility, *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. NUREG/CR-6850 Volumes 1 and 2 (Ref. 2.2.51) and (Ref. 2.2.52) are also considered in the development of this analysis method. The method complies with the applicable requirements of *Fire PRA Methodology* (Ref. 2.2.3) that are relevant to a non-reactor facility. The steps in the analysis are summarized below and described in detail in Attachment F, Section F4.

1. Identification of initiating events. Subsurface 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 Subsurface Operations are identified in the event sequence development analysis (Ref. 2.2.40). The steps of this process are detailed below:
  - A. Identify subsurface areas where waste containers can be present.

The processes for the movement of waste forms on site, while outside of buildings, are evaluated and the areas where the waste forms either sit or traverse are identified. Each area where waste can be present, even if only for a brief time, is listed

- 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 have been grouped into broader categories for use in this study.

- C. Define initiating events.

Fire ignition occurrences are identified for each outside area where a waste form can be present.

2. 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 (USCB), which conducts an economic census (Ref. 2.2.86). The second piece of data is tracked by NFPA. This approach uses historical data over a 10 year period (1988 to 1997) 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 on fires in or at industrial chemical, hazardous chemical, and plastic manufacturing plants (Ref. 2.2.1). These data are used to develop estimates for the total frequency of fires and the distribution of fires on the grounds of the facility:

- A. *Fires in or at Industrial Chemical, Hazardous Chemical, and Plastic Manufacturing Facilities: 1988 – 1997*. Unallocated Annual Averages and Narratives (Ref. 2.2.1).
- B. *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology* (Ref. 2.2.76).
- C. *1997 Economic Census: Summary Statistics for the United States 1997 NAICS Basis* (Ref. 2.2.86)

3. Determine initiating event frequency. The next step is to determine where these subsurface 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 North American Industry Classification System (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.

### **4.3.6 Event Sequence Quantification**

#### **4.3.6.1 Overview of Quantification**

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

1. The number of demands (sometimes called trials) or the time exposure interval of the operation or activity that gives rise to the event sequence. For example, this could be the total number of transfers of a cask in a facility preparation area.
2. The frequency of occurrence per demand or per time interval of the initiating event. For example, this could be the frequency of cask drop per transfer by a crane. Initiating event frequencies are developed either using fault trees or by direct application of industry-wide data, as explained in Section 4.3.2. Factors one and two are represented in the initiator event trees.
3. The conditional probability of each of the pivotal events of the event sequence, which appear in the associated system-response event tree. These probabilities are the results of a passive equipment failure analyses, fault tree analyses (e.g., HVAC), and direct probability input (e.g., moderator introduced), or judgment.

Calculated fault tree top event frequency or probability is 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 sequence, and there is 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." It is 32-bit software that runs under Microsoft Windows. Features of SAPHIRE that help an analyst build and quantify fault trees are as follows:

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

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

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

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

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

The fundamental viewpoint of the PCSA is probabilistic in order to develop information suitable for the risk informed nature of 10 CFR Part 63 (Ref. 2.3.2). Any particular event sequence may or may not occur during any operating time interval, and the quantities of the parameters of the models may not be precisely known. Characterizing uncertainties and propagating these uncertainties through the event tree/fault tree model is an essential element of the PCSA. The PCSA includes both aleatory and epistemic uncertainties. Aleatory uncertainty refers to the inherent variation of a physical process over many similar trials or occurrences. For example, development of a fragility curve to obtain the probability of canister breach after a drop would involve investigating the natural variability of tensile strength of stainless steel. Epistemic

uncertainty refers to our state of knowledge about an input parameter or model. Epistemic uncertainty is sometimes called reducible uncertainty because gathering more information can reduce the uncertainty. For example, the calculated uncertainty of a SSC failure rate developed from industry-wide data will be reduced when sufficient GROA specific operational information is included in a Bayesian analysis of the SSC failure rate.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Implementation of the regulatory definition of ITS has produced the following specific criteria in the PCSA to classify SSCs: A SSC is classified as ITS if it is relied upon to reduce the frequency of an event sequence 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 an SSC (such as permanent shielding) is used solely to reduce normal operating radiation exposure, it is classified as non-ITS.

#### 4.3.7.2 Development of Nuclear Safety Design Bases

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

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

The safety functions for this analysis were developed from the applicable Category 1 and Category 2 event sequences for the SSCs that were classified as ITS. In general, the controlling parameters and values were grouped in, but were not limited to, the following five categories:

1. Mean frequency of SSC failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of failure (e.g., failure to operate, failure to breach), with consideration of uncertainties, less than or equal to the stated criterion value.
2. Mean frequency of seismic event-induced failure. It shall be demonstrated by analysis that the ITS SSC will have a mean frequency of a seismic event-induced failure (e.g., tipover, breach) of less than 1E-04 over the preclosure period, considering the full spectrum of seismic events less severe than that associated with a frequency of 1E-07/yr.
3. High confidence of low mean frequency of failure. It shall be demonstrated by analysis that the ITS SSC will have a high confidence of low mean frequency of failure associated with seismic events of less than or equal to the criterion value. The high confidence of low mean frequency of failure value is a function of uncertainty, expressed as  $\beta_c$ , 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 assure availability, at intervals not to exceed the criterion value.
5. Mean unavailability over time period. It shall be demonstrated by analysis that the ITS SSCs (e.g., HVAC and emergency electrical power) will have a mean unavailability over a period of a specified number of days, with consideration of uncertainties, of less than the criterion value.

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

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

#### **4.3.7.3 Identification of Procedural Safety Controls**

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

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

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

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

#### **4.3.8 Event Sequence to Dose Relationship**

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

1. Event sequence designator—A unique designator is provided for each event sequence to permit cross-references between event sequence categorization and consequence and criticality analysis.
2. End state conditions—One of the following is provided for each event sequence:
  - A. DE-SHIELD-DEGRADE or DE-SHIELD-LOSS (Direct Exposure). Condition leading to potential exposure due to degradation of shielding provided by the TEV, cask or the aging overpack.
  - B. RR-FILTERED (Radionuclide Release, Filtered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister). However, the availability of the secondary confinement (structural and HVAC with HEPA filtration) provides mitigation of the consequences. This end state is not used for the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.
  - C. RR-UNFILTERED (Radionuclide Release, Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister), and a breach in the secondary confinement boundary (e.g., no HEPA filtration to provide mitigation of the consequences or breach of the structural confinement).
  - D. RR-FILTERED-ITC and RR-UNFILTERED-ITC (Radionuclide Release, Important to Criticality, Filtered or Unfiltered). Condition leading to a potential release of radionuclide due to loss of waste form primary containment (e.g., cask with uncanistered commercial SNF or canister) with or without HEPA filtration. In addition, the potential of exposing the unconfined waste form to moderator could result in conditions important to criticality. This characteristic of the end state is used by both the dose consequence analysts and the criticality analysts. The RR-FILTERED-ITC end state is not used for the IHF because the IHF HVAC system was not relied upon to prevent or mitigate an event sequence frequency or consequences.
  - E. ITC (Important to Criticality). This end state is not used for the IHF because all potential criticality initiators are associated with a radiological release (i.e., end state RR-UNFILTERED-ITC).
3. General description of the event sequence—This is a high level description that will be explained by the other conditions described above. For example, “Filtered radionuclide release resulting from a drop from the TEV that causes a breach of both sealed waste package and sealed canister.”
4. Material at risk— Identify and define the number of each waste form that contributes to the radioactivity or criticality hazard of the end state (e.g., number of TAD canisters, DPCs, uncanistered commercial SNF assemblies, etc., involved in the event sequence).

5. Expected number of occurrences— Provide the expected mean number of occurrences of the designated event sequences over the preclosure period and associated median and standard deviation.
6. The event sequence categorization— Provide the categorization of the designated event sequence and the basis for the categorization.
7. The bounding consequences. Provide the bounding consequence analysis cross-reference, as applicable, for each Category 1 or 2 event sequence to the bounding event number from the preclosure consequence analysis.

10 CFR 63.111 (Ref. 2.3.2) requires that the doses associated with Category 1 and Category 2 event sequences meet specific performance objectives. There are no performance objectives for Beyond Category 2 event sequences. Dose consequences associated with each Category 1 and Category 2 event sequence are evaluated in preclosure consequence analyses, by comparison, to pre-analyzed release conditions (or dose categories) that are intended to characterize or bound the actual event sequences (Ref. 2.2.36). As such, the results of the event sequence analysis and categorization serve as inputs to the consequence analysis for assignment to dose categories.

#### **4.3.9 Event Sequence to Criticality Relationship**

The requirements for compliance with preclosure safety regulations are defined in 10 CFR 63.112 (Ref. 2.3.2). Particularly germane to criticality considerations, is the requirement in 10 CFR 63.112, Paragraph (e) and Subparagraph (e) (6). Paragraph (e) requires an analysis to identify the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. This is a general requirement imposed on all event sequence analyses. Subparagraph (e) (6) specifically notes that the analyses should include consideration of “means to prevent and control criticality.” The PCSA criticality analyses (Ref. 2.2.38) employs specialized methods that are beyond the scope of the present calculation. However, the event sequence development analyses inform the PCSA criticality analyses by identifying the event sequences and end states that may have a potential for criticality. As noted in Section 4.3, some event sequence end states include the phrase “important to criticality.” This indicates that the end state implies the potential for criticality and that a criticality investigation is indicated.

To determine the criticality potential for each waste form and associated facility and handling operations, criticality sensitivity calculations are performed. These calculations evaluate the impact on system reactivity of variations in each of the parameters important to criticality during the preclosure period, that is, waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor ( $k_{eff}$ ) to variations in any of these parameters as a function of the other parameters. The criticality calculations demonstrate that one of the following is true for 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 a no in Table 4.3-1.

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

The criticality control parameters analysis, which comprises the background calculations that led to Table 4.3-1, is presented in detail in the *Preclosure Criticality Safety Analysis* (Ref. 2.2.38). 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

NOTES: <sup>a</sup> The *Preclosure Criticality Safety Analysis* (Ref. 2.2.38) considers bounding waste form characteristics. Therefore, there is no potential for a waste form misload.  
<sup>b</sup> The *Preclosure Criticality Safety Analysis* (Ref. 2.2.38) 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; SNF = spent nuclear fuel; WHF = Wet Handling Facility.

Source: *Preclosure Criticality Safety Analysis* (Ref. 2.2.38, Table 6)

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

#### 4.3.10.1 Boundary Conditions

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

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

Other boundary conditions used in the PCSA include:

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

#### 4.3.10.2 Use of Engineering Judgment

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

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

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

As described in Section 4.3.3, for example, active SSC reliability parameters will be developed using a Bayesian approach; and the use of judgment in expressing prior state-of-knowledge is a well-recognized and accepted practice (Ref. 2.2.59), (Ref. 2.2.4), (Ref. 2.2.9), and (Ref. 2.2.66).

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

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

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

### **When Empirical Information is Not Available**

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

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

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

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

In those cases where applicable, quantitative historical component reliability information is available, the PCSA followed 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, fires, and flooding analyses with judgment-based adjustments as appropriate for Subsurface Operations and GROA operating conditions.

### **Use of Qualitative Information When Reliability Information is Not Available**

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

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

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

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

## 5. LIST OF ATTACHMENTS

	<b>Number of Pages</b>
Attachment A Event Trees	22
Attachment B System/Pivotal Event Analysis – Fault Trees	243
Attachment C Active Component Reliability Data Analysis	51
Attachment D Passive Equipment Failure Analysis	91
Attachment E Human Reliability Analysis	63
Attachment F Fire Analysis	14
Attachment G Event Sequence Quantification Summary Tables	2
Attachment H EXCEL and SAPHIRE Model and Supporting Files	2 + CD

## 6. BODY OF ANALYSIS

The *Subsurface Operations Event Sequence Development Analysis*, which describes the Subsurface Operations and equipment (Ref. 2.2.40, Section 6.1.2, Attachment A, and Attachment B), should be consulted in conjunction with the present analysis.

### 6.0 INITIATING EVENT SCREENING

The NRC's interim staff guidance for its evaluation of the level of information and reliability estimation related to the Yucca Mountain repository, *Preclosure Safety Analysis – Level of Information and Reliability Estimation* (Ref. 2.2.73, p. 3), states that there are multiple approaches that DOE could use to estimate the reliability of SSCs that contribute to initiating events or event sequence propagation (i.e., pivotal events), including the use of judgment. By the definition provided in 10 CFR 63.102(f) (Ref. 2.3.2) 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 initiators that are either incapable of initiating an event sequence having radiological consequences or are too improbable to occur during the preclosure period. 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 other 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 more severe, or plausibility arguments based on the combinations of conditions that must be present to allow the initiating event to occur or the event sequence to propagate.

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

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

Manufacturing, loading, and transportation of casks and canisters are subject to regulations other than 10 CFR Part 63 (Ref. 2.3.2) (e.g., 10 CFR Part 50 (Ref. 2.3.1), 10 CFR Part 71 (Ref. 2.3.3), and 10 CFR Part 72 (Ref. 2.3.4)) and associated quality assurance programs. As a result of compliance with such regulations, the affected SSCs provide reasonable assurance that the health and safety of the public are protected. However, if a potential precursor condition could result in an airborne release that could exceed the performance objectives for Category 1 or Category 2 event sequences, or a criticality condition, then a qualitative argument that the boundary condition is reasonable is provided. A potential initiating event that is outside of the boundary conditions but has been found to require a qualitative discussion is the failure to properly dry a SNF canister prior to sealing it and shipping it to the repository.

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

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

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

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

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

The procedure described appears to ensure that very little water is left behind. However, the probability of undetected failure when performing the process is not addressed in the deterministic regulation 10 CFR Part 71 (Ref. 2.3.3) or in NUREG-1536 (Ref. 2.2.68). Indeed, there is no after-the-fact water or error detection method in NUREG-1536 or the regulation. Therefore, some unknown number of canisters may arrive in the GROA 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 will be accepting, handling, and emplacing TAD canisters in a manner consistent with the specifications laid out in the TAD canister system performance specification (Ref. 2.2.47) which prescribes the use of consensus codes and standards along with design requirement 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 the drop and breach of a naval canister are Beyond Category 2 as shown in Section 6.8. To receive a license to transport SNF, 10 CFR 71.55 (Ref. 2.3.3) requires the licensee to demonstrate subcriticality given that “the fissile material is in the most reactive credible configuration consistent with the damaged condition of the package and the chemical and physical form of the contents” under the hypothetical accident conditions specified in 10 CFR 71.73 (Ref. 2.3.3). Drop events, which are unlikely to breach the canister, are also unlikely to impart sufficient energy to the fuel to reconfigure it so dramatically that criticality would be possible even if water is present. It is concluded that existing regulations that apply to the canister and transportation cask for transportation to the repository provide reasonable assurance that a criticality event sequence that depends on the presence of residual water inside the canister and reconfiguration of the fuel would not occur under conditions that could reasonably be achieved during handling at the repository.
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 or explosion event could occur. However, precautions taken at the generator sites are expected to make receipt of a canister that was improperly dried unlikely. In addition, an ignition source would be required for an explosion or deflagration to occur. High electrical conductivity of the metal canister would dissipate any high voltage electrical discharge (which is unlikely in any case) and preclude arcing within the canister. Normal handling operations do not subject the canisters to energetic impacts that could cause frictional sparking inside the canister. Therefore, an unlikely event during handling, such as a canister drop would have to occur to ignite the gas. Considering the combination of unlikely events that must occur, event sequences involving this

combination of failures are screened out from further consideration on the judgment that they contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.

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 off-site.

## 6.0.2 Screening of External Initiating Events

### 6.0.2.1 Initial Screening of External Initiating Events

The *External Events Hazards Screening Analysis* (Ref. 2.2.34) identifies potential external initiating events at the repository for the preclosure period and screens a number of them from further evaluation based on severity or frequency considerations. The four questions that constitute the evaluation criteria for external events screening are:

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

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

As noted in Table 6.0-1, the potential external initiating event categories that are retained for further evaluation are seismic activity and loss of power. Seismically induced event sequences are developed, categorized, and documented in a separate analysis (Ref. 2.4.4). Loss of offsite power (LOSP) is treated together with internal causes of power loss in Section 6.0.2.2.

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

External Event Category	Retention Decision. If Not Retained, Basis for Screening.
Seismic activity	YES. Retained for further analysis.
Non-seismic 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. Section 6.0.2.2 contains a screening analysis of loss of electrical power as an initiating event.
Loss of cooling capability event	NO. The primary requirements for cooling water at the Yucca Mountain site during the preclosure period are makeup water for the Wet Handling Facility (WHF) pool and cooling of HVAC chilled water. The chance of a loss of cooling capability occurring at the repository over the preclosure period is less than 1/10,000.
Aircraft crash	NO. The chance of an accidental aircraft crash occurring at the repository over the preclosure period is less than 1/10,000.
Nearby industrial/military facility accidents	NO. The chance of an industrial or military facility accident occurring at the repository over the preclosure period is less than 1/10,000.
Onsite hazardous materials release	NO. The chance of an accident event sequence initiated by the release of onsite hazardous materials at the repository over the preclosure period is less than 1/10,000.
External fires	NO. The chance of an external fire severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Extraterrestrial activity	NO. Extraterrestrial activity is defined as an external event involving objects outside the earth's atmosphere and enters the earth's atmosphere, survive the entry through the earth's atmosphere and strike the surface of the earth. Extraterrestrial activity include: meteorites, asteroids, comets, and satellites. The chance of an occurrence at the repository over the preclosure period is less than 1/10,000.

NOTE: The source document defines the external event categories.

HVAC = heating, ventilation, and air conditioning; WHF = Wet Handling Facility.

Source: Adapted from *External Events Hazards Screening Analysis External Events Screening Analysis* (Ref. 2.2.34, Sections 6 and 7).

### 6.0.2.2 Screening Analysis of Loss of Electrical Power

Loss of electrical power, whether caused by onsite or offsite failures, is expected to occur during the preclosure period. Loss of electrical power causes all equipment in the drift and the TEV to stop operating. The TEV is designed to hold the waste package in place upon loss of power indefinitely. Loss of offsite power is not explicitly shown as an initiating event in the event trees because, by itself, it does not cause mechanical handling equipment to malfunction in a way that causes a drop or other mechanical impact of the waste package.

Loss of offsite power could lead to the TEV stranded under the sun for a period of time that may lead to TEV shielding degradation due to the potential melting of the TEV neutron polymer shielding layer. The loss of offsite power (LOSP) frequency is estimated at 3.6E-02/yr (Ref. 2.2.48, Table 3-8), with a failure to recover power within 24 hours of 1.8E-02 (Ref. 2.2.48, Table 4-1). Thus, during the 50 years of preclosure operations, the expected number of LOSP events (LOSP) is 3.2E-02; the initiating frequency of a loss of offsite power lasting more than 24 hours would be:

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

Conservatively, the probability of the TEV shielding degradation under this scenario is assigned to be 1. This would lead to a worker exposure to neutron radiation with frequency of 3.2E-02/ preclosure period which is a Category 2 event sequence. Category 2 event sequences are not analyzed for on-site worker exposure per 10 CFR 63.111 (Ref. 2.3.2).

### 6.0.3 Screening of Internal Initiating Events

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

Potential initiating events were qualitatively identified in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) for quantitative treatment in the present analysis. For completeness, some events were identified in the event sequence development analysis that are extremely unlikely and can reasonably be qualitatively screened out from further consideration. Table 6.0-2 provides bases for the screening decisions for certain internal initiating events. Section 6.0.4 provides a detailed screening argument for internal flooding, which is too long to be included in Table 6.0-2. The screened out initiating events are assigned frequencies of zero in the quantification of the model.

Table 6.0-2. Bases for Screening Internal Initiating Events

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
SSO-ESD-04-SEQ-2-2	Inadvertent entry into a drift	YMP will establish a program to control access to the drift and provide appropriate training to the operators. This access control program includes the portal security building with controlled and locked access doors to the drifts. Inadvertent entry into the drifts is qualitatively screened to be beyond Category 2. Therefore, a worker dose assessment is not needed to comply with 10CFR 6.3111(Ref. 2.3.2). No further work is done on this initiating event. This drift access control program is described in Table 6.9-2.
SSO-ESD-04-SEQ-3-2	Prolonged worker proximity to TEV	YMP will establish a program to control proximity to the TEV and provide appropriate training to the operators. This proximity control program includes establishing controlled access to areas along the TEV travel routes, and an early warning system for TEV arrival to prevent inadvertent exposure to workers due to prolonged proximity to the TEV. Inadvertent lengthy close proximity to the TEV is qualitatively screened to be beyond Category 2. Therefore, a worker dose assessment is not needed to comply with 10CFR 6.3111(Ref. 2.3.2). No further work is done on this initiating event. This proximity control program is described in Table 6.9-2.
No applicable event trees	Loss of ventilation to the drift	According to <i>Waste Package Misplacement Probability</i> (Ref. 2.2.41), prolonged loss of ventilation to the drift (30 days) may lead to elevated temperature conditions of the waste package but such conditions are hundreds of degrees lower than needed for waste package breach (See Attachment D). Moreover, (Ref. 2.2.41) concludes that the probability of misplaced waste packages causing temperature elevation is Beyond Category 2.
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened out from further analysis. A detailed screening argument is in Section 6.0.4.
SSO-ESD-03-SEQ-2-3	TEV runaway	TEV runaway event could occur when it is on an incline and all eight motor gear boxes (one for each wheel) are stripped and the TEV free-wheels down the incline. The damage to the WP caused by a TEV runaway would be very high, such that the failure probability of the WP is conservatively considered as 1. Based on the TEV runaway fault tree model (Section 6.2 and Attachment B), the event probability is dominated by the common-cause failure of 8 of 8 motor gear boxes, which is estimated at $1.42E-09$ ( $7.86E-8/hr * 2 \text{ hr mission time} * 0.00906$ alpha factor for 8 of 8 configuration). Given a total number of TEV/WP trips during the preclosure period as 12,268, the TEV runaway initiating event frequency is estimated at $(1.42E-9/trip * 12,268 \text{ trips}) = 1.7E-5$ during the preclosure period. The event sequence is Beyond Category 2, and thus, is screened out from further analysis.

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

TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

#### 6.0.4 Screening of Internal Flooding as an Initiating Event

By the definition of an event sequence, a flood inside a facility would be an initiating event if it leads to a sequence of events that would either breach waste containers, causing a release, or leads to an elevated radiological exposure without a release (i.e., direct exposure of personnel). Internal floods, whether caused by random failures or earthquakes, emerge from two sources. The first is inadvertent actuation of the fire-suppression system. The second is failure of water-carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems.

Transportation casks, canisters, and waste packages are not physically susceptible to breach associated with water in the short-term. With extremely long exposure to water, corrosion may be a factor but intervention to drain water from the buildings would prevent such exposure. Short-term breaches do not occur owing to exposure to water. Canisters are surrounded by transportation casks, and waste packages. Transportation casks are elevated as all times at least five feet above the floor by railcar, truck, or canister transfer trolley. Waste packages are similarly elevated on the waste package transfer trolley. Inside the TEV, the waste package is elevated approximately 1 foot above the floor. A lifted canister or/and cask is higher than these minimum elevations. Therefore, water from fire suppression and other water systems is unlikely to attain a depth that would contact transportation casks, waste packages, or canisters. Of greater significance, however, is that the fuel is contained in canisters within a sealed waste package during subsurface operations all the time and these containers do not fail from short-term exposure to flood water. In this context, short-term is a time period that is at least 30 days but less than the length of time in which significant corrosion may occur.

Event sequences initiated by internal floods are considered to be Beyond Category 2. Moderator intrusion into canisters resulting from event sequences that might breach a waste container are treated quantitatively as described in the pivotal event descriptions of Section 6.2.

The construction schedule for the subsurface facilities requires the excavation of drifts at the same time that waste packages are being placed into completed portions of the drifts (Ref. 2.2.17). A potential flooding scenario of concern during subsurface excavation of Panels 1 and 2 involves the failure of the water supply piping to the Tunnel Boring Machine (TBM) and a consequent buildup of water against the construction barrier that separates the completed portion of a drift. This could occur because the 25 ft access main drift for Panels 1 and 2 slopes downward 1.35 degrees towards the completed drifts (on the other side of the construction barrier) (Ref. 2.2.27); these will be filled with waste packages while drift excavation is proceeding.

The construction barrier consists of two circular barriers, separated by approximately 30 ft that control ventilation flow and prevent construction debris from entering the completed drifts. The barriers are equipped with an access door and are designed for maximum ventilation system differential pressure. They are sealed to the tunnel wall with Shotcrete that is a minimum of 8 in. thick and extends 2 ft away from each barrier in both directions (Ref. 2.2.14). If the construction barrier were to fail or leak during a flood on the construction side, water could potentially enter the filled drifts, because Shotcrete is not watertight in the long term.

Water is provided to the TBM for dust control purposes; water is sprayed on the belt that removes the cut rock (muck), on drilling rigs, etc. Some water will be taken out in the muck and the rest will collect in the tunnel, where it usually seeps into the ground or is evaporated through the ventilation system. There is also a discharge system that can be used to remove water.

The liquid systems design includes one supply pipe with a diameter between six and eight inches, depending on its position in the tunnel. It is hung from the tunnel side three to four ft above the invert and is therefore not as vulnerable to damage as in many underground tunnels where pipe is run on the ground. Pipe sections are put together with couplings and have block valves located every 200 to 260 ft. The supply pipe also serves a fire protection function. Three 10,000 gallon water tanks are located on the surface, as are the supply pumps. In the event of a flood, portal security personnel can isolate flow to the tunnel (underground communications are provided during construction operations).

As a part of this effort, existing databases (including publicly available databases associated with the mining industry) were searched and no information was obtained concerning the frequency of water pipe breaks in construction tunnels; however, anecdotal information indicates that such breaks are unusual. If a pipe were to break during construction of Panels 1 or 2, water would begin to accumulate at the construction barrier (near the TBM). An approximately 18 in. step will exist between the construction tunnel floor and the completed invert upon which the construction barrier stands. If a break could be isolated before the top of the invert is reached, no potential will exist for water to migrate into the completed drift. Eighteen inches of water is substantial and would be noticed by the construction crew. Prior to this point it is expected that a request to isolate water flow would be transmitted to portal security. In addition, the discharge pump would be started to pump water out of the tunnel.

If the water height were to exceed 18 in, water would begin to rise against the construction barrier. At this point the barrier may deform or the Shotcrete seal begin to leak, allowing water to flow down the completed access drift on the emplacement side of the barrier. Even if this were the case, water would not reach the filled drifts because each is located 4 ft, 10 in. above the access main. An additional 4.5 in. of height is provided by the emplacement pallet, resulting in a waste package height over 5 ft above the access main (Ref. 2.2.29) and (Ref. 2.2.19). In addition, emplaced waste packages are protected by emplacement drift doors that would prevent any water splash from contacting the waste packages.

The maximum expected water height against the construction barrier and invert lip is 5 ft, based on the drainage of the three 10,000 gallon tanks plus water in the supply line (about 46,000 gallons total). Of this, water to a height of 3.5 ft could be against the construction barrier and available for leakage to the emplacement side of the barrier. Because of the 1.5 ft separation between the maximum water height and the waste packages and the provision of barriers at the front of each emplacement drift, water from a flood on the construction side will not contact the waste packages. If a very unusual set of circumstances resulted in water contact, a waste package could be removed for inspection. Based on this, subsurface flooding was not addressed further.

The water height was estimated by considering the access drift to be a circular cylinder skewed from “right” by 1.35 degrees, the downward slope of the drift. For a flood height  $h$  at the construction barrier, the flood height at distance  $d$  along the drift floor from the barrier is  $h - d \times$

$\sin(1.35^\circ)$  (by simple trigonometry). Using this height and the drift radius  $r$  (12.5 ft), the area of a segment at distance  $d$  is  $\frac{1}{2} \times r^2 \times (\theta - \sin \theta)$ , where  $\theta$  (in radians) =  $2 \cos^{-1} \{ [r - (h - d \sin(1.35^\circ))] / r \}$ . The total flooded volume can be estimated by iteration using Excel. For example, using a flood height against the construction barrier and 18-in step of 5 ft and a distance increment of 3 ft, the following flood volumes are calculated:

Table 6.0-3. Flood Height Estimation

Distance d (ft)	Flood Height (ft)	$\theta/2$ (radians)	Segment Area (ft <sup>2</sup> )	Segment Volume (ft <sup>3</sup> )
0	5.00	1.85	69.9	209
3	4.93	1.84	68.5	205
6	4.86	1.83	67.1	201
*		.		
*		.		
*		.		
207	0.12	0.281	0.288	0.862
210	0.05	0.183	0.080	0.240

NOTE: Table entries from 9 ft to 204 ft are removed for clarity.

Source: Excel Spreadsheet *tunnel flooding calcs.xls* located in Attachment H.

The total volume is 6180 ft<sup>3</sup>, or about 46,200 gallons. For a 5-ft flood height, the flooded volume is about 79,700 gals, approximately 70% more than the capacity of existing site tanks and piping. Based on this, subsurface flooding into the drifts is not considered credible and was not addressed further.

## 6.1 EVENT TREE ANALYSIS

The event trees that are quantified in this analysis were developed from ESDs in *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40). This section describes the modeling of event sequences. The event trees are discussed and presented in Attachment A.

### 6.1.1 Event Tree Analysis Methods

#### 6.1.1.1 Linked Event Trees and Fault Trees

As described in Section 4, the PCSA uses event trees with fault trees to calculate the frequency of occurrence of event sequences. The event tree quantification is supported by fault tree analysis (FTA) (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), and PEFA (Section 6.3 and Attachment D). The SAPHIRE computer program (Section 4.2) is used for the fault tree quantification process. The YMP preclosure handling is performed using four kinds of buildings as summarized below:

1. The Receipt Facility (RF) accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.
2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program (NNPP) for placement in waste packages destined for

emplacement in the repository emplacement drifts. Three CRCFs are currently considered.

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 canisters from the NNPP and some canisters containing high-level radioactive waste for placement in waste packages destined for emplacement in the repository emplacement drifts.

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

Event sequences are developed for each of the four building types, TEV and Subsurface Operations, and Intra-site Operations. As described in the *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40), event sequences are developed separately for each major group of waste handling processes, by location, from the facilities where the waste packages are picked up by the TEVs, to the emplacement drifts. Therefore, event sequences also distinguish among the various steps in waste handling.

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

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

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 the Subsurface Operations is less complex than those of the surface processing facilities, event sequences are not completely handled by 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 models.
- Initiating event frequencies derived from waste-form throughputs and numbers of opportunities for initiating an event sequence. In some cases, initiating events are

modeled as fault trees, and in those instances, SAPHIRE is used to quantify the initiating event frequencies, 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, whose resultant probability distributions are also calculated in Excel spreadsheet. SAPHIRE accounts for the correlation between analogous basic events sharing the same reliability information, which ensures the spread of the probability distribution of the event sequences in which these basic events intervene is not underestimated.

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

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

1. **Self-contained event trees.** Self-contained event trees are used when only one initiating event appears in the corresponding ESD (Ref. 2.2.40, Attachment F). An example is SSO-ESD-04, which is shown in Figure A5-5 in Attachment A. The feed on the left side of the event tree is an event that represents the frequency of the 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 waste packages that are handled over the preclosure period. The initiating events are 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 and no branching occurs in the event tree. Each pathway through a self-contained event tree terminates in an end state. End states that are labeled "OK" mean that the sequence of events does not result in one of the specifically identified undesired outcomes. "OK" may mean that normal operation can continue.
2. **Separate initiator and system-response event trees.** Separate event trees for initiating events and the system response are used when more than one initiating event appears in the corresponding ESD (Ref. 2.2.40, Attachment F). The initiator event tree decomposes a group of initiating events into the specific failure events that comprise the group. For example, an initiator event tree, SSO-ESD-01, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, RESPONSE-FACILITY, is shown in Figure A5-7. The feed to the left side of the initiator event tree is an event that represents the frequency of challenge to the

successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of waste packages that are handled over the preclosure period. Unlike the self-contained event tree that has only one defined initiating event, initiator event trees do not end at end states but transfer to a system response event tree. The models to be used for the initiating events associated with each initiator event tree are specified in SAPHIRE “basic rules,” which are attached to the initiator event tree. Each initiator event trees contain multiple initiating events. As an example, there are five initiating events for SSO-ESD01 (Attachment A, Table A4.1-2). Each of these initiating events leads through a series of challenges of the pivotal events to arrive at corresponding end states. Since each of these initiating events leads to the same set of challenges to the pivotal events, a common response event tree is constructed to model these challenges. In this example, the system response event tree is RESPONSE-FACILITY. The models to be used for the initiating events associated with each initiator event tree are specified in Excel event tree models.

System response event trees contain only pivotal events. The Excel event tree models uses results from specific SAPHIRE fault tree model or a basic event as input for a pivotal event. Because the conditional probability of each pivotal event may be specific to the initiating event for each event sequence, the same system response event tree is quantified by Excel as many times as there are initiating events in the initiator event tree. The models to be used for the pivotal events associated with each initiating event and system response event tree are specified in the Excel model associated with a given initiator event tree.

### **6.1.1.3 Summary of the Major Pivotal Events**

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

Each of the specific failure events included in a self-contained or system-response event tree may be linked to a basic event or to the top event of a fault tree. The fault tree models are, in turn, linked to basic event reliability information separately entered into SAPHIRE. Some of the pivotal events do not have associated fault trees because they are linked directly to probabilities from the reliability database. Sections 6.2 and 6.3 provide more information about the reliability information developed for this analysis.

### **6.1.2 Waste Form Throughputs**

Each initiator event tree and self-contained event tree begins with the container throughputs, that is, the numbers of waste packages to be handled over the period of Subsurface Operations. There are 12,068 waste packages to be emplaced during subsurface operations (Ref. 2.2.31). This number is drawn into the descriptions of specific event trees as needed. With the number of waste packages as a multiplier in the event tree and the initiating events specified as a probability per waste package, the value passed to the system response is the number of occurrences of the initiating event expected over the period of Subsurface Operations.

### 6.1.3 Guide to Event Trees

Event trees are located in Attachment A. Table 6.1-2 contains the crosswalk from the ESD (Ref. 2.2.40, Attachment F) to the initiating event tree and response tree figure location in Attachment A.

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

ESD Number	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
SSO-ESD-01	Event sequences for TEV activities inside facility WP load-out area	SSO-ESD-01	Figure A5-2	RESPONSE-FACILITY	Figure A5-7
SSO-ESD-02	Event sequences for TEV activities during transit	SSO-ESD-02	Figure A5-3	RESPONSE-TRANSIT	Figure A5-8
SSO-ESD-03	Event sequences for TEV activities within the emplacement drift	SSO-ESD-03	Figure A5-4	RESPONSE-DRIFT	Figure A5-9
SSO-ESD-04	Event sequences for loss or lack of shielding	SSO-ESD-04	Figure A5-5	No Response tree	N/A
SSO-ESD-05	Event sequences for internal fires	SSO-ESD-05	Figure A5-6	RESPONSE-TRANSIT	Figure A5-8

NOTE: IE = initiating event; TEV = transport and emplacement vehicle; WP = waste package.

Source: Attachment A, Table A5-1

## 6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS

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

Section 4.3.2 provides a brief introduction to the application of fault tree analysis (FTA) for initiating and pivotal events, including an example fault tree. Many of the initiating events involve faults in complex machinery for which no historical data exists at the system level, an exception being historical data on the derailment of railed vehicles. 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.

A top event of a system fault tree 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 subsurface operations.

Attachment B, Section B1 through B6 presents the fault trees for the subsurface analysis, including CRCF HVAC, and CRCF AC power. HVAC and AC power fault trees are included in

the subsurface analysis because the study includes TEV movement from the CRCF and IHF. This section describes the bases for the fault trees and the quantification of their top events.

Attachment B, Section B7 presents the linking fault trees. The linking fault trees are self explanatory. They serve as a way of linking system fault trees or fault trees with basic events to correctly model the initiating events. No quantification is performed for the linking trees alone.

Each of the top events for the initiating event fault trees represent the conditional probability that the top event will occur when the system is put into service. That is, the results of the FTA answer a question such as “what is the probability given a waste package transit to the North Portal that the TEV will collide into a SSC?” The expected number of collision initiating events during the preclosure period is the product of the number of waste packages emplaced during the preclosure period and the conditional probability of the top event. The conditional probability is generated by the SAPHIRE fault tree and the number of waste packages is obtained from the throughput values. Both pieces of data are inputted into the Excel event tree model and subsequently processed as part of the solution of the complete event sequence that includes pivotal events.

By contrast, the top event for the confinement function of the HVAC represents the conditional probability that the confinement feature is not achieved for the required duration following an airborne release of radioactive material inside the CRCF. The quantification of the top event, as summarized in Section 6.2.2.2 and detailed in Attachment B, Section B2, is expressed as unavailability. The results provide insight into the reliability of the HVAC and its contribution to event sequence quantification. Again, the quantified top event is not used directly in the event sequence quantification. Instead, the fault tree for the HVAC is solved and inputted into the Excel event tree model.

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 functions are to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (electrical, mechanical, etc.) and failures from the loss of a supporting system (e.g., loss of power).

For quantification of the probability of the top event, failure probabilities are developed for each basic event (hardware or HFE) and are used to compute the probability of each 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 conservative mission time is used. Where mission time is critical, appropriate times are justified and incorporated into the event sequence quantification. Hardware failure probabilities are taken from the reliability analysis data discussed in Sections 6.3. HFE probabilities are taken from the HFE analysis discussed in Section 6.4.

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

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

- Basic event data
- Common-cause and common mode failures such as failures induced by common training, maintenance practices, fabrication, common electrical supplies, etc.
- Support systems and subsystems such as HVAC and electrical
- 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 as applicable:

- 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 Transport and Emplacement Vehicle Fault Tree Analysis**

The FTA is detailed in Attachment B, Section B1. The quantification of each fault tree top event represents an estimate of the conditional probability of TEV failures given an operation. The initiating event frequency of TEV related event sequences is dependent on the number of challenges to the TEV safety functions, which is calculated from the number of WP loadout and emplacement operations conducted over the preclosure period. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B1 for sources of information on the physical and operational characteristics of the TEV.

#### **6.2.2.1.1 Physical Description**

The TEV is a shielded, remotely-operated vehicle that transports a waste package and emplacement pallet from either the CRCF or the IHF to the subsurface. The TEV, illustrated in Figure B2-1, is a rail-based vehicle that interfaces with a WPTT to receive a waste package in the loadout area of the CRCF and IHF and then travels directly into the emplacement drift to emplace the waste package. The TEV is powered by a third rail and contains programmable logic

controllers (PLCs) for localized control of the device. The TEV carries a battery for backup power to temporarily maintain power to the control units in the event that third rail power is lost.

The TEV has eight wheels, each driven by an electric motor, and disc brakes integral to each motor. The wheels travel on 171 lb crane rail with a gauge of 3.35 m (11 ft), installed in accordance with the requirements of ASME NOG-1 2004, 2005 (Ref. 2.2.8). The wheels on one side of the vehicle are double-flanged to resist derailment. The unloaded TEV weighs approximately 180 tons and has nominal height, width, and length of 11.2 ft × 15.4 ft × 29.7 ft, respectively.

In most cases, operation of the TEV is under PLC control with only general oversight from a central control, but manual control is performed as needed. The instrumentation of the TEV is described in associated process and instrumentation diagrams contained in *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (Ref. 2.2.24).

The following describe the major subsystems of the TEV:

- **TEV Control Compartment** –Electronic controls of the TEV are housed in a compartment at the rear and outside of the TEV shielded enclosure. Sub-enclosures separate and totally enclose duplicate equipment to provide protection against potential fire and internal explosions. The compartment contains a heating, ventilation, and air-conditioning (HVAC) unit to maintain the operating environment and fire-detection and fire suppression systems.
- **TEV Shielding** –The TEV provides neutron and gamma ray shielding for a waste package during the export from a CRCF or IHF to an emplacement drift. The shield enclosure is not airtight but prevents direct radiation streaming and provides an external, shielded dose rate not to exceed 100 mrem/hr at 30 cm (11.81 in). The neutron shielding material is the only non-metallic component but is a fire-resistant synthetic polymer material.
- **TEV Lift System** –The TEV engages the waste package by raising the entire shielded enclosure using six screw jacks. The front and rear jacks are used in normal operations and two central jacks provide backup. These jacks have the ability to self-lock in the event of drive failure.
- **TEV Base Plate** –A moveable radiation shield, termed the base plate, forms the bottom of the TEV shielding enclosure during transit operation. The base plate is retracted for waste package loading and emplacement operations. The base plate is extended and retracted from below the TEV by a motor driving a rack and pinion drive system. The bed plate is mechanically interlocked with the TEV front shield doors to prevent extension of the bed plate if the shield doors are closed. The bed plate can not be retracted when the enclosure has been lowered.
- **TEV Shield Doors** –The TEV has two hinged shield doors at the front of the TEV for loading and emplacement of waste packages. Door movement is provided by electromechanical linear actuators. The door hinge system consists of four structures

mounted to the chassis of the TEV. Each hinge structure houses radial and thrust bearings that allow easy and precise movement of the heavy doors, which have the same shielding composition as the shielded enclosure. A mechanical interlock prevents the shielded enclosure from being lowered until the front shield doors are fully opened. To prevent the inadvertent opening of the shield doors during transit, the TEV incorporates an electro-mechanical interlock that prevents actuation of the doors unless the TEV is near to the WP loadout area or an emplacement drift

- **TEV Linear Drive Gear Motors** –Each of the TEV's eight wheels is driven by a 20 hp (15kW) AC, 460 volt, 1750 rpm motor featuring integral disc brakes.

#### 6.2.2.1.2 Operations

The TEV operations involving waste packages comprises three phases termed Loadout; Transit, and Emplacement. These operational phases are addressed in the PCSA. Other TEV operations, when no waste package is on board, are not addressed in the PCSA.

All operations are performed remotely and are discussed in greater detail in Attachment B. The following paragraphs provide an overview of each of the operational phases.

**Loadout** consists of loading the waste package into the TEV and moving out of the facility. The TEV is controlled by an on-board PLC system and monitored from the Central Control Center Facility. The TEV receives waste packages from four facilities: the IHF, and CRCF1, 2 and 3. The loadout configuration and operations are the same for all facilities.

Prior to bringing a waste package into the loadout, the TEV enters the facility and moves forward to position the vehicle directly over the loadout station. The facility's exterior shield doors are closed and the TEV is positioned so that its lifting features can engage the waste package pallet after the pallet and waste package are correctly positioned.

After receiving confirmation on positioning from control, the TEV's front shield door safety interlocks are disengaged; and the front shield doors are opened. The TEV raises its rear shield door and extends the base-plate from under the shielded enclosure. The lifting system (screw jacks) is used to position the shield enclosure to the proper collection height for the waste package and emplacement pallet.

A WPTT brings a closed waste package to the waste package loadout area and places it horizontally on the loading dock. A screw-driven traveling table moves the waste package and pallet under the TEV shield. The TEV shield enclosure is raised to its full travel height, engaging and raising the waste package and pallet into the TEV. The base-plate is retracted under the shield enclosure, the rear shield door is lowered and the TEV shield enclosure front doors are closed, thus engaging all safety interlocks.

The facility exterior shield doors are opened, and the TEV exits the waste handling facility. As the TEV exits, a mechanical interlock is activated to prevent a spurious signal from inadvertently opening the shield doors during transit.

**Transit** comprises the processes for moving the waste package from the surface facility to the entrance of an emplacement drift. The TEV operating speed is approximately 2.7 km/hr (1.7 mph or 150 ft/min). TEV operations are defined within rail segments designated by control points within the software of the PLC system. The TEV stops upon reaching a control point and proceeds to the next segment only upon receiving a confirmation from central control. Upon a loss of power, the TEV is designed to stop, retain its load, and enter a locked mode where it remains until operator action is taken. Visual and auditory monitoring is performed by central control for all transit operations and the central control operator has override control to stop the TEV in case of an emergency.

The TEV moves along the surface track from the waste handling facility through several switches to reach the North Portal. At the North Portal entrance, the TEV stops for diagnostic checks and system tests and then proceeds down the North Ramp to reach the repository level. The TEV proceeds on the subsurface rail along the appropriate access main(s) until the TEV reaches the rail switch in front of the emplacement access door of the selected emplacement drift and stops.

**Emplacement** comprises the processes of moving the waste package into an emplacement drift, placing the waste package and pallet on the invert and moving the empty TEV out of the drift. After the TEV stops at the emplacement access door, various positional sensors and devices on board establish a positional datum point. The emplacement access door panels are opened just long enough to admit the TEV into the drift. An electro-mechanical switch de-activates the interlock so that the TEV shield doors may be opened. The TEV passes into a curved tunnel segment (with a positive grade of approximately 1.75%) and then into a straight section to enter the emplacement drift proper, which has a nominal grade of 0 %, where it stops and confirms its location. The front shield doors are opened, the rear shield door is raised, and the base-plate is retracted. The lifting system raises the shielded enclosure to engage the pallet and moves forward at a crawl speed, on the order of 4.6 m/min (15 ft/min), stopping at a position close to a previously emplaced waste package.

At this stage, additional on-board positional sensors and devices (e.g., lights, cameras, and ultrasonic sensors) are activated, and measurements are made to re-confirm to the position of the TEV and the waste package. The TEV then moves forward at a slow positioning speed (at approximately 0.46 m/min [1.5 ft/min]), until the required final position is achieved. The shield enclosure is lowered to place the waste package and pallet on the emplacement drift invert. The TEV is backed away at the positioning speed from the emplaced waste package and pallet to a predetermined distance where the shield doors and base plate are closed prior to the TEV exiting the drift and returning to the surface.

### 6.2.2.1.3 Control System

All operations are performed remotely and discussed in greater detail in Attachment B. The control system includes the following features:

- Automated control using PLCs with oversight via audio and video signals from a central control station, in most cases

- Manual control when required via override from central control
- Shield door safety interlocks to prevent spurious opening during waste package transport
- Automatic operational sequences to load a waste package and pallet in a facility loadout area
- Automatic operational sequences to unload a waste package and pallet in an emplacement
- Automatic stop at each rail segment to await a permissive signal to proceed from central control
- Fail-safe on loss of power: TEV stops, retains its load, and enters a locked mode until operator action is taken
- Sensors and logic to confirm the position of the TEV when emplacing a waste package near a previously emplaced waste package.
- Programmed variable travel speeds (e.g., normal speed of 1.7 mph (150 ft/min) on surface tracks and access drifts, crawl speed of 15 ft/min for initial positioning in an emplacement drift, and a final waste package positioning speed of 1.5ft/min.

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

Success criteria for the TEV are the following:

- Prevent impact on a waste package due to spurious movement of TEV or front shield doors
- Prevent collisions of the TEV within the facility
- Prevent collisions of the TEV with objects during transit or when entering an emplacement drift by preventing spurious operations of the TEV and drift access doors
- Prevent spurious opening of front shield doors
- Prevent dropping of a waste package due to spurious operations or structural failure of the TEV
- Prevent dropping or dragging of a waste package in an emplacement drift due to spurious operations or structural failure of the TEV
- TEV structure can sustain impacts without damage to the waste package
- TEV shielding can sustain its shielding function over a prolonged period without operational support.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion is basis for defining the top event of one or more fault trees for the TEV.

#### 6.2.2.1.5 Mission Time

Generally, a mission time of 4 hours is used for the fault tree quantification for TEV failure scenarios. Four hours is a conservative bound for operations involving waste package loading in the facility or emplacing in a drift. For some basic events that involve time-base failure rates, however, the following mission times are used:

- 5.7E-3 hr for fault exposure times during transit between facility doors,
- 1 hr for spurious operation of TEV motors while WP is being placed in the emplacement
- 8 hr for transit from the surface facility to the emplacement drift for potential exposure times for stopped TEV

#### 6.2.2.1.6 Fault Tree Results

The application of the TEV fault trees to ESDs for the Subsurface is documented in Attachment B, Section B1, including the application of basic event data, common-cause failures, and human reliability analysis.

There are 11 separate failure scenarios represented by fault trees associated with the TEV:

1. TEV door impacts a waste package.
2. TEV collision within facility.
3. TEV collides with object during transit.
4. Impact to TEV during transit.
5. TEV stops for extended time.
6. Inadvertent TEV door opening during transit.
7. Waste package drop in facility.
8. Waste package dropped during transit.
9. Waste package drop or dragging in an emplacement drift.
10. TEV collides with emplaced waste package.

The results of the analysis are summarized in Table 6.2.-1.

Table 6.2-1 Summary of Top Event Quantification for the TEV

Top Event	Mean Probability	Standard Deviation
TEV door impacts a waste package	1.2E-5	1.3E-5
TEV collision within facility	1.0E-3	1.2E-3
TEV collides with object during emplacement	3.0E-3	3.8E-3
Impact to TEV during transit	2.9E-4	7.4E-4
TEV stops for extended time	6.9E-4	6.1E-5

Table 6.2-1 Summary of Top Event Quantification for the TEV (Continued)

Top Event	Mean Probability	Standard Deviation
Inadvertent TEV door opening during transit	1.2E-7	1.2E-6
Waste package drop in facility	5.4E-11	1.6E-11
Waste package dropped during transit	7.5E-8	1.1E-8
Waste package drop or dragging in an emplacement drift	9.1E-7	1.1E-6
TEV collides with emplaced waste package	9.9E-4	1.2E-3

NOTE: TEV = Transport emplacement vehicle.

Source: Attachment B, Figure B1.4-1, Figure B1.4-3, Figure B1.4-5, Figure B1.4-7, Figure B1.4-9, Figure B1.4-11, Figure B1.4-13, Figure B1.4-15, Figure B1.4-17 and Figure B1.4-19.

### 6.2.2.2 HVAC Fault Tree Analysis

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

#### 6.2.2.2.1 HVAC Description and Function

The ITS HVAC is a two train system of identical components. One train is always operational and one train is in standby mode. This system is not configured to run both trains at the same time without bypassing control circuitry. This off-normal situation is not addressed in this analysis.

In the CRCF, the train A HVAC equipment is located on the opposite end of the building from train B HVAC equipment. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. Although these trains are interconnected through interior duct work, the trains are independent. A back-draft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

Each HVAC train is composed of four subsystems:

1. A series of dampers are used to control pressure, flow, as well as flow direction in this system.
2. Three HEPA filters, each consisting of one medium efficiency roughing filter (60-90 percent efficiency), two high efficiency filters for particulate removal in air (99.97 percent efficiency), and a mister/demister for maintaining proper humidity levels.
3. One exhaust fan with a rated capacity of 40,500 cubic feet per minute (cfm) and an exhaust fan motor rated at 200 horsepower (hp).
4. Control circuitry with logic contained in an erasable programmable read-only memory located in the adjustable speed drive controller used for controlling the speed of the

operating fan and on fault detection, and for off-nominal conditions, shutting down the operating train and transmitting signals to the standby system to start.

#### **6.2.2.2.2 Success Criteria**

One success criterion is defined for the each of independent trains, A and B, for providing the HVAC confinement function—maintain negative differential pressure in the CRCF for the specified mission time.

The respective trains of the ITS portions of the HVAC are identical. Various design features are provided to achieve each of the success criteria for the respective trains and for the combined system.

The HVAC FTA for the HVAC includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the HVAC.

#### **6.2.2.2.3 Mission Time**

The mission time for the HVAC system is 720 hours (Attachment B, Section B7). However, the mission time for the standby train (modeled as train B) has been taken as half of the active system (i.e., 360 hours), which is a conservative estimate of the average run time should the standby train be demanded.

#### **6.2.2.2.4 Fault Tree Results**

The top event in this fault tree is “Delta pressure not maintained in CRCF facility.” This is defined as the inability of the ITS HVAC system to maintain proper delta pressure within the facility. The system failure probability and standard deviation, including failure of electrical power are as follows:

- The mean system probability of failure value is 3.5E-02
- The standard deviation is 9.4E-02.

These values include the contribution of support system failures; specifically the contribution of failures of ITS AC Power System components

### **6.2.2.3 ITS AC Power Fault Tree Analysis**

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

#### **6.2.2.3.1 System Description**

The ITS AC power system supplies power to the ITS systems (the HVAC Systems) in the CRCF. The ITS power system consists of two elements; those used during normal operations

and those used during off-normal conditions. During normal operations AC power is supplied from one of two offsite 138 kV offsite power lines through the 138kV to 13.8 kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site.

Off-normal conditions for the distribution of AC power occur during a loss of offsite power (LOSP). A LOSP may be the result of problems on the power grid, or may be the result of failures within the plant AC power systems. Under these conditions, the AC power source for the CRCF ITS equipment is two onsite ITS diesel generators. Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each diesel generator supplies power to one division (A or B) of ITS systems. Each ITS diesel generator, its associate support systems, and the power distribution system are independent and electrically isolated from the other ITS diesel generator, its support systems and power distribution system.

The ITS loads within the CRCF are powered via two ITS 480V load centers and two ITS 480 V motor control centers (MCC) located within separate areas in the CRCF. Each division of the AC power supply from the 13.8kV ITS switchgears to the CRCF passes through a 13.8 kV to a 480 V transformer. Separate AC power systems are provided for each of the three CRCFs from the connection to the diesel generator switchgear through the individual loads. The systems supplying power to MCC A1 and B1 are representative of the systems used to power MCCs A2, A3, B2, and B3. The two fault trees developed for the AC power supplies to MCC A1 and B1 are representative of the fault trees for the remaining four MCCs.

The ITS on site power portion of the ITS power supply system is intended to provide back-up power to selected buildings and operations in the event of a main transmission power loss (a LOSP). The primary components in each division include: a diesel generator, support systems for the diesel generator, and a load sequencer. Both ITS diesel generators are located in the Emergency Diesel Generator Building (EDGB). Each is sized to provide sufficient 13.8 kV power to support all ITS loads in six facilities (i.e., three CRCFs, the WHF, and RF, and the EDGB).

The ITS diesel generator starts upon detection of an under voltage condition via an under voltage relay of the diesel generator switchgear. Each ITS diesel generator is equipped with a complete independent set of support systems including HVAC systems, uninterruptible and DC power systems, a fuel oil system, diesel generator start subsystem, diesel generator cooling subsystem and lube oil subsystem.

The load sequencer controls sequence of events that occur after a LOSP and the ITS diesel generator start. Upon a LOSP the load sequencer opens the CRCF ITS load center feed breaker. After the ITS diesel generator starts and reaches rated capacity, the load sequence connects the ITS diesel generator to the 13.8kV ITS switchgear and then reconnects the CRCF loads.

#### **6.2.2.3.2 Operations**

Under normal operating conditions, AC power is supplied from two 138 kV offsite power lines. Power is passed through the 138 kV to 13.8 kV Switchyard to the two independent 13.8 kV ITS switchgear. From here, power is transmitted via separate lines to a 13.8 kV to 480 V transformers supporting divisions A and B of the CRCF. Power to individual ITS components

within each facility is provided via 480 V Load Centers and MCCs (one of each for division A and one of each for division B in each facility) powered through these transformers

During a LOOP, both ITS diesel generators will start and accept loads in a timely manner. Upon a LOOP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8kV ITS switchgear and the switchyard 13.8 kV switchgear in each division automatically opens. Both ITS diesel generators start automatically and are connected to the 13.8kV ITS switchgear when the connecting breaker is closed by the load sequencer. The load sequencer then reconnects the CRCF loads to the 13.8kV ITS switchgear. Both ITS diesel generators continue to supply AC power until normal power is restored.

Environmental systems are provided to maintain the temperature in the various EDGB rooms and CRCF ITS electrical rooms within acceptable levels.

#### **6.2.2.3.3 Control System**

The ITS diesel generator starts upon detection of an under voltage condition via an under voltage relay of the 13.8kV ITS switchgear. The 13.8kV ITS switchgears are isolated from the main switchyard upon a loss of power in the switchyard. The loads in the CRCF are shed upon a loss of power indication.

A load sequencer controls the loading of the ITS diesel generator onto the 13.8kV ITS switchgear upon the diesel generator reaching rated output. The same load sequencer controls reloading the CRCF loads onto the AC power system.

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

Success criterion for the AC power system is defined in terms of its support function for the ITS HVAC confinement function. The AC power system must operate in support of the HVAC system for as long as necessary to successfully provide confinement after the potential release of radioactive material inside the CRCF. There are two independent trains of HVAC and each of these must be supported by an independent AC power system. Therefore, the following success criteria apply to the respective AC power supply trains:

- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG A) to the HVAC division powered through CRCF ITS Load Center A and ITS MCC A1 for the mission time of 720 hours
- Provide AC power from either the normal offsite power lines or from the ITS diesel generator (DG B) to the HVAC division powered through CRCF ITS Load Center A and ITS MCC B1 for the mission time of 720 hours.

The respective trains of the ITS portions of the AC power system are essentially identical. Various design features are provided to achieve each of the success criteria for the respective trains.

The FTA for the AC power system includes separate analyses for the respective trains. The failure to achieve the success criterion defines the top event for the fault tree for each train of the AC power system.

#### **6.2.2.3.5 Mission Time**

The mission time for the ITS AC power system is the same as for the HVAC system, 720 hours.

#### **6.2.2.3.6 Fault Tree Results**

Two fault trees are developed for the AC power system, one for train A and one for train B. The respective top events are:

- “Loss of AC power at Load Center A for the CRCF,” defined as a failure of the normal and ITS on-site power supplies to provide power to Load Center A
- “Loss of AC power at Load Center B for the CRCF,” defined as a failure of the normal and ITS on-site power supplies to provide power to Load Center B.

The results are essentially the same for either train:

- The mean probability of failure or either train value is 3.0E-02
- The standard deviation is 7.3E-02.

These results are presented in Attachment B, Section B3, Figure B3.4-1.

#### **6.2.2.4 Drip Shield Emplacement Gantry Analysis**

Just prior to closure of the subsurface facility, drip shields will be placed over the waste packages within the emplacement drifts. The drip shields are to prevent any seepage entering the drift from dripping onto the waste packages after repository closure and to protect the waste package from the direct impact of a rockfall. Each drip shield segment is designed to interlock with a previously emplaced drip shield segment, and when properly interlocked, the drip shield does not contact the emplacement pallet, the waste package, the rock wall or the runway beams of the invert.

The FTA is detailed in Attachment B, Section B4. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

##### **6.2.2.4.1 Physical Description**

The Drip Shield Emplacement Gantry (DSG) is a remotely-operated vehicle that transports drip shields from the Heavy Equipment Maintenance Facility into emplacement drifts. Similar to the TEV, the DSG is a rail-based vehicle which is powered by a third rail, and contains PLCs for localized control of the device. In most cases, operation of the DSG is under PLC control with only general oversight from a central control, but some in some cases, operations under remote manual control are performed as needed.

#### **6.2.2.4.2 Operations**

The DSG transports a drip shield from the Heavy Equipment Maintenance Facility to a designated emplacement drift turnout using the same rail system as the TEV. The DSG will travel into the emplacement drift to a predetermined position, where the gantry stops, and re-confirms its location. The DSG then moves forward at a crawl speed until the required final position is achieved. Once the correct position is achieved, the gantry lowers the lift beams, lowering the drip shield, the drip shield engages the previously emplaced drip shield interlock (if present), and it rests upon the steel frame of the emplacement drift invert. The emplacement gantry lowers its lifting features to its travel height and moves at a crawl speed away from the newly emplaced drip shield. Upon confirmation of emplacement status, the gantry slowly accelerates to the full operational speed and leaves the emplacement drift.

#### **6.2.2.4.3 Control Systems**

All operations are performed remotely. The control system includes the following features:

- Automated control using PLCs with oversight via audio and video signals from a central control station, in most cases
- Manual control when required via override from central control
- Automatic operational sequences to emplace drip shield
- Automatic stop at each rail segment to await a permissive signal to proceed from central control
- Fail-safe on loss of power: DSG stops, retains its load, and enters a locked mode until operator action is taken
- Sensors and logic to confirm the position of the DSG when emplacing a Drip Shield segment near a previously emplaced segment
- Programmed variable travel speeds (e.g., normal speed of 1.7 mph (150 ft/min) on surface tracks and access drifts, crawl speed of 15 ft/min for initial positioning in an emplacement drift, and a final positioning speed of 1.5ft/min).

#### **6.2.2.4.4 Success Criteria**

One scenario and fault tree is associated with the DSG:

1. Drop of drip shield onto a waste package

Success criteria for the DSG during the drip shield emplacement process require that the DSG subsystems operate without failure or spurious operations. During the emplacement operations, the DSG lift system should maintain the drip shield above the waste package as the gantry moves along the emplacement drift at an operational speed of 2.7 km/hr (1.7 mph).

#### **6.2.2.4.5 Fault Tree Results**

The top event in this fault tree is “Drip Shield Dropped on WP.” The top event is drop of the drip shield where at least two of the four lift pins or lift beam systems (rigs) have failed. The system value and standard deviation is:

- The mean system probability of failure value is 3.7E-9
- The standard deviation is 1.0E-12.

These results are presented in Attachment B, Section B4, Figure B4.4-1.

#### **6.2.2.5 Shield Door System Analysis**

The FTA is detailed in Attachment B, Section B5. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

##### **6.2.2.5.1 Physical Description**

Each of the CRCF Waste Package Positioning Rooms (room numbers 1018, 1019) has a shield door providing access to the Waste Package Loadout Room (room number 1015). The shield doors provide shielding during canister unloading and loading. The shield doors are ITS, protecting workers from the hazardous operations that go on inside the loading and unloading rooms.

The shield doors consist of a pair of large heavy doors that close together. The shield doors have the following design requirements: Motor over-torque sensors prevent the shield doors from causing damage to casks or waste packages in the event of closure on a conveyance.

##### **6.2.2.5.2 Operation**

The shield doors are opened to allow the TEV to leave the CRCF and then closed.

The shield door system has one credible failure scenarios for subsurface operations as follows:

1. Shield door closes on conveyance [TEV].

##### **6.2.2.5.3 Control System**

This is a manually operated system.

##### **6.2.2.5.4 Success Criteria**

The shield door system has one credible failure scenario for subsurface operations as follows:

1. Shield door closes on conveyance [TEV].

The success criterion for this scenario is defined as the shield doors not causing a release due to closure on the conveyance. Specifically, success criteria are defined as follows:

- In the event that the shield doors do close on a conveyance, the motor over-torque sensors prevent excessive closure force ensuring no release.

#### **6.2.2.5.5 Fault Tree Results**

The top event in this fault tree is “Facility Door closes on TEV.” This is defined as an inadvertent closure of the shield doors due to either operator action or component failure while the conveyance is in position to be hit by the doors. Faults considered in the evaluation of this top event include: failure of components in the control circuitry of the shield doors and human events that could contribute to the inadvertent shield door closing. The system value and standard deviation is:

- The mean system probability of failure value is 2.0E-03
- The standard deviation is 2.6E-03.

These results are presented in Attachment B, Section B3, Figure B5.4-1.

#### **6.2.2.6 Emplacement Drift Access Door Analysis**

The FTA is detailed in Attachment B, Section B6. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

##### **6.2.2.6.1 Physical Description**

The emplacement access door is a counter-opening, 2-panel design in which one panel opens inward and the other panel opens outward. The door is intended to control entry and is not to provide radiation shielding.

##### **6.2.2.6.2 Operation**

The emplacement drift access door is typically closed to maintain security and positive control of the emplacement drift. Normal door operation requires central control's input to prevent inadvertent access to the high radiation areas; however, a manual override switch is provided to open the door locally within a locked access box. When a TEV is ready to proceed into an emplacement drift, the emplacement access door is remotely opened by the operator in the Central Control Center Facility. Upon visual confirmation that the TEV has passed through the threshold and has completely entered the turnout drift, the operator in the Central Control Center Facility closes the door system. The process is reversed when the TEV is to exit the emplacement drift.

##### **6.2.2.6.3 Control System**

This system is either remotely controlled by operators in the central control facility or locally through manual override switch in locked access box.

#### 6.2.2.6.4 Success Criteria

One scenario and fault tree is associated with the emplacement drift access door:

1. Emplacement access door closes on TEV.

The success criterion for the scenario is that the emplacement access door operates without failure or spurious operations and that the operator does not close the door prematurely. During the normal operations, the emplacement access door system is not to close onto the TEV during the waste package emplacement. The door should not collapse onto the TEV.

The following requirements are identified with respect to this scenario:

- The operational status of the door is clearly displayed on visual monitor for remote operations on the control panel including opening and closing of the door.
- The TEV shielded enclosure shall be able to maintain the shielding function in case of closure of the access door onto the TEV.
- Normal periodic maintenance and inspection are performed on the bulkhead and door mounting supports and door mechanism to allow for the safe operation of the door without collapsing the door panels onto the TEV.

#### 6.2.2.6.5 Fault Tree Results

The top event is the initiating event of the doors closing and impacting on the TEV. This top event is realized by either the occurrence of the door closure due to human error or by mechanical failure. The system value and standard deviation is:

- The mean system probability of failure value is 2.0E-03
- The standard deviation is 2.3E-03.

These results are presented in Attachment B, Section B3, Figure B6.4-1.

#### 6.2.2.7 Additional Fault Trees

Seventeen additional fault trees were developed to address events that could impact either a TEV with a waste package or the waste package alone during waste package emplacement operations. These fault trees are identified in Table 6.2-2. Sixteen of these trees are top level trees. The results of quantifying the trees were input directly into the Excel spreadsheet used to quantify subsurface event sequences as initiating events. The last tree, DSGANT-INIT, is input into the top level fault tree DRIFT-WP-IMPACT.

Table 6.2-2 Top Level and Linking Fault Trees

<b>Fault Tree</b>	<b>Description</b>	<b>Events considered</b>	<b>Top Level Fault Tree</b>	<b>System Fault Trees Used as Input</b>
FACILITY-DROPON	Object dropped on Waste Package as it leaves facility	Drops from Crane operation	Top level tree	None
TRANSIT-DERAIL	TEV derails during surface transit to emplacement	Derailment of TEV during surface transit	Top level tree	None
TRANSIT-DROPON	Impact to TEV during transit from falling object	Rockfalls	Top level tree	None
DRIFT-TEV-IMPACT	Impact to TEV during subsurface travel and emplacement	Emplacement door impacts, derailment, and TEV overrun of rails	Top level linking tree	ACDRIMP-INIT (B6), DRIFT-DERAIL (B4), TEV-end-rail (B4)
DRIFT-WP-DROPON	Drop of heavy load on WP during subsurface operation	Rockfall and drop of drip shield onto WP	Top level tree	DRIPSHIELD-DROPPED (B4)
DRIFT-WP-IMPACT	WP impacted in the drift	Linking tree to TEV-IMPACTS-WP and DSGANT-INIT	Top level tree	TEV-IMPACTS-WP (B1.10), DSGANT-INIT
DSGANT-INIT	Gantry derails and strikes WP	Drip shield gantry derailment	Input to DRIFT-WP-IMPACT	None
SSO-CRCF-SD-IMPACT-HVAC	WP impact facility door In the CRCF where HVAC is available	Impacts with facility door and HVAC failures	Top level linking tree	FACILITY-SHIELD-DOOR (B5), HVAC (B2)
SSO-HVYLOAD-DROPON-HVAC	Heavy load dropped on WP in CRCF where HVAC is available	Crane drops of objects onto WP and HVAC failures	Top level linking tree	FACILITY-DROPON, HVAC (B2)
SSO-TEV-COLL-HVAC	TEV collision in CRCF where HVAC is available	TEV collisions with facility structures with HVAC failures	Top level linking tree	FACILITY-COLLISION (B1.2), HVAC (B2)
SSO-WP-DROP-HVAC	WP dropped in CRCF where HVAC is available	TEV drops WP with HVAC failures	Top level linking tree	FACILITY-DROP (B1.7), HVAC (B2)
SSO-WP-TEV-SD-HVAC	TEV shield door impacts WP in CRCF where HVAC is available	TEV doors close on WP with HVAC failures	Top level linking tree	FACILITY-TEV-DOOR (B1.1), HVAC (B2)
SHIELD-PROXIMITY	Direct exposure due to extended proximity to TEV during transit	Human errors	Top level tree	None
SHIELD- ENTRY	Direct exposure due to emplacement drift entry by workers	Human errors	Top level tree	None
FIRE-DRIFT	Fire impacts WP in Drift	Drift Fires	Top level tree	None

Table 6.2-2. Top Level and Linking Fault Trees (Continued)

Fault Tree	Description	Events considered	Top Level Fault Tree	System Fault Trees Used as Input
FIRE-SUBSURFACE	Fire impacts WP on subsurface rail	Subsurface fires during transit	Top level tree	None
FIRE-SURFACE	Fire impacts WP on surface rail	Surface fires during transit	Top level tree	None

NOTE: TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

## 6.2.2.8 Potential Moderator Sources

### 6.2.2.8.1 Internal Floods

While the waste package in a TEV is inside a building, internal floods are a potential source of moderator addition into a canister associated with pivotal events in the event sequences included in Section 6.1. Moderator addition into a canister can occur following a breach of the canister and a subsequent internal flood. The internal flooding analysis considers all waste handling facilities.

During most of its handling at the repository, a canister is surrounded by at least one other barrier to water intrusion: a transportation cask, a transportation cask within a CTT, an aging overpack, a waste package, a waste package within a WPTT, or a waste package within a TEV.

Each facility is equipped with a normally dry, double-pre-action sprinkler system in areas where waste forms are handled (Ref. 2.2.16), (Ref. 2.2.35), (Ref. 2.2.26), and (Ref. 2.2.42). Such systems, which require both actuation of smoke and flame detectors to allow the pre-action valve to open and heat actuation of a fusible link sprinkler head to initiate suppression, have a very low frequency of spurious operation. . A 30-day period from the occurrence of the canister breach to the time definitive action can be taken to prevent introduction of water into the canister is reasonable and is the same as the period used to assess dose for a radiological release. The spurious actuation frequency over a 30 day mission time after a breach is calculated below.

An estimate of the probability of spurious actuation is developed using a simplified screening model that addresses the following cut sets that result in actuation:

- Spurious pre-action valve opens before canister breach × failure of a sprinkler head during post-breach mission time (30 days)
- Failure of a sprinkler head during building evacuation × water left in dry piping after last test (First quarter following annual test).

The frequency of sprinkler failure is estimated using an individual sprinkler head failure frequency of 1.6E-6/yr (Ref. 2.2.10, Table 1), the estimated number of sprinklers (1 per 130 ft<sup>2</sup> based on NFPA 13 (Ref. 2.2.63, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2.23). For example, the area of CRCF Waste Package Loadout Room 1015 is listed as 7,470 ft<sup>2</sup> in (Ref.

2.2.23, Table 10). At 130 ft<sup>2</sup>/sprinkler, 58 sprinklers are estimated. The failure of any sprinkler in the room is then estimated to be  $58 \times 1.6E-6/\text{yr} \times 1/8,760 \text{ hrs/yr}$ , or  $1.1E-8/\text{hr}$ .

The frequency of pre-action valve spurious open is estimated using the solenoid valve spurious open data in Section 6.3 of  $8.1E-07/\text{hr}$ . This is reasonable because a solenoid valve must open to relieve the air pressure from the diaphragm which keeps the valve closed.

The value of the first cutset is  $(1.6E-6/\text{yr} \times 1/8,760 \text{ hr/yr} \times 720 \text{ h}) \times (8.1E-7/\text{hr} \times 720 \text{ h}) = 8E-11/\text{sprinkler head}$ . The second cutset is more significant:  $0.025$  (human error screening value)  $\times (1.6E-6/\text{yr} \times 1/8,760 \text{ hr/yr} \times 720 \text{ h}) = 3E-9/\text{sprinkler head}$ .

Applying the sum of these values,  $3E-9/\text{sprinkler head}$ , to the number of sprinklers calculated for the waste handling areas of the four facilities results in the following estimates of the probability of spurious sprinkler actuation found in Table 6.2-3.

Table 6.2-3 Probability of Spurious Sprinkler Actuation

Facility	Waste Handling Area (ft <sup>2</sup> ) <sup>a</sup>	Number of Sprinkler Heads	Probability of Spurious Actuation in 30 day Period in Waste Handling Areas
CRCF(ea)	42,000	330	1E-6
IHF	30,000	240	9E-7
RF	19,000	150	5E-7
WHF	28,000	215	6E-7

NOTE: <sup>a</sup> CRCF area based on room numbers 1005E, 1016-1026, 2004,2007, 2007A, and 2007B

IHF area based on room numbers 1001-1003, 1006-1008, 1011,1012, 1026 and 2004

RF area based on room numbers 1013, 1015, 1016, 1017, 1017A, and 2007

WHF area based on room numbers 1007-1010, 1016, 2004, 2006, and 2008.

CRCF = Canister Receipt and Closure Facility, ft = feet; IHF = Initial Handling Facility; RF = Receipt Facility; WHF = Wet Handling Facility.

Source: (Ref. 2.2.23)

Piping carrying water is present in the waste form handling areas of the CRCF, IHF and WHF. Piping lengths in these areas of the CRCF and WHF are below 100 feet per facility. The probability of a pipe crack in a 30 day period was estimated using the pipe leak data from *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*, NUREG/CR-6928 (Ref. 2.2.49, Table 5-1). Piping leaks and large break rates applicable to non-service water applications are used in the analysis. These values are considered appropriate for repository systems because the conditioning applied to the fluids in the systems is that typical of commercial nuclear power plants:

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

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

Multiplying the sum of the small and large crack frequencies ( $2.8E-10 \text{ hr}^{-1}\text{ft}^{-1}$ ) by the length of piping in the waste handling areas of each facility, and the number of hours in a 30 day period (720 hr), a conditional probability of water leakage in all waste handling areas given a breach is approximated as follows:

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

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

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

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

It is appropriate to use the waste handling area piping lengths because they are separated by concrete walls from the non-waste handling areas of buildings.

The above applies to event sequences that do not involve fires as an initiating event. During fire initiating event sequences, fire suppression would actuate in the locations sufficiently heated by the fire. The fire initiating event analysis is described in Section 6.5, and the conditional probability of canister failure owing to fires is described in Section 6.3. The analysis is performed without the salutary effects of fire suppression in order to demonstrate large margins of safety during fire event sequences. Furthermore, the location of each fire is analyzed as around the outer shell of the overpack that surrounds the canister. The frequency of containment breach due to fire is significantly overestimated because of this conservative approach.

For fires that occur in locations that contain canisters sealed within bolted transportation casks, the fire location is floor level and the transportation casks rise as much as 20 feet above the floor. Casks are relatively thick walled compared to canisters and sustain a relatively small internal pressurization when compared to canisters. Therefore, if a fire is large enough, it will fail the internal canister first, as indicated in Attachment D. This will cause the bolted and sealed cask to bear the overpressure that is inside the canister. The cask bolts might act as elastic springs allowing the top to break the seal and relieve the internal pressure. This would be a mechanism that prevents cask breach. However, a hot fire may result in sufficient loss of strength of the bottom portion of the stainless steel cask such that it breaches. If failure occurs because of bolt stretching, the cask lid remains on top of the cask preventing fire suppression water from entering. Commercial DPCs and TAD canisters will require at least 100 liters of water to enter the canister if optimally distributed among the fuel rods (Ref. 2.2.38). Casks are raised above the floor. They lay on top of railcars, are lifted from there by cranes, sit inside a CTT, or lay sideways on a pallet. They are at least five feet from the floor. If the bottom portion of the canister breaches, there is no physical mechanism for this much water to enter the cask and then the canister, remain as water (not boil off), and optimally mix with the fuel rods.

This latter situation also applies to canisters sealed within a welded waste package. The waste package sits inside a WPTT or is inside a TEV. In the former case it is more than three feet from the floor (Ref. 2.2.18) and in the latter case about one foot from the floor (Ref. 2.2.20). In the latter case, however, the TEV offers an additional layer of protection against fires. In addition, it is physically unrealistic for a sufficient amount of available fire suppression water to cause 100

liters to leak into a breached canister, but not extinguish the fire or at least reduce the severity of the fire such that a breach would not occur.

For a canister inside of an open transportation cask or waste package, the orientation of these is always vertical, and the cask and waste package are always elevated above the floor where the fire occurs. The occurrence of a fire of sufficient severity will fail the canister first as described above. An open transportation cask or waste package might allow fire suppression water to spray in from the top. The building configuration, however, precludes this occurrence. The cask lids are removed while in the upload cell below the CTM. The cask and waste package ports are above the casks and waste package. There is no fire suppression piping spanning the ports because the ports must be kept clear in order to perform lift and load operations. In the Waste Package Positioning Room and welding area, the lid is on the waste package and fire suppression piping can not be above an open waste package because of the welding machine. In the cutting cell in which a cask is open (WHF only), there can be no fire suppression piping above an open cask because of the cutting equipment.

Upon failure of the canister inside the cask, the cask will not be susceptible to pressurization failures as above. Instead, water can only enter in a cask (or waste package) if the cask body melts through. Fires capable of melting stainless steel or Alloy 22, however, have an occurrence frequency within the waste handling facilities of less than 1E-05 over the preclosure period (Attachment D). Thus, breach of the cask or waste package in a manner that would allow water to enter the canister is essentially not physically realizable.

When a canister is being lifted, transferred inside the shield bell, and lowered. It is not inside an outer cask. However, fires can not be severe enough to breach a canister while being moved, as described in more detail in Attachment D. Water intrusion, therefore, is not physically realizable for this situation.

It is concluded that moderator entry into breached canisters during fire event sequences is not physically realizable because of a combination of physical mechanisms, building and equipment configuration, and overpack material properties. Furthermore, the existence of water from fire suppression is inconsistent with the fire analyses performed to obtain the probability of containment failure owing to fire. If fire suppression were indeed available, the probabilities of canister breach would be far lower. However, in order to complete an event sequence quantification, the conditional probability of moderator entry into a canister after canister breach during a fire initiating event sequence is assessed as *extremely unlikely* and assigned a lognormal distribution with a median of 0.001 and an error factor of 10. This yields a mean value of 3E-03. The large error factor is assigned because of the potential of human error to defeat some of the reasons that water will not enter the cask or waste package (e.g., neglecting to place a lid on the waste package just before a severe fire). These assignments are consistent with the methodology on the use of judgment provided in Section 4.3.10.

#### **6.2.2.8.2 Lubricating Fluid**

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a welded gear box with a leak pan below it capable of capturing the entire gearbox fluid inventory. An estimate of the leakage rate through the gear box and drip pan

is found by multiplying the gearcase motor failure frequency (all modes) of  $0.88E-06$  per hour (Ref. 2.2.45, Page 2-104 and Section 6.3) by 0.5 (Ref. 2.2.44, Page 2-90), over the 50 years by the conditional probability of oil pan failure. A loss of lubrication would fail the crane operation and also be detected by oil pressure indicators. The conditional probability of oil pan failure may be estimated by analogy to receiver tank leakage during the interval between gearbox failure and detection. The interval is conservatively estimated to be 30 days. The all modes failure rate of a receiver tank is  $0.34E-06$  per hour (Ref. 2.2.45, Page 2-213). Using an exposure interval of 50 years (which represents the operating life of the surface facilities), the conditional probability of lubricating fluid entering a breached canister would be less than:

$$0.88E-06/\text{hr} \times 50 \text{ yrs} \times 8760 \text{ hrs/yr} \times 0.34E-06/\text{hr} \times 720 \text{ hrs/30days} = 9.4E-05 \text{ over the preclosure period.}$$

This probability is overstated because a) it does not account for inspections during the operating period of the facility, and b) it does not account for the conditional probability that lubricating fluid can find its way into a breached canister. Therefore, lubricating fluid is eliminated as a potential moderator.

## 6.3 DATA UTILIZATION

### 6.3.1 Active Component Reliability Data

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

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

While data from the facility being studied are the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP is a one-of-kind facility and has no operating history, it was necessary to develop the required data from the experience of other nuclear and nonnuclear operations. Industry-wide data sources are documents containing industrial or military experience on component performance. These sources are from previous safety/risk analyses and reliability studies performed nationally or internationally and also can be standards or published handbooks. For the YMP PCSA, a database is constructed using a library of industry-wide data sources of reliability data from nuclear power plants, equipment used by the military, chemical processing plants and other facilities. The sources used are listed in Attachment C, Section C1.2.

The data source scope has to be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might be used for electronics data versus mechanical data, so long as the detail and the applicability of the information provided justify its use. Lastly, the quality of the data source is considered to be a measure of the source's

credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort is made in this analysis to use the highest quality data source available for each active component type and failure mode.

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

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

Among the active components whose reliability is quantified with industry-wide data are the 200-ton cranes, jib cranes, waste package maneuvering cranes and the spent fuel transfer machine (SFTM). The SFTM is not used in the IHF; however it is being discussed in this section for completeness. The rationale for using such data for these estimates is that a significant amount of crane experience exists within the commercial nuclear power industry and other applications and that this experience can be used to bound the anticipated crane performance at YMP. Furthermore, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants. Crane and SFTM handling incidents that result in a drop are included in the drop probability regardless of cause; they may be caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

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

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

The application of 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. 2.2.9). 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:

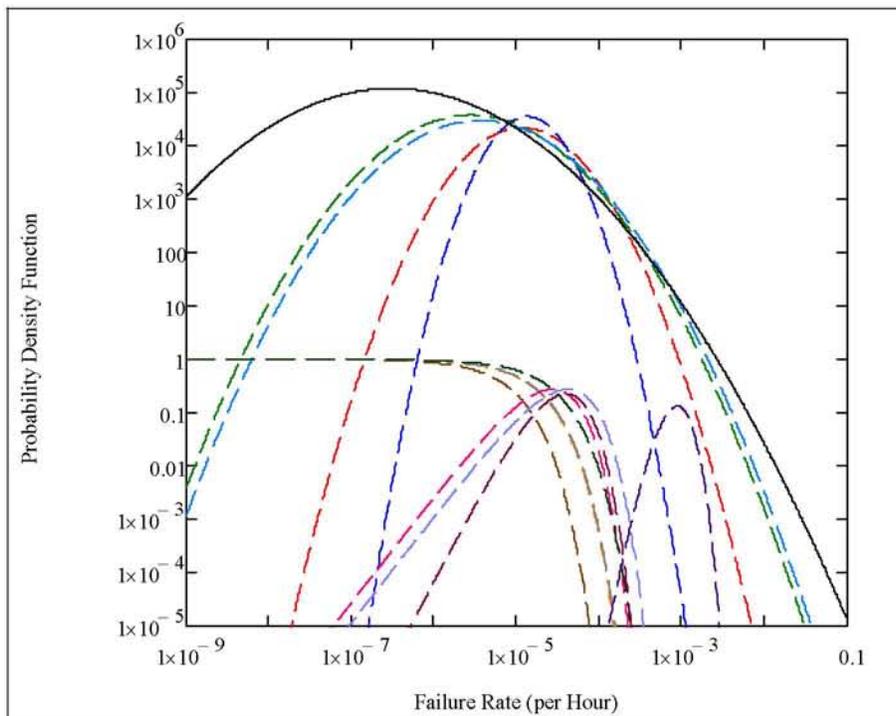
1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, 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, Equation C2.1.

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. 2.2.57, 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 probability density function for the combination are produced and plotted for comparison, as in the example shown as Figure 6.3-1.



Source: Attachment C, Figure C2.1-1

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

If only a single data source is considered applicable to a given TYP-FM combination and if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. However, if the data source does not readily provide a probability distribution,

but instead exposure data, (i.e., a number of recorded failures over an exposure time for failure rates or over a number of demands for failure probabilities), the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffrey's noninformative prior distribution (i.e., gamma for time-related failure modes and beta for demand based failure modes).

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

### 6.3.1.3 Common-Cause Failure Data

Dependent failures are modeled in event tree and fault tree logic models. When possible, potential dependent failures are modeled explicitly via the logic models. For example, failure of the HVAC system is explicitly dependent upon failure in the electrical supply system that is modeled in the fault trees. Similarly, the effects of erroneous calibration or other human failure events can be explicitly included in the system fault tree models and the basic event probabilities considered during the human reliability analysis (HRA). Otherwise, potential dependencies known as common-cause failures (CCFs) are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate common-cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the *Beta Factor Method* (Ref. 2.2.53), the *Analytical Background and Techniques. Volume 2 of Procedures for Treating Common Cause Failures in Safety and Reliability Studies* (Ref. 2.2.61), and the *Alpha Factor Method* (Ref. 2.2.62). In a parametric model, the probability of two or more components failing by a CCF is estimated by use of equations provided in Section 4.3.3.3.

For the PCSA, common-cause failure rates or probabilities are estimated using the *Alpha Factor Method* (Ref. 2.2.62) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in *NUREG/CR-5485* (Ref. 2.2.62) consisted of:

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

The data analysis also produces prior distributions for the alpha factors. The results are the mean alpha factors and uncertainty bounds, reported in *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment* (Ref. 2.2.62 Table 5-11) and reproduced in Attachment C, Table C3-1).

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

#### 6.3.1.4 Input To SAPHIRE Models

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

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

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

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

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

The template data is utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the SAPHIRE code, then by using the modify event feature to link the template data to each basic event in the fault tree. This permits each active component of the

same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the data investigation and Bayesian combination process.

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

### 6.3.1.5 Summary of Active Component Reliability Data in Subsurface Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the Subsurface models. Development of this table is discussed in detail in Attachment C, Section C4. Mission times are discussed in Section 6.2.

Table 6.3-1. Active Component Reliability Data Summary

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS TRANSFORMER TRAIN A CCF	4.92E-06	2.91E-07	34
060-#EEE-CRCF1-A-XMR-FOH	CRCF ITS TRAIN A TRANSFORMER FAILURE	2.10E-04	2.91E-07	720
060-#EEE-CRCF1-B-XMR-FOH	CRCF ITS TRANSFORMER TRAIN B FAILURE	2.10E-04	2.91E-07	720
060-#EEE-LDCNTRA-BUA-FOH	CRCF LOAD CENTER A FAILS	4.39E-04	6.10E-07	720
060-#EEE-LDCNTRA-C52-FOD	LOAD CENTER A FEED BREAKER (AC) FAILS TO RECLOSE	2.24E-03		
060-#EEE-LDCNTRA-C52-SPO	LOAD CENTER A FEED CIRCUIT BREAKER (AC) SPURIOUS OPERATION	3.82E-03	5.31E-06	720
060-#EEE-LDCNTRB-C52-FOD	13.8 ITS SWGR TO CRCF ITS LC B CIRCUIT BREAKER FAILS ON DEMAND	2.24E-03		
060-#EEE-LDCNTRB-C52-SPO	CRCF ITS LOAD CENTER CIRCUIT BREAKER (AC) SPUR OP	3.82E-03	5.31E-06	720
060-#EEE-LDCNTRS-C52-CCF	COMMON CAUSE FAILURE OF THE LOAD CENTER FEED BREAKERS TO RECLOSE	1.05E-04		
060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 FEED BREAKER SPURIOUS OPERATION	3.82E-03	5.31E-06	720
060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 FAILS	5.38E-03	7.49E-06	720
060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 FEED BREAKER SPURIOUS OPERATION	3.82E-03	5.31E-06	720
060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 FAILURE	5.38E-03	7.49E-06	720

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
060-VCOO-SFAN001-FAN-FTR	SUPPLY FAN FOR CRCF FAILS	5.06E-02	7.21E-05	720
060-VCOO-SFAN002-FAN-FTR	FAN (MOTOR-DRIVEN) FAILS TO RUN	5.06E-02	7.21E-05	720
060-VCT0-AHU0001-AHU-FTR	CRCF ITS ELEC AHU 00001 FAILS TO RUN	2.65E-03	3.68E-06	720
060-VCT0-AHU0001-CTL-FOD	CRCF ITS ELEC AHU 00001 CONTROLLER FAILS	2.03E-03		
060-VCT0-AHU0002-AHU-FTR	CRCF ITS ELEC AHU 00002 FAILS TO RUN	2.65E-03	3.68E-06	720
060-VCT0-AHU0002-CTL-FOD	CRCF ITS ELEC AHU 00002 CONTROLLER FAILS	2.03E-03		
060-VCT0-AHU0002-FAN-FTS	CRCF ITS ELEC AHU 00002 FAILS TO START	2.02E-03		
060-VCT0-AHU0004-AHU-FTR	CRCF ITS ELEC AHU 00004 FAILS TO RUN	2.65E-03	3.68E-06	720
060-VCT0-AHU0004-CTL-FOD	CRCF ITS ELEC AHU 00004 CONTROLLER FAILS	2.03E-03		
060-VCT0-AHU0004-FAN-FTS	CRCF ITS ELEC AHU 00004 FAILS TO START	2.02E-03		
060-VCT0-AHU0103-AHU-CCR	CCF OF THE RUNNING CRCF ITS ELEC AHUS TO CONTINUE TO RUN	6.20E-05		
060-VCT0-AHU0202-AHU-CCR	CCF OF STANDBY CRCF ITS ELEC AHUS TO START/RUN	1.60E-04		
060-VCT0-EXH-005-CTL-FOD	CRCF ITS ELEC EXH FAN 00005 CONTROLLER FAILS	2.03E-03		
060-VCT0-EXH-005-FAN-FTR	CRCF ITS ELEC EXHAUST FAN 00005 FAILS TO RUN	5.06E-02	7.21E-05	720
060-VCT0-EXH-006-FAN-FTR	CRCF ITS ELEC EXH. FAN FAILS TO RUN	5.06E-02	7.21E-05	720
060-VCT0-EXH-006-FAN-FTS	CRCF ITS ELEC EXH FAN 00006 FAILS TO START	2.02E-03		
060-VCT0-EXH-007-CTL-FOD	CRCF ITS ELEC EXH FAN 00007 CONTROLLER FAILS	2.03E-03		
060-VCT0-EXH-007-FAN-FTR	CRCF ITS ELEC EXHAUST FAN 00007 FAILS TO RUN	5.06E-02	7.21E-05	720
060-VCT0-EXH-008-FAN-FTR	CRCF ITS ELEC EXH. FAN 8 FAILS TO RUN	5.06E-02	7.21E-05	720
060-VCT0-EXH-008-FAN-FTS	CRCF ITS ELEC EXH FAN 00008 FAILS TO START	2.02E-03		
060-VCT0-EXH006-CTL-FOD	CRCF ITS ELEC EXH FAN 0006 CONTROLLER FAILS	2.03E-03		
060-VCT0-EXH008-CTL-FOD	CRCF ITS ELEC EXH FAN 0008 CONTROLLER FAILS	2.03E-03		

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
060-VCT0-EXH0507-FAN-CCR	CCF OF RUNNING EXH FANS FOR CRCF ITS ELEC.	1.20E-03		
060-VCT0-EXH0608-FAN-CCF	CCF TO START/RUN: STANDBY EXH FANS FOR THE CRCF ITS ELEC	1.30E-03		
060-VCT0-AHU0003-AHU-FTR	CRCF ITS ELEC AHU 00003 FAILS TO RUN	2.65E-03	3.68E-06	720
060-VCT0-AHU0003-CTL-FOD	CRCF ITS ELEC AHU 00003 CONTROLLER FAILS	2.03E-03		
060-VCT0-AHU0103-AHU-CCR	CCF OF THE RUNNING CRCF ITS ELEC AHUS TO CONTINUE TO RUN	6.20E-05		
060-VCT0-DMP000A-DMP-FRO	MANUAL DAMPER FOR TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP000B-DMP-FRO	MANUAL DAMPER FOR TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP001A-DMP-FRO	MANUAL DAMPER INPUT TO EXHAUST FAN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP001B-DMP-FRO	MANUAL DAMPER INPUT TO EXHAUST FAN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP009I-DMP-FRO	MANUAL DAMPER #09 INPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP009O-DMP-FRO	MANUAL DAMPER #09 OUTPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP010I-DMP-FRO	MANUAL DAMPER #10 INPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP010O-DMP-FRO	MANUAL DAMPER #10 OUTPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP011I-DMP-FRO	MANUAL DAMPER #11 INPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP011O-DMP-FRO	MANUAL DAMPER #11 OUTPUT TRAIN A FAILS	6.03E-05	8.38E-08	720
060-VCT0-DMP012I-DMP-FRO	MANUAL DAMPER #12 INPUT TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP012O-DMP-FRO	MANUAL DAMPER #12 OUTPUT TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP013I-DMP-FRO	MANUAL DAMPER #13 INPUT TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP013O-DMP-FRO	MANUAL DAMPER #13 OUTPUT TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP014I-DMP-FRO	MANUAL DAMPER #14 IN TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DMP014O-DMP-FRO	MANUAL DAMPER #14 OUTPUT TRAIN B FAILS	3.02E-05	8.38E-08	360
060-VCT0-DTC0A-DTC-RUP	DUCT FAILS BETWEEN HEPA AND EXHAUST FAN (10 FEET)	2.68E-03	3.72E-06	720

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
060-VCTO-DTC0B-DTC-RUP	DUCT FAILS BETWEEN HEPA AND EXHAUST FAN (10 FEET)	1.34E-03	3.72E-06	360
060-VCTO-FAN00A-FAN-FTR	EXHAUST FAN IN TRAIN A FAILS	5.06E-02	7.21E-05	720
060-VCTO-FAN00B-FAN-FTR	EXHAUST FAN IN TRAIN B FAILS	2.56E-02	7.21E-05	360
060-VCTO-FAN00B-FAN-FTS	EXHAUST FAN IN TRAIN B FAILS TO START	2.02E-03		
060-VCTO-FANA-PRM-FOH	SPEED CONTROL EXHAUST FAN TRAIN A FAILS TO MAINTAIN DELTA P	3.87E-04	5.38E-07	720
060-VCTO-FANB-PRM-FOH	SPEED CONTROL EXHAUST FAN TRAIN B FAILS TO MAINTAIN DELTA P	1.94E-04	5.38E-07	360
060-VCTO-FSLAB0-SRF-FOH	LOW FLOW TRAIN A SENSOR FAILURE	7.70E-04	1.07E-06	720
060-VCTO-HEPA-CCF	COMMON CAUSE FAILURE OF HEPA FILTERS (2 OF 3)	7.68E-05	1.07E-07	720
060-VCTO-HEPA09-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 09 FAILS	6.55E-03	9.12E-06	720
060-VCTO-HEPA0A9-HEP-LEK	HEPA #09 TRAIN A LEAKS	2.16E-03	3.00E-06	720
060-VCTO-HEPA10-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 10 FAILS	6.55E-03	9.12E-06	720
060-VCTO-HEPA11-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 11 FAILS	6.55E-03	9.12E-06	720
060-VCTO-HEPA12-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 12 FAILS	3.28E-03	9.12E-06	360
060-VCTO-HEPA13-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 13 FAILS	3.28E-03	9.12E-06	360
060-VCTO-HEPA14-DMS-FOH	MOISTURE SEPARATOR/DEMISTER HEPA 14 FAILS	3.28E-03	9.12E-06	360
060-VCTO-HEPAA09-HEP-LEK	HEPA #09 TRAIN A LEAKS	2.16E-03	3.00E-06	720
060-VCTO-HEPAA09-HEP-PLG	HEPA #A09 TRAIN A PLUGGED	3.07E-03	4.27E-06	720
060-VCTO-HEPAA10-HEP-LEK	HEPA #10 TRAIN A LEAKS	2.16E-03	3.00E-06	720
060-VCTO-HEPAA10-HEP-PLG	HEPA #A10 TRAIN A PLUGGED	3.07E-03	4.27E-06	720
060-VCTO-HEPAA11-HEP-LEK	HEPA #11 TRAIN A LEAKS	2.16E-03	3.00E-06	720

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
060-VCTO-HEPAA11-HEP-PLG	HEPA #A11 TRAIN A PLUGGED	3.07E-03	4.27E-06	720
060-VCTO-HEPAB-CCF	COMMON CAUSE FAILURE OF HEPA FILTERS (2 OF 3)	3.84E-05	1.07E-07	360
060-VCTO-HEPAB12-HEP-LEK	HEPA #B12 TRAIN B LEAKS	1.08E-03	3.00E-06	360
060-VCTO-HEPAB12-HEP-PLG	HEPA #B12 TRAIN B PLUGGED	1.54E-03	4.27E-06	360
060-VCTO-HEPAB13-HEP-LEK	HEPA #B13 TRAIN B LEAKS	1.08E-03	3.00E-06	360
060-VCTO-HEPAB13-HEP-PLG	HEPA #B13 TRAIN B PLUGGED	1.54E-03	4.27E-06	360
060-VCTO-HEPAB14-HEP-LEK	HEPA #B14 TRAIN B LEAKS	1.08E-03	3.00E-06	360
060-VCTO-HEPAB14-HEP-PLG	HEPA #B14 TRAIN B PLUGGED	1.54E-03	4.27E-06	360
060-VCTO-IEL0001-IEL-FOD	CRCF DOOR INTERLOCK FAILURE	2.75E-05		
060-VCTO-PDSLA0B-SRP-FOD	PRESSURE DIFFERENTIAL TRAIN A SWITCH FAILS	3.99E-03		
060-VCTO-SUPPLY-FAN-CCF	COMMON CAUSE FAILURE OF CRCF SUPPLY FANS	1.20E-03	1.67E-06	720
060-VCTO-TDMP00A-DTM-FOD	TORNADO DAMPER TRAIN A FAILS	8.71E-04		
060-VCTO-TDMP00B-DTM-FOD	TORNADO DAMPER B FAILS ON DEMAND	8.71E-04		
060-VCTO-TDMP00B-DTM-FOH	TORNADO DAMPER TRAIN B FAILS	8.10E-03	2.26E-05	360
060-VCTO-UDMP000-UDM-FOH	BACKDRAFT DAMPER FOR TRAIN B EXHAUST FAILS	8.10E-03	2.26E-05	360
26D-##EG-DAYTNKA-TKF-FOH	ITS DG A DAY TANK (00002A) FAILS	1.58E-04	4.40E-07	360
26D-##EG-DAYTNKB-TKF-FOH	ITS DG B DAY FUEL TANK FAILS	1.58E-04	4.40E-07	360
26D-##EG-FLITLKA-IEL-FOD	ITS DG A FUEL TRANSFER PUMPS INTERLOCK FAILURE	2.75E-05		
26D-##EG-FLITLKB-IEL-FOD	ITS DG B FUEL TRANSFER PUMPS INTERLOCK FAILURE	2.75E-05		
26D-##EG-FTP1DGA-PMD-FTR	ITS DG A FUEL TRANSFER PUMP FAILS TO RUN	1.23E-02	3.45E-05	360
26D-##EG-FTP1DGA-PMD-FTS	ITS DG A FUEL PUMP 1A FAILS TO START	2.50E-03		
26D-##EG-FTP1DGB-PMD-FTR	ITS DG B FUEL TRANSFER PUMP 1 (MOTOR DRIVEN) FAILS TO RUN	1.23E-02	3.45E-05	360
26D-##EG-FTP1DGB-PMD-FTS	ITS DG B FUEL TRANSFER PUMP 1 (MOTOR DRIVEN)	2.50E-03		

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
	FAILS TO START			
26D-##EG-FTP2DGA-PMD-FTR	ITS DG A FUEL TRANSFER PUMP 2A FAILS TO RUN	1.23E-02	3.45E-05	360
26D-##EG-FTP2DGA-PMD-FTS	ITS DG A FUEL TRANSFER PUMP 2A FAILS TO START	2.50E-03		
26D-##EG-FTP2DGB-PMD-FTR	ITS DG B FUEL TRANSFER PUMP 2 (MOTOR DRIVEN) FAILS TO RUN	1.23E-02	3.45E-05	360
26D-##EG-FTP2DGB-PMD-FTS	ITS DG B FUEL TRANSFER PUMP 2 (MOTOR DRIVEN) FAILS TO START ON DEMAND	2.50E-03		
26D-##EG-FULPMPA-PMD-CCR	COMMON CAUSE FAILURE OF ITS DG A FUEL PUMPS TO RUN	2.90E-04		
26D-##EG-FULPMPA-PMD-CCS	COMMON CAUSE FAILURE OF ITS DG A FUEL PUMPS TO START	1.20E-04		
26D-##EG-FULPMPB-PMD-CCR	COMMON CAUSE FAILURE OF ITS DG B FUEL PUMPS TO RUN	2.90E-04		
26D-##EG-FULPMPB-PMD-CCS	COMMON CAUSE FAILURE OF ITS DG B FUEL PUMPS TO START	1.20E-04		
26D-##EG-HVACFN1-FAN-FTR	ITS DG B ROOM FAN 1 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EG-HVACFN1-FAN-FTS	ITS DG B ROOM FAN (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EG-HVACFN2-FAN-FTR	ITS DG B ROOM FAN 2 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EG-HVACFN2-FAN-FTS	ITS DG B ROOM FAN (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EG-HVACFN3-FAN-FTR	ITS DG B ROOM FAN 3 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EG-HVACFN3-FAN-FTS	ITS DG B ROOM FAN 3 (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EG-HVACFN4-FAN-FTR	ITS DG B FAN 4 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EG-HVACFN4-FAN-FTS	ITS DG B ROOM FAN 4 (MOTOR-DRIVEN) FAILS TO START	2.02E-03		

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
26D-##EG-STRTDGA-C72-SPO	ITS SWITCHGEAR A BATTERY CIRCUIT BREAKER (DC) SPUR OP	3.85E-04	1.07E-06	360
26D-##EG-STRTDGB-C72-SPO	13.8KV ITS SWGR BATTERY B CIRCUIT BREAKER (DC) SPUR OP	3.85E-04	1.07E-06	360
26D-##EG-WKTNK_A-TKF-FOH	ITS DG A BULK FUEL TANK (00001A) FAILS	1.58E-04	4.40E-07	360
26D-##EG-WKTNK_B-TKF-FOH	ITS DG B BULK FUEL TANK FAILS	1.58E-04	4.40E-07	360
26D-##EGBATCHRGA-BYC-FOH	ITS SWITCHGEAR A BATTERY: BATTERY CHARGER FAILURE	1.28E-03	7.60E-06	168
26D-##EGBATCHRGA-BYC-FOH	ITS DG B BATTERY CHARGER FAILURE	1.28E-03	7.60E-06	168
26D-###SWGRDGA-BUA-FOH	13.8KV ITS SWITCHGEAR A FAILURE	4.39E-04	6.10E-07	720
26D-###SWGRDGB-AHU-FTR	EDGB SWITCHGEAR ROOM AIR HANDLING UNIT FAILURE TO RUN	2.65E-03	3.68E-06	720
26D-###SWGRDGB-BUA-FOH	13.8KV ITS SWITCHGEAR B BUS FAILURE	4.39E-04	6.10E-07	720
26D-###SWGRDGA-AHU-FTR	13.8KV ITS SWITCHGEAR ROOM AIR HANDLING UNIT FAILS	2.65E-03	3.68E-06	720
26D-##EEG-HVACFA1-FAN-FTR	ITS DG A ROOM FAN 1 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EEG-HVACFA1-FAN-FTS	ITS DG A ROOM FAN 1 (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EEG-HVACFA2-FAN-FTR	ITS DG A ROOM FAN 2 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EEG-HVACFA2-FAN-FTS	ITS DG A ROOM FAN 2 (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EEG-HVACFA3-FAN-FTR	ITS DG A ROOM FAN 3 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EEG-HVACFA3-FAN-FTS	ITS DG A ROOM FAN 3 (MOTOR-DRIVEN) FAILS TO START	2.02E-03		
26D-##EEG-HVACFA4-FAN-FTR	ITS DG A ROOM FAN 4 (MOTOR-DRIVEN) FAILS TO RUN	2.56E-02	7.21E-05	360
26D-##EEG-HVACFA4-FAN-FTS	ITS DG A ROOM FAN 4 (MOTOR-DRIVEN) FAILS TO	2.02E-03		

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
	START			
26D-#EEU-208_DGA-BUD-FOH	ITS DC PANEL A DC BUS FAILURE	8.64E-05	2.40E-07	360
26D-#EEU-208_DGB-BUD-FOH	ITS DG B DC PANEL FAILURE	8.64E-05	2.40E-07	360
26D-#EEY-DGALOAD-C52-FOD	DG A LOAD BREAKER (AC) FAILS TO CLOSE	2.24E-03		
26D-#EEY-DGBLOAD-C52-FOD	ITS DG B LOAD BREAKER (AC) FAILS TO CLOSE	2.24E-03		
26D-#EEY-DGLOADS-C52-CCF	COMMON CAUSE FAILURE OF ITS DG LOAD BREAKERS TO CLOSE	1.05E-04		
26D-#EEY-ITS-DGB-#DG-FTS	DIESEL GENERATOR FAILS TO START	8.38E-03		
26D-#EEY-ITSDG-A-#DG-FTR	ITS DIESEL GENERATOR A FAILS TO RUN	7.70E-01	4.08E-03	360
26D-#EEY-ITSDG-A-#DG-FTS	DIESEL GENERATOR FAILS TO START	8.38E-03		
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B FAIL TO RUN	1.80E-02		
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A AND B TO START	3.90E-04		
26D-#EEY-ITSDGB-#DG-FTR	ITS DG B FAILS TO RUN	7.70E-01	4.08E-03	360
26D-#EEY-OB-SWGA-C52-FOD	13.8KV ITS SWGR FEED BREAKER (AC) FAILS TO OPEN	2.24E-03		
26D-#EEY-OB-SWGA-C52-SPO	13.8KV ITS SWGR A FEED BREAKER SPURIOUS OPERATION	3.82E-03	5.31E-06	720
26D-#EEY-OB-SWGB-C52-FOD	13.8KV FEED BREAKER (FROM SWYD) FAILS ON DEMAND	2.24E-03		
26D-#EEY-OB-SWGB-C52-SPO	13.8KV ITS SWGR FEED BREAKER (AC) SPURIOUS OP	3.82E-03	5.31E-06	720
26D-#EEY-OB-SWGS-C52-CCF	COMMON CAUSE FAILURE OF 13.8KV ITS SWGR FEED BREAKERS TO OPEN	1.04E-04		
26D-#EG-BATTERYB-BTR-FOD	ITS SWGR CONTROL BATTERY B NO OUTPUT	8.20E-03		
26D-#EG-LCKOUTRL-RLY-FTP	13.8KV ITS SWITCHGEAR FEED BREAKER LOCK OUT RELAY FAILS TO OPEN CB	3.15E-03	8.77E-06	360
26D-#EG-LDSQNCRB-SEQ-FOD	ITS DG B LOAD SEQUENCER FAILS	2.67E-03		
26D-#EG-LOCKOUTB-RLY-FTP	13.8 ITS SWGR LOCKOUT RELAY (POWER) FAILS TO OPEN CB	3.15E-03	8.77E-06	360

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
26D-#EGLDSQNCRA-SEQ-FOD	DG A LOAD SEQUENCER FAILS	2.67E-03		
26D-EG-BATTERYA-BTR-FOD	ITS SWITCHGEAR A BATTERY NO OUTPUT GIVEN CHALLENGE	8.20E-03		
27A-#EEE-BUS2DGA-C52-SPO	13.8KV OPEN BUS 2 ITS LOAD BREAKER SPURIOUS OPERATION	3.82E-03	5.31E-06	720
27A-#EEE-BUS3DGB-C52-SPO	13.8KV OPEN BUS 4 TO ITS B LOAD BREAKER (AC) SPURIOUS OP	3.82E-03	5.31E-06	720
27A-#EEN-OPENBS2-BUA-FOH	13.8KV OPEN BUS 2 BUS FAILURE	4.39E-04	6.10E-07	720
27A-#EEN-OPENBS4-BUA-FOH	13.8KV OPEN BUS 4 BUS FAILURE	4.39E-04	6.10E-07	720
27A-#EEN-OPNBS1A-SWP-SPO	13.8KV OPEN BUS 2 TO ITS DIV A ELECTRIC POWER SWITCH SPUR. XFER	1.12E-04	1.55E-07	720
27A-#EEN-OPNBS3B-SWP-SPO	13.8KV OPEN BUS 4 TO ITS B ELECTRIC POWER SWITCH SPUR XFER	1.12E-04	1.55E-07	720
800-FAC-WPCRNDP-CRW-DRP	WP (NON-SFP) CRANE DROP	1.05E-04		1
800-HEE0-3RDRAIL-THR-BRK	THIRD RAIL BREAKS	8.08E-08	1.01E-08	8
800-HEE0-ACTADR1-ATP-SPO	ACTUATOR SPURIOUS OP - ACCESS DOOR	7.64E-09	1.34E-06	0
800-HEE0-ACTADR2-ATP-SPO	ACTUATOR SPURIOUS OP - ACCESS DOOR	7.64E-09	1.34E-06	0
800-HEE0-ACTDR01-ATP-SPO	ACTUATOR SPURIOUS OP - TEV DOOR	5.36E-06	1.34E-06	4
800-HEE0-ACTDR02-ATP-SPO	ACTUATOR SPURIOUS OP - TEV DOOR	5.36E-06	1.34E-06	4
800-HEE0-AXSDR00-PLC-SPO	PROGRAMMABLE LOGIC CONTROLLER SPURIOUS OPERATION	2.08E-09	3.65E-07	0
800-HEE0-AXSMO01-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	7.70E-11	1.35E-08	0
800-HEE0-AXSMO02-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	7.70E-11	1.35E-08	0
800-HEE0-BEDEXTD-ATP-SPO	ACTUATOR SPURIOUS OP - TEV BASE PLATE	5.36E-06	1.34E-06	4
800-HEE0-DERAILS-DSG-DER (DER-FOH)	DRIP SHIELD GANTRY DERAILS	1.18E-05		
800-HEE0-DERAILS-TEV-DER (DER-FOH)	TEV DERAILS - PER MILE	1.18E-05		
800-HEE0-DSLIFT1-LRG-FOH	LIFTING RIG OR HOOK FAILS - DSG	7.45E-07	7.45E-07	1

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
800-HEE0-DSLIFT2-LRG-FOH	LIFTING RIG OR HOOK FAILS - DSG	7.45E-07	7.45E-07	1
800-HEE0-DSLIFT3-LRG-FOH	LIFTING RIG OR HOOK FAILS - DSG	7.45E-07	7.45E-07	1
800-HEE0-DSLIFT4-LRG-FOH	LIFTING RIG OR HOOK FAILS -DSG	7.45E-07	7.45E-07	1
800-HEE0-DSLIFTC-LRG-CCF	COMMON CAUSE FAILURE OF 2 OF 4 LIFTING RIG OR HOOKS	3.73E-09 <sup>1</sup>		
800-HEE0-FACMO01-MOE-SPO	SHIELD DOOR MOTOR #1 SPURIOUS OPERATION	6.74E-07	6.74E-07	1
800-HEE0-FACMO02-MOE-SPO	SHIELD DOOR MOTOR #2 ) SPURIOUS OPERATION	6.74E-07	6.74E-07	1
800-HEE0-FACTOR1-TL-FOH	SHIELD DOOR MOTOR #1 OVER TORQUE LIMITER FAILURE	2.86E-02	8.05E-05	360
800-HEE0-FACTOR2-TL-FOH	SHIELD DOOR MOTOR #2 OVER TORQUE LIMITER FAILURE	2.86E-02	8.05E-05	360
800-HEE0-GEARBX1-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX2-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX3-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX4-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX5-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX6-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX7-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBX8-GRB-STH	GEAR BOX STRIPPED	3.14E-07	7.86E-08	4
800-HEE0-GEARBXC-GRB-STH	COMMON CAUSE FAILURE OF TEV GEARBOXES	2.85E-09	7.12E-10	4
800-HEE0-INTRLCK-IEL-FOH	INTERLOCK FAILURE - TEV DOOR INTERLOCK	1.37E-04	3.43E-05	4
800-HEE0-JACK000-SJK-CCF	SCREW JACK CCF FAILURE	8.10E-07		
800-HEE0-JACK001-SJK-FOH	TEV SCREW JACK FAILURE	3.26E-05	8.14E-06	4
800-HEE0-JACK002-SJK-FOH	TEV SCREW JACK FAILURE	3.26E-05	8.14E-06	4
800-HEE0-JACK003-SJK-FOH	TEV SCREW JACK FAILURE	3.26E-05	8.14E-06	4
800-HEE0-JACK004-SJK-FOH	TEV SCREW JACK FAILURE	3.26E-05	8.14E-06	4
800-HEE0-LIFT000-LRG-CCF	COMMON CAUSE FAILURE OF ALL FOUR LIFTING RIG/HOOKS	7.45E-08		
800-HEE0-LIFT001-LRG-FOH	LIFTING RIG OR HOOK FAILURE	2.98E-06	7.45E-07	4
800-HEE0-LIFT002-LRG-FOH	LIFTING RIG OR HOOK FAILURE	2.98E-06	7.45E-07	4
800-HEE0-LIFT003-LRG-FOH	LIFTING RIG OR HOOK	2.98E-06	7.45E-07	4

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
	FAILURE			
800-HEE0-LIFT004-LRG-FOH	LIFTING RIG OR HOOK FAILURE	2.98E-06	7.45E-07	4
800-HEE0-MOTACT1-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT2-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT3-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT4-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT5-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT6-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT7-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACT8-ATP-SPO	ACTUATOR SPURIOUS OP - TEV MOTOR	1.34E-06	1.34E-06	1
800-HEE0-MOTACTC-ATP-CCF	CCF - TEV MOTOR ACTUATION (.009 TIMES HOURLY)	1.21E-08		
800-HEE0-MOTOR01-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR02-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR03-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR04-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR05-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR06-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR07-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-MOTOR08-MOE-FSO	MOTOR (ELECTRIC) FAILS TO SHUT OFF	5.40E-08	1.35E-08	4
800-HEE0-PLCDOOR-PLC-SPO	PLC SPURIOUS OP - TEV DOORS	1.46E-06	3.65E-07	4
800-HEE0-PLCLDR1-PLC-SPO	DRIVE CONTROLLER - PLC SPURIOUS OP	1.46E-06	3.65E-07	4
800-HEE0-PLCRETR-PLC-SPO	PLC SPURIOUS OP - WP RETRIEVAL CONTROLLER	3.65E-07	3.65E-07	1
800-HEE0-PLCSPD1-PLC-SPO	SPEED CONTROLLER - PLC SPURIOUS OP	1.46E-06	3.65E-07	4

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
800-HEE0-ROTARY1-ECP-FOH	TEV POSITION ENCODER FAILURE - 1	7.16E-06	1.79E-06	4
800-HEE0-ROTARY2-ECP-FOH	TEV POSITION ENCODER FAILURE - 2	7.16E-06	1.79E-06	4
800-HEE0-ROTARY3-ECP-FOH	TEV POSITION ENCODER FAILURE - 3	7.16E-06	1.79E-06	4
800-HEE0-ROTARY4-ECP-FOH	TEV POSITION ENCODER FAILURE - 4	7.16E-06	1.79E-06	4
800-HEE0-ROTARY5-ECP-FOH	TEV POSITION ENCODER FAILURE - 5	7.16E-06	1.79E-06	4
800-HEE0-ROTARY6-ECP-FOH	TEV POSITION ENCODER FAILURE - 6	7.16E-06	1.79E-06	4
800-HEE0-ROTARY7-ECP-FOH	TEV POSITION ENCODER FAILURE - 7	7.16E-06	1.79E-06	4
800-HEE0-ROTARY8-ECP-FOH	TEV POSITION ENCODER FAILURE - 8	7.16E-06	1.79E-06	4
800-HEE0-ROTARYC-ECP-CCF	COMMON CAUSE FAILURE OF 8 ROTARY ENCODERS	6.40E-08	1.60E-08	4
800-HEE0-SHTBLT0-PIN-CCF	COMMON CAUSE FAILURE OF 2 OR MORE TEV SHOT BOLTS	8.23E-10		
800-HEE0-SHTBLT1-PIN-FOH	TEV SHOT BOLT 1 FAILS	3.29E-08	8.23E-09	4
800-HEE0-SHTBLT2-PIN-FOH	TEV SHOT BOLT 2 FAILS	3.29E-08	8.23E-09	4
800-HEE0-SHTBLT3-PIN-FOH	TEV SHOT BOLT 3 FAILS	3.29E-08	8.23E-09	4
800-HEE0-SHTBLT4-PIN-FOH	TEV SHOT BOLT 4 FAILS	3.29E-08	8.23E-09	4
800-HEE0-SPSHFC-AXL-CCF	COMMON CAUSE FAILURE OF SPLINE SHAFT	9.60E-10	2.40E-10	4
800-SD--SRU001--SRU-FOH	SHIELD DOOR ULTRASONIC OBSTRUCTION SENSOR FAILS	9.62E-05	9.62E-05	1
800-TEV1-ECP0001-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0002-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0003-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0004-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0005-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0006-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0007-ECP-FOH	POSITION ENCODER FAILURE	7.16E-06	1.79E-06	4
800-TEV1-ECP0008-ECP-FOH	POSITION ENCODER	7.16E-06	1.79E-06	4

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

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT MEAN PROBABILITY	MEAN FAILURE RATE	MISSION TIME (HOURS)
	FAILURE			
800-TEV1-HNDSWCH-SEL-FOH	SPEED SELECTOR FAILS – HAND SWITCH INCLUDED	1.66E-05	4.16E-06	4
800-TEV1-SRS0001-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0002-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0003-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0004-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0005-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0006-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0007-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4
800-TEV1-SRS0008-SRS-FOH	OVER SPEED SENSOR FAILS	8.56E-05	2.14E-05	4

NOTE: <sup>1</sup> FOR COMMON CAUSE FAILURE OF 2 OF 4 LIFTING RIGS OR HOOKS, AN ALPHA OF 0.0213 SHOULD APPLY. IT APPEARS THAT AN ALPHA OF 0.00528 WAS USED. THE FAILURE RATE IS SO SMALL THAT THE INCORRECT VALUE HAS NO IMPACT ON THE OVERALL RESULTS.

AC = ALTERNATING CURRENT; AHU = AIR-HANDLING UNIT; CCF = COMMON-CAUSE FAILURE; CRCF = CANISTER RECEIPT AND CLOSURE FACILITY; CTM = CANISTER TRANSFER MACHINE; DG = DIESEL GENERATOR; ELEC = ELECTRICAL; EXH = EXHAUST; HEPA = HIGH-EFFICIENCY PARTICULATE AIR; ITS = IMPORTANT TO SAFETY; MCC = MOTOR CONTROL CENTER; PLC = PROGRAMMABLE LOGIC CONTROLLER; SFP = SPENT FUEL POOL; SPMRC = SITE PRIME MOVER RAILCAR; SPMTT = SITE PRIME MOVER TRUCK TRAILER; ST = SITE TRANSPORTER; WP = WASTE PACKAGE; WPTT = WASTE PACKAGE TRANSFER TROLLEY; XFER = TRANSFER.

**SOURCE:**

**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. 2.2.73), the methodology essentially consists of comparing the demand upon the equipment to a capacity curve. The probability of failure is the value of the cumulative distribution function for the capacity curve, evaluated at the demand upon the container. More detailed discussion is presented in Attachment D, Section D1. The methodology is applicable to all of the waste containers that are processed, including transportation casks, aging overpacks, canisters, and waste packages. As described in Section 4.3.2.2, the condition at which a passive component is said to fail depends on the success criteria defined for the component. Passive components are designed and manufactured to ensure that the success criteria are met in normal operating conditions and with margin, to ensure that the success criteria are also met when subjected to abnormal loads, including those expected during event sequences. The design margins, and in some cases materials, may be dictated by the code and standards applied to a given type of container as characterized by tensile elongation data for impact loads and by strength at temperature data for thermal loads.

As described in Sections 4.3.2.2, the probability of a passive failure is often based on consideration of variability (uncertainty) in the applied load, and the variability in the strength (resistance) of the component. The variability in the physical and thermal loading are derived from the systems analysis that defines the probabilities of physical or thermal loads of a given magnitude in a given event sequence. Such conditions arise from the event sequence analysis described in Section 6.1. For the analysis of the effects of fires on waste containers, probability distributions were developed for both the load and the response. For drops and impacts, however, an event sequence analysis is used to define conservative conditions for the load rather than deal with possible ranges of such parameters. Therefore, the calculation of the probability of passive failures is based on the response or resistance characteristics of the container, given the conservative point value for the drop or impact load defined for a given event sequence.

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

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

- *Seismic and Structural Container Analysis for the PCSA* (Ref. 2.2.39)
- *Structural Analysis Results of the DOE SNF Canisters Subjected to the 23-foot Vertical Repository Drop Event to Support Probabilistic Risk Evaluations* (Ref. 2.2.82) and *Qualitative Analysis of the Standardized DOE SNF Canister for Specific Canister-on-Canister Drop Events at the Repository* (Ref. 2.2.81)
- *Naval Long Waste Package Vertical Impact on Emplacement Pallet and Invert* (Ref.2.2.25)

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

Failure probabilities for drops are summarized in Table 6.3-2. Conservative representations of drop height are defined for operations with each type of container. Sometimes more than one conservative drop height is specified, for example, for normal height crane lifts and two-block height crane lift. LLNL predicts failure probabilities of  $<1.0 \times 10^{-8}$  for most of the events (Ref. 2.2.39). If a probability for the event sequence is less than  $1 \times 10^{-8}$ , 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 calculates strains by modeling representative casks, aging overpacks, and canisters that encompass TAD canisters, naval SNF canisters, and a variety of DPCs with the dynamic finite element code, LSDyna (Ref. 2.2.39). For these canisters, only flat-bottom drops are considered to model transfers by a CTM. This is justified because these canisters fit sufficiently tightly within the CTM and potential dropped canisters are guided by the canister guide sleeve of the CTM to remain in a vertical position.

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

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

	Drop Height (ft)	Failure Probability	Note
Waste package	2	$1.0 \times 10^{-5}$	BSC FEA, horizontal orientation

NOTE: BSC = Bechtel SAIC; FEA=finite element analysis.

Source: Attachment D, Table D1.4-1.

Containment failure probabilities due to other physical impact conditions, equivalent to drops, are listed in Table 6.3-3. These probabilities were modeled by LLNL using FEA, resulting in prediction of failure probabilities of  $<1.0 \times 10^{-8}$ . Again, additional conservatism was incorporated by using a failure probability of  $1.0 \times 10^{-5}$  for most of these events. The side impact event was not adjusted from the LLNL result of  $< 1.0 \times 10^{-8}$  because of the very low velocities involved. A comparison of the strains induced by drops and slow speed, side impacts indicates significantly lower strains for the low velocity impacts.

Table 6.3-3.Failure Probabilities Due to Miscellaneous Events

Event	Failure Probability	Note
Derail	$1.0 \times 10^{-5}$	LLNL, adjusted, analogous to 6', 3° from horizontal

Rollover	$1.0 \times 10^{-5}$	LLNL, adjusted, analogous to 6', 3° from horizontal
Drop on	$1.0 \times 10^{-5}$	LLNL, adjusted 10-metric-ton load onto container
Tip over	$1.0 \times 10^{-5}$	LLNL, adjusted, analogous to 13.1-foot drop plus slap-down
Side Impact from collision with rigid surface	$1.0 \times 10^{-8}$	Or value for low speed collision, whichever is greater (Table 6.3-4) Crane moving 20 ft/min
Tilt down/Up	$1.0 \times 10^{-5}$	LLNL, adjusted; Bounded by slap-down

NOTE: LLNL = Lawrence Livermore National Laboratory.

Source: Attachment D.

Table 6.3-4 shows failure probabilities for various collision events for various containers as a function of impact speed. For each of the events, the collision speed, whether in 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 of gravity.

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

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

where

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

The probabilities of failure for the collision cases listed in Table 6.3-4 are then determined using the above formula with  $H_m$  determined above and with  $H_d$  being the drop height corresponding to the collision speed as listed in Table 6.3-4.

Two-blocking events are also included in Table 6.3-4. The failure probabilities of these events are shown in *PEFA Chart.xls* included in Attachment H. The CTM, which lifts canisters, is designed such that drops from the height associated with two-blocking is very low probability and no higher than drops from normal operation. The design features that ensure this are: slide gate closure and two levels of shut-off switches as the normal lift height is exceeded, and a tension relief device that prevents over tensioning of hoist cables if the two-block height is reached. Transportation cask handling cranes are also equipped with the shut-off switches and the tension relief device.

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

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

NOTE: <sup>a</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.

CTM = canister transfer machine; CTT = cask transfer trolley; ft = feet; MCO = multicask overpack; min = minutes; mph = miles per hour; sec = seconds; ST = site transporter; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Attachment D

### 6.3.2.3 Probability of Canister Failure in a Fire

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

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

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

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

To determine whether the temperature reached by a waste form container is sufficient to cause the container to fail, the fire fragility distribution curve for the container is evaluated. In the PCSA, this curve is expressed as the probability of breach of the container as a function of its temperature. Two failure modes are considered for a container that is subjected to a thermal challenge: creep-induced failure and limit load failure. Creep, the plastic deformation that takes

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

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

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

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

Configuration <sup>b</sup>	Failure Probability	
	Mean	Standard Deviation
Thin-Walled Canister in a Waste Package <sup>a</sup>	$3.2 \times 10^{-4}$	$5.7 \times 10^{-5}$
Thick-Walled Canister in a Waste Package <sup>a</sup>	$1.0 \times 10^{-4}$	$2.2 \times 10^{-5}$
Thin-Walled Canister in a Transport Cask	$2.0 \times 10^{-6}$	$1.4 \times 10^{-6}$
Thick-Walled Canister in a Transport Cask	$1.0 \times 10^{-6}$	$1.0 \times 10^{-6}$
Thin-Walled Canister in a Shielded Bell	$1.4 \times 10^{-4}$	$2.6 \times 10^{-5}$
Thick-Walled Canister in a Shielded Bell	$9.0 \times 10^{-5}$	$1.7 \times 10^{-5}$

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 the 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, so that failures for these configurations can be screened. For conservatism, a screening conditional probability of  $1 \times 10^{-6}$  could be used.

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

Note that, no failure probability is provided for a bare canister configuration. The reason for this is that the canister is outside of a waste package or cask for only a short time. During that time, the canister is usually inside the shielded bell of the CTM. The preceding analysis addressed a fire outside the shielded bell. When in that configuration, the canister is shielded from the direct effects of the fire. A fire inside the shielded bell, which could directly heat the canister, is not considered to be credible for two reasons. First, the hydraulic fluid used in the CTM equipment is non-flammable and no other combustible material could be present inside the bell to cause a fire. Second, the annular gap between the canister and the bell is only 3 inches wide, but is approximately 27 feet long. Given this configuration, it is unlikely that there 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, 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 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 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 is exposed to the fire. Furthermore, this exposure would only be for the short time that the canister was in motion.

For these reasons, failure of a bare canister was not considered credible and is not explicitly modeled in the PCSA.

#### **6.3.2.4 Probability of Loss of Containment from Heatup**

In addition to fire-related passive failures, the PCSA considered other passive equipment failures due to abnormal thermal conditions. The thermal event of greatest concern for the surface facilities is loss of HVAC cooling. If HVAC cooling is lost, the ambient temperature in the facility will increase. This increase is particularly significant for relatively small enclosures such as the transfer cells.

A series of bounding calculations was performed to determine the maximum temperature that could be reached by a canister following loss of HVAC cooling (Ref. 2.2.12). These calculations consider a range of decay heat levels and a loss of cooling for 30 days. These analyses indicate that the canister temperature would remain well below 500°C (773°K) (Ref. 2.2.12). This temperature is hundreds of degrees below the temperature at which the canister would fail (see Figure D2.1-4 Attachment D). For that reason, canister failure due to a loss of HVAC is physically unrealizable and considered beyond Category 2.

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

Loss or degradation of shielding probabilities is summarized in Table 6.3-6.

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

shielding function, sealed transportation casks and shielded transfer casks exert a containment function. Only those items used in the WHF are discussed further.

A structural challenge may cause shielding degradation or shielding loss. Loss of shielding occurs when an SSC fails in a manner that leaves a direct path for radiation to stream, for example as a result of a breach. Degradation of shielding occurs when a shielding SSC is not breached but its shielding function is degraded. In the PCSA, a shielding degradation probability after a structural challenge is derived for those transportation casks that employ lead for shielding. Finite-element analyses on the behavior of transportation casks subjected to impacts associated with various collision speeds, reported in *Reexamination of Spent Fuel Shipment Risk Estimates*, NUREG/CR-6672 (Ref. 2.2.83), indicate that lead slumping after an end impact could result in a reduction of shielding; transportation casks without lead are not susceptible to such shielding degradation. This information is used in Attachment D to derive the shielding degradation probability of a transportation cask at drop heights characteristic of crane operations. The distribution is developed for impacts on surfaces made of concrete, which compare to the surfaces onto which drops could occur at the GROA. No impact limiter is relied upon to limit the severity of the impact. Conservatively, the distribution is applied to transportation casks and also shielded transfer casks, regardless of whether or not they use lead for shielding. Thus, for containers that have both a containment and shielding function, the PCSA considers a probability of containment failure (which is considered to result in a concurrent loss of shielding), and also a probability of shielding degradation (which is associated with those structural challenges that are not sufficiently severe to cause loss of containment). Table 6.3-6 displays the resulting shielding degradation probabilities for transportation casks and shielded transfer casks after a structural challenge. Given that there is significant conservatism in the calculation of strain and the uncertainty associated with the fragility (strength), the resulting estimates include uncertainties and are considered conservative

Shielding loss is also considered to potentially affect an aging overpack subjected to a structural challenge, if the waste form container inside does not breach. Given the robustness of aging overpacks, a shielding loss after a 3-ft drop height is calculated to have a probability of  $5 \times 10^{-6}$  per aging overpack impact, based upon the judgment that this probability may be conservatively related to but lower than the probability of breach of an unprotected waste form container inside the aging overpack (Attachment D). If the structural challenge is sufficiently severe to cause the loss of containment (breach) of the waste form container inside the aging overpack, the loss of the aging overpack shielding function is considered guaranteed to occur.

A CTM provides shielding with the shield bell, shield skirt, and associated slide gates. Also, the CTM is surrounded by shield walls and doors, which are unaffected by structural challenges resulting from internal random initiating events. Therefore, such challenges leave the shielding function intact.

The PCSA treats the degradation or loss of shielding of an SSC due to a thermal challenge as described in the following paragraphs:

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

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

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

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

Table 6.3-6. Probabilities of Degradation or Loss of Shielding

	Probability	Note
Sealed transportation cask and shielded transfer casks shielding degradation after structural challenge	$1 \times 10^{-5}$	Section D, Section D3.4.
Aging overpack shielding loss after structural challenge	$5 \times 10^{-6}$	Section D, Section D3.4
CTM shielding loss after structural challenge	0	Structural challenges sufficiently mild to leave the shielding function intact
Shielding loss by fire for waste forms in transportation casks or shielded transfer casks	1	Lead shielding could potentially expand and degrade. This probability is conservatively applied to transportation casks and STCs that do not use lead for shielding.
Shielded loss by fire for aging overpacks and CTM shield bell	0	Type of concrete used for aging overpacks is not sensitive to spallation; Uranium used in CTM shield bell shielding does not lose its shielding function as a result of a fire.

NOTE: CTM = canister transfer machine.

Source: Attachment D, Table D3.4-1.

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

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

### 6.3.2.7 Application to Event Sequence Models

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

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

Table 6.3-7. Summary of Passive Event Failure Probabilities

	10 T DROPPED ON CONTAINER	CONTAINER VERTICAL DROP FROM NORMAL OPERATING HEIGHT	CONTAINER 30-FOOT VERTICAL DROP	CONTAINER 45-FOOT VERTICAL DROP	2-FOOT HORIZONTAL DROP, ROLLOVER	2.5 MPH FLAT SIDE IMPACT/ COLLISION	2.5 MPH LOCALIZED SIDE IMPACT/ COLLISION	9 MPH FLAT SIDE IMPACT/ COLLISION	2.5 MPH END- TO-END COLLISION	9 MPH END- TO-END COLLISION	SLAPDOWN (BOUNDS TIP OVER)	THIN- WALLED CANISTER FIRE	THICK- WALLED CANISTER FIRE
LOSS OF CONTAINMENT													
WASTE PACKAGE	1.E-05	N/A	N/A	N/A	1.E-05	1.E-08	N/A	1.E-08	1.E-05	N/A	NO CHALLENGE	3.E-04	1.E-04
LOSS OF SHIELDING													
TEV	NO CHALLENGE	NO CHALLENGE	N/A	N/A	NO CHALLENGE	NO CHALLENGE	N/A	NO CHALLENGE	NO CHALLENGE	NO CHALLENGE	NO CHALLENGE	~ 0	~ 0

NOTE: N/A = NOT APPLICABLE, NO SCENARIOS IDENTIFIED.  
SOURCE: ATTACHMENT D.

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

Basic Event (BE) ID	Basic Event Description	BE Value	Basis
SSO-ESD-01 - CRCF			
WP impact facility shield door (sequence 2)	Failure of Waste Package due to facility shield door impact	1.00E-08	Table 6.3-7. WP 2.5-mph flat side impact
TEV shielding (sequences 2, 3, 4, 5, 6)	Loss of gamma shielding	0.00E+00	No challenge to TEV gamma shielding due to physical impact
Canister containment (sequences 2, 3, 4, 5, 6)	Canister containment fails when WP containment fails	1.00E+00	No credit taken for canister containment when Waste Package fails, so conditional probability set to 1
WP impact TEV shield door (sequence 3)	Failure of Waste Package due to TEV shield door impact	1.00E-08	Table 6.3-7. WP 2.5-mph flat side impact
WP TEV collision (sequence 4)	Failure of Waste Package due to TEV collision	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
WP drop (sequence 5)	Failure of Waste Package due to drop of Waste Package	1.00E-05	Table 6.3-7. WP horizontal drop
Heavy load drop on WP (sequence 6)	Failure of Waste Package due to drop of heavy load onto Waste Package	1.00E-05	Table 6.3-7. 10 T dropped on WP
SSO-ESD-01 - IHF			
WP impact facility shield door (sequence 2)	Failure of Waste Package due to facility shield door impact	1.00E-08	Table 6.3-7. WP 2.5-mph flat side impact
TEV shielding (sequences 2, 3, 4, 5, 6)	Loss of gamma shielding for canister	0.00E+00	No challenge to TEV gamma shielding due to physical impact
Canister containment (sequences 2, 3, 4, 5, 6)	Canister containment fails when TEV containment fails	1.00E+00	No credit taken for canister containment when Waste Package fails
WP impact TEV shield door (sequence 3)	Failure of Waste Package due to TEV shield door impact	1.00E-08	Table 6.3-7. WP 2.5-mph flat side impact
WP TEV collision (sequence 4)	Failure of Waste Package due to TEV collision	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
WP drop (sequence 5)	Failure of Waste Package due to drop of Waste Package	1.00E-05	Table 6.3-7. WP horizontal drop
Heavy load drop on WP (sequence 6)	Failure of Waste Package due to drop of heavy load onto Waste Package	1.00E-05	Table 6.3-7. 10 T dropped on WP
SSO-ESD-02			

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

Basic Event (BE) ID	Basic Event Description	BE Value	Basis
TEV impact (sequence 2)	Failure of WP due to TEV impact, collision, or derailment	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
TEV shielding (sequences 2, 3, 4, 5)	Loss of gamma shielding	0.00E+00	No challenge to TEV gamma shielding due to physical impact
Canister containment (sequences 2, 3, 4, 5)	Canister containment fails when WP containment fails	1.00E+00	No credit taken for canister containment when Waste Package fails, so conditional probability set to 1
TEV impact during transit (sequence 3)	Failure of WP due to TEV impact during transit	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
WP drop during transit (sequence 4)	Failure of Waste Package due to drop of Waste Package during transit	1.00E-05	Table 6.3-7. WP horizontal drop
Heavy load drop on TEV (sequence 5)	Failure of Waste Package due to drop of heavy load onto TEV	1.00E-05	Table 6.3-7. 10 T dropped on WP
SSO-ESD-03			
TEV impact (sequence 2)	Failure of WP due to TEV impact, collision, or derailment	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
TEV shielding (sequences 2, 3, 4, 5, 6, 7)	Loss of gamma shielding	0.00E+00	No challenge to TEV gamma shielding due to physical impact
Canister containment (sequences 2, 3, 4, 5, 6, 7)	Canister containment fails when WP containment fails	1.00E+00	No credit taken for canister containment when Waste Package fails, so conditional probability set to 1
Direct impact to WP – collision (sequence 3)	Waste Package containment fails due to direct impact during collision	1.00E-08	Table 6.3-7. WP 2.5-mph flat side collision
Drop or drag of WP (sequence 4)	Waste Package fails due to drop or drag	1.00E-05	Table 6.3-7. WP horizontal drop
Heavy load drop on TEV (sequence 5)	Failure of Waste Package due to drop of heavy load onto TEV	1.00E-05	Table 6.3-7. 10 T dropped on WP
WP impact due to TEV doors (sequence 6)	Failure of Waste Package due to impact by TEV doors	1.00E-08	Table 6.3-7. WP 2.5-mph flat side impact
Heavy load drop on WP (sequence 7)	Failure of Waste Package due to drop of heavy load onto WP	1.00E-05	Table 6.3-7. 10 T dropped on WP
SSO-ESD-04			

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

Basic Event (BE) ID	Basic Event Description	BE Value	Basis
Inadvertent entry No passive equipment failure (sequence 2)	Worker exposure due to inadvertent entry into active drift		
Prolonged worker proximity No passive equipment failure (sequence 3)	Worker exposure due to prolonged stay in proximity to TEV		
Inadvertent TEV door opening No passive equipment failure (sequence 4)	Worker exposure due to inadvertent opening of TEV shield door		
Loss of movement loss of shielding (sequence 5)	Loss of gamma shielding due to loss of TEV movement	0.00E+00	No challenge to TEV gamma shielding due to prolonged exposure to sun (see Section 6.0)
SSO-ESD-05			
TEV fire affects WP (sequences 2, 3, 4)	Waste Package failure due to fire engulfing TEV in drift	1.00E+00	Canister failure causes WP failure, so conditional probability set to 1
TEV shielding (sequences 2, 3, 4)	Loss of gamma shielding	0.00E+00	No challenge to TEV gamma shielding due to fire
Canister containment (sequences 2, 3, 4)	Canister containment fails when WP containment fails	3.20E-04	Thin-walled canister failure due to fire

NOTE: Refer to Attachment D for discussion.  
PEFA = passive equipment failure analysis; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

### 6.3.3 Miscellaneous Data

Data that is not defined as Active Component Reliability Data (Section 6.3.1) or Passive Equipment Failure Data (Section 6.3.2), but are used in the reliability analysis for this facility are listed in Table 6.3-9.

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
No. of WPs	Number of Waste Packages	12,268	This basic event represents the number of waste packages emplaced during the preclosure period. The value for this basic event is obtained by adding the number of waste packages from the CRCF (11,668) and from the IHF (600) which is documented in the throughput analysis. However the throughput analysis also shows a total number of waste packages of 12,068 assigned for the Subsurface Operations. The value of 12,268 used here is a conservative estimate.	<i>Waste Form Throughputs for Preclosure Safety Analysis</i> (Ref. 2.2.31) (Analyzed a value greater than listed in the reference.)
800-TRANSIT-ROCKFALL	Rockfall Probability (captured in seismic analysis)	0.00E+00	Rockfall impacting the TEV or WP is analyzed in the seismic analysis, and thus, no further analysis is evaluated in this report. The sequence is screened from further analysis, and the basic event is set to 0.	<i>Seismic Event Sequence Quantification and Categorization</i> (Ref 2.4.4)
ROCKFALL-ON-WP	Rockfall on WP in drift (bound by seismic anal.)	0.00E+00	Rockfall impacting the TEV or WP is analyzed in the seismic analysis, and thus, no further analysis is evaluated in this report. The sequence is screened from further analysis, and the basic event is set to 0.	<i>Seismic Event Sequence Quantification and Categorization</i> (Ref 2.4.4)
ROCKFALL-TEV	Rockfall on TEV subsurface (addressed in seismic)	0.00E+00	Rockfall impacting the TEV or WP is analyzed in the seismic analysis, and thus, no further analysis is evaluated in this report. The sequence is screened from further analysis, and the basic event is set to 0.	<i>Seismic Event Sequence Quantification and Categorization</i> (Ref 2.4.4)
FIRE-IN-DRIFT	Large Fire in the Drift (Total frequency divided by 3)	3.0E-07	Large fire frequency of 9E-7 (fire/ operations) is equally contributed by a large fire occurring in the three areas where the TEV and the WP might be present. Thus, the large fire frequency in the drift is 1/3 of the total large fire frequency or 3E-7 (fire/operations)	Section 6.5

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
FIRE-IN-SUBSURFACE	Large Fire in Subsurface (Total fire frequency divided by 3)	3.0E-07	Large fire frequency of 9E-7 (fire/ operations) is equally contributed by a large fire occurring in the three areas where the TEV and the WP might be present. Thus, the large fire frequency in subsurface is 1/3 of the total large fire frequency or 3E-7 (fire/operations)	Section 6.5
FIRE-ON-SURFACE	Large Fire on the Surface (Total fire frequency divided by 3)	3.0E-07	Large fire frequency of 9E-7 (fire/ operations) is equally contributed by a large fire occurring in the three areas where the TEV and the WP might be present. Thus, the large fire frequency on the surface is 1/3 of the total large fire frequency or 3E-7 (fire/operations)	Section 6.5
060-VCTO-DRS0000-DRS-OPN	Vestibule Door Open During Receipt/Export	1.60E-04	During receipt of a transportation cask or aging overpack or during the export of a waste package or aging overpack, delta pressure is lost for a period of time not to exceed 7 minutes per event (this is a conservative estimate of the time it will take for the HVAC system to return the vestibule to a negative pressure). This occurs as a direct consequence of opening vestibule doors to allow the site transporter, the site prime mover or the transport and emplacement vehicle.	Attachment B, Section B2
800-TRANSIT-TIME	Transit time from entrance to emplacement drift in yrs	2.20E-04	This basic event represents the transit time between the facility and the drift, which is estimated at 2 hours or 2.2E-4 year. This is based on an average TEV speed of 150 feet per minute and a longest distance of 3.4 miles.	(Ref. 2.2.27) (Ref. 2.2.24)
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS Maintenance	1.95E-03	Diesel Generator A out of service for maintenance	Attachment B, Section B3
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS Maintenance	1.95E-03	Diesel generator B out of service for maintenance	Attachment B, Section B3
LOSP	Loss of offsite power	2.99E-03	Frequency of loss of off site power 3.6E-2/yr or 4.1E-6/hr, multiplied by 720 hours (30 days) for diesels in HVAC system	(Ref. 2.2.48), (Ref. 2.2.33, Attachment B, Sections B7 and B8)

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
060-VCTO-TRAINB-MAINT	Train B HVAC is Off-Line for Maintenance	4.57E-03		Attachment B, Section B2
060-EXCESSIVE-WIND-SPEED	Sustained Wind Exceeds 40 MPH & Gust to 90 MPH	4.70E-03	Sustained wind with speed exceeding 40 MPH and gust to 90 MPH has an estimated frequency of 5.7E-02 per yr, and with a mission time of 720 hours, the probability of such an occurrence is 4.7E-3.	(Ref. 2.2.30)
060-VCOO-NITS-PWR-FAILS	Non-ITS Power Failure to CRCF Supply Fan	3.54E-02	This basic event is the loss of offsite power frequency given in NUREG/CR-6890.	(Ref. 2.2.48)
DSG-MILES	Miles drip shield gantry travels	1.00E-01	This value represents the number of miles that the drip shield gantry will travel in subsurface during normal operations.	Attachment B, Section B1
TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.00E-01	Although the TEV operations are totally conducted remotely and controlled by the DCMIS, there are occasions that manual controls of TEV may be required. Thus, it is conservatively assigned a fraction of 10% of the TEV operations is conducted manually.	Attachment B, Section B1
TEV-DECLINE	TEV on decline	5.00E-01	The longest distance between the entrance and the emplacement drift is 3.4 miles (Ref. 2.2.26) or (3.4 miles * 5280 ft/mile) about 18,000 ft. Based on Ref 2.2.95, the incline from the entrance to the end of the incline is about 2642 m or about 8700 ft. Thus, the fraction of the incline in relation to the total subsurface distance is (8700 ft / 18000 ft) 0.48 or about 0.5	(Ref. 2.2.28) (Ref.2.2.11)
060-VCTO-CONTDOORS-OPEN	Vestibule Doors Open Receipt or Export from CRCF	1.00E+00	Set as "TRUE" that the vestibule doors are open during receipt or export of a TC or AO	Attachment B, Section B2
TEV-DERAIL-MILES-SURF	Miles travelled by TEV on surface	2.00E+00	This value represents the number of miles that the TEV will travel on the surface during normal operations.	(Ref. 2.2.32)
TEV-DERAIL-MILES-DRIFT	Miles travelled by TEV in subsurface	4.00E+00	This value represents the number of miles that the TEV will travel in subsurface during normal operations. The distance is 3.4 miles, but it is conservatively rounded up to 4 miles	(Ref. 2.2.26)

Table 6.3-9. Miscellaneous Data Used In the Reliability Analysis (Continued)

Basic Event (BE) ID	Basic Event Description	BE Value	Bases	References
MODERATOR - CRCF	Moderator present	2.10E-05	This value is based on either water or oil being present as a potential moderator while the WP is in the CRCF. Water moderator sources other than inadvertent actuation of the fire suppression system is estimated at 2E-5 for the CRCF. Another water source in the CRCF is the inadvertent actuation of the fire suppression system, which has a calculated probability of 1E-6. The value of Moderator is the sum of these two moderator sources.	Section 6.2.2.8
MODERATOR - IHF	Moderator present	1.50E-03	This value is based on either water or oil being present as a potential moderator while the WP is in the IHF. Water moderator sources other than inadvertent actuation of the fire suppression system is estimated at 1.4E-3 for the IHF. Another water source in the IHF is the inadvertent actuation of the fire suppression system, which has a calculated probability of 9E-7. The value of Moderator is the sum of these two moderator sources.	Section 6.2.2.8
Generic Mission time	Generic Mission time	720 hrs	Under most all scenarios identified in the reliability analysis for this facility, post accident response time is limited to 720 hours per ISG-03 and NUREG 0800. Thus, all systems that are required to function during post accident period are assigned with a mission time of 720 hours.	(Ref. 2.2.89) (Ref. 2.2.67)

NOTE: WP =waste package; TEV = Transport and Emplacement Vehicle.

Source: Original

## 6.4 HUMAN RELIABILITY ANALYSIS

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

### 6.4.1 HRA Scope

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

1. HFES are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers. Such scenarios may include the need for mitigation of radionuclides, for example, provided by the confinement HVAC system.
2. Pursuant to the above, the following types of HFES are excluded:
  - A. HFES resulting in standard industrial injuries (e.g., falls)
  - B. HFES resulting in the release of hazardous nonradioactive materials, regardless of amount
  - C. HFES resulting solely in delays to or losses of process availability, capacity, or efficiency.
3. The identification of HFES is restricted to those areas of the facility that handle waste forms, and only during the times that waste forms are being handled (e.g., HFES are not identified for the surface transportation of empty TEVs when there are no loaded TEVs on the surface).
4. The exception to #3 is that system-level HFES are considered for support systems (e.g., electrical power for confinement HVAC) when those HFES could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.
5. Post-initiator actions (as defined in Attachment E, Section E5.1.1.1) are not credited in the analysis; therefore, HFES associated with them are not considered.
6. In accordance with Section 4.2.10.1 (on boundary conditions of the PCSA), initiating events associated with conditions introduced in SSCs before they reach the site are not, by definition of 10 CFR 63.2 (Ref. 2.3.2) within the scope of the PCSA nor, by extension, within the scope of the HRA.

### 6.4.2 Base Case Scenarios

The first step in this analysis is to describe Subsurface 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. Subsurface Operations are significantly less complicated than a set of facility operations; therefore, the entire set of Subsurface Operations is analyzed as one group of operations. Figure E6.4-1 below provides an overview of Subsurface Operations.



NOTE: CRCF = Canister Receipt and Closure Facility; IHF = Initial Handling Facility; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Figure 6.4-1. Subsurface Operations

For each block of Figure 6.4-1, a base case scenario is developed and documented. The base case scenario represents the most 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, procedural controls, etc.).

### 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.

<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.

Each of these types of HFEs is defined in Attachment E, Section E5.1.1.1. The PCSA model was developed and quantified with pre-initiator and human-induced initiator HFEs in the model. The safety philosophy of waste handling operations is that an operator need not take any action after an initiating event and there are no actions identified that could exacerbate the consequences of an initiating event. This stems from the definitions and modeling of initiating events and subsequent pivotal events as described in Section 6.1 and Attachment A. All initiating events are proximal causes of either radionuclide release or direct exposure to personnel. With respect to the latter, personnel evacuation was not considered in reducing the frequency of direct exposure but personnel action could cause an initiating event. With respect to the former, pivotal events address containment integrity, confinement availability, shielding integrity, and moderator availability that have no post-initiator human interactions. Containment and shielding integrity are associated only with the physical robustness of the waste containers. Confinement availability is associated with a continuously operating HVAC and the status of equipment confinement doors. Human interactions for HVAC are pre-initiator. Human actions for shielding are associated with the initiator phase. Moreover, recovery post-initiator HFEs were not identified and not relied upon to reduce event sequence frequency. Thus, the focus of the HRA task is to support the other PCSA tasks to identify these two HFE phases.

### **Pre-Initiator HFEs**

Pre-initiators are identified by the system analysts when modeling fault trees during the system analysis task. Special attention is paid to the possibility that an error can be repeated in similar redundant components or trains, leading to a human CCF.

### **Human-Induced Initiator HFEs**

Human-induced initiator HFEs are identified through an iterative process whereby the human reliability analysts, in conjunction with other PCSA analysts and engineering and operations personnel, meet and discuss the design and operations of the facility and the SSCs in order to appropriately model the human interface. This iterative process began with the HAZOP evaluation, the MLD and event sequence development, and the event tree and fault tree modeling, and it culminated in the preliminary analysis and incorporation of HFEs into the model. Included in this process is an extensive information collection process where subject matter experts (i.e. from the Engineering and Operations departments) were interviewed in conjunction with examination of the engineering design drawings, concept of operations document and other available documentation. HFEs identified include both EOOs and EOCs.

The result of this identification process is a list of HFEs and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., PSFs). This combination of conditions and human factors concerns then becomes the EFC for a specific HFE. Additions and refinements to these initial EFCs are made during the preliminary and detailed analyses.

#### 6.4.4 Preliminary Analysis

A preliminary analysis is performed to allow HRA resources for the detailed analyses to be focused on only the most risk-significant HFEs. The preliminary analysis includes verification of the validity of HFEs included in the initial PCSA model, assignment of conservative HEPs to all HFEs and verification of those probabilities. The actual quantification of preliminary values is a six-step process that is described in detail in Appendix E.III of Attachment E. Once the preliminary probabilities are assigned, the PCSA model is quantified (initial quantification) to determine which HFEs require a detailed quantification. HFEs are identified for a detailed analysis if (1) the HFE is a risk-driver for a dominant sequence, and (2) using the preliminary values, an aggregated event sequence is above Category 1 or Category 2 according to 10 CFR 63.111 (Ref. 2.3.2) performance objectives.

In cases where HFEs are completely mitigated by hardware (i.e., interlocks), the HFE is generally assigned a value of 1.0 unless otherwise noted, and the hardware is modeled explicitly in the fault tree.

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

Detailed HRA quantification is performed for those HFEs that were found in dominant event sequences after the initial fault tree or event sequence quantification. The preliminary values were sufficient to demonstrate compliance with the performance objectives of 10 CFR 63.111 (Ref. 2.3.2); therefore no detailed analyses were performed for this HRA.

#### 6.4.6 Human Failure Event Probabilities used in Subsurface 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
060-#EEE-LDCNTRA-BUA-ROE	Operator Fails to Restore Load Center A Post Maintenance	1	1.03E-05	10	Preliminary
060-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore Load Center B Post Maintenance	1	1.03E-05	10	Preliminary
060-VCTO-DR00001-HFI-NOD	Operators Open Two or More Vestibule Doors in CRCF	1	1E-02	3	Preliminary
060-VCTO-HFIA000-HFI-NOM	Human Error: Exhaust Fan Switch in Wrong Position	1	1E-01	3	Preliminary

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
060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1	1.0	N/A	Preliminary
26D-#EEY-ITSDG-A-#DG-RSS	Operator Fails to Restore Diesel Generator A to Service	1	1.95E-04	10	Preliminary
26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator B to Service	1	1.95E-04	10	Preliminary
800-HEE0-WKRDRFT-HFI-NOD	Worker Enters Drift from Access Main	4	N/A <sup>b</sup>	N/A	Omitted from Analysis
800-HEE0-WKRPROX-HFI-NOD	Worker Stands too Close to TEV for an Extended Period of Time	4	N/A <sup>b</sup>	N/A	Omitted from Analysis
800-HEE0-WKRFACD-HFI-NOD	Operator Causes Collision of TEV with Facility Doors	1	2.0E-03	5	Preliminary
800-HEE0-SIDEIMP-HFI-NOW	Operator Causes Collision of TEV with SSC	2	3.0E-04	10	Preliminary
800-HEE0-TEVDOOR-HFI-NOD	Human Error Causes TEV Doors to Open during Transit	4	1.0E-03	5	Preliminary
800-HEE0-AXSDR00-HFI-NOD	Operator Causes Collision of TEV with Access Doors	2, 3	2.0E-03	5	Preliminary
800-HEE0-IMPACT-HFI-NOD	Human Error Causes TEV to Impact WP in the Drift	3	1.0E-03	5	Preliminary
Drip shield emplacement	Operator Error Causes Impact to WP during Drip Shield Emplacement	3	N/A <sup>b</sup>	N/A	Omitted from Analysis
HFE-RUNAWAY-RESPONSE	Operator Fails to Stop TEV Using Manual Override during a Runaway Event	1, 2, 3	N/A <sup>b</sup>	N/A	Omitted from Analysis

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
OP-FAILS-ENDOFRAIL	Operator Error Causes TEV to Run Over End of Rail	2, 3	1.0E-03	5	Preliminary
TEV derailment	Operator Causes TEV to Derail as It Travels between the Facility and the Drifts	2, 3	N/A <sup>a, b</sup>	N/A	Historical Data

NOTE: <sup>a</sup> HRA value replaced by use of historic data (see Attachment C on active component failure data).  
<sup>b</sup> These HFEs were initially identified, but omitted from analysis for various reasons, including a design change precluding the human failure, or the failure would require a series of unsafe actions in combination with mechanical failures, such that the event is no longer credible. See the appropriate HFE group in Attachment E for a case-by-case justification for these omissions.

CRCF = Canister Receipt and Closure Facility; ESD = event sequence diagram; HEPA = high-efficiency particulate air filter; HFE = human failure event; N/A = not applicable; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

## 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 a part of the PCSA. The internal events of the PCSA model are evaluated with respect to fire initiating events and modified as necessary to address fire-induced failures that lead to exposures. The list of fire-induced failures included in the model is evaluated as to fire vulnerability. Fragility analyses are conducted as needed (Section 6.3.2 and Attachment D).

Fire initiating event frequencies have been calculated for each initiating event identified for the subsurface operations. Section F5 of Attachment F details the analysis performed to determine these frequencies, using the methodology described in Section F4 of Attachment F.

### 6.5.1 Input to Initiating Events

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. 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.

### 6.5.2 Initiating Event Frequencies

The result of the fire initiating event analysis is the fire initiating event frequency and its associated distribution, as presented in Table 6.5-1. The frequency represents the probability, over the length of the pre-closure surface operation period, that a fire will threaten the stated waste form during onsite transportation. Calculations performed to obtain the initiating event frequency are detailed in Section F5.2 of Attachment F.

Uncertainty distributions are utilized in the initiating event frequency calculation to account for statistical uncertainty in the data. Uncertainty distributions utilized for this analysis are lognormal.

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	9.0E-07 fires/operation	15	Lognormal

Source: Original

## 6.6 NOT USED

## 6.7 EVENT SEQUENCE FREQUENCY RESULTS

This section provides the results of the event sequence quantification as produced from the Excel spreadsheet analyses. Quantification of an event sequence consists of calculating its number of occurrences over the preclosure period by combining the frequency of a single initiating event with the conditional probabilities of pivotal events that comprise the sequence. The quantification results are presented as an expression of the mean number of occurrences of each event sequence over the preclosure period, and the standard deviation as a measure of uncertainty. Section 6.8 describes the process for aggregation of similar event sequences to permit categorization as Category 1, Category 2, or Beyond Category 2 event sequences.

The section presents a summary of how the quantification is performed by the use of event trees, fault trees, and basic event input parameters. The discussion includes the rationale for truncating low values and analyzing uncertainties.

The results include a summary of all event sequences that are quantified and a table summarizing the results of the final quantification (found in Attachment G).

### 6.7.1 Process for Event Sequence Quantification

Internal event sequences that are based on the event trees presented in Section 6.1 and fault trees presented in Section 6.2 are quantified as follows. The fault tree quantification was performed using SAPHIRE; the event sequences, on the other hand, are quantified using Excel spreadsheets (Section 4.3). The quantification of an event sequence consists of calculating the number of occurrences over the preclosure period by combining frequencies of 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 (Attachment G, Table G-1).

The event sequence quantification methodology is presented in Section 4.3.6. An event sequence frequency is the product of several factors, as follows (with examples):

- The number of times the operation or activity that gives rise to the event sequence is performed over the preclosure period, for example, the total number of emplacements of

a waste package by a TEV over the preclosure period. In the Excel spreadsheet, this number is entered in the first column of the initiator event tree from which the event sequence arises or in the first event of the system-response event tree if no initiator event tree exists.

- The probability of occurrence of the initiating event for the event sequence considered. Continuing with the previous example, this could be the probability of dropping a waste package during its transfer to the TEV in the CRCF Waste Package Loadout Room, or the probability of occurrence of a fire that could affect the waste package in the drift. The initiating event probability is modeled in SAPHIRE with a fault tree or with a basic event. In an initiator event tree, this probability is assigned on the branch associated with the event sequence as a direct input to the Excel spreadsheet. If no initiator event tree exists, this probability is entered in the second event of the system-response event tree.
- The conditional probability of each of the pivotal events of the event sequence, which appear in the system-response event tree. The pivotal event may represent a passive failure such as the breach of the containment boundary of the waste package or canister or an active system failure such as the unavailability of the HVAC system. If the conditional probability of the pivotal event is represented as a mean value with a probability distribution or a point estimate (such as a passive failure estimate), it is entered directly into the Excel spreadsheet. On the other hand, if the pivotal event is modeled as a fault tree, the fault tree model is solved and the results are input into the spreadsheet.

Uncertainties in input parameters such as throughput rates, equipment failure rates, passive failure probabilities, and human failure events used to calculate basic event probabilities are propagated through the fault tree and event sequence logic to quantify the uncertainty in the event sequence quantification.

To quantify an event sequence, SAPHIRE is used to graphically draw the event tree. Then the event tree logic (i.e., the combination of individual successes and failures of pivotal events after the initiating event) is incorporated into the Excel spreadsheet. Where appropriate, SAPHIRE is then used to solve the fault trees that support the initiating event and the pivotal events and provide results that are used in the event quantification. The frequency for each event sequence is calculated as the product of the initiating event frequency and the pivotal event probabilities.

As an illustration of the above process, the quantification of the event sequences established in the ESD-03 in Table 6.7-1 is as follows: (1) the initiating event (e.g., collision or drop of the waste package) and the number of waste packages handled over the preclosure period, (2) the failure of the waste package, (3) the subsequent failure of the canister, and (4) the potential moderator entry into the canister. This sequence logic is input into the Excel spreadsheet shown in Table 6.7-1. The values associated with each initiating event or pivotal event are then input in the same spreadsheet.

Table 6.7-1. Event Sequence Quantification Example

(Col. 1)	(Col. 2)	(Col. 3)	(Col. 4)			(Col. 5)	(Col. 6)	(Col. 7)	(Col. 8)	(Col. 9)	(Col. 10)	(Col. 11)
Initiating Events (IEs)			IE values			WP Remains Intact	Canister(s) Remain Intact	Moderator excluded from entering canister	Calc'd Mean	Calc'd Median	Calc'd StdDev	End State
	SSO-ESD-03 - SEQ	No. of WP	IE mean (Col. 4A)	IE median (Col. 4B)	IE Std Dev (Col. 4C)	WP	CANISTER	MODERATOR	#Waste forms x IE mean x PE Prob			
Pt Values =====>		12,268										
<b>sm. bub1</b> – TEV impact collision or derail	2-1	12,268	3.40E-03	2.42E-03	3.34E-03	1.00E+00			4.17E+01	2.97E+01	4.10E+01	OK
	2-2					1.00E-08	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	2-3					1.00E-08	1.00E+00	1.00E+00	4.17E-07	2.97E-07	4.10E-07	RRU
	2-4					1.00E-08	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC
<b>Sm. Bub2</b> - Direct impact to WP- collision	3-1	12,268	1.00E-03	6.28E-04	1.17E-03	1.00E+00			1.23E+01	7.71E+00	1.43E+01	OK
	3-2					1.00E-08	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	3-3					1.00E-08	1.00E+00	1.00E+00	1.23E-07	7.71E-08	1.43E-07	RRU
	3-4					1.00E-08	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC
<b>sm. bub3</b> - Drop or drag of WP	4-1	12,268	2.68E-10	1.09E-10	6.14E-10	9.95E-01			3.27E-06	1.33E-06	7.49E-06	OK
	4-2					5.00E-03	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	4-3					5.00E-03	1.00E+00	1.00E+00	1.64E-08	6.70E-09	3.77E-08	RRU
	4-4					5.00E-03	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC
<b>sm. bub4</b> - Heavy load drop on TEV	5-1	12,268	1.95E-03	1.23E-03	2.33E-03	1.00E+00			2.39E+01	1.51E+01	2.86E+01	OK
	5-2					1.00E-08	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	5-3					1.00E-08	1.00E+00	1.00E+00	2.39E-07	1.51E-07	2.86E-07	RRU
	5-4					1.00E-08	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC
<b>sm. bub5</b> - WP impact due to TEV doors	6-1	12,268	1.20E-05	8.02E-06	1.31E-05	9.95E-01			1.46E-01	9.79E-02	1.60E-01	OK
	6-2					1.00E-08	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	6-3					1.00E-08	1.00E+00	1.00E+00	1.47E-09	9.84E-10	1.61E-09	RRU
	6-4					1.00E-08	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC
<b>sm. bub6</b> - Heavy load drop on WP	7-1	12,268	1.01E-02	6.20E-03	1.33E-02	1.00E+00			1.24E+02	7.61E+01	1.63E+02	OK
	7-2					1.00E-08	0.00E+00		0.00E+00	0.00E+00	0.00E+00	OK
	7-3					1.00E-08	1.00E+00	1.00E+00	1.24E-06	7.61E-07	1.63E-06	RRU
	7-4					1.00E-08	1.00E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	RRC

NOTE: bub = bubble; Calc'd = calculated; dev = deviation; IE = initiating event; No. = number; Prob = probability; Seq = sequence; sm = small; std = standard; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Table 6.7-1 provides the following information:

- Column 1: the initiating events depicted as “small bubbles” in the ESD and the initiating event tree.
- Column 2: event sequence identification number as “SSO-ESD-03-SEQ-2-1”, etc. This identification scheme provides the following information about the event sequence: the ESD it comes from (e.g., SSO-ESD-03) and event sequence from the event tree (e.g., SEQ-2-1), etc.
- Column 3: the number of waste forms during the preclosure period, in this case, the number of waste packages.
- Column 4: values associated with the initiating event, which comprise 4a) initiating event mean value, (4b) initiating event median value, (4c) initiating event standard deviation.
- Column 5: the conditional probability of failure accorded to the first pivotal event, “WP”, which is defined as “WP remains intact” in the example. The conditional failure probability of “WP” is estimated at 1E-8 for all initiating event, except for the “**sm. bub3** – Drop or drag of WP” initiating event for which the conditional probability of failure of “WP” is estimated at 5E-3.
- Column 6: the conditional probability of failure accorded to the second pivotal event, “CANISTER”, which is defined as “Canister(s) remain intact” in this example. The conditional probability of failure for the canister inside the waste package is conservatively estimated at 1, given the waste package failure. If the canister succeeds (not fails), then the end state is OK in Column 11 since there is no radioactive material released.
- Column 7: the conditional probability of failure accorded to the third pivotal event, “MODERATOR”, which is defined as “Moderator excluded from entering canister” in this example. The conditional probability of failure for moderator entering the waste package is estimated at 0, since there is no source of moderator available in the proximity of the event sequence location. Given a canister failure occurs, but there is no moderator entering the canister, the end state is then labeled as “RRU” in Column 11 for unfiltered radioactive release. However, had there been a moderator entering the canister event, the end state of the sequence would have been labeled as “RRC” in Column 11 for radioactive release with importance to criticality.
- Column 8: “Calc’d Mean”, the mean value of the event sequence estimated by multiplying the number of waste form (value in column 3) by the IE mean value (value in Column 4 – subcolumn A) and by the PE value(s) (value in Column 5, 6 or 7, where appropriate).

- Column 9: “Calc’d Median”, the median value of the event sequence estimated by multiplying the number of waste form (value in column 3) by the initiating event median value (value in Column 4 – subcolumn B) and by the pivotal event value(s) (value in Column 5, 6 or 7, where appropriate).
- Column 10: “Calc’d StdDev”, the standard deviation value of the event sequence estimated by multiplying the number of waste form (value in column 3) by the initiating event standard deviation value (value in Column 4 – subcolumn C) and by the pivotal event value(s) (value in Column 5, 6 or 7, where appropriate).
- Column 11: “End State” denotes the end state assigned to each event sequence. For example, for event sequence SSO-ESD-03-SEQ-3-3, the assigned end state is RRU, which represents an unfiltered radioactive material release following a failure of waste package(WP), a conditional failure of the canister (CANISTER) due to direct impact to the waste package caused by a collision (initiating event), but no moderator enters the failed canister (/MODERATOR).

As an example, event sequence SSO-ESD-03-SEQ-2-3, which leads to an unfiltered radionuclide release that is not important to criticality, starts with an initiator event tree that depicts the number of waste packages in the TEV in the drift and the initiating events that could occur during the emplacement process over the preclosure period. Based on *Waste Form Throughputs for Preclosure Safety Analysis* (Ref. 2.2.31, Table 4), there are 12,068 such operations; however, to be conservative, 12,268 value was used to match the total number of waste packages from IHF and CRCF. Next, the branch on the initiator event tree that deals with the “TEV impact due to collision or derail” is selected. The fault tree whose top event models the probability of a “TEV impact due to collision or derail” is solved and the results are input into the spreadsheet as IE mean (Col. 4A), IE median (Col. 4B) and IE Std Dev (Col. 4C). Multiplying the number of TEV/WP operations in the drift by the probability of a TEV impact per operation yields the number of occurrences, over the preclosure period, of the initiating event for the event sequence considered.

The event quantification continues with the input of event sequence logic from the system-response event tree which provides the basis for quantifying the rest of the event sequence through the use of the pivotal events described in Section 6.1 and Attachment A. First, the breach of the waste package, given an impact to the TEV, is evaluated under the pivotal event called “WP”. The analyst ensures that the probability assigned to this pivotal event pertains to the waste form considered in this event sequence – WP; in this example, the passive equipment failure analysis yields a failure probability of 1E-8 for the TEV impact due to collision or derailment. The next pivotal event that appears in the system-response event tree is called “CANISTER”. This pivotal event has a probability of one (1), indicating that a canister failure is considered to have occurred if a WP has failed. Finally, the last pivotal event is called “MODERATOR.” This event models moderator intrusion into the breached canister. In the event sequence analyzed, no moderator entry occurs, that is, the success branch is followed. Since there is no ITS air filtering medium available for the drift operations, release of radioactive materials is considered unfiltered, or a “RRU” End State.

The mean event sequence frequency is then obtained by calculating the product of the mean initiating event frequency and the pivotal event probabilities:

$(12,268 \text{ waste packages/preclosure period}) \times (3.4\text{E-}3 \text{ mean impact occurrence/waste packages}) \times (1\text{E-}8 \text{ probability of a waste packages failure given a slow speed impact}) \times (1 \text{ canister failure probability given a failure of the waste packages}) \times (1 \text{ probability of no moderator intrusion}) = 4.2\text{E-}7 \text{ occurrence/preclosure period.}$

As noted, uncertainties in input parameters are propagated through the fault tree and event sequence logic to quantify the uncertainty in the event sequence quantification. The fault tree quantification uncertainty analysis uses the Monte Carlo method that is built into SAPHIRE. The fault tree quantification was analyzed using 10,000 trials. The number of trials is considered sufficient to ensure accurate results for the distribution parameters.

The uncertainty analysis for the event sequence quantification is propagated by multiplying the probability distribution with a series of scalar quantities. For example, the initiating event is normally represented by a probability distribution with a mean, median and standard deviation, where the number of waste packages is a scalar quantity. Thus, for the example above, the event sequence median value is  $(12,268 \times 2.4\text{E-}3 \times 1\text{E-}8 \times 1 \times 1) = 2.97\text{E-}7$  with a standard deviation of  $(12,268 \times 3.3\text{E-}3 \times 1\text{E-}8 \times 1 \times 1) = 4.1\text{E-}7$ .

In the case where the event sequence is comprised of two or more events (initiating or pivotal) that each of them is represented by a probability distribution, the uncertainty propagation for that event sequence is calculated by first, obtaining the uncertainty propagation for the product of the events that have a probability distribution using SAPHIRE software (Section 4.2), and then, multiplying the resulting product (and the calculated probability distribution) with the remaining scalar quantities using the method described above.

### 6.7.2 Event Sequence Quantification Summary

Table G-1 of Attachment G presents the result of the event sequence quantification. Table G-1 summarizes the results of the event sequence quantification and lists the following elements: (1) the initiating event, (2) the event tree from which the sequence is generated, (3) event sequence designator (ID), (4) event sequence description, (5) event sequence logic, (6) event sequence end state, (7) event sequence mean value, (8) event sequence median value, and (9) event sequence standard deviation value.

## 6.8 EVENT SEQUENCE GROUPING AND CATEGORIZATION

An aggregation grouping process is applied prior to a categorization of event sequences as was described in Section 4.3.1. It is appropriate for purposes of categorization, to add the frequencies of event sequences that are derived from the same ESD, that elicits the same combination of failure and success of pivotal events, and have the same end state. This is termed final event sequence quantification, discussed in Section 6.8.1, and the results give the final frequency of occurrence. Using the final frequency of occurrence, the event sequences are categorized according to the definition of Category 1 and Category 2 event sequences given in 10 CFR 63.2 (Ref. 2.3.2). Dose consequences for Category 1 and Category 2 event sequences are subject to the performance objectives of 10 CFR 63.111 (Ref. 2.3.2), which is performed in *Preclosure*

*Consequence Analyses* (Ref. 2.2.36). Event sequences with a frequency of occurrence less than one chance in 10,000 of occurring before permanent closure of the repository are designated as Beyond Category 2 event sequences and are not analyzed for dose consequences.

Rather than calculate dose consequences for each Category 2 event sequence identified in the categorization process, dose consequences are performed for a set of bounding events that encompass the end states and material at risk for event sequences. Therefore, dose consequences are determined for a representative set of postulated Category 2 event sequences, identified in Table 6.8-1 (Ref. 2.2.36, Table 2 and Section 7). Once event sequence categorization is complete, Category 2 event sequences are cross referenced with the bounding event number given in Table 6.8-1, thus assuring that Category 2 event sequences have been evaluated for dose consequences and compared to the 10 CFR 63.111 (Ref. 2.3.2) performance objectives.

Table 6.8-1. Bounding Category 2 Event Sequences

Bounding Event Number	Affected Waste Form	Description of End State	Material At Risk
2-01*	LLWF inventory and HEPA filters	Seismic event resulting in LLWF collapse and failure of HEPA filters and ductwork in other facilities.	HEPA filters LLWF inventory
2-02*	HLW canister in transportation cask	Breach of sealed HLW canisters in a sealed transportation cask	5 HLW canisters
2-03*	HLW canister	Breach of sealed HLW canisters in an unsealed waste package	5 HLW canisters
2-04*	HLW canister	Breach of sealed HLW canister during transfer (one drops onto another)	2 HLW canisters
2-05*	Uncanistered commercial SNF in transportation cask	Breach of uncanistered commercial SNF in a sealed truck transportation cask in air	4 PWR or 9 BWR commercial SNF
2-06*	Uncanistered commercial SNF in pool	Breach of uncanistered commercial SNF in an unsealed truck transportation cask in pool	4 PWR or 9 BWR commercial SNF
2-07*	DPC in air	Breach of a sealed DPC in air	36 PWR or 74 BWR commercial SNF
2-08*	DPC in pool	Breach of commercial SNF in unsealed DPC in pool	36 PWR or 74 BWR commercial SNF
2-09*	TAD canister in air	Breach of a sealed TAD canister in air within facility	21 PWR or 44 BWR commercial SNF
2-10*	TAD canister in pool	Breach of commercial SNF in unsealed TAD canister in pool	21 PWR or 44 BWR commercial SNF
2-11*	Uncanistered commercial SNF	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 non combustible LLW	Fire involving LLWF inventory	Combustible and non combustible LLW

Bounding Event Number	Affected Waste Form	Description of End State	Material At Risk
2-14*	Uncanistered commercial SNF in truck transportation cask	Breach of a sealed truck transportation cask due to a fire	4 PWR or 9 BWR commercial SNF

NOTE: Items marked with an asterisk (\*) are not applicable to the Subsurface.

BWR = boiling water reactor; DPC = dual-purpose canister; HEPA = high-efficiency particulate air; HLW = high-level radioactive waste; LLWF = Low-Level Waste Facility; PWR = pressurized water reactor; SNF = spent nuclear fuel; TAD = transportation, aging and disposal. Items marked with an asterisk (\*) are not applicable to the Subsurface.

Source: (Ref. 2.2.36, Table 2).

### 6.8.1 Event Sequence Grouping and Final Quantification

Event sequences are modeled to represent the GROA operations and SSCs. Accordingly, an event sequence is unique to a given operational activity in a given operational area, which is depicted in an event sequence diagram. When more than one initiating event (for example, the drop, collision, or other structural challenges that could affect the canister) share the same ESD (and therefore elicit the same pivotal events and the same end states), it may be necessary to quantify the event sequence for each initiating event individually because the conditional probabilities of the pivotal events depend on the specific initiating event. In such cases, the frequencies of event sequences that are represented in the same ESD and have the same end state are added together, thus comprising an event sequence grouping.

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 form configuration at the event ESD level. Note that the subsurface operations only consider one waste form, which is the waste package.

The grouping of event sequences is carried out by summing “like” event sequences listed in the Excel spreadsheet for each ESD. The event sequence frequencies from this step comprise the final event sequence quantification. Continuing the example listed in Table 6.7-1, the grouping of event sequences is as follows.

Table 6.7-1 listed 6 different initiating events, with each initiating event having 4 event sequences. The end states assigned to the event sequences 1, 2, 3, and 4 for each initiating event are “OK”, “OK”, “RRU”, and “RRC”, respectively. Since the end states of the event sequences are the same for each IE, the event sequences are then grouped as follows:

- Event sequence 1 of all initiating events are summed together.
- The summed event sequence, which represents the final event sequence, is then labeled with an event sequence number denoting the ESD where it is originated from (SSO03),

the waste form (waste package), the summed sequence number (SEQ1) and the end state given to the original event sequence (OK). For this example, the final event sequence is labeled as SSO03-WP-SEQ1-OK.

- The mean, median and standard deviation values are derived as shown in Section 4.3.1.1. The mean value of the final event sequence is calculated as the sum of the mean value of all event sequences bearing the same end state. The standard deviation value of the final event sequence is calculated as the square root of the sum of the squares of the standard deviation values of all event sequences bearing the same end state. Because the event sequence probability distribution approximates a lognormal, the median is derived from the mean.

The above information is then compiled and listed in Table 6.8-2 below.

Table 6.8-2.Event Sequence Grouping and Quantification Example

End State	Total WP Sequence ID	Mean	Median	Std Dev
OK	SSO03-WP-SEQ1-OK	2.02E+02	3.51E+01	1.71E+02
OK	SSO03-WP-SEQ2-OK	0.00E+00	0.00E+00	0.00E+00
RRU	SSO03-WP-SEQ3-RRU	2.04E-06	4.64E-07	1.71E-06
RRC	SSO03-WP-SEQ4-RRC	0.00E+00	0.00E+00	0.00E+00

NOTE: ID = identification; Std = standard; Dev = deviation; WP = waste package.

Source: Original

### 6.8.2 Event Sequence Categorization

Based on the resultant frequency of occurrence, the event sequences are categorized as Category 1 or Category 2 per the definitions in 10 CFR 63.2 (Ref. 2.3.2) or Beyond Category 2. The categorization is done on the basis of the expected number of occurrences of each event sequence during the preclosure period. For purposes of this discussion, the expected number of occurrences of a given event sequence over the preclosure period is represented by the quantity *m*.

Some event sequences are not directly dependent on the duration of the preclosure period. For example, the expected number of occurrences of waste package drops in subsurface operations over the preclosure period is essentially controlled, among other things, by the number of waste packages and the number of times these waste packages are transported. The duration of the preclosure period is not directly relevant for this event sequence, but implicitly built into the operations. In contrast, for other event sequences, time is a direct input. For example, seismically induced event sequences are evaluated over a period of time. In such cases, event sequences are evaluated and categorized for the time during which they are relevant. Seismically induced event sequences for a surface facility are evaluated over a period of 50 years, because surface facilities are expected to operate for no longer than 50 years (Ref. 2.2.15, Section 2.2.2.7). Seismically induced event sequences for the emplacement drifts are evaluated over the entire preclosure period, which is 100 years (Ref. 2.2.15, Section 2.2.2.7).

Using the parameter  $m$  for a given event sequence, categorization is performed using the screening criteria set out in 10 CFR 63.2 (Ref. 2.3.2), as follows:

- Those event sequences that are expected to occur one or more times before permanent closure of the GROA are referred to as Category 1 event sequences (Ref. 2.3.2). Thus, a value of  $m$  greater than or equal to one means the event sequence is a Category 1 event sequence.
- Other event sequences that have at least one chance in 10,000 of occurring before permanent closure are referred to as Category 2 event sequences (Ref. 2.3.2). Thus, a value of  $m$  less than one but greater than or equal to  $10^{-4}$ , means the event sequence is a Category 2 event sequence.
- A measure of the probability of occurrence of the event sequence over the preclosure period is given by a Poisson distribution that has a parameter taken equal to  $m$ . The probability,  $P$ , that the event sequence occurs at least one time before permanent closure is the complement to one that the event sequence occurs exactly zero times during the preclosure period. Using the Poisson distribution,  $P = 1 - \exp(-m)$  (Ref. 2.2.9, p. A-13). A value of  $P$  greater than or equal to  $10^{-4}$  implies the value of  $m$  is greater than or equal to  $-\ln(1 - P) = -\ln(1 - 10^{-4})$ , which is approximately equal to  $10^{-4}$ . Thus, a value of  $m$  greater than or equal to  $10^{-4}$ , but less than one, implies the corresponding event sequence is a Category 2 event sequence.
- Event sequences that have a value of  $m$  less than  $10^{-4}$  are designated as Beyond Category 2.

An uncertainty analysis is performed on  $m$  to determine the main characteristics of its associated probability distribution, specifically the 50th percentile (i.e., the median), and the standard deviation. The uncertainty analysis is performed as described in Section 4.3.6.2.

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

### 6.8.3 Final Event Sequence Quantification Summary

Initially, the results of the event sequence gathering and quantification process are reported in a single table of all event sequences for the subsurface operations (Attachment G, Table G-2). Following the final categorization, the event sequences for the respective Category 2 (Table 6.8-4) and Beyond Category 2 (Attachment G, Table G-3) are tabulated separately. There are no Category 1 (Table 6.8-3) events for the CRCF. As desired, other sorting may be performed. For example, event sequences that have end states important to criticality are tabulated separately (Attachment G, Table G-4). The format of the table headings and content are the same for each table as follows:

1. Event sequence group ID –assigned during the grouping process

2. End state – taken from the event tree
3. Event sequence description – narrative to describe the initiating event(s) and pivotal events that are involved
4. Material at risk – describes the quantity and type of waste form involved
5. Mean event sequence frequency (number of occurrences over the preclosure period).
6. Median event sequence frequency (number of occurrences over the preclosure period).
7. Standard deviation of the event sequence frequency (number of occurrences over the preclosure period).
8. Event sequence category – declaration of Category 1, Category 2, or Beyond Category 2.
9. Basis for categorization (e.g., categorization by mean frequency, or from sensitivity study for mean frequencies near a threshold as described in Section 4.3.6.2).
10. Consequence analysis – cross-reference to the bounding event number in the dose consequence analysis (Table 6.8-1) (Ref. 2.2.36, Table 2 and Section 7).

Table 6.8-3. Category 1 Final Event Sequences Summary

Event Sequence Group ID	End State	Description	Material-At-Risk	Mean	Median	Std Dev	Event Sequence. Cat.	Basis for Categorization	Consequence Analysis
None									

NOTE: ID = identification; Std = standard; Dev = deviation; WP = waste package.

Source: Original

Table 6.8-4. Category 2 Final Event Sequences Summary

Event Sequence Group ID	End State	Description	Material-At-Risk	Mean <sup>3</sup>	Median <sup>3</sup>	Std. Dev <sup>3</sup>	Event Sequence Category	Basis for Categorization	Consequence Analysis <sup>1</sup>
SSO05-WP-SEQ3-DEL	Direct exposure, loss of shielding	This event sequence represents a thermal challenge to a canister inside a waste package, due to a fire, resulting in a direct exposure from loss of shielding. In this sequence, the waste package fails, and the canister remains intact.	1 waste package with canister(s) inside	1.E-02	7.E-03	1.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A <sup>2</sup>
SSO04-WP-SEQ2-DEL	Direct exposure, loss of shielding	This event sequence represents a direct exposure due to inadvertent TEV door opening or prolonged immobilization of the TEV in the heat causing a loss of shielding. In this sequence there are no pivotal events.	1 waste package with canister(s) inside	1.E-03	1.E-04	1.E-02	Category 2	Mean of distribution for number of occurrences of event sequence	N/A <sup>2</sup>

**NOTE:** <sup>1</sup> The bounding event number provided in this column identifies the bounding Category 2 event sequence identified in Table 6.8-1 from *Preclosure Consequence Analyses* (Ref. 2.2.36, Table 2) that results in dose consequences that bound the event sequence under consideration.

<sup>2</sup> Because of the great distances to the locations of the offsite receptors, doses to members of the public from direct radiation after a Category 2 event sequence are reduced by more than 13 orders of magnitude to insignificant levels (*GROA External Dose Rate Calculation* (Ref. 2.2.22)).

<sup>3</sup> The mean, median, and standard deviation displayed are for the number of occurrences, over the preclosure period, of the event sequence under consideration.

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 procedural safety controls that, in conjunction with the repository design ensure operations are conducted within the limits of the PCSAs.

Section 6.9.1 identifies ITS SSCs and Section 6.9.2 identifies the procedural safety controls.

### **6.9.1 Important to Safety Structures, Systems, and Components**

Table 6.9-1 contains the nuclear safety design bases for the Subsurface ITS SSCs.

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

System or Facility (System Code)	Subsystem or Function (as Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
DOE and Commercial Waste Package System (DS)	DOE and Commercial Waste Package	Entire	Provide containment	1. The mean conditional probability of breach of a sealed waste package resulting from a side impact shall be less than or equal to $1 \times 10^{-8}$ per impact.	SSO-ESD03-WP Seq. 6-3	Table 6.3-7
				2. The mean conditional probability of breach of a sealed waste package resulting from a drop of a load onto the waste package shall be less than or equal to $1 \times 10^{-5}$ per drop.	SSO-ESD01-WP Seq. 6-4	Table 6.3-7
				3. The mean conditional probability of breach of a sealed waste package inside the transport and emplacement vehicle (TEV) resulting from an end-on impact or collision shall be less than or equal to $1 \times 10^{-8}$ per impact.	SSO-ESD03-WP Seq. 2-3	Table 6.3-4
				4. The mean conditional probability of breach of a representative canister inside a sealed waste package as a result of the spectrum of fires <sup>c</sup> shall be less than or equal to $3 \times 10^{-4}$ per fire event.	SSO-ESD05-WP Seq. 3-4	Table 6.3-7

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

System or Facility (System Code)	Subsystem or Function (as Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source		
			Safety Function	Controlling Parameters and Values				
<b>Emplacement and Retrieval/ Drip Shield Installation System (HE)</b>	Emplacement and Retrieval/ Drip Shield Installation System	Transport and Emplacement Vehicle (TEV)	Protect against <sup>a</sup> TEV runaway	5. The mean probability of runaway of a TEV that can result in a potential breach of a waste package shall be less than or equal to $2 \times 10^{-9}$ per transport.	Initiating event does not require further analysis <sup>b</sup>	Fault tree gate "RNWY-INIT" (See Attachment B)		
			Protect against <sup>a</sup> direct exposure of personnel	6. The mean probability of inadvertent TEV door opening shall be less than or equal to $1 \times 10^{-7}$ per transport.				
<b>Naval SNF Waste Package System (DN)</b>	Naval SNF Waste Package	Entire	Provide containment	7. The mean conditional probability of breach of a sealed waste package resulting from a side impact shall be less than or equal to $1 \times 10^{-8}$ per impact.	SSO-ESD03-WP Seq. 6-3	Table 6.3-7		
				8. The mean conditional probability of breach of a sealed waste package resulting from a drop of a load onto the waste package shall be less than or equal to $1 \times 10^{-5}$ per drop.			SSO-ESD01-WP Seq. 6-4	Table 6.3-7
				9. The mean conditional probability of breach of a sealed waste package in the TEV resulting from an end-on impact or collision shall be less than or equal to $1 \times 10^{-8}$ per impact.				

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

System or Facility (System Code)	Subsystem or Function (as Applicable)	Component	Nuclear Safety Design Bases		Representative Event Sequence (Sequence Number)	Source
			Safety Function	Controlling Parameters and Values		
				10. The mean conditional probability of breach of a canister inside a sealed waste package as a result of the spectrum of fires <sup>c</sup> shall be less than or equal to $1 \times 10^{-4}$ per fire event.	SSO-ESD05-WP Seq. 3-4 <sup>d</sup>	Table 6.3-7

NOTE: <sup>a</sup> 'Protect against' in this table means either 'reduce the probability of' or 'reduce the frequency of'.  
<sup>b</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>c</sup> Discussion on "the spectrum of fires" is provided in Attachment D, Section D2.1.5  
<sup>d</sup> Although the failure probability of the Naval canister (considered as thick walled canister) inside a sealed waste package in a fire is  $1 \times 10^{-4}$ , the analysis for the event sequence does not differentiate between the Naval canister and other canisters inside the waste package, and as a result, a conservative value for the canister failure probability of  $3 \times 10^{-4}$  is used for the analysis.

Source: Original

## 6.9.2 Procedural Safety Controls

Procedural safety controls (PSCs) are the controls that are relied upon to limit or prevent potential event sequences or mitigate their consequences. For this analysis, all PSCs were derived to reduce the initiating event sequence to an acceptable level.

Table 6.9-2 lists the PSCs that are required to support the event sequence analysis and categorization.

Table 6.9-2. Summary of Procedural Safety Controls for the Subsurface Operations

Item	Procedural Safety Controls	Basis for Selection	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.
2	YMP will establish a program to control access to the drift and provide appropriate training to the operators. This access control program will include controlled and locked access door to the drift and clearly posted warning signs.	To prevent worker direct exposure to radiation.	SSO-ESD-04-SEQ-2-2
3	Only one TEV containing a waste package (i.e., a "loaded" TEV) is in transit at one time in the repository. Also, an unloaded TEV is not operated at the same time a loaded TEV is in transit on a surface or on a subsurface rail.	The control is to mitigate the potential for a TEV containing a WP colliding with another loaded or unloaded TEV by restricting the number of TEVs in operation at one time. However, the movement of an unloaded TEV at the surface is permitted concurrent with transit and emplacement operations of a TEV in the subsurface.	SSO-ESD-04-SEQ-3-2
4	Workers are prevented from being in proximity to a TEV while the TEV contains a waste package	The control is to mitigate the potential of a worker to be close proximity to the TEV if a TEV system failure occurs inducing an exposure hazard It is also to reduce the long-term worker exposure from the TEV itself.	SSO-ESD-04-SEQ-3-2
5	Vehicular crossings over the TEV railway are closed whenever a TEV is in transit to or from the subsurface. In the subsurface drifts, traffic will be restricted from being in the same area as a loaded TEV.	The control is to mitigate the potential for a loaded TEV collision with another vehicle stalled or otherwise halted at a rail crossing, and inducing a derailment of the TEV	SSO-ESD-02-SEQ-2-4

Table 6.9-2. Summary of Procedural Safety Controls for the Subsurface Operations (Continued)

Item	Procedural Safety Controls	Basis for Selection	Event Sequence ID References
6	Combustible Material Control Program requires that each emplacement drift is inspected to ensure that all combustibles have been removed from the drift at the completion of construction and outfitting operations and prior to the utilization of an emplacement drift for waste storage, and prohibits the storage or accumulation of combustibles in access mains along the path of travel of the TEV.	The requirement is to mitigate the potential for fire occurring in the emplacement drift (and potentially breaching a waste package). A fire can start in collections of combustible materials that were required for construction and inadvertently left behind.	SSO-ESD-05
7	Rock condition is to be observed as emplacement drift boring is accomplished. Observed faults are to be specifically evaluated to ensure that conditions cannot credibly lead to a breach of the waste package during the preclosure period, or a standoff distance from the fault is to be established.	This control is to limit the potential for fault displacement (or related rockfall hazard) from a seismic event to induce a breach of the waste package at rest in an emplacement drift during the preclosure period.	SSO-ESD-03-SEQ-7-3
8	Installation and configuration of the Subsurface isolation barriers is controlled such that development operations do not impact on emplacement operations.	The control is to prevent personnel exposure and drift impact due to activities at the construction side of the drift.	N/A
9	Operations and Construction areas are physically separated by distance and temporary barriers to preclude construction activities from affecting operations activities.	The control is to prevent personnel exposure and drift impact due to activities at the construction side of the drift.	N/A
10	Full-service fire and rescue capabilities are available to support subsurface activities.	Maintain fire frequency associated with WP within limits established by PCSA analysis	SSO-ESD-05

NOTE: TEV = transport and emplacement vehicle, WP = waste package.

Source: Original

## 7. RESULTS AND CONCLUSIONS

This analysis and its predecessor, the event sequence development analysis (Ref. 2.2.42), are part of the preclosure safety analysis (PCSA) for the geologic repository operations area (GROA) that supports the license application. In combination these documents identify, evaluate, quantify, and categorize event sequences for the GROA facilities and operations. They are part of a collection of analysis reports that encompass all waste handling activities and facilities of the GROA from initial operations to the end of the preclosure period. Probabilistic risk assessment techniques derived from both nuclear power plant and aerospace methods are used to perform the analyses to comply with the risk-informed aspects of 10 CFR 63.111 and 63.112 (Ref. 2.3.2), and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report* (Ref. 2.2.75). The identification and development of the event sequences is limited to those that might lead to direct radiation exposure of workers or onsite members of the public; radiological releases that may affect the workers or public (onsite and offsite); and nuclear criticality.

The results of the analysis are discussed and presented in the logical progression through Section 6 of this document and are not reiterated here. Instead, only key points are highlighted. For the ungrouped event sequence results and the complete grouped event sequence summaries, electronic files are provided due to the large size of hard copy versions (refer to Attachments G and H). In addition, although the results from the SAPHIRE model are used and presented in Section 6 and Attachment B, the model itself is difficult to completely represent in paper form. Therefore, these outputs are also provided electronically (refer to Attachment H). Table 7-1 describes the results and indicates the location within this analysis for each result provided.

Table 7-1. Key to Results

Result	Description	Cross Reference
Grouping & quantification of event sequences	Calculation of probability distributions for the numbers of occurrences of internal event sequence groups over the preclosure period	Table G-1
Categorization of event sequences	Assignment of frequency categories Category 1, Category 2, or Beyond Category 2 to internal event sequence groups based on mean numbers of occurrences	Table 6.8-3 Table 6.8-4 Table 6.8-5
Designation of SSCs as ITS	Identification of SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1
Statement of nuclear safety design bases	Determination of nuclear safety design bases for SSCs that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-1
Statement of procedural safety controls	Determination of procedural safety controls that are relied on in the quantification of internal event sequences for prevention or mitigation	Table 6.9-2

NOTE: ITS = important to safety; SSCs = structures, systems, and components.

Source: Original

## Summary of Event Sequences

For the Subsurface Operations, as shown in Table 6.8-4, the analysis concludes that there are no Category 1 event sequences and two Category 2 event sequences.

Table 7-2. Summary of Category 2 Event Sequences

End State	Description	Canister Types
		Waste Package
DE-SHIELD-DEGRADE	Direct exposure due to degradation of shielding	None
DE-SHIELD-LOSS	Direct exposure due to loss of shielding	2
RR-UNFILTERED	Radionuclide release, unfiltered	None
RR-FILTERED	Radionuclide release, filtered	None
RR-UNFILTERED-ITC	Radionuclide release, unfiltered, also important to criticality	None
RR-FILTERED-ITC	Radionuclide release, filtered, also important to criticality	None
ITC	Important to criticality	None

Source: Original

## Summary of Conservatism

It is noted that the event sequence identification and categorization were conducted with conservatisms built into the analysis inputs, including the following:

1. Fire frequency and damage analyses are performed without relying on fire suppression. This increases the calculated frequency of large fires and also increases the duration and peak temperature of fires, thereby significantly increasing the calculated probability of waste container failure.
2. If a fire is calculated to propagate out of the initiating location fire zone, the entire building is considered to be involved in the fire.
3. In the passive equipment failure analysis (PEFA) for thermal and fire scenarios, conservatism is built into the boundary conditions, which consider the fire as occurring next to the waste forms instead of only a fraction of the fire occurrence being near the waste form. A fire closer to the target will lead to a higher target failure probability than a fire located further away. By considering all fires to be next to the waste forms, the thermal PEFA yields higher waste form failure probabilities than is likely.
4. For event sequences in which a cask containing a canister is subjected to a drop, slapdown, or in which a load is dropped onto the cask, the calculated containment failure probability pertains to the canister inside without regard to the integrity of the cask. That is, cask containment is not relied upon to reduce probability of containment failure.

5. The structural PEFA uses a conservative failure probability of  $1E-5$ , whereas the actual PEFA assessment indicates values of less than  $1E-8$  failure probabilities (Table D1.2-7 of Attachment D). This conservatism provides event sequence quantification results of magnitude higher than what they would be if the actual PEFA assessment values are used.
6. The 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 object for the dropped load.
8. The probabilities of event sequences involving drops of casks and canisters represent a drop height of 30 feet for casks and bare canisters. This is much higher than the normal operational lift height but is applied for all drop heights. Lower drop heights would result in less structural challenge to casks and canisters.
9. When a canister is inside a waste package, failure of the waste package is considered to fail containment. That is, the canister is not relied upon to reduce the probability of containment failure.
10. The speed limitation of crane and conveyances within facilities to 20 ft/min and 2.5 mph, respectively, is set to ensure no breach of casks or canisters. The probability of breach at such speeds is calculated to be less than  $1E-08$  per impact. Speeds could be considerably larger without changing the categorizations of event sequences.
11. The reliability evaluation of the ITS HVAC system, which provides confinement of radioactive material releases following a breach of a waste container, is based a mission time of 720 hrs (30 days). The use of this mission time in the analysis leads to a requirement that the emergency diesel generators provide power to the HVAC for 720 hours following a release. The analysis does not account for the high likelihood of recovering offsite power within the mission time. Recovery of offsite power would reduce the length of time that the diesel generators would be required to run and would thereby reduce the calculated unavailability of the diesel generators. This conservative consideration leads to a lower ITS HVAC availability than is realistically expected.
12. The human reliability analysis screening values used for human failure events are typically one or more orders of magnitude higher than values that are obtained through detailed analysis.
13. The probability of failure associated with the structural analysis of mechanical impact loads to casks and canisters is conservatively based on the maximum effective plastic strain of any brick (i.e., finite element mesh) in the modeled structure rather than on evidence of through-wall cracking.
14. Categorization of event sequences is based on the highest category after application of a conservative adjustment to account for the uncertainty in the calculated uncertainties

15. To preserve flexibility in the conduct of operations, the throughput analysis (Ref. 2.2.29) embeds multiple and bounding waste handling scenarios in the throughput numbers. For example, of about 350 DPCs available for transfer in the WHF, the throughput analysis considers 350 DPCs are transferred from vertical transportation casks, another 350 DPCs are transferred from horizontal transportation casks, and another 350 DPCs are transferred from the horizontal aging modules (HAMs) on the aging pad. Including this conservatism in the analysis yields calculated event sequence frequencies that are higher than is realistically expected.

**ATTACHMENT A**  
**EVENT TREES**

---

## CONTENTS

	<b>Page</b>
A1 INTRODUCTION .....	A-5
A2 READER'S GUIDE TO THE EVENT TREE DESCRIPTIONS .....	A-5
A3 SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES .....	A-6
A4 EVENT TREE DESCRIPTIONS .....	A-7
A4.1 EVENT TREES FOR SSO-ESD-01 .....	A-7
A4.2 EVENT TREES FOR SSO-ESD-02 .....	A-8
A4.3 EVENT TREES FOR SSO-ESD-03 .....	A-9
A4.4 EVENT TREE FOR SSO-ESD-04 .....	A-11
A4.5 EVENT TREES FOR SSO-ESD-05 .....	A-12
A5 EVENT TREES .....	A-13

## FIGURES

	<b>Page</b>
A5-1. Example Initiator Event Tree Showing Navigation Aids .....	A-13
A5-2. Event Tree SSO-ESD01 – TEV Activities Inside Facility Waste PackageLoadout Area .....	A-15
A5-3. Event Tree SSO-ESD02 – TEV Activities During Transit.....	A-16
A5-4. Event Tree SSO-ESD03 – TEV Activities within the Emplacement Drift .....	A-17
A5-5. Event Tree SSO-ESD04 – Loss or Lack of Shielding .....	A-18
A5-6. Event Tree SSO-ESD05 – Internal Fires .....	A-19
A5-7. Event Tree RESPONSE-FACILITY – Response tree for TEV in Facility [Response for SSO-ESD01].....	A-20
A5-8. Event Tree RESPONSE-TRANSIT – Response tree for TEV in Transit [Response for SSO-ESD02, SSO-ESD04 and SSO-ESD05] .....	A-21
A5-9. Event Tree RESPONSE-DRIFT – Response tree for TEV in Emplacement Drift [Response for SSO-ESD03].....	A-22

**TABLES**

	<b>Page</b>
A4.1-1. Summary of Event Trees for SSO-ESD-01 .....	A-7
A4.1-2. Initiating Event Assignments for SSO-ESD-01 .....	A-8
A4.2-1. Summary of Event Trees for SSO-ESD-02 .....	A-8
A4.2-2. Initiating Event Assignments for SSO-ESD-02 .....	A-9
A4.3-1. Summary of Event Trees for SSO-ESD-03 .....	A-10
A4.3-2. Initiating Event Assignments for SSO-ESD-03 .....	A-11
A4.4-1. Summary of Event Trees for SSO-ESD-04 .....	A-11
A4.4-2. Initiating Event Assignments for SSO-ESD-04 .....	A-12
A4.5-1. Summary of Event Trees for SSO-ESD-05 .....	A-12
A4.5-2. Initiating Event Assignments for SSO-ESD-05 .....	A-13
A5-1. ESDs to Event Trees .....	A-14

## ATTACHMENT A EVENT TREES

### A1 INTRODUCTION

This attachment presents event trees that are derived from the event sequence diagrams (ESDs) in Attachment F of the *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40). All initiator event trees and system response event trees are located at the end of this attachment. Refer to Table A5-1 for the figure locations of specific event and response trees. The event trees are presented in Figures A5-2 through A5-9; the ESD initiating event trees (ESDs 01-05) are presented first, followed by the corresponding response trees for ESDs 01-03. ESD-04 has no response tree and ESD-05 has the same response tree as ESD-02.

### 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 are briefly described and listed (initiator and system-response event trees or self contained event trees, as applicable).
2. The initiating events are described and listed. The listing is provided as a table that includes the assignments of fault trees or basic events to the initiating events. The assignments are made in SAPHIRE using basic rules or by fault-tree construction. The goal of the initiating event table is to provide a link to the underlying fault tree (covered in Section 6.2 and Attachment B) or basic event (covered in Section 6.3 and Attachment C). In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the fault tree or basic event level (covered in Attachment B). Note that the initiating event frequencies are defined on a per-unit-handled basis. Thus, when the initiating event frequencies are multiplied by the number of waste packages handled over the preclosure period, the result is an initiating event frequency over the preclosure period.
3. The system-response event tree that corresponds to the initiator event tree or the system response for a self-contained event tree is covered as follows. Each pivotal event used in an event tree is listed in the event tree description section and summarized in Section A3. Each pivotal event is accompanied by a table that provides a link between the name given to the pivotal event in the event tree and the associated fault tree or basic event. The goal of the pivotal event table is to provide a link to the underlying fault tree (covered in Section 6.2) or basic event (covered in Section 6.3). In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the fault tree or basic event level.

### A3 SUMMARY OF THE MAJOR PIVOTAL EVENT TYPES

A self-contained event tree or a system response event tree may include pivotal events of following types:

**WP.** This pivotal event represents the success or failure of the waste package to contain radioactive material after the impact caused by the initiating event. The failure of this pivotal event leads to loss of the waste package's containment function. The failure probability for this pivotal event depends on the selection of initiating event and is determined by passive equipment failure analysis (PEFA), and is given in Table 6.3-4 in Section 6.3.2.

**CANISTER.** This pivotal event represents the success or failure of the canister to contain radioactive material after the impact caused by the initiating event. Failure of a containment pivotal event means that a release could occur if the canister containment barrier is breached (along with the cask or waste-package containment, as applicable). In accordance with a simplifying approximation, the conditional probability of canister breach given waste package breach is taken to be 1.

**SHIELDING.** Failure of a shielding pivotal event means that a direct exposure could occur. Waste package and some canister lids, and the transport and emplacement vehicle (TEV) shielding structure (including shield doors) provide radiation shields that could be pierced or degraded in some impact or thermal challenges. . In the subsurface analysis, waste packages and canisters are conservatively considered to provide no shielding; only the TEV provides the necessary radiation shielding. Thus, this pivotal event represents the success or failure of the shielding function provided by the TEV after the impact caused by the initiating event. Failure of shielding in this instance refers to an unspecified degree of the TEV shielding degradation due to the impact.

**CONFINEMENT.** This pivotal event represents the success or failure of the HVAC system in continuing to provide HEPA filtration (radiological confinement) after the initiating event. Success of the pivotal event requires the facility structural integrity as well as the functioning of equipment associated with the HVAC system. Failure results in a potential airborne release that is not mitigated by the HEPA filtration system; in this case, the release is termed as unfiltered release.

This pivotal event only applies to the TEV when it is in the CRCF. The IHF does not have an ITS HVAC system, therefore, there is no confinement challenge (CONFINEMENT always fails (pivotal event is set to 1)). When the loaded TEV is outside of the CRCF, the confinement no longer exists and thus, it is not modeled in the corresponding response event trees.

**MODERATOR.** This pivotal event represents the conditional probability of introducing liquid moderator (water) into a breached canister, given that a breached canister occurs. The conditional probability of failure (introduction of liquid moderator) is the same for all waste forms and all initiating events. Failure of a moderator pivotal event results in an end state that may be susceptible to nuclear criticality. In addition to the probability of the event MODERATOR being dependent upon the condition of the canister (intact vs. breached), the opportunity for criticality also depends on the physical properties of the waste form.

Specifically, HLW is not subject to the possibility of criticality; therefore, all moderator trees pertaining to criticality sequences for HLW are set to “0.00E+00.”

Each of the specific failure events included in a self-contained or system-response event tree may be linked to a basic event or to the top event of a fault tree that represents equipment failure modes and human failure events that can initiate the specific event. The fault tree models are, in turn, linked to basic events that provide the failure frequencies. Some of the pivotal events represent failure of equipment whose failure probabilities are linked to a separately developed basic event and not to a fault tree.

## A4 EVENT TREE DESCRIPTIONS

### A4.1 EVENT TREES FOR SSO-ESD-01

SSO-ESD-01 covers event sequences associated with TEV activities inside a facility waste package load-out area (Ref. 2.2.40, Figure F-1). This ESD covers only waste packages; therefore, there is only one event tree associated with SSO-ESD-01. An initiator event tree and a system response event tree represent the ESD (Table A4.1-1).

Table A4.1-1. Summary of Event Trees for SSO-ESD-01

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste Package in CRCF	Initiator: SSO-ESD01 Response: RESPONSE-FACILITY	11,668
Waste Package in IHF	Initiator: SSO-ESD01 Response: RESPONSE-FACILITY	600

Source: (Ref. 2.2.31, Table 4)

#### A4.1.1 Initiating Events for SSO-ESD-01

Initiating event assignments for SSO-ESD-01 are located in Table A4.1-2.

**WP Impact –Facility Shield Door.** This initiating event accounts for the potential impact to the waste package due to a TEV collision with the facility shield door.

**WP Impact –TEV Shield Door.** This initiating event accounts for the potential impact to the waste package due to the TEV shield door closing on the waste package.

**TEV Collision.** This initiating event accounts for the potential impact to the waste package due to a TEV collision with a structure.

**Drop of Waste Package.** This initiating event covers the potential impact to the waste package due a drop of the waste package.

**Heavy Load Dropped on TEV.** This initiating event covers the potential impact to the waste package due to the drop of a heavy object (e.g., empty waste package) by the waste package handling crane.

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

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment at Fault Tree Level
WP Impact – Facility Shield Door	SSO-ESD-01	TEV fault tree
WP Impact – TEV Shield Door	SSO-ESD-01	TEV fault tree
TEV Collision	SSO-ESD-01	TEV fault tree
Drop of WP	SSO-ESD-01	TEV fault tree
Object Dropped onto WP	SSO-ESD-01	TEV fault tree

NOTE: TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

#### A4.1.2 System Response Event Tree RESPONSE-FACILITY

The pivotal events that appear in RESPONSE-FACILITY are listed below and summarized in Section A3.

- Waste Package
- Shielding
- Canister
- Confinement
- Moderator.

#### A4.2 EVENT TREES FOR SSO-ESD-02

SSO-ESD-02 covers event sequences associated with TEV activities during transit (Ref. 2.2.40), Figure F-2). An initiator event tree and a system response event tree represent the ESD (Table A4.2-1).

Table A4.2-1. Summary of Event Trees for SSO-ESD-02

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste Package	Initiator: SSO-ESD02 Response: RESPONSE-TRANSIT	12,268

NOTE: The value for this basic event is obtained by adding the number of waste packages from the CRCF (11,668) and from the IHF (600) which is documented in the throughput analysis. However the throughput analysis also shows a total number of waste packages of 12,068 assigned for the Subsurface Operations. The value of 12,268 used here is a conservative estimate.

Source: (Ref. 2.2.31, Table 4)

##### A4.2.1 Initiating Events for SSO-ESD-02

Initiating event assignments for SSO-ESD-02 are located in Table A4.2-2.

**TEV Impact – Collision or Derail.** This initiating event accounts for the potential impact to the waste package due to a TEV collision into a structure or TEV derailment.

**TEV Impact During Transit.** This initiating event accounts for the potential impact to the waste package due to collision of another vehicle with the TEV.

**Drop of Waste Package.** This initiating event covers the potential impact to the waste package due a drop of the waste package.

**Heavy Load Dropped on TEV.** This initiating event covers the potential impact to the waste package due to the drop of a heavy object (i.e., rock fall) on the TEV.

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

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment at Fault Tree Level
TEV impact – Collision or Derail	SSO-ESD-02	TEV fault tree
TEV impact during transit	SSO-ESD-02	TEV fault tree
Drop of WP	SSO-ESD-02	TEV fault tree
Object dropped onto WP	SSO-ESD-02	TEV fault tree

NOTE: EV = transport and emplacement vehicle; WP = waste package.

Source: Original

#### A4.2.2 System Response Event Tree RESPONSE-TRANSIT

The pivotal events that appear in RESPONSE-TRANSIT are listed below and summarized in Section A3.

- Waste Package
- Shielding
- Canister
- Moderator.

#### A4.3 EVENT TREES FOR SSO-ESD-03

SSO-ESD-03 covers event sequences associated with TEV activities within the emplacement drift (Ref. 2.2.40, Figure F-3). An initiator event tree and a system response event tree represent the ESD (Table A4.3-1).

Table A4.3-1. Summary of Event Trees for SSO-ESD-03

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package	Initiator: SSO-ESD03 Response: RESPONSE-DRIFT	12,268

Source: (Ref. 2.2.31, Table 4)

### A4.3.1 Initiating Events for SSO-ESD-03

Initiating event assignments for SSO-ESD-03 are located in Table A4.3-2.

**TEV Impact – Collision or Derail.** This initiating event accounts for the potential impact to the waste package due to a TEV collision into a structure or TEV derailment.

**Direct Impact to WP - Collision.** This initiating event accounts for the potential impact to the waste package due to collision of the TEV or other structure, system, or component (SSC) directly with the waste package.

**Drop or Drag of Waste Package.** This initiating event covers the potential impact to the waste package due a drop or drag of the waste package.

**Heavy Load Dropped on TEV.** This initiating event covers the potential impact to the waste package due to the drop of a heavy object (i.e. rock fall) on the TEV.

**WP Impact Due to TEV Doors.** This initiating event covers the potential impact to the waste package by the TEV shield doors.

**Heavy Load Dropped on WP.** This initiating event covers the potential impact to the waste package due to the drop of a heavy object (i.e. rock fall) on the waste package.

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

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment at Fault Tree Level
TEV impact – collision or derail	SSO-ESD-03	TEV fault tree
TEV collision	SSO-ESD-03	TEV fault tree
Drop or drag of WP	SSO-ESD-03	TEV fault tree
Object dropped onto TEV	SSO-ESD-03	TEV fault tree
WP impact – TEV shield door	SSO-ESD-03	TEV fault tree
Object dropped onto WP	SSO-ESD-03	TEV fault tree

NOTE: TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

### A4.3.2 System Response Event Tree RESPONSE-DRIFT

The pivotal events that appear in RESPONSE-DRIFT are listed below and summarized in Section A3.

- Waste Package
- Canister
- Moderator.

### A4.4 EVENT TREE FOR SSO-ESD-04

SSO-ESD-04 covers event sequences associated with loss or lack of shielding during subsurface operations (Ref. 2.2.40, Figure F-4). This self contained event tree represents the ESD (Table A4.4-1).

Table A4.4-1. Summary of Event Trees for SSO-ESD-04

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package	Initiator: SSO-ESD04 Response: RESPONSE-TRANSIT	12,268

Source: (Ref. 2.2.31, Table 4)

#### A4.4.1 Initiating Events for SSO-ESD-04

Initiating event assignments for SSO-ESD-04 are located in Table A4.4-2.

**Inadvertent Entry into Drift.** This initiating event accounts for the potential direct exposure of a worker due to his inadvertent entry into an active drift.

**Prolonged Worker Proximity to TEV.** This initiating event accounts for the potential direct exposure of a worker because he/she spends too much time near the TEV.

**Inadvertent TEV Door Open.** This initiating event accounts for the potential direct exposure of a worker due to inadvertent opening of the TEV shield door.

**Loss of Movement – Loss of Shielding.** This initiating event accounts for the potential direct exposure of a worker due to degraded shield of the TEV from solar insolation.

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

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment at Fault Tree Level
Inadvertent entry into drift	SSO-ESD-04	Screened – See Section 6.0
Prolonged worker proximity to TEV	SSO-ESD-04	Screened – See Section 6.0
Inadvertent TEV door open	SSO-ESD-04	TEV fault tree
Loss of movement – loss of shielding	SSO-ESD-04	TEV fault tree

NOTE: TEV = transport and emplacement vehicle.

Source: Original

#### A4.5 EVENT TREES FOR SSO-ESD-05

SSO-ESD-05 covers event sequences associated with internal fires (Ref. 2.2.40, Figure F-5). An initiator event tree and a system response event tree represent the ESD (Table A4.5-1).

Table A4.5-1. Summary of Event Trees for SSO-ESD-05

Waste Form Unit	Associated Event Trees	Number of Waste Form Units
Waste package	Initiator: SSO-ESD05 Response: RESPONSE-TRANSIT	12,268

Source: (Ref. 2.2.31, Table 4)

##### A4.5.1 Initiating Events for SSO-ESD-05

Initiating event assignments for SSO-ESD-05 are located in Table A4.5-2.

**TEV Fire Affects WP in Drift.** This initiating event accounts for the potential damage to a waste package in the drift due to fire.

**TEV Fire Affects WP on Subsurface Rail.** This initiating event accounts for the potential damage to a waste package in the access main due to fire.

**TEV Fire Affects WP on Surface Rail.** This initiating event accounts for the potential damage to a waste package on the surface due to fire.

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

Initiating Event Description	Initiator Event Tree	SAPHIRE Assignment at Fault Tree Level
TEV fire affects WP in drift	SSO-ESD-05	TEV fault tree
TEV fire affects WP on subsurface rail	SSO-ESD-05	TEV fault tree
TEV fire affects WP on surface rail	SSO-ESD-05	TEV fault tree

NOTE: TEV = transport and emplacement vehicle; WP = waste package.

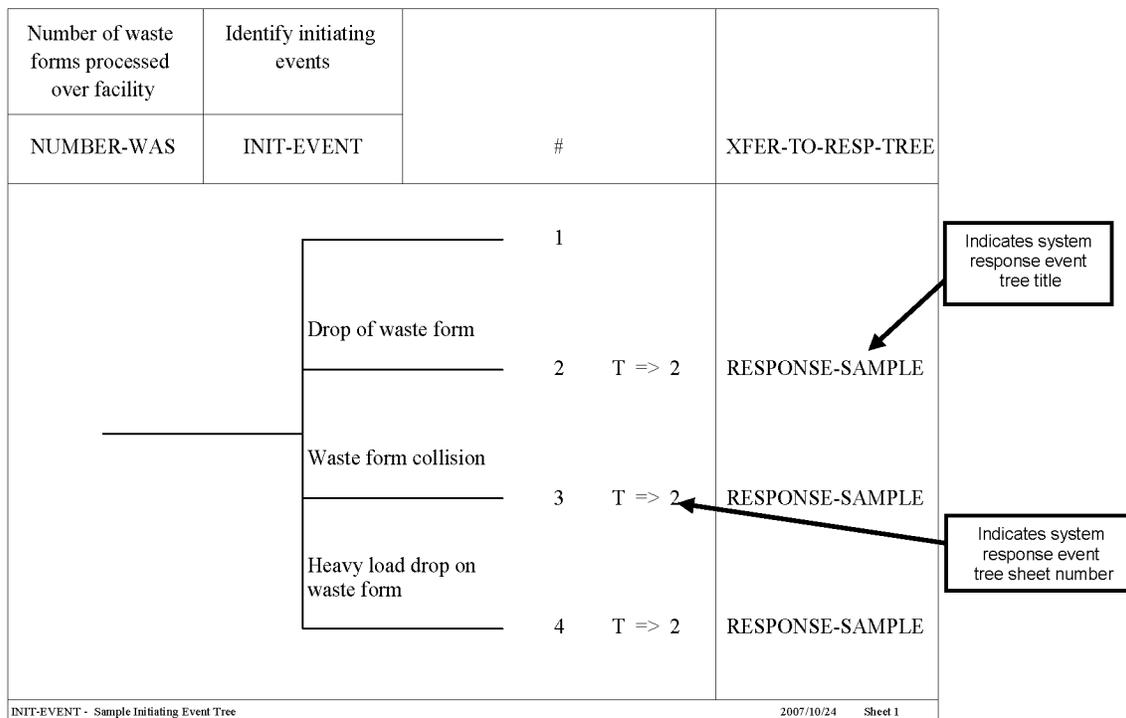
Source: Original

### A4.5.2 System Response Event Tree RESPONSE-TRANSIT

The pivotal events that appear in RESPONSE-TRANSIT as well as the association of pivotal event names with basic event or fault tree names have been described in Section A4.2.2.

## A5. EVENT TREES

Navigation from an initiator event tree to the corresponding response event tree is assisted by the rightmost two columns on the initiator event trees as shown in Figure A5-1. The numbers under the “#” symbol may be used by the reader to refer to a particular branch of an event tree, but it is not used elsewhere in this analysis.



Source: Original

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

Table A5-1. ESDs to Event Trees

<b>ESD#</b>	<b>ESD Title</b>	<b>IE Event Tree Name</b>	<b>IE Event Tree Location</b>	<b>Response Tree Name</b>	<b>Response Tree Location</b>
SSO-ESD-01	Event sequences for TEV activities inside facility WP load-out area	SSO-ESD-01	Figure A5-2	RESPONSE-FACILITY	Figure A5-7
SSO-ESD-02	Event sequences for TEV activities during transit	SSO-ESD-02	Figure A5-3	RESPONSE-TRANSIT	Figure A5-8
SSO-ESD-03	Event sequences for TEV activities within the emplacement drift	SSO-ESD-03	Figure A5-4	RESPONSE-DRIFT	Figure A5-9
SSO-ESD-04	Event sequences for loss or lack of shielding	SSO-ESD-04	Figure A5-5	No response tree	N/A
SSO-ESD-05	Event sequences for Internal Fires	SSO-ESD-05	Figure A5-6	RESPONSE-TRANSIT	Figure A5-8

NOTE: IE = initiating event; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Number of WPs processed over facility life	Identify initiating events		
NUMB-WP	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	WP impact - facility shield door	2	T => 2
	WP impact - TEV shield door	3	T => 2
	TEV collision	4	T => 2
	Drop of WP	5	T => 2
	Heavy load drop on TEV	6	T => 2
SSO-ESD-01 - TEV activities inside facility WP loadout area			2007/10/25 Page 1

Source: Original

Figure A5-2. Event Tree SSO-ESD01 – TEV Activities Inside Facility Waste Package Loadout Area

Number of WPs processed over facility life	Identify initiating events			
NUMB-WP	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	TEV impact - collision or derail	2	T => 4	RESPONSE-TRANSIT
	TEV impact during transit	3	T => 4	RESPONSE-TRANSIT
	Drop of WP during transit	4	T => 4	RESPONSE-TRANSIT
	Heavy load drop on TEV	5	T => 4	RESPONSE-TRANSIT

SSO-ESD-02 - TEV activities during transit 2007/10/19 Page 3

Source: Original

Figure A5-3. Event Tree SSO-ESD02 – TEV Activities During Transit

Number of WPs processed over facility life	Identify initiating events		
NUMB-WP	INIT-EVENT	#	XFER-TO-RESP-TREE
		1	OK
	TEV impact - collision or derail	2	T => 6
	Direct impact to WP - collision	3	T => 6
	Drop or drag of WP	4	T => 6
	Heavy load drop on TEV	5	T => 6
	WP impact due to TEV doors	6	T => 6
	Heavy load drop on WP	7	T => 6

SSO-ESD-03 - TEV activities within the emplacement drift

2007/10/19 Page 5

Source: Original

Figure A5-4. Event Tree SSO-ESD03 – TEV Activities within the Emplacement Drift

Exposure period for emplacement activities	Identify initiating events		
EXPOSURE	INIT-EVENT	#	END-STATE
	Inadvertent entry into drift	1	OK
	Prolonged worker proximity to TEV	2	DE-SHIELD-LOSS
	Inadvertent TEV door open	3	DE-SHIELD-LOSS
	Loss of movement - loss of shielding	4	DE-SHIELD-LOSS
		5	DE-SHIELD-LOSS

SSO-ESD-04 - Loss or lack of shielding 2007/10/25 Page 7

Source: Original

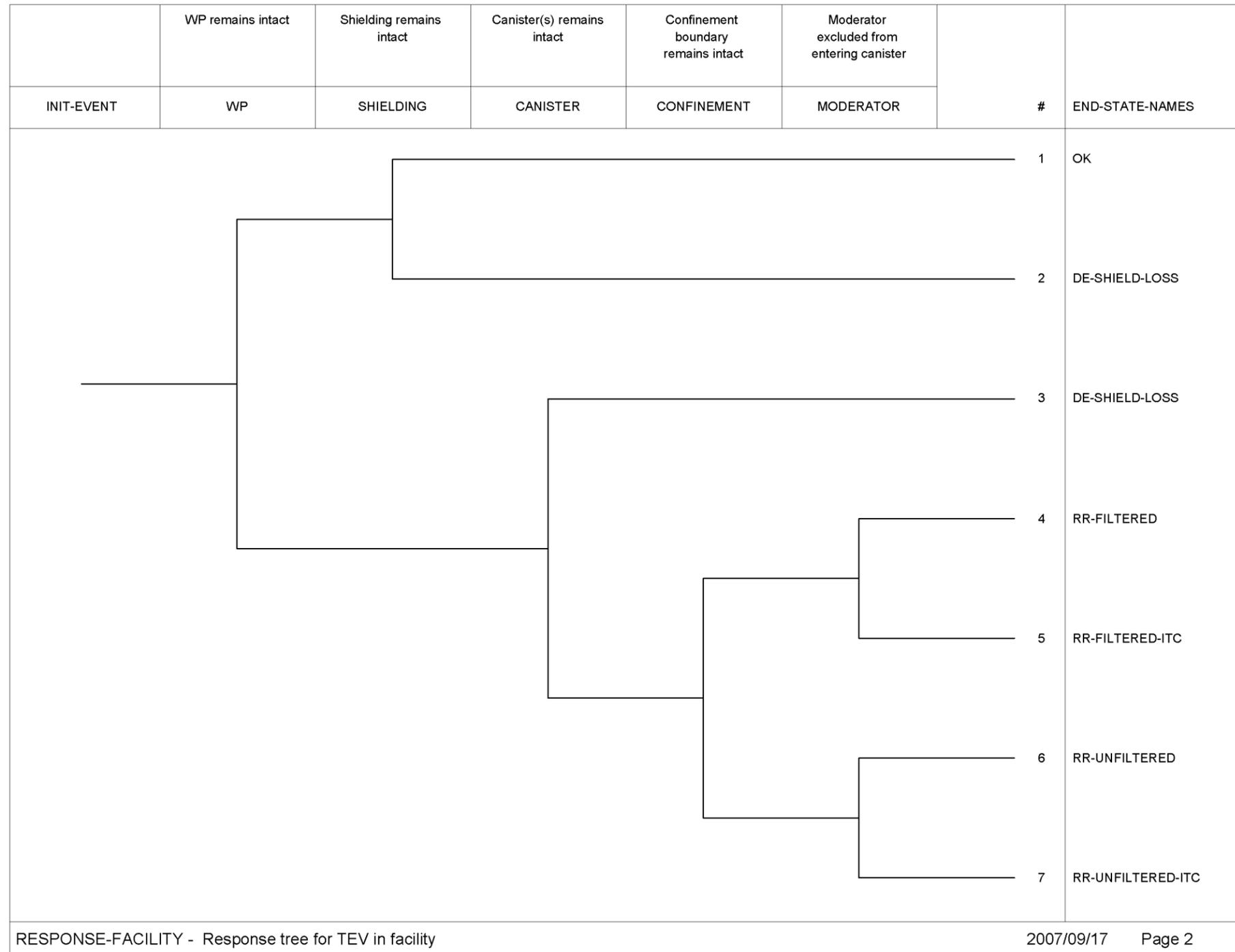
Figure A5-5. Event Tree SSO-ESD04 – Loss or Lack of Shielding

Number of WPs processed over facility life	Identify initiating events			
NUMB-WP	INIT-EVENT	#		XFER-TO-RESP-TREE
		1		OK
	TEV fire affects WP in drift	2	T => 4	RESPONSE-TRANSIT
	TEV fire affects WP on subsurface rail	3	T => 4	RESPONSE-TRANSIT
	TEV fire affects WP on surface rail	4	T => 4	RESPONSE-TRANSIT

SSO-ESD-05 - Internal fires 2007/10/19 Page 8

Source: Original

Figure A5-6. Event Tree SSO-ESD05 – Internal Fires



Source: Original

Figure A5-7. Event Tree RESPONSE-FACILITY  
– Response tree for TEV in Facility  
[Response for SSO-ESD01]

	WP remains intact	Shielding remains intact	Canister(s) remains intact	Moderator excluded from entering canister		
INIT-EVENT	WP	SHIELDING	CANISTER	MODERATOR	#	END-STATE-NAMES
					1	OK
					2	DE-SHIELD-LOSS
					3	DE-SHIELD-LOSS
					4	RR-UNFILTERED
					5	RR-UNFILTERED-ITC
RESPONSE-TRANSIT - Response tree for TEV in transit					2007/09/17	Page 4

Source: Original

Figure A5-8. Event Tree RESPONSE-TRANSIT – Response tree for TEV in Transit [Response for SSO-ESD02, and SSO-ESD05]

	WP remains intact	Canister(s) remains intact	Moderator excluded from entering canister		
INIT-EVENT	WP	CANISTER	MODERATOR	#	END-STATE-NAMES
				1	OK
				2	OK
				3	RR-UNFILTERED
				4	RR-UNFILTERED-ITC
RESPONSE-DRIFT - Response tree for WP in emplacement drift				2007/10/19	Page 6

Source: Original

Figure A5-9. Event Tree RESPONSE-DRIFT – Response tree for TEV in Emplacement Drift [Response for SSO-ESD03]

**ATTACHMENT B**  
**SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES**

## CONTENTS

	<b>Page</b>
ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES.....	B1-1
B1 TRANSPORT AND EMPLACEMENT VEHICLE — FAULT TREES ANALYSIS.....	B1-11
B1.1 REFERENCES .....	B1-11
B1.2 TRANSPORT AND EMPLACEMENT VEHICLE DESCRIPTION .....	B1-13
B1.3 DEPENDENCIES AND INTERACTIONS ANALYSIS .....	B1-20
B1.4 TEV RELATED FAILURE SCENARIOS .....	B1-21
B2 HEATING VENTILATION AND AIR CONDITIONING FAULT TREE ANALYSIS.....	B2-1
B2.1 REFERENCES .....	B2-1
B2.2 ITS HVAC DESCRIPTION .....	B2-1
B2.3 DEPENDENCIES AND INTERACTIONS.....	B2-6
B2.4 HVAC RELATED FAILURE SCENARIO .....	B2-7
B3 IMPORTANT TO SAFETY AC POWER FAULT TREE ANALYSIS.....	B3-1
B3.1 REFERENCES .....	B3-1
B3.2 ITS AC POWER DESCRIPTION.....	B3-3
B3.3 Dependencies and Interactions .....	B3-19
B3.4 ITS AC Power Failure Scenarios.....	B3-20
B4 DRIP SHIELD EMPLACEMENT GANTRY—FAULT TREE ANALYSIS .....	B4-1
B4.1 REFERENCES .....	B4-1
B4.2 DRIP SHIELD OVERVIEW.....	B4-1
B4.3 DEPENDENCIES AND INTERACTIONS ANALYSIS .....	B4-5
B4.4 DSG RELATED FAILURE SCENARIOS .....	B4-6
B5 SHIELD DOOR— FAULT TREE ANALYSIS .....	B5-1
B5.1 REFERENCES .....	B5-1
B5.2 SHIELD DOOR SYSTEM DESCRIPTION .....	B5-1
B5.3 DEPENDENCIES AND INTERACTIONS.....	B5-2
B5.4 SHIELD DOOR FAILURE SCENARIOS.....	B5-2
B6 EMPLACEMENT ACCESS DOOR ANALYSIS .....	B6-1
B6.1 REFERENCES .....	B6-1
B6.2 EMPLACEMENT ACCESS DOOR DESCRIPTION .....	B6-1
B6.3 DEPENDENCIES AND INTERACTIONS ANALYSIS .....	B6-4
B6.4 EMPLACEMENT ACCESS DOOR RELATED FAILURE SCENARIO ...	B6-4
B7 ADDITIONAL FAULT TREES.....	B7-1

**FIGURES**

	<b>Page</b>
B1.2-1. Illustration of the Transport and Emplacement Vehicle (TEV).....	B1-13
B1.2-2. Illustration of the Waste Package on Pallet .....	B1-16
B1.2-3. Illustration of the Waste Package Components .....	B1-17
B1.4-1. Uncertainty Results for the TEV Doors Impact Waste Package (FACILITY- TEV-DOOR and DRIFT-DOOR-IMPACT) Fault Tree.....	B1-24
B1.4-2. Cut Set Generation Results for the (FACILITY-TEV-DOOR and DRIFT- DOOR-IMPACT) Fault Tree.....	B1-24
B1.4-3. Uncertainty Results for TEV Collides with Object in a Facility .....	B1-27
B1.4-4. Cut Set Results for TEV Collides with Object in a Facility .....	B1-27
B1.4-5. Uncertainty Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT).....	B1-32
B1.4-6. Cut Set Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT).....	B1-32
B1.4-7. Uncertainty Results for Impact to TEV during Transit (TRANSIT-IMPACT) ...	B1-38
B1.4-8. Cut Set Generation Results for Impact to TEV during Transit (TRANSIT-IMPACT).....	B1-39
B1.4-9. Uncertainty Results for TEV Stops for Extended Time (SHIELD-STOP) .....	B1-43
B1.4-10. Cut Set Generation Results for TEV Stops for Extended Time (SHIELD- STOP) .....	B1-43
B1.4-11. Uncertainty Results for TEV Exits Facility with Open Shield Doors (SHIELD DOOR).....	B1-46
B1.4-12. Cut Sets for TEV Exits Facility with Open Shield Doors (SHIELD DOOR).....	B1-47
B1.4-13. Uncertainty Results for Package Drop During Loading in Facility (FACILITY-DROP).....	B1-50
B1.4-14. Cut Set Generation Results for Package Drop during Loading in Facility (FACILITY-DROP).....	B1-50
B1.4-15. Uncertainty Results for Waste Package Drop during Transit (TRANSIT- DROP).....	B1-55
B1.4-16. Cut Sets Generation Results for Waste Package Drop during Transit (TRANSIT-DROP).....	B1-55
B1.4-17. Uncertainty Results for Drop or Drag of Waste Package by TEV in Emplacement Drift (DRIFT-DRAG).....	B1-61
B1.4-18. Cut Set Generation Results for Drop or Drag of Waste Package by TEV in Emplacement Drift (DRIFT-DRAG).....	B1-62

**FIGURES (Continued)**

	<b>Page</b>
B1.4-19. Uncertainty Results for TEV Impacts Waste Package in Emplacement Drift (TEV-IMPACTS-WP) .....	B1-66
B1.4-20. Cut Set Generation Results for TEV Impacts Waste Package in Emplacement Drift (TEV-IMPACTS-WP) .....	B1-66
B1.4-21. DRIFT-WP-IMPACT – TEV Impacts Waste Package .....	B1-68
B1.4-22. FACILITY COLLISION – TEV Collides with Object in a Facility .....	B1-69
B1.4-23. DRIFT-TEV-IMPACT (Page 1 of 3) – TEV Collides with Object in Emplacement Drift.....	B1-70
B1.4-24. DRIFT-TEV-IMPACT (Page 2 of 3) – Subtree: DRIFT-DERAIL – TEV Derails in Emplacement Drift .....	B1-71
B1.4-25. DRIFT-TEV-IMPACT (Page 3 of 3) – Impact to TEV during Transit.....	B1-72
B1.4-26. TRANSIT-IMPACT (Page 1 of 9) – Impact to TEV during Transit.....	B1-73
B1.4-27. TRANSIT-IMPACT (Page 2 of 9) – Impact to TEV during Transit.....	B1-74
B1.4-28. TRANSIT-IMPACT (Page 3 of 9) – Impact to TEV during Transit.....	B1-75
B1.4-29. TRANSIT-IMPACT (Page 4 of 9) – Impact to TEV during Transit.....	B1-76
B1.4-30. TRANSIT-IMPACT (Page 5 of 9) – Impact to TEV during Transit.....	B1-77
B1.4-31. TRANSIT-IMPACT (Page 6 of 9) – Impact to TEV during Transit.....	B1-78
B1.4-32. TRANSIT-IMPACT (Page 7 of 9) – Impact to TEV during Transit.....	B1-79
B1.4-33. TRANSIT IMPACT (Page 8 of 9) Impact to TEV during Transit.....	B1-80
B1.4-34. TRANSIT IMPACT (Page 9 of 9) Impact to TEV during Transit.....	B1-81
B1.4-35. SHIELD-STOP – TEV Stops for Extended Time .....	B1-82
B1.4-36. SHIELD-DOOR – Inadvertent TEV Door Opening.....	B1-83
B1.4-37. FACILITY-DROP – WP Dropped While Leaving Facility .....	B1-84
B1.4-38. TRANSIT- DROP (1 of 2) Waste Package Dropped During Transit.....	B1-85
B1.4-39. TRANSIT- DROP (2 of 2) Waste Package Dropped During Transit.....	B1-86
B1.4-40. DRIFT-DRAG (1 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift.....	B1-87
B1.4-41. DRIFT-DRAG (2 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift.....	B1-88
B1.4-42. DRIFT-DRAG (3 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift.....	B1-89
B1.4-43. TEV-IMPACTS-WP – TEV Impacts Waste Package in Emplacement Drift .....	B1-90

**FIGURES (Continued)**

	<b>Page</b>
B2.2-1. Block Diagram of the CRCF ITS HVAC System .....	B2-3
B2.4-1. Uncertainty Results of the CRCF Failure to Maintain Delta Pressure Fault Tree .....	B2-13
B2.4-2. Cut Set Generation Results for the CRCF Failure to Maintain Delta Pressure Fault Tree .....	B2-14
B2.4-3. Delta Pressure not Maintained in CRCF Facility .....	B2-19
B2.4-4. Loss of Normal and Degrade HVAC Trains.....	B2-20
B2.4-5. HVAC Trains Fail in Degraded Mode.....	B2-21
B2.4-6. Train A Failure with Supply Fan Down Reduced .....	B2-22
B2.4-7. Exhaust Fan in Train A Fails Reduced .....	B2-23
B2.4-8. Exhaust HEPA Train A with Loss of Supply Fan Fails.....	B2-24
B2.4-9. HEPA Input/Output Manual Damper Fail Reduced .....	B2-25
B2.4-10. Moisture Separator/Demister HEPA Train A Fails Reduced .....	B2-26
B2.4-11. Loss of Delta Pressure Train B with Inoperative Supply Fan Reduced .....	B2-27
B2.4-12. Exhaust Fan in Train B Fails .....	B2-28
B2.4-13. HEPA Filters in Train B Failed Reduced Operation .....	B2-29
B2.4-14. HEPA Input/Output Manual Damper Train B Fail Reduced.....	B2-30
B2.4-15. HEPA Input/Output Manual Damper Train B Fail Reduced.....	B2-31
B2.4-16. HVAC Train A is Inoperable.....	B2-32
B2.4-17. Exhaust HEPA Equipment in Train A Fails .....	B2-33
B2.4-18. HEPA Input/Output Manual Damper Fail .....	B2-34
B2.4-19. Moisture Separator/Demister HEPA Train A Fails .....	B2-35
B2.4-20. HVAC Train B is Inoperable .....	B2-36
B2.4-21. Exhaust HEPA Equipment in Train B Fails .....	B2-37
B2.4-22. HEPA Input/Output Manual Damper Train B Fail.....	B2-38
B2.4-23. Moisture Separator/Demister .....	B2-39
B3.2-1. AC Power – Main Electrical Distribution.....	B3-4
B3.2-2. AC Power – 13.8 kV ITS Switchgear Train A .....	B3-5
B3.2-3. AC Power – 13.8 kV ITS Switchgear Train B.....	B3-6
B3.2-4. Emergency Diesel Generator Facility – 480 V ITS Motor Control Center Train A .....	B3-7

**FIGURES (Continued)**

	<b>Page</b>
B3.2-5. ITS 125 V DC System Train A.....	B3-8
B3.2-6. Emergency Diesel Generator facility – 480V ITS Motor Control Center Train B .....	B3-9
B3.2-7. ITS 125 V DC System Train B.....	B3-10
B3.2-8. CRCF ITS Load Center Train A.....	B3-11
B3.2-9. CRCF ITS Load Center Train B.....	B3-12
B3.2-10. CRCF ITS MCC Train A.....	B3-13
B3.2-11. CRCF ITS MCC Train B .....	B3-14
B3.2-12. ITS Diesel Generator Fuel Oil System .....	B3-16
B3.2-13. Simplified Diagram of Representative Train of CRCF ITS Electrical and ITS Battery Rooms Ventilation System.....	B3-17
B3.4-1. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree .....	B3-29
B3.4-2. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train A.....	B3-29
B3.4-3. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train B Fault Tree .....	B3-41
B3.4-4. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train B.....	B3-41
B3.4-5. Loss of Power to CRCF ITS Load Center Train A Sheet 1.....	B3-45
B3.4-6. Loss of Power to CRCF ITS Load Center Train A Sheet 2.....	B3-46
B3.4-7. Loss of Power to CRCF ITS Load Center Train A Sheet 3.....	B3-47
B3.4-8. Loss of Power to CRCF ITS Load Center Train A Sheet 4.....	B3-48
B3.4-9. Loss of Power to CRCF ITS Load Center Train A Sheet 5.....	B3-49
B3.4-10. Loss of Power to CRCF ITS Load Center Train A Sheet 6.....	B3-50
B3.4-11. Loss of Power to CRCF ITS Load Center Train A Sheet 7.....	B3-51
B3.4-12. Loss of Power to CRCF ITS Load Center Train A Sheet 8.....	B3-52
B3.4-13. Loss of Power to CRCF ITS Load Center Train A Sheet 9.....	B3-53
B3.4-14. Loss of Power to CRCF ITS Load Center Train A Sheet 10.....	B3-54
B3.4-15. Loss of Power to CRCF ITS Load Center Train A Sheet 11.....	B3-55
B3.4-16. Loss of Power to CRCF ITS Load Center Train A Sheet 12.....	B3-56
B3.4-17. Loss of Power to CRCF ITS Load Center Train B Sheet 1.....	B3-57

**FIGURES (Continued)**

	<b>Page</b>
B3.4-18. Loss of Power to CRCF ITS Load Center Train B Sheet 2 .....	B3-58
B3.4-19. Loss of Power to CRCF ITS Load Center Train B Sheet 3 .....	B3-59
B3.4-20. Loss of Power to CRCF ITS Load Center Train B Sheet 4 .....	B3-60
B3.4-21. Loss of AC Power to CRCF ITS Load Center Train B Sheet 5 .....	B3-61
B3.4-22. Loss of AC Power to CRCF ITS Load Center Train B Sheet 6 .....	B3-62
B3.4-23. Loss of AC Power to CRCF ITS Load Center Train B Sheet 7 .....	B3-63
B3.4-24. Loss of AC Power to CRCF ITS Load Center Train B Sheet 8 .....	B3-64
B3.4-25. Loss of AC Power to CRCF ITS Load Center Train B Sheet 9 .....	B3-65
B3.4-26. Loss of AC Power to CRCF ITS Load Center Train B Sheet 10 .....	B3-66
B3.4-27. Loss of AC Power to CRCF ITS Load Center Train B Sheet 11 .....	B3-67
B3.4-28. Loss of AC Power to CRCF ITS Load Center Train B Sheet 12 .....	B3-68
B4.2-1. Illustration of a Drip Shield .....	B4-2
B4.2-2. Illustration of the Drip Shield Emplacement Gantry (DSG) .....	B4-3
B4.4-1. Uncertainty Results for the DRIPSHIELD-DROPPED Fault Tree .....	B4-8
B4.4-2. Cut Set Generation Results for the DRIPSHIELD-DROPPED Fault Tree .....	B4-8
B4.4-3. DRIPSHIELD-DROPPED - Fault Tree for Drop of Drip Shield onto a Waste Package .....	B4-10
B5.4-1. Uncertainty Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree .....	B5-4
B5.4-2. Cut Set Generation Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree .....	B5-5
B5.4-3. FACILITY-SHIELD-DOOR – Facility Door Closes on TEV Fault Tree Sheet.....	B5-7
B6.2-1. Illustration of an Emplacement Access Door .....	B6-3
B6.4-1. Uncertainty Results for AC-DRIMP-INIT .....	B6-7
B6.4-2. Cut Set Generation Results for AC-DRIMP-INIT .....	B6-7
B6.4-3. DRIFT-TEV-DROPON - Fault Tree for Emplacement Access Door Closes on TEV .....	B6-9
B7-1. Facility-Drop on Fault Tree .....	B7-3
B7-2. Transit-Derail Fault Tree .....	B7-4
B7-3. Transit-Drop on Fault Tree .....	B7-5
B7-4. DRIFT-TEV-IMPACT Fault Tree .....	B7-6

**FIGURES (Continued)**

	<b>Page</b>
B7-5. Drift-WP-Drop on Fault Tree .....	B7-7
B7-6. Drift-WP-Impact Fault Tree .....	B7-8
B7-7. DSGANT-INIT Fault Tree .....	B7-9
B7-8. SSO-CRCF-SD-IMPACT-HVAC Fault Tree.....	B7-10
B7-9. SSO-HVYLOAD-DROPON-HVAC Fault Tree .....	B7-11
B7-10. SSO-TEV-COLL-HVAC Fault Tree .....	B7-12
B7-11. SSO-WP-DROP-HVAC Fault Tree.....	B7-13
B7-12. SSO-WP-TEV-SD-HVAC Fault Tree .....	B7-14
B7-13. SHIELD-PROXIMITY Fault Tree .....	B7-15
B7-14. SHIELD-ENTRY Fault Tree .....	B7-16
B7-15. FIRE-DRIFT Fault Tree .....	B7-17
B7-16. FIRE-SUBSURFACE Fault Tree .....	B7-18
B7-17. FIRE-SURFACE Fault Tree .....	B7-19

**TABLES**

	<b>Page</b>
B1.2-1. TEV Shielding Configuration .....	B1-14
B1.3-1. Dependencies and Interactions Analysis .....	B1-20
B1.4-1. Basic Event Probabilities for Waste Package Impact from the TEV Front Shield Doors.....	B1-23
B1.4-2. DRIFT-DOOR-IMPACT Cut Sets .....	B1-25
B1.4-3. Basic Event Probabilities for TEV Collision within Facility.....	B1-26
B1.4-4. Facility-Collision Cut Sets .....	B1-28
B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit.....	B1-30
B1.4-6. DRIFT-TEV-IMPACT Cut Sets .....	B1-33
B1.4-8. TRANSIT-IMPACT Cut Sets.....	B1-39
B1.4-9. Basic Event Probabilities for TEV Stops for Extended Time.....	B1-41
B1.4-10. SHIELD STOP Cut Sets .....	B1-44
B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit.....	B1-45
B1.4-12. SHIELD-DOOR Cut Sets .....	B1-47
B1.4-13. Basic Event Probabilities for Waste Package Drop in Facility.....	B1-49
B1.4-14. FACILITY-DROP Cut Sets .....	B1-51
B1.4-15. Basic Event Probabilities for Waste Package Dropped during Transit .....	B1-53
B1.4-16. TRANSIT-DROP Cut Sets .....	B1-56
B1.4-17. Basic Event Probabilities for a Waste Package Drop or Dragging in an Emplacement Drift.....	B1-59
B1.4-18. DRIFT-DRAG Cut Sets.....	B1-62
B1.4-19. Basic Event Probabilities for TEV Collides with Emplaced Waste Package.....	B1-65
B1.4-20. TEV-IMPACTS-WP Cut Sets .....	B1-67
B2.2-1. ASD Response to Variations in Delta Pressure .....	B2-5
B2.3-1. Dependencies and Interactions Analysis .....	B2-7
B2.4-1. Basic Event Probability for the HVAC Failure to Maintain Delta Pressure in the CRCF .....	B2-10
B2.4-2. Human Failure Events.....	B2-12
B2.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure in the CRCF .....	B2-15
B3.3-1. Dependencies and Interactions Analysis .....	B3-19

**TABLES (Continued)**

	<b>Page</b>
B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree .....	B3-23
B3.4-2. Human Failure Events.....	B3-27
B3.4-3. Common-Cause Basic Events.....	B3-28
B3.4-4. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train A.....	B3-30
B3.4-5. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train B Fault Trees.....	B3-35
B3.4-6. Human Failure Events.....	B3-39
B3.4-7. Common-Cause Basic Events.....	B3-40
B3.4-8. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train B .....	B3-42
B4.3-1. Dependencies and Interactions Analysis .....	B4-5
B4.4-1. Drip Shield Dropped on Waste package.....	B4-7
B4.4-2. DRIPSHIELD-DROPPED Cut Sets.....	B4-9
B5.3-1. Dependencies and Interactions Analysis .....	B5-2
B5.4-1. Basic Event Data.....	B5-3
B5.4-2. Cut Sets for Facility Shield Door – Facility Door Closes on TEV.....	B5-5
B6.3-1. Dependencies and Interactions Analysis .....	B6-4
B6.4-1. Basic Event Data for Closure of Drift Doors on TEV.....	B6-6
B6.4-2. AC-DRIMP-INIT Cut Sets .....	B6-8
B7-1. Top Level and Linking Fault Trees .....	B7-1
B7-2. Basic Events for Additional Fault Trees.....	B7-2

## **ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES**

This attachment describes the fault trees developed for subsurface 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.

This Attachment is not intended to be a stand-alone analysis. Inputs to the fault tree models are documented in different sections of the report. These include:

- Basic events related to active component failure, the data development is provided in Attachment C and Section 6.3-1.
- Human reliability assessment is documented in Attachment E and Section 6.4.

Fault trees results, including cut sets, mean probabilities and uncertainties, are outputs from SAPHIRE modeling.

### **B1 TRANSPORT AND EMPLACEMENT VEHICLE — FAULT TREES ANALYSIS**

#### **B1.1 REFERENCES**

The PCSA is a safety analysis 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), paragraph 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

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

B1.1.1 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.

B1.1.2 Not used

B1.1.3 Not used

B1.1.4 Not used

B1.1.5 Not Used.

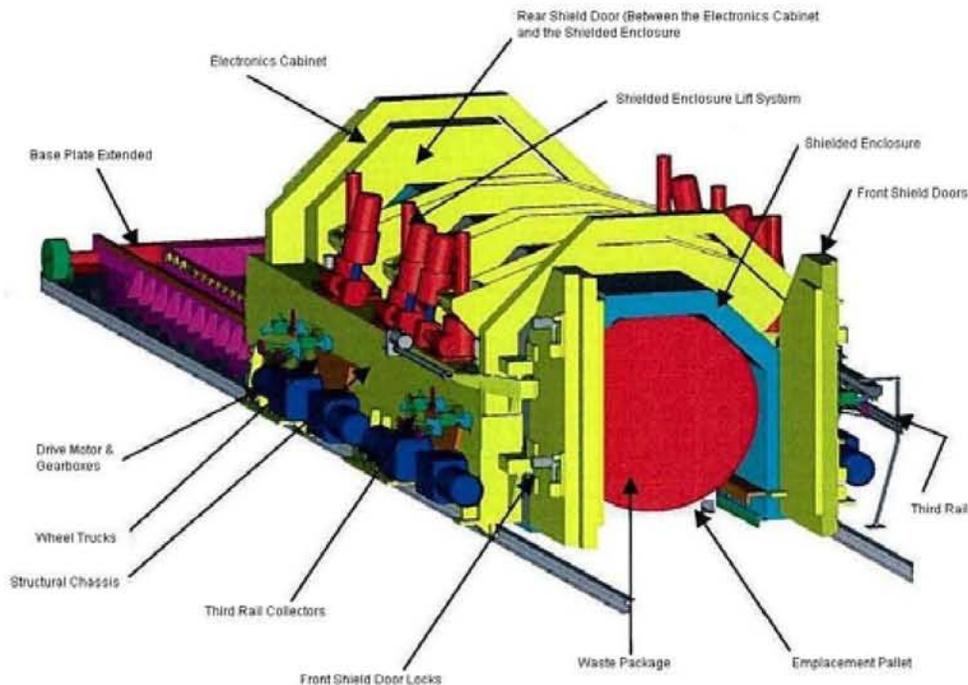
- B1.1.6 BSC 2007. *Emplacement and Retrieval Transport And Emplacement Vehicle Mechanical Equipment Envelope*. 800-MJ0-HE00-00101-000-REV B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070918.0041.
- B1.1.7 BSC 2007. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle*. 000-30R-HE00-00200-000 REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071205.0002.
- B1.1.8 Not used
- B1.1.9 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.
- B1.1.10 BSC 2007. *Naval Waste Package Design Report*. 000-00C-DNF0-00800-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071030.0043.
- B1.1.11 BSC 2007. *Project Design Criteria Document*. 000-3DR-MGR0-00100-000-007. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071016.0005.
- B1.1.12 BSC 2007. *TAD Waste Package Configuration*. 000-MW0-DSC0-00101-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0010.
- B1.1.13 BSC 2007. *Transport and Emplacement Vehicle Envelope Calculation*. 800-MQC-HE00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0043.
- B1.1.14 BSC 2007. *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3*. 800-MH0-HEE0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0034.
- B1.1.15 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 1 of 3)*. 800-M60-HE00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0041.
- B1.1.16 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 2)*. 800-M60-HE00-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0042.
- B1.1.17 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 3)*. 800-M60-HE00-00103-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0043.
- B1.1.18 \*CRWMS M&O 1998. *Evaluation of WP Transporter Neutron Shielding Materials*. BCAA00000-01717-0210-00002 REV 000. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990119.0320.

B1.1.19 BSC (Bechtel SAIC Company) 2007. *Drip Shield and Waste Package Emplacement Pallet Design Report*. 000-00C-SSE0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070810.0008; ENG.20080305.0004.

## B1.2 TRANSPORT AND EMPLACEMENT VEHICLE DESCRIPTION

### B1.2.1 Overview

The transport and emplacement vehicle (TEV) is an electrically powered, rail-based, vehicle (Figure B1.2.-1) that is used to transport a waste package and an emplacement pallet from a surface nuclear facility into the subsurface repository for emplacement (Ref. B1.1.7). The equipment on the TEV is proven and commercially available technology, primarily nuclear and heavy industrial crane applications. The TEV travels along a dedicated rail system. The TEV is radiation shielded so that it is capable of safely transporting radioactive waste packages. The TEV contains multiple mechanical features for handling of the waste packages. The TEV contains multiple mechanical features for handling of the waste packages. The TEV is remotely controlled and monitored by operators in the central control center, using the Digital Control and Management Information System (DCMIS) interfacing to an onboard redundant programmable logic controller (PLCs). (Ref. B1.1.7, Section 2.1) In most cases, operation of the TEV is under PLC control with only general oversight from a central control, but some in some cases, operations that are solely under manual control are performed as needed.



Source: Modified from *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle*, (Ref. B1.1.7)

Figure B1.2-1. Illustration of the Transport and Emplacement Vehicle (TEV)

The maximum loaded TEV weighs approximately 300 short tons and has nominal height, width, and length of 11.1 × 15.4 × 29.8 ft respectively (Ref. B1.1.6). The instrumentation of the TEV is described in associated process and instrumentation diagrams (Ref. B1.1.15), (Ref. B1.1.16), and (Ref. B1.1.17).

Specific components of the TEV that are considered in fault trees are described in the following sections. The discussions are based on *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (Ref. B1.1.7).

### B1.2.2 TEV Drive Wheels

The TEV has eight wheels (four on each side) each driven by an electric motor. To limit derailment, the wheels on one side of the vehicle are double-flanged (Ref. B1.1.7). The wheels travel on 171 lb crane rail with a gauge of 11 ft, installed in accordance with the requirements of ASME NOG-1 2004, 2005 (Ref. B1.1.1).

### B1.2.3 TEV Electronics Cabinet

The PLCs and other electronic controls of the TEV are housed in a separate cabinet, positioned externally at the rear of the TEV shielded enclosure. This compartment houses a number of sub-enclosures that contain the control and instrumentation components with duplicate equipment to provide defense in depth. Each sub-enclosure is totally enclosed to provide fire protection and protection against internal explosions. The overall compartment also contains a heating, ventilation, and air-conditioning (HVAC) unit to maintain the operating environment for the control instrumentation, as well as a fire detection system that activate the onboard fire suppression system, should fire be detected within this compartment (Ref. B1.1.7).

### B1.2.4 TEV Shielding

The shielding of the TEV shielded enclosure is approximately 10 in thick and constructed of a layered metal/polymer composite (Table B1.2-1). The TEV shield enclosure is not airtight, but the shielding prevents a dose rate in excess of 100 mrem/hr at 11.81 in. from the external accessible surfaces, based on design requirements (Ref. B1.1.11, Table 4.10.1-1). The only non-metallic component, the synthetic polymer material, NS-4-FR, is a fire-resistant neutron shielding material with a maximum continuous operating temperature limit of 150° C (300° F) (Ref. B1.1.18, Attachment II).

Table B1.2-1. TEV Shielding Configuration

Component	Material	Layer Thickness (inches)
Inner layer	Austenitic stainless steel, SS316L (UNS S31603)	1.5
Gamma shield	Depleted Uranium	1.5
Structural steel	Austenitic stainless steel, SS316L (UNS S31603)	0.5

Table B1.2-1. TEV Shielding Configuration (Continued)

Component	Material	Layer Thickness (inches)
Neutron shield	Synthetic polymer material, NS-4-FR	6.0
Outer layer	Stainless steel, SS3316L	0.5
Total shielding thickness		-10.0

NOTE: Material layers start with inner material at the top of the list and progresses to the shielding outer layer at the base of the list.

Source: Modified from (Ref. B1.1.7, Table 3).

### B1.2.5 TEV Lift System

The TEV engages the waste package by raising the entire shielded enclosure. To lower and raise the enclosure, six screw jacks are mounted on the TEV exterior frame, with the front and rear jacks used in normal operations and two central jacks acting as backup units. The jacks for normal operations are to be nominally 100 tons screw jacks with 20 inch travel. The backup units are to have a nominal 150 tons capacity. These jacks have the ability to self-lock in the event of drive failure (Ref. B1.1.13, Section 6.5).

### B1.2.6 TEV Base Plate

The TEV incorporates a moveable radiation shield for the bottom of the TEV known as the base shielding plate, or simply the base plate. The base plate is extended and retracted from below the TEV by a simple gear motor driving a rack and pinion drive system mounted to the chassis on each side of the base plate. As the base plate extends, the end is supported by a separate set of wheels at the rear of the TEV (Figure B1.2-1). The base plate is mechanically interlocked with the TEV front shield doors; this interlock prevents the extension of the base plate if the shield doors are closed. In addition, as the plate interfaces with the shielded enclosure, it prevents the enclosure from dropping (Ref. B.1.1.7).

### B1.2.7 TEV Shield Doors

To allow the loading and emplacement of waste packages, the TEV has two-hinged shield doors at the front of the TEV. Door movement is provided by electromechanical linear actuators. The door hinge system consists of four structural features at the front and on both sides of the main TEV chassis, which provide a solid mounting for four hinge pins or vertical pivot shafts. Additionally, the four door hinge structures house radial and thrust bearings that allow easy and precise radial movement of the doors. The shield doors have the same shielding configuration as the shielded enclosure.

The door hinges are mounted to the structural chassis of the TEV, not to the shielded enclosure, which provides a mechanical interlock that prevents the shielded enclosure from being lowered until the front shield doors are fully opened. In addition, to prevent the inadvertent opening of the shield doors during transit, the TEV incorporates an electro-mechanical interlock for the front shield doors. To allow the doors to open, a special switch is placed along the rail line next to

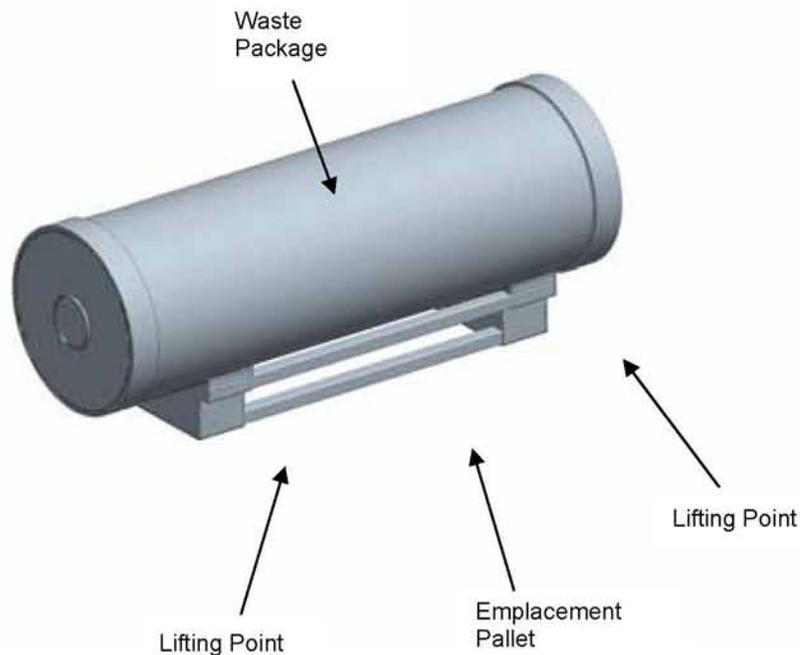
waste handling facilities or in front to emplacement drift turnouts. The switch deactivates an interlock on the TEV upon entry to allow the TEV shield doors to open. Conversely, the switch reactivates the interlock as the TEV exits either a facility or emplacement drift (Ref. B.1.1.7).

### B1.2.8 TEV Linear Drive Gear Motors

Each of the TEV's eight wheels are driven by a 20 hp (15kW) AC, 480 volt, 1750 rpm motor featuring integral disc brakes. Each motor is coupled to a flange mounting gear gearbox that has a nominal output speed of seventeen (17) rpm, a torque output of 72,200 lb-in., and a gearbox ratio of one hundred point seven five to one (100.75:1) (Ref.B1.1.7, Section 3.3.4).

### B1.2.9 Waste Package

Waste packages are emplaced in the subsurface facility, each containing canisterized nuclear waste (Figure B1.2-2). A nuclear waste canister (or several canisters) is placed into a cylindrical waste package which is then welded closed within a surface handling facility prior to transport into the subsurface. The waste package provides containment to prevent or limit the introduction of a moderator into the disposed waste form, and to prevent or limit the release of radionuclides into the environment (Ref. B1.1.12).

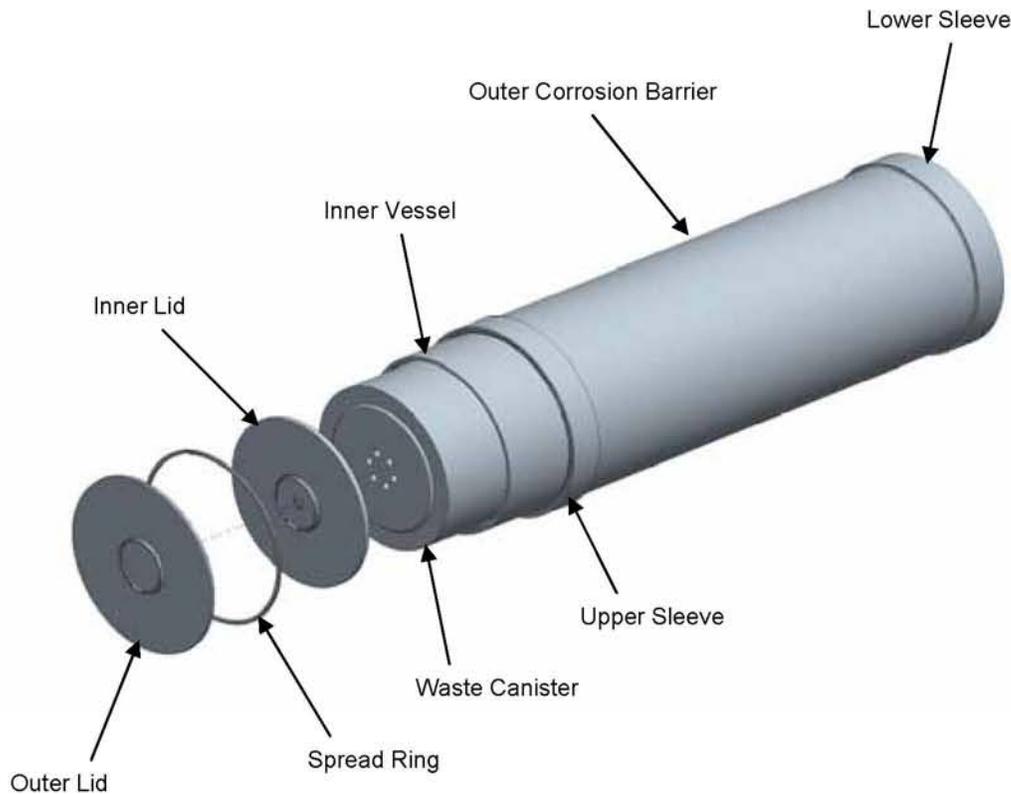


Source: Modified from (Ref. B1.1.19, Figure 2).

Figure B1.2-2. Illustration of the Waste Package on Pallet

The waste canisters within the waste package contain one of several waste forms, including: (1) spent nuclear fuel (SNF) in a transportation, aging, and disposal (TAD) canisters; (2) canistered U.S. Department of Energy (DOE) SNF, including canistered naval SNF; and (3) canistered high-level radioactive waste (HLW) from prior commercial and defense fuel-reprocessing operations.

Approximately 12,000 waste packages of various sizes will be emplaced in the repository (Ref. B1.1.9). The general waste package design consists of two concentric cylinders in which the canisters are placed, illustrated in Figure B1.2-3.



Source: Modified from Ref. B1.1.10, Figure 1.

Figure B1.2-3. Illustration of the Waste Package Components

Within the emplacement drift and above the invert, each waste package rests upon a composite metal frame or pallet. The pallet consists of two V-shaped supports of Alloy 22 (UNS N06022), which are tied together by stainless steel tubes (UNS S31600). To prevent damage to the waste package, the waste package is handled solely using this pallet, to ensure that the handling equipment does not make direct contact with the waste package during normal subsurface operations.

### **B1.2.10 Operations**

The TEV operations can be divided into three aspects:

1. **Waste Package and Pallet Receipt**—the process of the TEV loading the waste package and moving out of the facility.
2. **Waste Package and Pallet Transportation**—the process of the TEV moving the waste package from the facility on the surface into subsurface up to the entrance of the emplacement drift.
3. **Waste Package and Pallet**—the process of the TEV moving the waste package into the emplacement drift, placing the waste package and pallet on the invert and then moving out of the drift.

Block diagrams on TEV operations are provided in *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3* (Ref. B1.1.14).

### **B1.2.11 Waste Package and Pallet Receipt**

The TEV is designed to remotely receive a waste package and emplacement pallet in the waste package loadout rooms within a surface nuclear facility. Prior to staging a waste package and emplacement pallet within the surface nuclear facility waste package loadout room, the TEV enters the surface nuclear facility; the TEV passes over a stationary actuating bracket, which closes an ITS switch located on the TEV, allowing the TEV shielded enclosure to be opened. The facility shield doors and confinement doors are closed and secured after the TEV has entered the waste package loadout room.

After ensuring the facility doors are secured, the TEV front shield door locks are unlocked and the front shield doors are opened. The rear shield door is raised to the open position and the base plate is extended. The screw jacks are raised from a lowered park position to engage the lifting features and to support the weight of the shielded enclosure. When this action is completed, the transportation shot bolts are retracted into an unlocked position. The entire shielded enclosure is then lowered for waste package and emplacement pallet receipt. After the shielded enclosure has been lowered, a waste package and emplacement pallet are loaded into the shielded enclosure, such that the integral shielded enclosure lifting features are positioned under the emplacement pallet lifting points. Onboard cameras are used to identify the waste package. The shielded enclosure is then raised to the transport height and the transportation shot bolts are extended back into a locked position. This action allows the screw jacks to be driven back into a lowered park position. The base plate is retracted and the rear shield door is lowered, which mechanically prevents movement of the base plate. The front shield doors are closed and locked. Once this operation is completed, the facility doors are opened and the TEV moves, in reverse, out of the facility waste package loadout room. Movement of the TEV out of this room past the stationary actuating bracket opens the ITS switch on the TEV, which disables unlocking of the front shield doors and raising of the rear shield door (Ref. B1.1.7).

### **B1.2.12 Waste Package and Pallet Transportation**

The TEV travels along a rail line spur from the surface nuclear facilities, through a switch allowing access onto the surface main TEV rail line that proceeds to the North Portal. Prior to arrival at the North Portal, the TEV passes through a series of switches to establish the correct direction of travel. Confirmation of the rail switch positions are verified by operators in the central control center via the TEV front and rear cameras or by DCMIS of the rail switch position.

The TEV stops at the North Portal for an inspection and remote monitoring check of TEV systems by operators in the central control center prior to descent of the North Ramp. After the inspection and monitoring check, the TEV then proceeds through the North Portal, down the North Ramp, through the curve (at the ramp base), and continues to the turnout of the selected emplacement drift.

Each emplacement drift turnout has an emplacement bulkhead with emplacement access doors. The configuration of each turnout is an initial curve, a straight segment, and a transition into an emplacement drift.

As the TEV nears the predetermined emplacement drift turnout rail switch, the operators in the central control center confirm the correct position of the rail switch. The TEV proceeds through the rail switch to the emplacement access door where it stops. TEV onboard positional sensors (linear drive encoders) are then calibrated to confirm the vehicle location and establish a waste package positional datum point. The operators in the central control center perform this calibration remotely. When calibration is complete, the emplacement access doors are opened, the TEV enters, and the emplacement access doors close after the TEV has passed through. The stationary actuating bracket located on the TEV rails inside the emplacement access doors close the ITS switch on the TEV, allowing unlocking of the front shield doors and raising of the rear shield door (Ref. B1.1.7).

### **B1.2.13 Waste Package and Pallet Emplacement**

After entering an emplacement drift, the TEV travels at a nominal design speed of 150 ft per minute and stops at a predetermined position that is relative to a previously emplaced waste package. The locks on the front shield doors are unlocked and opened. The rear shield door is raised to the open position and the base plate is extended.

The TEV then moves forward at a crawl speed, nominally 15 feet per minute, to a predetermined position that is relative to a previously emplace waste package. At this stage, the cameras and lights mounted on the top of the TEV are turned on. The forward range detection indicator is also closely monitored during this time; these instruments add confirmation for positioning a waste package carried by a TEV as it nears a previously emplaced waste package.

The speed of the TEV is then decreased further and it proceeds forward at a slow crawl speed, nominally 1.5 ft per minute, until the emplacement position of the onboard waste package and emplacement pallet is reached. Onboard cameras and lights are used by operators in the central control center to confirm the final position. When the waste package is confirmed as correctly positioned, screw jacks are raised from a lowered parked position to engage the lifting features

and support the weight of the shielded enclosure. Transportation shot bolts are retracted into the unlocked position. The shielded enclosure is lowered, placing the waste package and pallet on the emplacement drift invert structure. The weight indications for the screw jacks are monitored to confirm that the waste package and emplacement pallet are not being supported.

After placing the waste package and emplacement pallet, the TEV moves at a slow crawl speed away from the emplaced waste package and pallet to a predetermined distance and stops, allowing proper operation of the front shield doors. The shielded enclosure is raised to the travel height and the transportation shot bolts are extended into the locked position, allowing the screw jacks to be driven into a lowered parked position. The base plate is retracted and the rear shield door is lowered, mechanically preventing movement of the base plate. The front shield doors are closed and locked. When these actions are completed, the TEV returns through the emplacement drift and turnout to the emplacement access doors at the design nominal operating speed of 150 ft per minute.

Movement of the TEV past the stationary actuating bracket inside the emplacement access doors opens the ITS switch on the TEV, disabling unlocking of the front shield doors and raising the rear shield door, thus ensuring that the shielded enclosure cannot be opened inadvertently. The TEV returns to the surface nuclear facility, reversing the steps taken during travel from the surface nuclear facility to the emplacement location (Ref. B1.1.7).

### B1.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B1.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B1.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Third rail electrical power	Provides powered for vehicle motion and controls	—	—	—	
Programmable logic controllers	Provide local control of mechanical systems	Failure due to high temperature or radiation	—	—	—

Table B1.3-1. Dependencies and Interactions Analysis (Continued)

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Control enclosure HVAC system	Provides proper environment for logic controllers	Provides proper environment for control system	—	—	—
Linear-drive gear motors for wheels	Provides motive force for vehicle	—	—	—	—
Rail system (including switches)	Constrains and supports vehicle movement	—	Controls vehicle path	—	Seismic loading can fail rail system
Motorized lifting screw jacks (lift system)	Lower and raise shielded enclosure	—	Constrains motion of shielded enclosure	—	—
Front shield doors	Provides shielding for waste package	—	Interlocks with base plate preventing movement while doors are closed	—	—
Base plate	Provides shielding for waste package	—	Interlocks with shield enclosure, preventing lowering of base plate when retracted	—	—
Shielded enclosure	Provides shielding for waste package	—	Engages pallet for waste package transport	—	—
Central control and communication system	Controls operation	—	—	Incorrect instruction	—

Source: Original

#### B1.4 TEV RELATED FAILURE SCENARIOS

There are 10 separate failure scenarios represented by fault trees associated with the TEV:

1. TEV front shield doors impact a waste package. Fault tree FACILITY-TEV-DOOR
2. TEV collision within facility. Fault tree FACILITY-COLLISION
3. TEV collides with object during emplacement in drift. Fault tree DRIFT-TEV-IMPACT
4. Impact to TEV during transit. Fault tree TRANSIT-IMPACT

5. TEV stops for extended time. Fault tree SHIELD-STOP
6. Inadvertent TEV door opening during transit. Fault tree SHIELD-DOOR
7. Waste package drop in facility. Fault tree FACILITY-DROP
8. Waste package dropped during transit. Fault tree TRANSIT-DROP
9. Waste package drop or dragging in an emplacement drift. Fault tree DRIFT-DRAG
10. TEV collides with emplaced waste package. Fault tree TEV-IMPACTS-WP.

#### **B1.4.1 TEV Door Impacts a Waste Package**

##### **B1.4.1.1 Description**

The scenario describes the closure of the TEV's front shield doors onto, and impacting, a waste package during either loadout or emplacement operations. During loadout operations, the occurrence can be realized when the TEV has moved to the loadout station and waste package is being inserted into the TEV shielded enclosure (prior to the start of TEV operations to engage the waste package pallet). During emplacement operations, the occurrence can be realized when the TEV has moved to the emplacement location within the drift and the waste package is being removed from the TEV for emplacement. If during either of these periods, one or both of the TEV shield doors is activated, the door or doors will impact laterally on the waste package pinching the waste package between the doors. Note that TEV interlock for the shield doors is not activated at this stage to prevent the door operation.

##### **B1.4.1.2 Success Criteria**

The success criterion for the scenario is that the TEV's front shield doors operate without spurious movement. During the normal operations, the shield door system is not to close onto the waste package during movement of the waste package under the TEV shielded enclosure.

##### **B1.4.1.3 Design Requirements and Features**

The following requirements are identified with respect to this scenario:

- The operational status of the TEV shield doors is clearly displayed for the remote operator on the control panel, including the opening and closing of the shield doors.
- The door actuators on the front shield door are sized so that the force of door closure on a waste package is minimized while assuring proper door operation.
- The waste package is designed to sustain the expected lateral force of door closure on a waste package without breach of the waste package containment.
- Normal periodic maintenance and inspection is performed on the TEV control system to minimize the generation of spurious signals.

### B1.4.1.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-TEV-DOOR or DRIFT-DOOR-IMPACT. Identical fault trees are used for both occasions. The top event is the occurrence of the TEV's front shield doors closing and impacting the waste package as the package is inserted into the TEV. This top event is realized by either the occurrence of the door closure due to a spurious signal from programmable logic controller or the spurious operation of the door actuators. The generation of the spurious signal from programmable logic controller is represented by a basic event. The spurious operation of a door actuator can be caused by either of the door actuators, as represented by two basic events connected through an OR gate. The fault tree is presented graphically in Figure B1.4-21. (DRIFT-DOOR-IMPACT is shown; FACILITY-TEV-DOOR is identical.)

### B1.4.1.5 Basic Events Data

Table B1.4-1 contains a list of basic events used in the fault tree, DRIFT-DOOR-IMPACT, for a waste package impact from the TEV front shield doors.

Table B1.4-1. Basic Event Probabilities for Waste Package Impact from the TEV Front Shield Doors

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda <sup>a</sup>
800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op – TEV Doors	3	1.460E-06	0.000E+00	3.650E-07
800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06
800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

#### B1.4.1.5.1 Human Failure Events

No basic event is identified as associated with human error involving the closure of the TEV doors.

#### B1.4.1.5.2 Common-Cause Failures

There are no common-cause failures (CCFs) identified for this model.

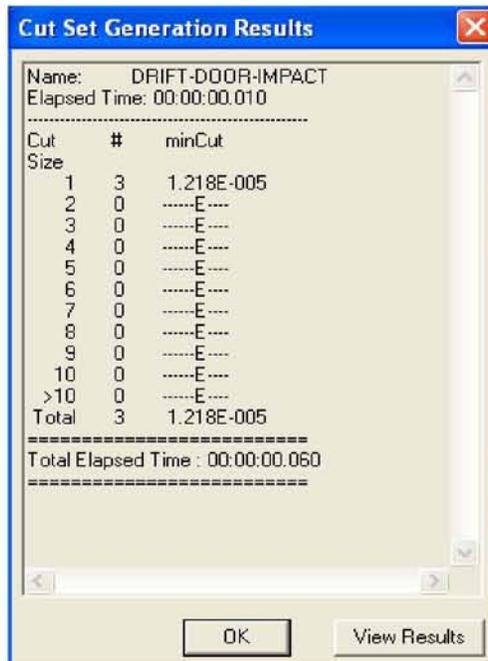
### B1.4.1.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Door Impacts a Waste Package” are presented in Figures B1.4-1 and B1.4-2.



Source: Original

Figure B1.4-1. Uncertainty Results for the TEV Doors Impact Waste Package (FACILITY-TEV-DOOR and DRIFT-DOOR-IMPACT) Fault Tree



Source: Original

Figure B1.4-2 Cut Set Generation Results for the (FACILITY-TEV-DOOR and DRIFT-DOOR-IMPACT) Fault Tree

### B1.4.1.7 Cut Sets

Table B1.4-2 contains the cut sets for the DRIFT-DOOR-IMPACT fault tree

Table B1.4-2 DRIFT-DOOR-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
44.01	44.01	5.360E-06	800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
88.02	44.01	5.360E-06	800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
100.00	11.99	1.460E-06	800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	1.460E-06

NOTE: Op = operation; PLC = programmable logic control; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

## B1.4.2 TEV Collision within Facility

### B1.4.2.1 Description

The scenario describes the collision of the TEV within the facility. After the TEV engages the waste package and pallet, and closes the shield doors, the TEV moves along the rail system to exit the facility. The scenario involves the collision of the TEV with a facility door or piece of equipment during uncontrolled movement of the TEV during the facility exit. If the facility shield door is impacted, the door system may fail, allowing the door to impact the TEV.

### B1.4.2.2 Success Criteria

Success criteria for the scenario is that the TEV moves out of the facility without spurious operations, and when under manual control, that the TEV functions properly. During the normal operations, the TEV is to move in a predictable fashion from the loadout station to outdoors without collision.

### B1.4.2.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The facility shield doors are be able to sustain the impact from the TEV such that after an impact from the TEV traveling at full operational speed, the facility shield door is retained in position and does not collapse onto the TEV.
- The operational status of the TEV is clearly displayed for the remote operator and cameras and other sensors are provided to monitor the TEV motion and avoid collision.

#### B1.4.2.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-COLLISION. Figure B1.4-22 presents the fault tree graphic for this model. The top event is the TEV collides with a structural component of a facility. This top event is realized by either the occurrence an improper command due to human error or by mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to TEV moving in an uncontrolled fashion, caused by either a spurious signal from programmable logic controller or the TEV activation to full operational speed by a switch failure when under manual control. The spurious signal generated by programmable logic controller is represented as a basic event. The switch failure requires the joint occurrence of the TEV being under manual control together with the switch failure when activated. These factors are each represented by as a basic event. The fault tree is presented graphically in Figure B1.4-22.

#### B1.4.2.5 Basic Events Data

Table B1.4-3 contains a list of basic events used in the fault tree, FACILITY-COLLISION, for a TEV collision within waste handling facility.

Table B1.4-3. Basic Event Probabilities for TEV Collision within Facility

Name	Description	Calc. Type	Calculated Probability	Mean Failure Probability	Lambda
800-HEE0-IMPACT-HFI-NOD	Operator causes uncontrolled movement of TEV	1	1.000E-03	1.000E-03	0.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC Spurious OP	3	1.460E-06	0.000E+00	3.650E-07
800-TEV1-HNSWCH-SEL-FOH	Speed Selector Fails – Hand switch included	3	1.664E-05	0.000E+00	4.160E-06
TEV-CONTROL-MANUAL	TEV is operating in manual mode	1	1.000E-01	1.000E-01	0.000E+00

NOTE: Calc. calculation; Op = operation; PLC = programmable logic control; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

##### B1.4.2.5.1 Human Failure Events

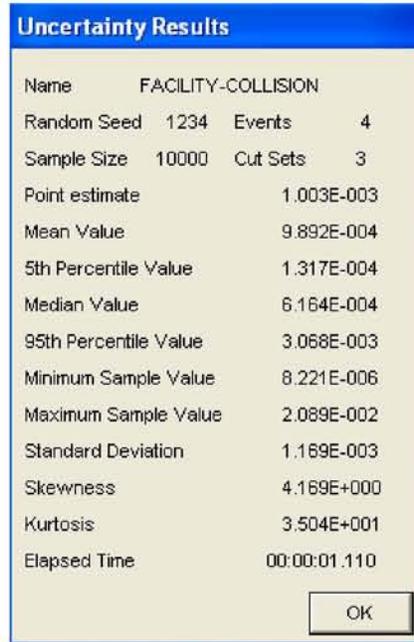
One basic event is identified as associated with human error involving the uncontrolled movement of the TEV. The basic event is identified as 800-HEE0-IMPACT-HFI-NOD.

##### B1.4.2.5.2 Common-Cause Failures

There are no CCFs identified for this model.

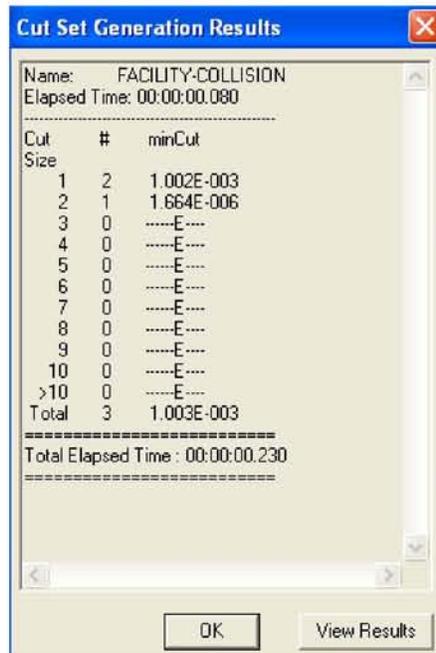
### B1.4.2.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Collision within Facility” are presented in Figures B1.4-3 and B1.4-4.



Source: Original

Figure B1.4-3. Uncertainty Results for TEV Collides with Object in a Facility



Source: Original

Figure B1.4-4. Cut Set Results for TEV Collides with Object in a Facility

### B1.4.2.7 Cut Sets

Table B1.4-4 contains the cut sets for the FACILITY-COLLISION fault tree.

Table B1.4-4. Facility-Collision Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.69	99.69	1.000E-03	800-HEE0-IMPACTF-HFI-NOD	Operator causes uncontrolled movement of TEV	1.000E-03
99.86	0.17	1.664E-06	800-TEV1-HNDSWCH-SEL-FOH	Speed selector fails – hand switch included	1.664E-05
—	—	—	TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.000E-01
100.00	0.15	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious Op	1.460E-06

NOTE: Op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

### B1.4.3 TEV Collides With Object during Emplacement

#### B1.4.3.1 Description

The scenario describes the collision of the TEV entering into, or traveling within, an emplacement drift, as the TEV moves to emplace a waste package. The scenario involves three potential modes of collision: (1) the TEV impacting the emplacement access door when the door is closed or only partially open; (2) the derailment of the TEV leading to the impact with the tunnel wall; and (3) the impact of the TEV moving off the end-of-rail at the end of the emplacement drift.

As the TEV enters the turnout drift leading to an emplacement drift, the TEV must pass through emplacement access doors which restrict access into the emplacement area. The remote operator controls the operation of the emplacement access door and may fail to open the door or close the door before the TEV reaches the threshold, inducing the TEV to collide with either a closed or partially open emplacement access door. (This failure mode is described in more detail in Section B.6)

The second collision mode can occur if the TEV derails due to mechanical failure of the TEV or of the rail system and collides with the tunnel wall.

The third collision mode can occur if the TEV passes the end-of-rail point. At the end of the turnout switch and at the end of the emplacement drift, the TEV rail terminates, and if the TEV inadvertently travels past this point, it can impact a bulkhead or tunnel wall. The TEV at this point may be under the local control or may be remotely operated. Position sensing of the TEV is based on rotary encoders located on each drive wheel.

### **B1.4.3.2 Success Criteria**

The success criterion for the scenario are that the TEV and the emplacement access door operate without spurious operations, and that if a collision does occur, that the TEV can sustain the impact without damage to the waste package. During normal operations, the TEV moves the waste package into the emplacement drift without incident.

### **B1.4.3.3 Design Requirements and Features**

The following requirements are identified with respect to this scenario:

- The TEV is able to sustain the impact from the emplacement access door such that after an impact from the TEV traveling at full operational speed, the shielding function of the TEV is preserved.
- The operational status of the TEV and the emplacement access door is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the TEV motion and avoid collision.

### **B1.4.3.4 Fault Tree Model**

The fault tree model for the sequence is labeled as DRIFT-TEV-IMPACT. The top event is the occurrence of the TEV colliding with an object as the TEV enters the emplacement drift and as the TEV travels to emplace the waste package. This top event is realized by either the occurrence of three events: (1) the TEV impacts the emplacement access door; (2) the TEV derails; and (3) TEV is commanded to travel past the end of rail; the three events are connected by an OR gate. Figures B1.4-23 through B1.4-25 present the fault tree graphics for this model.

The TEV impacting the emplacement access door can be caused by the premature emplacement access door closure due to human error or mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to the failure of the emplacement access door safety features together with the spurious activation of the door to close, and is represented by an AND gate. The safety feature for the emplacement access door is identified as the actuator motor stopping and opening upon sensing an increased load, and is represented by a basic event. The spurious activation of the access door can be due to either a spurious signal from the programmable logic controller or the failure of the actuator; the frequency of both occurrences is represented basic events.

The logic for the derailment of the TEV is transferred to a subtree, DRIFT-DERAIL. This fault tree represents the frequency of derailment as the combination of two basic events: the frequency of derailment of the TEV per mile and the miles traveled by the TEV.

The TEV is commanded to travel beyond the end-of-rail by either human error or by mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to the failure of the rotary encoders on the drive wheels of the TEV (which provide the location of the TEV to the control system) or the generation of a spurious signal to activate the motors when they not move. The failure of the rotary encoders is represented by both the failure of each of the eight encoders (as represented by eight basic events

joined under an AND gate) or the common-cause failure of all encoders. The spurious signal from programmable logic controller of the drive controller is represented as a single basic event. Although rail stops will be installed at the end of the rail, they are not modeled in the fault tree because they only affect a couple of, but not all “failure to stop the TEV” scenarios. Not crediting rail stops in the model would yield a conservative result.

### B1.4.3.5 Basic Event Data

Table B1.4-5 contains a list of basic events used in the fault tree, DRIFT-TEV-IMPACT, for a TEV colliding with object (e.g., a facility door, another vehicle) during transit.

Table B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit

Name	Description	Calculation Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	1	2.000E-03	2.000E-03	0.000E+00	0.000E+00
800-HEE0-AXSDR00-PLC-SPO	Programmable Logic Controller Spurious Operation	3	2.081E-09	0.000E+00	3.650E-07	5.700E-03
800-HEE0-AXSMO01-MOE-FSO	Motor (Electric) Fails to Shut Off	3	7.695E-11	0.000E+00	1.350E-08	5.700E-03
800-HEE0-AXSMO02-MOE-FSO	Motor (Electric) Fails to Shut Off	3	7.695E-11	0.000E+00	1.350E-08	5.700E-03
800-HEE0-ACTADR1-ATP-SPO	Actuator Spurious Op – Emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03
800-HEE0-ACTADR2-ATP-SPO	Actuator Spurious Op – Emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03
800-HEE0-DERAILSS-TEV-DOOR	TEV derails – per mile	1	1.180E-05	1.180E-05	0.000E+00	0.000E+00
TEV-DERAIL-MILES-DRIFT	Miles traveled by TEV in subsurface	V	4.000E+00	0.000E+00	0.000E+00	0.000E+00
OP-FAILS-ENDOFRAIL	Operator error causes TEV to run over end of rail	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
800-HEE0-ROTARYC-ECP-CCF	Common cause failure of 8 rotary encoders	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC Spurious Op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-ROTARY1-ECP-FOH	TEV Position Encoder Failure -1	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00

Table B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit (Continued)

Name	Description	Calculation Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-ROTARY2-ECP-FOH	TEV Position Encoder Failure -2	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY3-ECP-FOH	TEV Position Encoder Failure -3	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY4-ECP-FOH	TEV Position Encoder Failure -4	3	7.106E-06	0.0E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY5-ECP-FOH	TEV Position Encoder Failure -5	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY6-ECP-FOH	TEV Position Encoder Failure -6	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY7-ECP-FOH	TEV Position Encoder Failure -7	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY8-ECP-FOH	TEV Position Encoder Failure -8	3	7.106E-06	0.000E+00	1.79E-06	4.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Source: Original

#### B1.4.3.5.1 Human Failure Events

There are two basic events associated with human error: (1) the operator closes the emplacement access door prior to the TEV entering the emplacement drift, identified as 800-HEE0-AXSDR00-HFI-NOD; and (2) the operator error causes the TEV to continue past the end-of-rail, identified as OP-FAILS-ENDOFRAIL.

#### B1.4.3.5.2 Common-Cause Failures

One CCF is identified in the fault tree, associated with the CCF of the eight rotary encoders on the TEV's wheels. The CCF is represented by a basic event and labeled as 800-HEE0-ROTARYC-ECP-FOH.

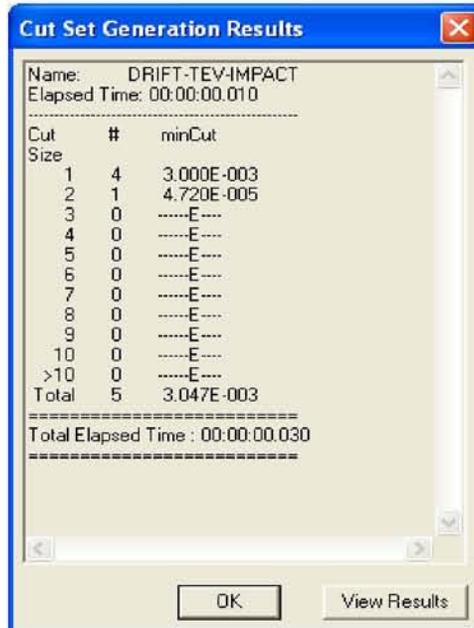
#### B1.4.3.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Collides with Object during Transit” are presented in Figures B1.4-5 and B1.4-6.



Source: Original

Figure B1.4-5. Uncertainty Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT)



Source: Original

Figure B1.4-6. Cut Set Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT)

### B1.4.3.7 Cut Sets

Table B1.4-6 contains the cut sets for the DRIFT-TEV-IMPACT fault tree.

Table B1.4-6. DRIFT-TEV-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
65.65	65.65	2.000E-03	800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	2.000E-03
98.47	32.82	1.000E-03	OP-FAILS-ENDOFRAIL	Operator error causes TEV to run over end of rail	1.000E-03
100.00	1.55	4.720E-05	800-HEE0-DERAILES-TEV-DER	TEV derails – per mile	1.180E-05
			TEV-DERAIL-MILES-DRIFT	Miles travelled by TEV in subsurface	4.000E+00
100.00	0.05	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC spurious Op	1.460E-06
100.00	0.04	6.400E-08	800-HEE0-ROTARYC-ECP-FOH	Common-cause failure of eight rotary encoders	6.400E-08

NOTE: NOTE: Op = operation; PLC = programmable logic control; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

#### B1.4.4 Impact to TEV during Transit

##### B1.4.4.1 Description

The scenario describes the collision of the TEV during transit with an object or vehicle. The scenario involves three potential modes of collision: (1) a worker drives another vehicle into the TEV which is possible at a vehicular crossing on the TEV rail line; (2) the TEV accelerates uncontrolled down the North Ramp (a runaway) leading to the impact with the tunnel wall; and (3) the impact of the TEV with an object along the rail line such as a stalled vehicle at a crossing or another TEV also moving along the rail.

##### B1.4.4.2 Success Criteria

The success criteria for the scenario are that the TEV operates without spurious operations and avoid impacts. If a collision does occur, then the TEV can sustain the impact without damage to the waste package. During the normal operations, the TEV is to move the waste package along the rail without incident.

##### B1.4.4.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The TEV is able to sustain the side impact load from a service vehicle such that the TEV does not roll over.
- The operational status (including speed) of all TEV systems is clearly displayed to the remote operator.

- The TEV moving at full operational speed is able to sustain an impact with another TEV moving similarly without breach of the contained waste package.
- The operational status of all TEV rail crossings is clearly displayed to all vehicles. The crossings are closed prior to TEV transit and crossing barriers restrain vehicles from proceeding along the barrier to cross the rail.

#### **B1.4.4.4 Fault Tree Model**

The fault tree model for the sequence is labeled as TRANSIT-IMPACT. The top event is an impact to the TEV due to a collision during transit. This top event is realized by one of three possible causes: (1) a worker drives a vehicle into the side of a TEV; (2) a runaway of the TEV occurs on decline such as the North Ramp, leading to an acceleration and derailment of the TEV which results in an impact with a tunnel wall; and (3) a TEV collision with an object along the rail line. Figures B1.4-26 through B1.4-34 presents the fault tree graphics for this model.

The first potential cause of an impact, the collision of a vehicle into the TEV, is represented by a basic event describing the vehicle's operator failure to yield at a crossing, and hitting the TEV. The second potential cause that of a runaway, can be realized by either by mechanical failure of the drive wheel system by shearing or by failure of TEV subsystems. The mechanical failure by shearing requires the joint occurrence of the TEV traveling on a decline (downward slope) and the mechanical failure leading to the TEV exceeding the design speed (termed, "over speed"). The logic of the mechanical failure is transferred to a subtree, RUNAWAY-MECH, which described later. Similarly, the failure of the TEV subsystems is transferred to a subtree, TEV-NONSHEARING, which is also described later in this section.

The third potential cause of an impact, the collision of the TEV with an object, can be realized by the generation of a spurious signal instructing the onboard controllers to drive the TEV into an object, or by the mechanical failure of the manual control switch. The spurious signal generated within the programmable logic controller system is represented as a basic event. The realization of the mechanical failure of the manual control switch requires the combined occurrence that the TEV is operating in manual mode together with the failure of the speed control switch. The switch failure and the frequency of the TEV in manual mode are represented by basic events.

The fault tree model RUNAWAY-MECH is the subtree representing the mechanical failure of the wheel system due to shearing of the wheel system. Shearing of the wheel system can be caused by either the shearing of all eight of motor's splined shafts (represented by a basic event) or the shearing of the gear system of the motors. The logic of the gearbox failure can be represented by the individual shearing of the gear boxes (and transferred to a subtree, GEARBOX-IND-EVENT) or the common-cause failure of all gearboxes, represented by a basic event. The fault tree model GEARBOX-IND-EVENT is the subtree describing the combined failure of all gear boxes at one time, represented by an OR gate linking eight basic events, one for each motor gearbox.

The fault tree model TEV-NONSHEARING is the subtree that represents a system failure as the initiator of a runaway. The event can be realized by the combined occurrence of the TEV brake system failing to slow the TEV to within design parameters and the control system instructing

the TEV motors to over speed. The control system condition can arise due to either of three causes: (1) a switch failure when in manual control; (2) a spurious signal in the programmable logic controllers instructs the TEV to over speed; or (3) a incorrect command instructs the TEV to over speed. The realization of the switch failure when in manual control requires the combined occurrence that the TEV is operating in manual mode together with the failure of the speed control switch. The switch failure and the frequency of the TEV in manual mode are both represented by basic events. A spurious signal in the programmable logic controllers can be induced in either the speed controller or the drive controller and again are both are represented by basic events. The logic for third possible cause is transferred to a subtree, RUNAWAY-SPURIOUS-SIGNAL. The event of the TEV brake system failing to slow the TEV is transferred to MOTOR-SEIZURE.

The fault tree model, RUNAWAY-SPURIOUS-SIGNAL, is the subtree representing the generation of spurious signal to cause the TEV to over speed. The event is represented by the joint occurrence (i.e., connected with an AND gate) of a spurious signal together with the failure of the operator to failure to halt the TEV as it starts to increase in speed. The source of the spurious signal is attributed to either the rotary position encoders or the speed indicators; the logic for these occurrences are transferred to subtree, SPUR-SIGN-ROTENCODE and subtree, SPUR-SIGN-DRIVEIND, respectively.

MOTOR-SEIZURE is the subtree describing the failure of any of the eight motors to seize at one time, represented by an OR gate linking eight basic events, one for each motor.

SPUR-SIGN-ROTENCODE is the subtree describing combined failure of all of the eight position encoders (i.e., one on each wheel) at one time, represented by an AND gate linking eight basic events, one for each position encoded.

SPUR-SIGN-DRIVEIND is the subtree describing the failure of at least of two of the eight over speed sensors (i.e., one on each wheel), represented by a conditioned OR gate linking eight basic events, one for each sensor.

#### **B1.4.4.5 Basic Event Data**

Table B1.4-7 contains a list of basic events used in the fault tree, TRANSIT-IMPACT, for a TEV impact from another vehicle during transit.

Table B1.4-7. Basic Event Probabilities for Impact to TEV during Transit

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
800-HEE0-GEARBX1-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX2-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX3-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX4-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX5-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX6-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX7-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX8-GRB-STH	Gear Box Stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBXC-GRB-STH	Common Cause Failure of TEV gearboxes	3	2.848E-09	1.080E-07	7.120E-10	4.000E+00
800-HEE0-MOTOR01-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR02-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR03-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR04-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR05-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR06-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR07-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR08-MOE-FSO	Motor (Electric) Fails to Shut Off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC Spurious Op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-SIDEIMP-HFI-NOW	Operator drives another vehicle into TEV side	1	3.000E-04	3.000E-04	0.000E+00	0.000E+00
800-HEE0-SPSHFC-AXL-CCF	Common cause failure of spline shaft	3	5.600E-10	1.000E+00	1.400E-10	4.000E+00
800-TEV1-ECP0001-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0002-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0003-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0004-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0005-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0006-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0007-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0008-ECP-FOH	Position Encoder Failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00

Table B1.4-7. Basic Event Probabilities for Impact to TEV during Transit (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
800-TEV1-HNSWCH-SEL-FOH	Speed Selector Fails – Hand switch included	3	1.664E-05	0.000E+00	4.160E-06	4.000E+00
800-TEV1-SRS0001-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0002-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0003-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0004-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0005-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0006-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0007-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0008-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.  
TEV = transport and emplacement vehicle.

Source: Original

### B1.4.4.5.1 Human Failure Events

There are two basic events associated with human error: (1) a worker drive another vehicle in the side of the TEV, identified as 800-HEE0-SIDEIMP-HFI-NOD; and (2) the operator failure to halt the TEV using the manual override during over speed, identified as HFE-RUNAWAY-RESPONSE.

### B1.4.4.5.2 Common-Cause Failures

Two CCFs are identified in the fault tree. The first is associated with the CCF of the splined shafts of the TEV's eight drive wheels. This CCF is represented by a basic event and labeled as 800-HEE0-SPSHFC-AXL-FOH. The second is associated with the CCF of the gearboxes of the TEV's eight drive wheels. This CCF is represented by a basic event and labeled as 800-HEE0-GEARBXC-GRB-ST.

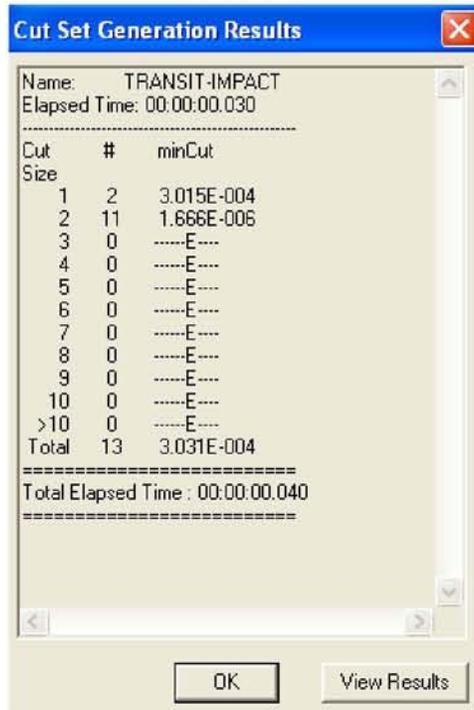
### B1.4.4.6 Uncertainty and Cut Set Generation Results

Uncertainty results from SAPHIRE for the fault tree for “Impact to TEV during Transit” are presented in Figure B1.4-7 and the cut set generation results are shown in Figure B1.4-8.

Uncertainty Results			
Name	TRANSIT-IMPACT		
Random Seed	1234	Events	16
Sample Size	10000	Cut Sets	13
Point estimate	3.031E-004		
Mean Value	2.936E-004		
5th Percentile Value	1.406E-005		
Median Value	1.139E-004		
95th Percentile Value	1.089E-003		
Minimum Sample Value	1.273E-006		
Maximum Sample Value	3.109E-002		
Standard Deviation	7.356E-004		
Skewness	1.636E+001		
Kurtosis	4.812E+002		
Elapsed Time	00:00:00.720		
<input type="button" value="OK"/>			

Source: Original

Figure B1.4-7. Uncertainty Results for Impact to TEV during Transit (TRANSIT-IMPACT)



Source: Original

Figure B1.4-8. Cut Set Generation Results for Impact to TEV during Transit (TRANSIT-IMPACT)

**B1.4.4.7 Cut Sets**

Table B1.4-8 contains the cut sets for the TRANSIT-IMPACT fault tree.

Table B1.4-8. TRANSIT-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.97	98.97	3.000E-04	800-HEE0-SIDEIMP-HFI-NOW	Operator drives another vehicle into TEV side	3.000E-04
99.52	0.55	1.664E-06	800-TEV1-HNDSWCH-SEL-FOH	Speed selector fails – hand switch included	1.664E-05
			TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.000E-01
100.00	0.48	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious Op	1.460E-06
100.00	0.00	7.120E-10	800-HEE0-GEARBXC-GRB-ST	Common-cause failure of TEV gearboxes	1.424E-09
			TEV-DECLINE	TEV on decline	5.000E-01
100.00	0.00	4.800E-10	800-HEE0-SPSHFC-AXL-FOH	Common-cause failure of spline shaft	9.600E-10
			TEV-DECLINE	TEV on decline	5.000E-01

Table B1.4-8. TRANSIT-IMPACT Cut Sets (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	0.00	7.884E-14	800-HEE0-MOTOR05-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR06-MOE-FSO	Motor (electric) fails to Shut Off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR07-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR08-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR01-MOE-FSO	Motor (electric) fails to shut Off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR02-MOE-FSO	Motor (electric) fails to shut Off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR03-MOE-FSO	Motor (electric) fails to shut Off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR04-MOE-FSO	Motor (electric) fails to shut Off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06

NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

## B1.4.5 TEV Stops for an Extended Period of Time

### B1.4.5.1 Description

The scenario describes the stopping of the TEV along the rail due to motive failure for an extended period time and the subsequent thermal heating and degradation of the TEV shielding.

The scenario can be initiated by a loss of offsite power, a local failure of the third rail power system, the failure of the TEV's onboard programmable controllers or the failure of the TEV's motor's speed sensors.

#### B1.4.5.2 Success Criteria

The success criterion for the scenario is that the TEV shielding can sustain its shielding function over a prolonged period without operational support.

#### B1.4.5.3 Design Requirements and Features

The following requirement is identified with respect to this scenario:

- The TEV shielding is able to sustain the thermal loading for all waste package loadings over an extended period of time without significant degradation of the shielding function.

#### B1.4.5.4 Fault Tree Model

The fault tree model for the sequence is labeled as SHIELD-STOP. The top event is the occurrence that the TEV is stopped for an extended period of time along the rail without active ventilation of the shielded enclosure. This top event is realized by lack of power and control to the drive motors together with the failure of the TEV fan, which provides air circulation for the shielded enclosure. The fan failure is represented by a basic event. The lack of power and control to the drive motors can be caused by either of four occurrences: (1) failure of the third rail system which powers the TEV; (2) the failure of the programmable logic controllers for the speed control of the TEV motors; (3) the loss of offsite power at the repository; and (4) failure of one of the eight the speed sensors which causes the TEV to stop and shutdown. The first three possible causes are represented by basic events. The fourth cause is represented by an OR gate linking eight basic events, one for the speed sensor on each motor. Figure B1.4-35 presents the fault tree graphic for this model.

#### B1.4.5.5 Basic Event Data

Table B1.4-9 contains a list of basic events used in the fault tree, SHIELD-STOP, for a TEV stopped for extended time.

Table B1.4-9. Basic Event Probabilities for TEV Stops for Extended Time

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-3RDRAIL-3RL-FOH	Third rail breaks	3	9.360E-08	0.000E+00	1.170E-08	8.000E+00
800-HEE0-PLCSPD1-PLC-SPO	Speed Controller – PLC Spurious Op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
LOSP-THERMAL	Loss of offsite power for thermal condition	1	7.940E-06	7.940E-06	0.000E+00	0.000E+00

Table B1.4-9. Basic Event Probabilities for TEV Stops for Extended Time (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-TEV1-SRS0001-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0002-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0003-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0004-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0005-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0006-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0007-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0008-SRS-FOH	Over Speed Sensor Fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Source: Original

#### B1.4.5.5.1 Human Failure Events

No basic event is identified as associated with human error for this model.

#### B1.4.5.5.2 Common-Cause Failures

There are no CCFs identified for this model.

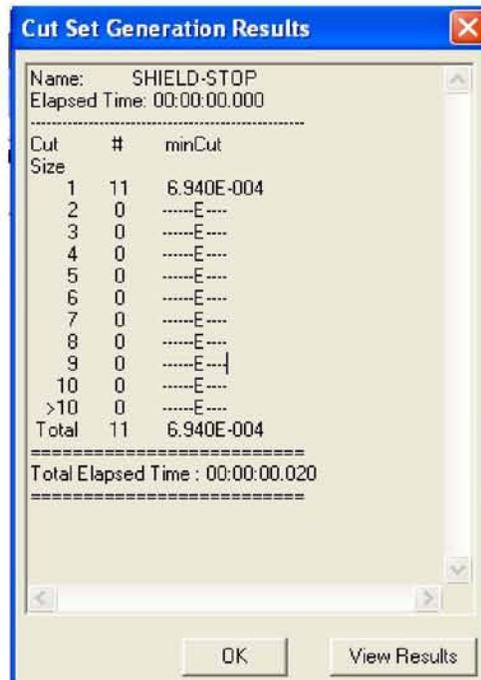
#### B1.4.5.6 Uncertainty and Cut Set Results

Uncertainty results from SAPHIRE for the fault tree for “TEV Stops for an Extended Period of Time” are presented in Figure B1.4-9 and the cut set generations results are shown in Figure B1.4.10.



Source: Original

Figure B1.4-9. Uncertainty Results for TEV Stops for Extended Time (SHIELD-STOP)



Source: Original

Figure B1.4-10. Cut Set Generation Results for TEV Stops for Extended Time (SHIELD-STOP)

### B1.4.5.7 Cut Sets

Table B1.4-10 contains the cut sets for the SHIELD-STOP fault tree.

Table B1.4-10. SHIELD STOP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
12.33	12.33	8.560E-05	800-TEV1-SRS0002-SRS-FOH	Over speed sensor fails	8.560E-05
24.66	12.33	8.560E-05	800-TEV1-SRS0003-SRS-FOH	Over speed sensor fails	8.560E-05
36.99	12.33	8.560E-05	800-TEV1-SRS0004-SRS-FOH	Over speed sensor fails	8.560E-05
49.32	12.33	8.560E-05	800-TEV1-SRS0005-SRS-FOH	Over speed sensor fails	8.560E-05
61.65	12.33	8.560E-05	800-TEV1-SRS0001-SRS-FOH	Over speed sensor fails	8.560E-05
73.98	12.33	8.560E-05	800-TEV1-SRS0006-SRS-FOH	Over speed sensor fails	8.560E-05
86.31	12.33	8.560E-05	800-TEV1-SRS0007-SRS-FOH	Over speed sensor fails	8.560E-05
98.64	12.33	8.560E-05	800-TEV1-SRS0008-SRS-FOH	Over speed sensor fails	8.560E-05
99.78	1.14	7.940E-06	LOSP-THERMAL	Loss of offsite power for thermal condition	7.940E-06
99.99	0.21	1.460E-06	800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious Op	1.460E-06
100.00	0.01	8.080E-08	800-HEE0-3RDRAIL-THR-BRK	Third rail breaks	8.080E-08

NOTE: Op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

### B1.4.6 Inadvertent TEV Door Opening during Transit

#### B1.4.6.1 Description

The scenario describes the opening of the TEV's front shield doors as the TEV exits a waste handling facility. The scenario can be initiated by a spurious signal or by a failure of the front shield door actuators. The interlock to prevent these shield doors has not been activated at this stage.

#### B1.4.6.2 Success Criteria

The success criterion for the scenario is that the TEV operates without spurious operations and subsystem failures.

### B1.4.6.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- Operational requirements require workers to be at a distance from the facility shield doors as a loaded TEV exits a facility.
- Both visual and audio alarms are used to alert workers of the TEV's movement along the rail line as the TEV exits a facility.

### B1.4.6.4 Fault Tree Model

The fault tree model for the sequence is labeled as SHIELD-DOOR. The top event is the occurrence of the TEV's shield doors opening during transit. The top event is realized by either (1) an interlock failure together with human error, or (2) a mechanical-based failure of the system. For the human-error initiated event, the opening of the door initiated erroneously by an operator command must be accompanied by the failure of the TEV interlock system (which is to prevent the front shield doors opening in transit) to be realized. This logic is represented by two basic events (representing the operator command and the interlock failure) joined by an AND gate. The mechanical-based failure also incorporates the failure of the interlock system (again represented by a basic event) together with the opening of the door initiated by a spurious signal or by spurious movement of the TEV's front shield door actuators. The spurious signal is (represented by basic event) joined by an OR gate to the spurious movement of the door actuators, which is represented as an OR joining basic failure events for each actuator. Figure B1.4-36 presents the fault tree graphic for this model.

### B1.4.6.5 Basic Event Data

Table B1.4-11 contains a list of basic events used in the fault tree, SHIELD-DOOR, for the inadvertent TEV door opening during transit.

Table B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op _ TEV doors	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-INTRLCK-IEL-FOH	Interlock Failure-TEV door interlock	3	1.372E-04	0.000E+00	3.430E-05	4.000E+00

Table B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

### B1.4.6.5.1 Human Failure Events

One basic event is identified as associated with human error of the operator opening the TEV shield doors. The basic event is identified as 800-HEE0-TEVDOOR-HFI-NOD.

### B1.4.6.5.2 Common-Cause Failures

There are no CCFs identified for this model.

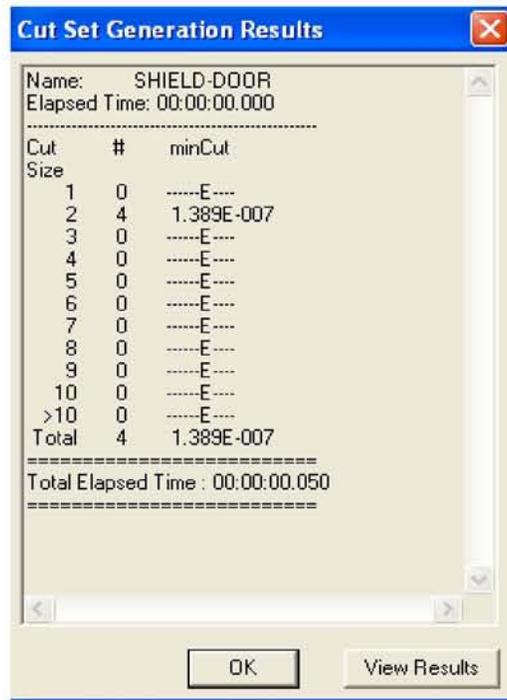
### B1.4.6.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for an “Inadvertent TEV Door Opening during Transit” are presented in Figures B1.4-11 and B1.4-12.



Source: Original

Figure B1.4-11. Uncertainty Results for TEV Exits Facility with Open Shield Doors (SHIELD DOOR)



Source: Original

Figure B1.4-12. Cut Sets for TEV Exits Facility with Open Shield Doors (SHIELD DOOR)

### B1.4.6.7 Cut Sets

Table B1.4-12 contains the cut sets for the SHIELD-DOOR fault tree.

Table B1.4-12. SHIELD-DOOR Cut Sets

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.80	98.80	1.372E-07	800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
			800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1.000E-03
99.33	0.53	7.353E-10	800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
99.86	0.53	7.353E-10	800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
100.00	0.14	2.003E-10	800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04

Table B1.4-12. SHIELD-DOOR Cut Sets (Continued)

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
			800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	1.460E-06

NOTE: Op = operation; PLC = programmable logic controllers; TEV = transport and emplacement vehicle.

Source: Original

## B1.4.7 Waste Package Drop in Facility

### B1.4.7.1 Description

The scenario describes the drop of a waste package within a facility during the loadout operation. After the waste package has been placed under the TEV at the loadout dock, the TEV's shielded enclosure raises the waste package to allow the retraction of the base plate. At this point, the lift system of screw jacks or the lifting features on the shielded enclosure can fail, allowing the drop of the waste package to the dock.

### B1.4.7.2 Success Criteria

The success criteria for the scenario are that the TEV operates without spurious operations and without structural or system failures.

### B1.4.7.3 Design Requirements and Features

The following requirement is identified with respect to this scenario:

- The operational status of the TEV is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the status of the TEV and the waste package.

### B1.4.7.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-DROP. The top event is the drop of a waste package by the TEV during the loadout operations within a waste handling facility. This top event is realized by either the failure of the lift system (jack failure) or the mechanical failure of the lift features holding the pallet and waste package configuration. Figure B1.4-37 presents the fault tree graphic for this model.

The lift system can fail if two of the primary jacks fail as represented by the failure of the individual jacks joined by a conditional OR gate. For the waste package to be dropped, a minimum of two of the primary jacks must fail (at either end of the TEV).

The lift features can also fail, allowing the waste package to drop. Again, for the waste package to be dropped, a minimum of two of the four lift features must fail. The failure of the lift features is represented by the failure of the lift features joined by a conditional OR gate requiring the failure of two of the four features for realization.

### B1.4.7.5 Basic Event Data

Table B1.4-13 contains a list of basic events used in the fault tree, FACILITY-DROP, for the drop of a waste package in a waste handling facility.

Table B1.4-13. Basic Event Probabilities for Waste Package Drop in Facility

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-JACK005-JCK-FOH	Screw Jack CCF Failure	1	8.100E-07	8.100E-07	0.000E+00	0.000E+00
800-HEE0-JACK001-JCK-FOH	TEV Screw Jack Failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK002-JCK-FOH	TEV Screw Jack Failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK003-JCK-FOH	TEV Screw Jack Failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK004-JCK-FOH	TEV Screw Jack Failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Source: Original

#### B1.4.7.5.1 Human Failure Events

No basic event is identified as associated with human error for this model.

#### B1.4.7.5.2 Common-Cause Failures

There are no CCFs identified for this model.

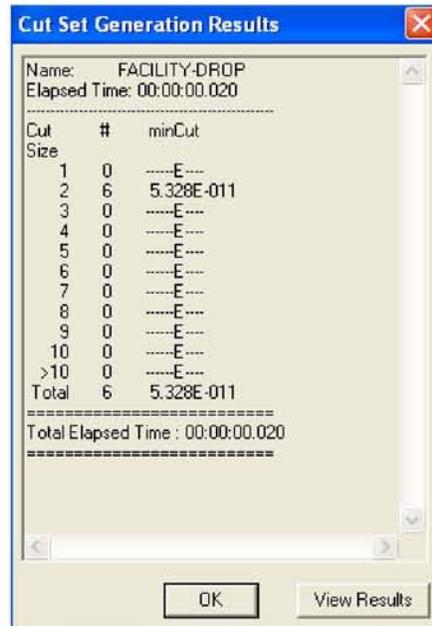
#### B1.4.7.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for “Waste Package Drop in Facility” are presented in Figures B1.4-13 and B1.4-14.



Source: Original

Figure B1.4-13. Uncertainty Results for Package Drop During Loading in Facility (FACILITY-DROP)



Source: Original

Figure B1.4-14. Cut Set Generation Results for Package Drop during Loading in Facility (FACILITY-DROP)

### B1.4.7.7 Cut Sets

Table B1.4-14 contains the cut sets for the FACILITY-DROP fault tree.

Table B1.4-14. FACILITY-DROP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
16.67	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
33.34	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
50.01	16.67	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
66.68	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
83.35	16.67	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	16.67	8.880E-12	800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
16.67	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
33.34	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
50.01	16.67	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
66.68	16.67	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
83.35	16.67	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	16.67	8.880E-12	800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06

NOTE: Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

### B1.4.8 Waste Package Drop during Transit

#### B1.4.8.1 Description

The scenario describes the drop of a waste package by the TEV during transit. To allow for a fall of the waste package to the invert during transit, the TEV's base plate must be first extended from underneath the TEV. To allow this extension, the TEV's front shield doors must open to disengage the mechanical interlock on base plate movement. However for the TEV's shield doors to open, the electro-mechanical interlock on the shield doors must fail as well. [Note: as the TEV exits a facility, an interlock is activated to restrict the opening of the front shield doors.]

After the base plate is extended, the lift system of screw jacks or the lifting features on the shielded enclosure fail, allowing the drop of the waste package to the dock.

#### **B1.4.8.2 Success Criteria**

The success criterion for the scenario is that the TEV operates without structural or system failures.

#### **B1.4.8.3 Design Requirements and Features**

The following requirements are identified with respect to this scenario:

- The TEV has an electro-mechanical interlock to prevent the front shield doors to open when the TEV is in transit outside of a facility or an emplacement drift.
- The operational status of the TEV is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the status of the TEV's shield doors.

#### **B1.4.8.4 Fault Tree Model**

The fault tree model for the sequence is labeled as TRANSIT-DROP. The top event is the drop of a waste package by the TEV during transit on the surface or in the subsurface. This top event is realized by the failure of the shot bolts holding the pallet and waste package configuration. However, for this type of drop to occur during transit, the TEV's base plate must be first extended. Therefore the failure of the shot bolts is joined by an AND gate to the extension of the base plate. Figures B1.4-38 and B1.4-39 present the fault tree graphic for this model.

For the base plate to be extended during transit, the base plate can be actuated by a spurious signal represented by a basic event. However, for the base plate to extend, the front shield doors must be first opened to disengage the interlock of the doors on the base plate movement. The logic for the shield door to open is transferred to a subtree, DOOR-INIT.

The lift system can fail if two of the primary jacks fail together with the failure of the backup jacks upon demand. For the waste package to be dropped, a minimum of two of the primary jacks must fail (at either end of the TEV).

The lift features can also fail and allow the waste package to drop. Again, for the waste package to be dropped, a minimum of two of the four<sup>1</sup> lift features must fail. The failure of the lift features is represented by the failure of the lift features joined by a conditional OR gate requiring the failure of two of the four features for realization.

DOOR-INIT is the subtree describing the opening of the TEV shield doors during transit. This event is realized by either (1) an interlock failure together with human error, or (2) a mechanical-

---

<sup>1</sup> The actual TEV lift features are continuous structural supports on either side of the waste package. However, for this analysis, the front support section is divided from the rear support section on a side, resulting in four lift "features" for the TEV and allowing for only a portion of the support to fail.

based failure of the system. For the human-error initiated event, the opening of the door imitated erroneously by an operator command must be accompanied by the failure of the TEV interlock system (which is to prevent the front shield doors opening in transit) to be realized. This logic is represented by two basic events (representing the operator command and the interlock failure) joined by an AND gate. The mechanical-based failure also incorporates the failure of the interlock system (again represented by a basic event) together with the opening of the door initiated by a spurious signal or by spurious movement of the TEV's front shield door actuators. The spurious signal is (represented by basic event) joined by an OR gate to the spurious movement of the door actuators, which is represented as an OR joining basic failure events for each actuator.

#### B1.4.8.5 Basic Event Data

Table B1.4-15 contains a list of basic events used in the fault tree, TRANSIT-DROP, for a waste package dropped during transit.

Table B1.4-15. Basic Event Probabilities for Waste Package Dropped during Transit

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-BEEXTD-ADP-SPO	Actuator Spurious Op – TEV base plate	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-LIFT000-LRG-CCF	Common cause failure of all four Lifting Rigs or Hooks	1	7.450E-08	7.450E-08	0.000E+00	0.000E+00
800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-SHTBLT0-PIN-CCF	Common Cause failure of 2 or more shot bolts	1	8.230E-10	8.230E-10	0.000E+00	0.000E+00
800-HEE0-SHTBLT1-PIN-FOH	TEV Shot Bolt 1 Fails	3	3.292E-08	0.000E+00	8.230E-09	4.000E+00
800-HEE0-SHTBLT2-PIN-FOH	TEV Shot Bolt 2 Fails	3	3.292E-08	0.000E+00	8.230E-09	4.000E+00
800-HEE0-SHTBLT3-PIN-FOH	TEV Shot Bolt 3 Fails	3	3.292E-08	0.000E+00	8.230E-09	4.000E+00
800-HEE0-SHTBLT4-PIN-FOH	TEV Shot Bolt 4 Fails	3	3.292E-08	0.000E+00	8.230E-09	4.000E+00
800-HEE0-INTRLCK-IEL-FOH	Interlock Failure – TEV door interlock	3	1.372E-04	0.000E+00	3.430E-05	4.000E+00
800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00

Table B1.4-15. Basic Event Probabilities for Waste Package Dropped during Transit (Continued)

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op – TEV doors	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Op = operation; PLC = programmable logic controllers; TEV = transport and emplacement vehicle.

Source: Original

#### B1.4.8.5.1 Human Failure Events

One basic event is identified as associated with human error of the operator opening the TEV shield doors. The basic event is identified as 800-HEE0-TEVDOOR-HFI-NOD.

#### B1.4.8.5.2 Common-Cause Failures

There are two CCFs identified for this model. Both are the failure of at least two of four components; 800-HEE0-LIFT000-LRG-CCF models the failure of at least two of four lifting rigs or hooks and 800-HEE0-SHTBLT0-PIN-CCF models the failure of at least two or four shot bolts.

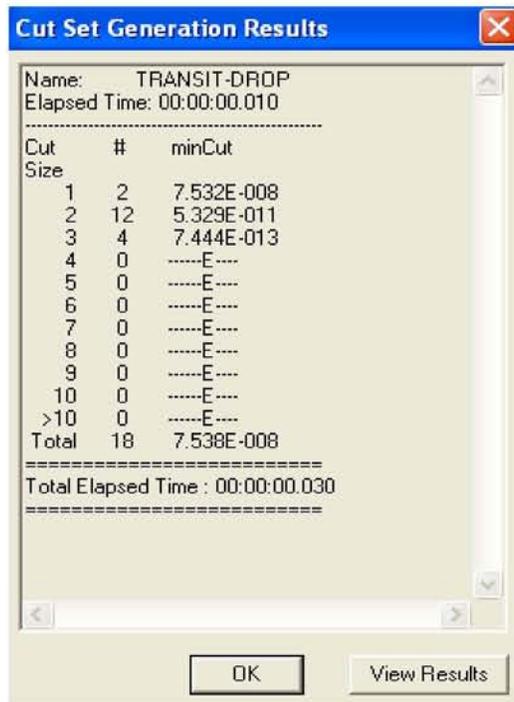
#### B1.4.8.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for “Waste Package Drop during Transit” are presented in Figures B1.4-17 and B1.4-18.



Source: Original

Figure B1.4-15. Uncertainty Results for Waste Package Drop during Transit (TRANSIT-DROP)



Source: Original

Figure B1.4-16. Cut Sets Generation Results for Waste Package Drop during Transit (TRANSIT-DROP)

**B1.4.8.7 Cut Sets**

Table B1.4-16 contains the cut sets for the TRANSIT-DROP fault tree.

Table B1.4-16. TRANSIT-DROP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.84	98.84	7.450E-08	800-HEE0-LIFT000-LRG-CCF	Common cause failure of all four lifting Rig/hooks	7.450E-08
99.93	1.09	8.230E-10	800-HEE0-SHTBLT0-PIN-CCF	Common Cause failure of 2 or more TEV Shot Bolts	8.230E-10
99.94	0.01	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.95	0.01	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.96	0.01	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.97	0.01	8.880E-12	800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.98	0.01	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.99	0.01	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
99.99	0.00	7.353E-13	800-HEE0-BEEXTD-ATP-SPO	Actuator Spurious Op - TEV base plate	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
			800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1.000E-03
99.99	0.00	3.941E-15	800-HEE0-ACTDR01-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
			800-HEE0-BEEXTD-ATP-SPO	Actuator Spurious Op - TEV base plate	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
99.99	0.00	3.941E-15	800-HEE0-ACTDR02-ATP-SPO	Actuator Spurious Op - TEV door	5.360E-06
			800-HEE0-BEEXTD-ATP-SPO	Actuator Spurious Op - TEV base plate	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
99.99	0.00	1.084E-15	800-HEE0-SHTBLT1-PIN-FOH	TEV Shot Bolt 1 fails	3.292E-08
			800-HEE0-SHTBLT2-PIN-FOH	TEV Shot Bolt 2 Fails	3.292E-08
99.99	0.00	1.084E-15	800-HEE0-SHTBLT1-PIN-FOH	TEV Shot Bolt 1 fails	3.292E-08
			800-HEE0-SHTBLT4-PIN-FOH	TEV Shot Bolt 4 Fails	3.292E-08
99.99	0.00	1.084E-15	800-HEE0-SHTBLT2-PIN-FOH	TEV Shot Bolt 2 Fails	3.292E-08
			800-HEE0-SHTBLT4-PIN-FOH	TEV Shot Bolt 4 Fails	3.292E-08

Table B1.4-16. FACILITY-DROP Cut Sets (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.99	0.00	1.084E-15	800-HEE0-SHTBLT3-PIN-FOH	TEV Shot Bolt 3 Fails	3.292E-08
			800-HEE0-SHTBLT4-PIN-FOH	TEV Shot Bolt 4 Fails	3.292E-08
99.99	0.00	1.084E-15	800-HEE0-SHTBLT1-PIN-FOH	TEV Shot Bolt 1 fails	3.292E-08
			800-HEE0-SHTBLT3-PIN-FOH	TEV Shot Bolt 3 Fails	3.292E-08
99.99	0.00	1.084E-15	800-HEE0-SHTBLT2-PIN-FOH	TEV Shot Bolt 2 Fails	3.292E-08
			800-HEE0-SHTBLT3-PIN-FOH	TEV Shot Bolt 3 Fails	3.292E-08
99.99	0.00	1.074E-15	800-HEE0-BEDEXTD-ATP-SPO	Actuator Spurious Op - TEV base plate	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
			800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	1.460E-06
98.84	98.84	7.450E-08	800-HEE0-LIFT000-LRG-CCF	Common cause failure of all four lifting Rig/hooks	7.450E-08
99.93	1.09	8.230E-10	800-HEE0-SHTBLT0-PIN-CCF	Common Cause failure of 2 or more TEV Shot Bolts	8.230E-10
99.94	0.01	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06

NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

## B1.4.9 Waste Package Drop or Dragging in an Emplacement Drift

### B1.4.9.1 Description

The scenario describes the drop or dragging of a waste package by the TEV during emplacement operations. Dragging can occur as the TEV moves away from an emplaced waste package with the shielded enclosure at its lowered position. At this point, a spurious signal could activate the shielded enclosure to be raised, which would induce the TEV to engage the pallet at one end. As the TEV continues to move, the pallet and the waste package are dragged along with the TEV, with one end of the pallet moving on the invert. With continued motion, waste package would eventually slide or drop from the pallet to the invert.

The TEV can also drop the waste package just prior to the placement of the pallet and package on the drift invert. At this point, the base plate is extended, the lift system of screw jacks or the lifting features on the shielded enclosure fail, allowing the drop of the waste package to the invert.

### B1.4.9.2 Success Criteria

The success criteria for the scenario are that the TEV operates without spurious operations and without structural or system failures.

### **B1.4.9.3 Design Requirements and Features**

The following requirement is identified with respect to this scenario:

- The operational status of the TEV is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the status of the TEV and the waste package.

### **B1.4.9.4 Fault Tree Model**

The fault tree model for the sequence is labeled as DRIFT-DRAG. The top event is the drop or dragging of the waste package within the emplacement drift. This top event is realized by either the occurrence of the TEV dragging the waste package and pallet along the invert or the drop of the waste package by the TEV just prior to emplacement. Figures B1.4-40 to B1.4-42 present the fault tree graphic for this model.

For the waste package to be dragged the TEV shielded enclosure must improperly engage the waste package during its movement away from the waste package and continues to move away after the engagement. This is represented as an AND gate connecting the events representing the improper engagement of waste package and the TEV's spurious movement.

The improper engagement of the waste package can be initiated by one of three causes: (1) a spurious signal driving the programmable logic controller for waste package retrieval; (2) the failure of the primary lift (jack) system; and (3) the failure of the lift features.

The lift system can fail if one of the four primary jacks fail. The failure of the primary jacks is represented by the failure of an individual jack (each represented as a basic event) joined by a conditional OR gate. The lift features can also fail, and the failure of the lift features is represented by the failure of the one of the four lift features (each represented as a basic event) joined by a conditional OR gate.

The generation of spurious signal to cause TEV movement can be caused by either a spurious signal within the speed controller or the start of movement by the TEV motors. The motors can be actuated from central control (represented by a basic event) or all the motors can activate independently. This independent activation is represented by basic events for each of the eight drive wheel motors connected by an AND gate.

The drop of the waste package by the TEV is realized by either the failure of the lift system (jack failure) or the mechanical failure of the lift features holding the pallet and waste package configuration. However, as stated in (Ref. B1.1.7), the TEV is constructed with vertical guide rollers that render the scenario of dragging the waste package scenario following a drop virtually impossible. Note that at this point in TEV operations, the baseplate is extended.

The lift system can fail if two of the primary jacks fail together with the failure of the backup jacks upon demand. The failure of the backup jacks is represented by a single basic event joined by an AND gate to the failure of the primary jacks, as represented by the failure of the individual jacks joined by a conditional OR gate. For the waste package to be dropped, a minimum of two

of the primary jacks must fail (at either end of the TEV). This drop model will yield a conservative result.

The lift features can also fail, allowing the waste package to drop. Again, for the waste package to be dropped, a minimum of two of the four lift features must fail. The failure of the lift features is represented by the failure of the lift features joined by a conditional OR gate requiring the failure of two of the four features for realization.

#### B1.4.9.5 Basic Event Data

Table B1.4-17 contains a list of basic events used in the fault tree, DRIFT-DRAG, for the drop or dragging of a waste package in an emplacement drift.

Table B1.4-17. Basic Event Probabilities for a Waste Package Drop or Dragging in an Emplacement Drift

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-PLCRETR-PLC-SPO	PLC Spurious Op – WP retrieval controller	3	3.650E-07	0.000E+00	3.650E-07	1.000E+00
800-HEE0-JACK000-JCK-CCF	Screw jack CCF failure	1	8.100E-07	8.100E-07	0.000E+00	0.000E+00
800-HEE0-JACK001-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.140E-06	4.000E+00
800-HEE0-JACK002-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.140E-06	4.000E+00
800-HEE0-JACK003-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.140E-06	4.000E+00
800-HEE0-JACK004-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.140E-06	4.000E+00
800-HEE0-LIFT000-LRG-CCF	Common cause failure of at least two lifting rigs/hooks	1	7.450E-08	7.450E-08	0.000E+00	0.000E+00
800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook fails	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook fails	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook fails	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook fails	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00

Table B1.4-17. Basic Event Probabilities for a Waste Package Drop or Dragging in an Emplacement Drift  
(Continued)

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-PLCSPD1-PLC-SPO	Speed Controller – POC spurious Op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-MOTACTC-ATP-CCF	CCF – TEV motor actuation (0.009 times hourly)	1	1.210E-08	1.210E-08	0.000E+00	0.000E+00
800-HEE0-MOTACT1-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT2-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT3-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT4-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT5-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT6-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT7-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	1.000E+00
800-HEE0-MOTACT8-ACT-SPO	Actuator Spurious Op – TEV motor	3	1.340E-06	0.000E+00	1.340E-06	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.

CCF = common-cause failure; Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

#### B1.4.9.5.1 Human Failure Events

No basic event is identified as associated with human error for this model.

#### B1.4.9.5.2 Common-Cause Failures

There are two CCFs identified for this model. The first is the CCF of the TEV screw jacks, conservatively modeled as any 2 of 4 (800-HEE0-JACK000-JCK-CCF) and the CCF of the lifting rigs, also conservatively modeled as any 2 of 4 (800-HEE0-LIFT000-LRG-CCF).

### B1.4.9.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for “Waste Package Drop or dragging in an Emplacement Drift” are presented in Figures B1.4-17 and B1.4-18.

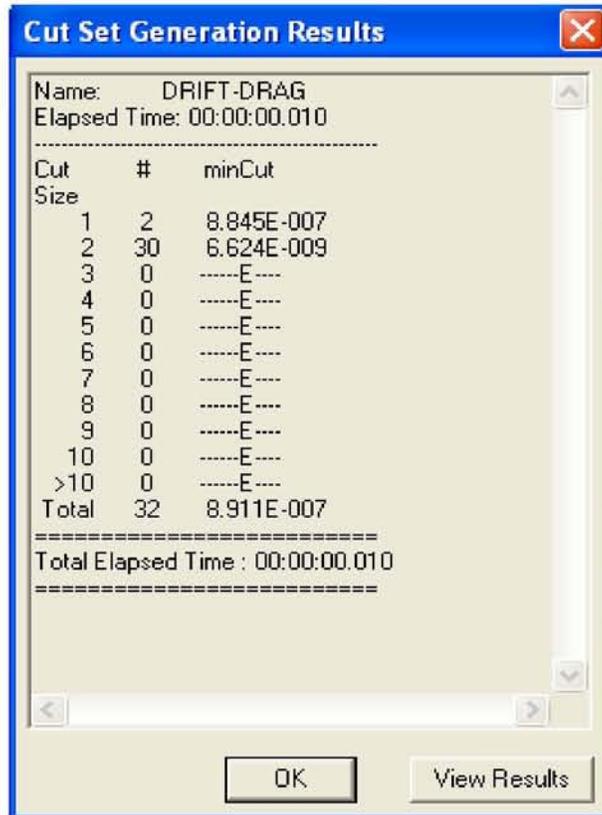


Uncertainty Results			
Name	DRIFT-DRAG		
Random Seed	1234	Events	13
Sample Size	10000	Cut Sets	32
Point estimate			8.911E-007
Mean Value			9.071E-007
5th Percentile Value			8.361E-008
Median Value			4.661E-007
95th Percentile Value			3.195E-006
Minimum Sample Value			5.010E-008
Maximum Sample Value			1.614E-005
Standard Deviation			1.144E-006
Skewness			2.726E+000
Kurtosis			1.449E+001
Elapsed Time			00:00:00.580

OK

Source: Original

Figure B1.4-17. Uncertainty Results for Drop or Drag of Waste Package by TEV in Emplacement Drift (DRIFT-DRAG)



Source: Original

Figure B1.4-18. Cut Set Generation Results for Drop or Drag of Waste Package by TEV in Emplacement Drift (DRIFT-DRAG)

Table B1.4-18 contains the top 20 cut sets for the DRIFT-DRAG fault tree.

Table B1.4-18. DRIFT-DRAG Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
90.90	90.90	8.100E-07	800-HEE0-JACK000-SJK-CCF	Screw jack CCF Failure	8.100E-07
99.26	8.36	7.450E-08	800-HEE0-LIFT000-LRG-CCF	Common cause failure of at least two lifting Rig/hooks	7.450E-08
99.38	0.12	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
99.50	0.12	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
99.62	0.12	1.060E-09	800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
99.74	0.12	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05
99.86	0.12	1.060E-09	800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05

Table B1.4-18. DRIFT-DRAG Cut Sets (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.98	0.12	1.060E-09	800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05
99.99	0.01	4.754E-11	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06
100.00	0.01	4.754E-11	800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06
100.00	0.01	4.754E-11	800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06
100.00	0.01	4.754E-11	800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	8.880E-12	800-HEE0-LIFT003-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
100.00	0.00	4.351E-12	800-HEE0-LIFT001-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06
100.00	0.00	4.351E-12	800-HEE0-LIFT002-LRG-FOH	Lifting Rig or Hook Failure	2.980E-06
			800-HEE0-PLCSPD1-PLC-SPO	Speed Controller - PLC Spurious Op	1.460E-06

NOTE: CCF = common-cause failure; Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

## **B1.4.10 TEV Collides with Emplaced Waste Package**

### **B1.4.10.1 Description**

The scenario describes the TEV impacting an emplaced waste package during emplacement operations. A collision can occur as a TEV enters the emplacement drift, and due to a system failure, human error or spurious signal, the TEV continues at full operational speed along the drift until it strikes a waste package emplaced earlier. A collision can also occur as the TEV moves away from the waste package after emplacement, and a signal directs the TEV to reverse direction, which would induce the TEV to move along the drift in the wrong direction until it collides with the waste package recently emplaced.

### **B1.4.10.2 Success Criteria**

The success criteria for the scenario are that the TEV operates without spurious operations and without system failures.

### **B1.4.10.3 Design Requirements and Features**

The following requirement is identified with respect to this scenario:

- The operational status of the TEV is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the status of the TEV including speed, operational direction and the potential for collision.

### **B1.4.10.4 Fault Tree Model**

The fault tree model for the sequence is labeled as TEV-IMPACTS-WP. . The top event is the impact of an emplaced waste package by the TEV during emplacement operations. This top event is realized by either a mechanical failure or by an operator error. The uncontrolled movement of the TEV leading to a collision, as caused by operator error, is represented by a basic event. Figure B1.4-43 presents the fault tree graphic for this model

For a collision due to the mechanical failure, the failure must induce the TEV to move in an uncontrolled fashion. The uncontrolled movement can be caused by either the failure of the mechanical speed control (if the TEV is operating in manual mode) or by a spurious operation directed by the drive controller. The failure of the mechanical speed selector is represented as basic event which is joined to the basic event that the TEV is operating in manual mode by an AND gate. The spurious operation directed by the drive controller is also represented as a basic event.

### B1.4.10.5 Basic Event Data

Table B1.4-19 contains a list of basic events used in the fault tree, TEV-IMPACTS-WP, for the TEV colliding with an emplaced waste package.

Table B1.4-19. Basic Event Probabilities for TEV Collides with Emplaced Waste Package

Name	Calculation Type <sup>a</sup>	Calc Prob	Mean Failure Probability	Lambda	Mission Time <sup>a</sup>
800-HEE0-IMPACTF-HFI-NOD	Operator causes uncontrolled movement of TEV	1	1.000E-03	1.000E-03	0.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC Spurious Op	3	1.460E-06	0.000E+00	3.650E-07
800-TEV1-HNSWCH-SEL-FOH	Speed selector fails – Hand switch included	3	1.664E-05	0.000E+00	4.160E-06
TEV-CONTROL-MANUAL	TEV is operating in manual mode	1	1.000E-01	1.000E-01	0.000E+00

NOTE: <sup>a</sup>For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Op = operation; PLC = programmable logic controller; Prob. = probability. TEV = transport and emplacement vehicle.

Source: Original

#### B1.4.10.5.1 Human Failure Events

One basic event is identified as associated with human error of the operator causing the uncontrolled movement of the TEV (which impacts the waste package). The basic event is identified as 800-HEE0-IMPACTF-HFI-NOD.

#### B1.4.10.5.2 Common-Cause Failures

There are no CCFs identified for this model.

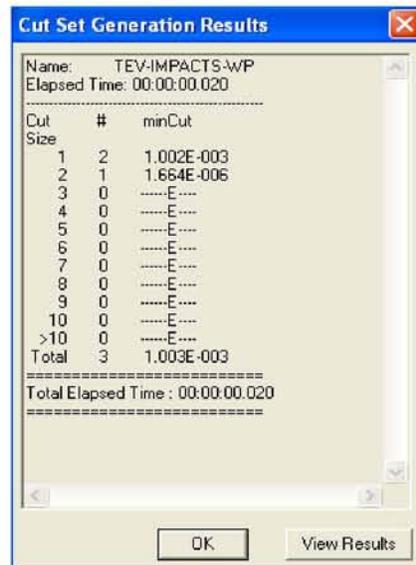
### B1.4.10.6 Uncertainty and Cut Set Generation Results

Uncertainty results and cut set generation results from SAPHIRE for the fault tree for “TEV Collides with Emplaced Waste Package” are presented in Figures B1.4-19 and B1.4-20.



Source: Original

Figure B1.4-19. Uncertainty Results for TEV Impacts Waste Package in Emplacement Drift (TEV-IMPACTS-WP)



Source: Original

Figure B1.4-20. Cut Set Generation Results for TEV Impacts Waste Package in Emplacement Drift (TEV-IMPACTS-WP)

### B1.4.10.7 Cut Sets

Table B1.4-20 contains the top 20 cut sets for the TEV-IMPACTS-WP fault tree.

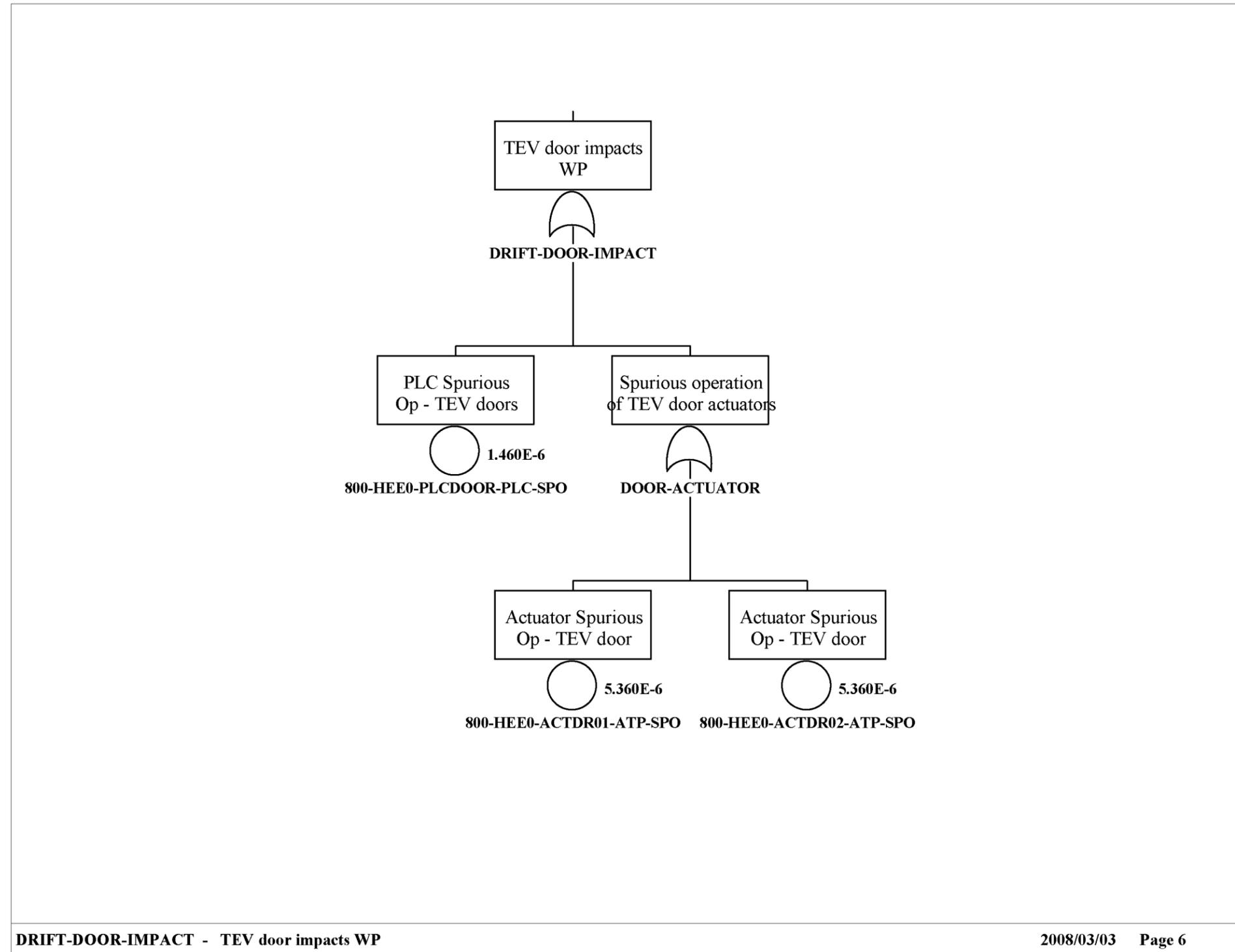
Table B1.4-20. TEV-IMPACTS-WP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.69	99.69	1.000E-03	800-HEE0-IMPACTF-HFI-NOD	Operator causes uncontrolled movement of TEV	1.000E-03
99.86	0.17	1.664E-06	800-TEV1-HNDSWCH-SEL-FOH	Speed selector fails – hand switch included	1.664E-05
			TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.000E-01
100.00	0.15	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious Op	1.460E-06

NOTE: Op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

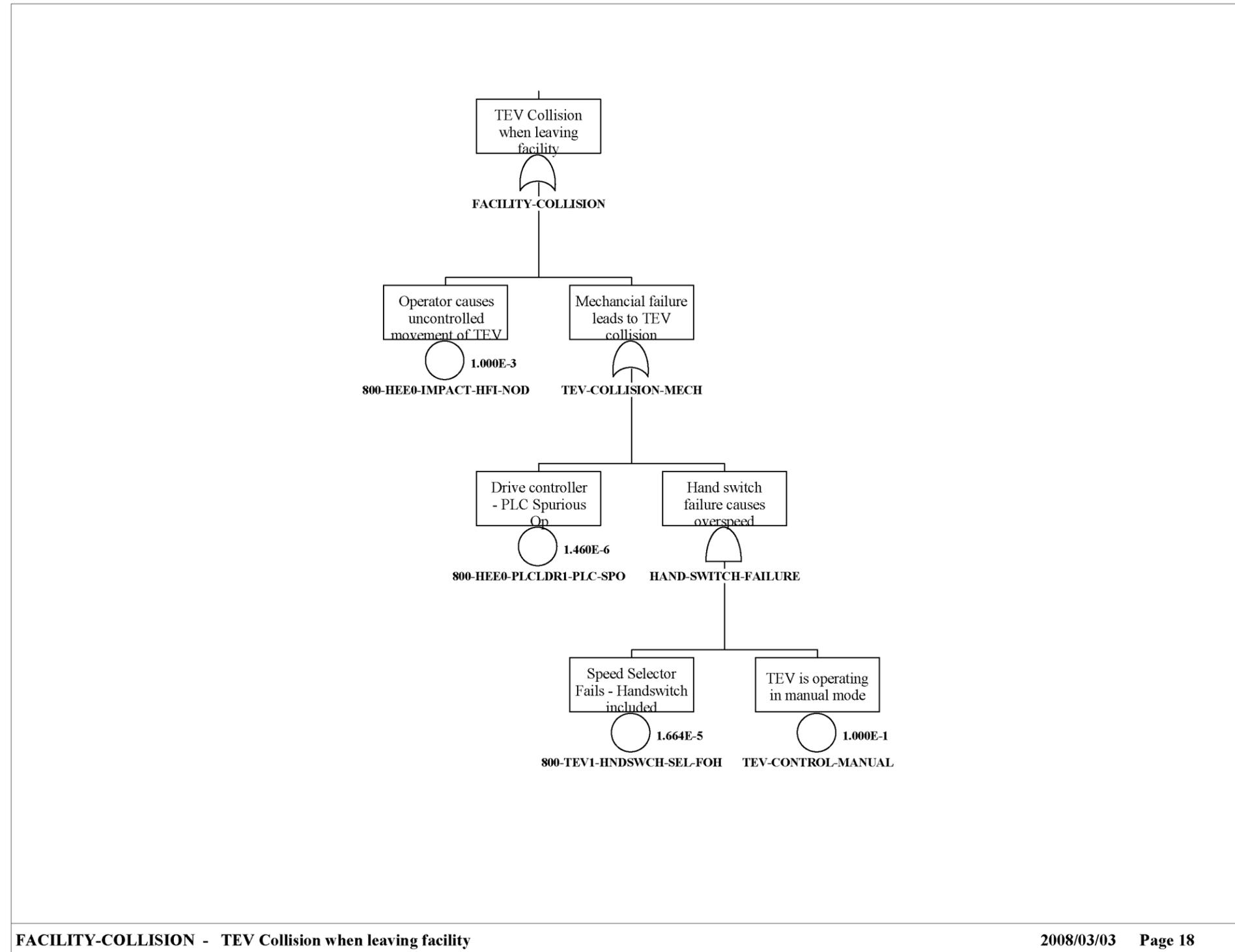
### B1.4.10.8 FAULT TREES



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

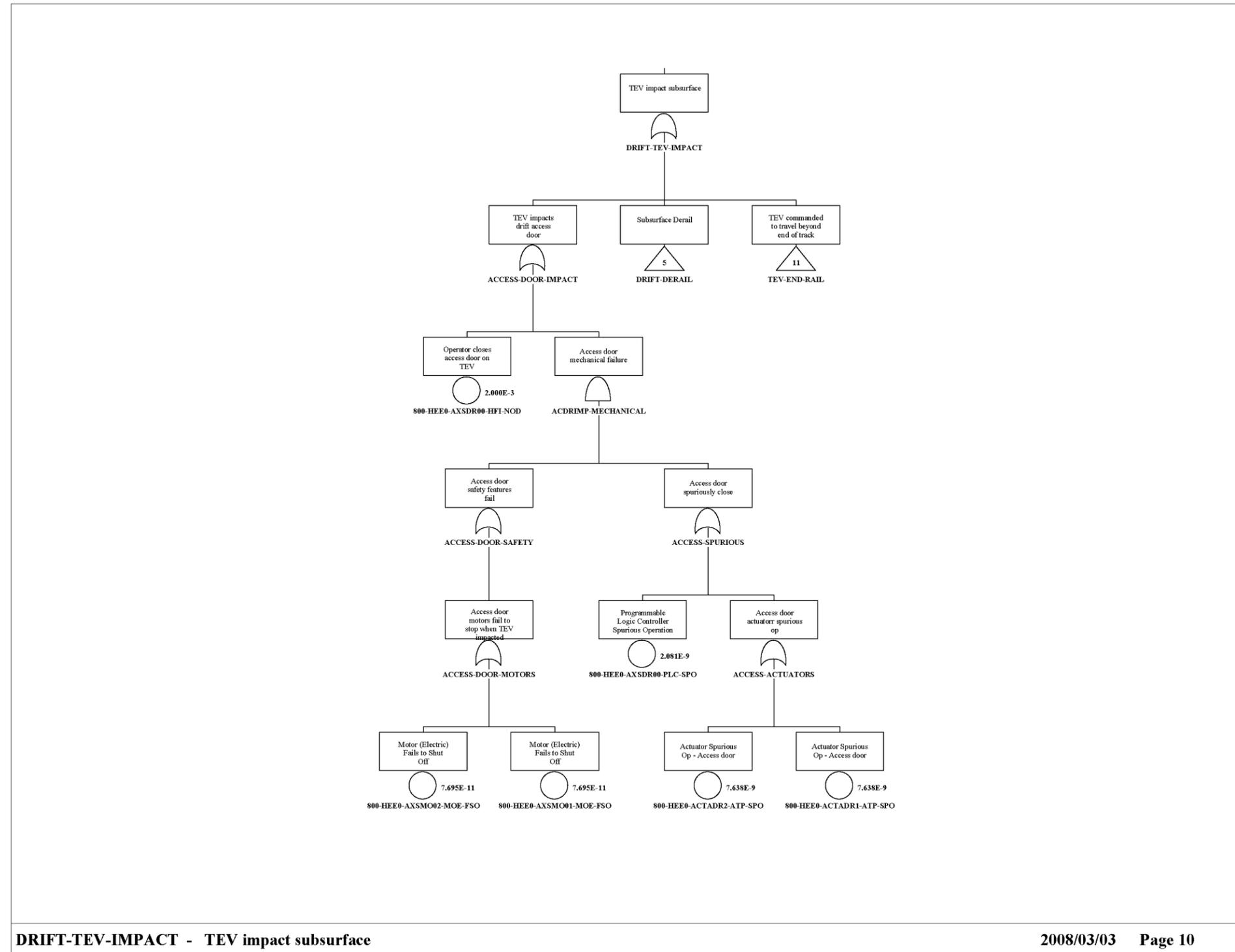
Figure B1.4-21. DRIFT-WP-IMPACT – TEV  
Impacts Waste Package



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

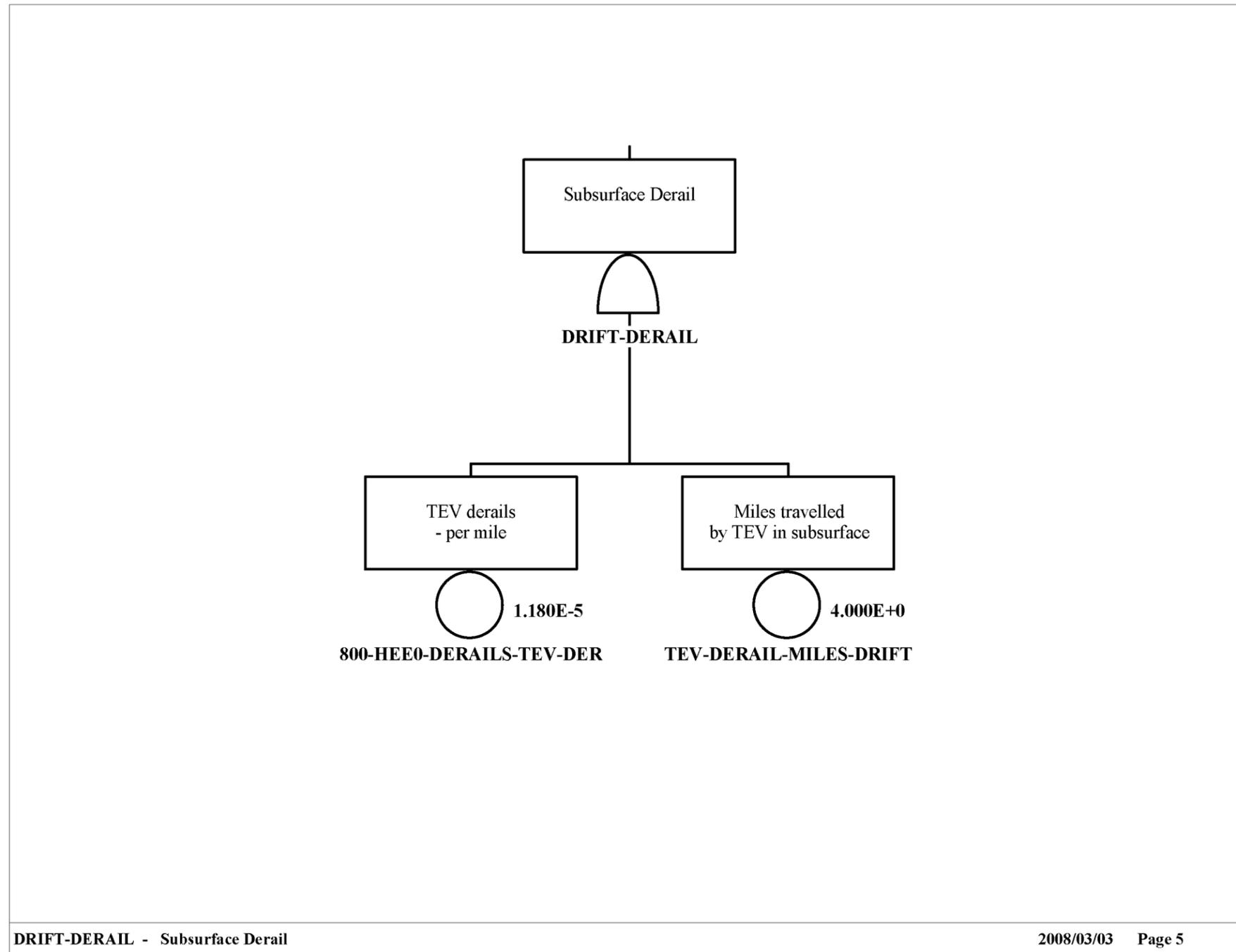
Source: Original

Figure B1.4-22. FACILITY COLLISION – TEV Collides with Object in a Facility



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.  
Source: Original

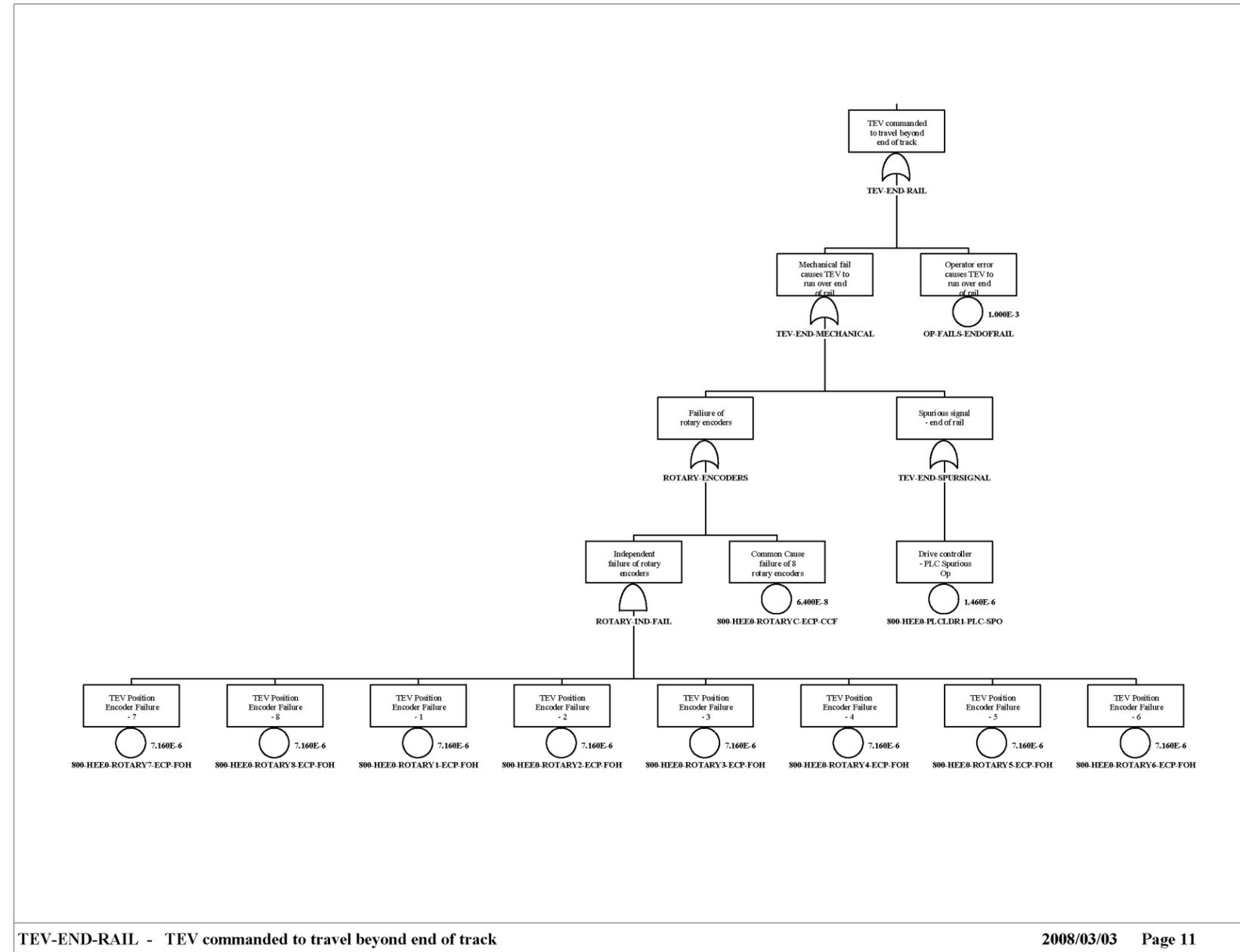
Figure B1.4-23. DRIFT-TEV-IMPACT (Page 1 of 3) – TEV Collides with Object in Emplacement Drift



NOTE: TEV = transport and emplacement vehicle.

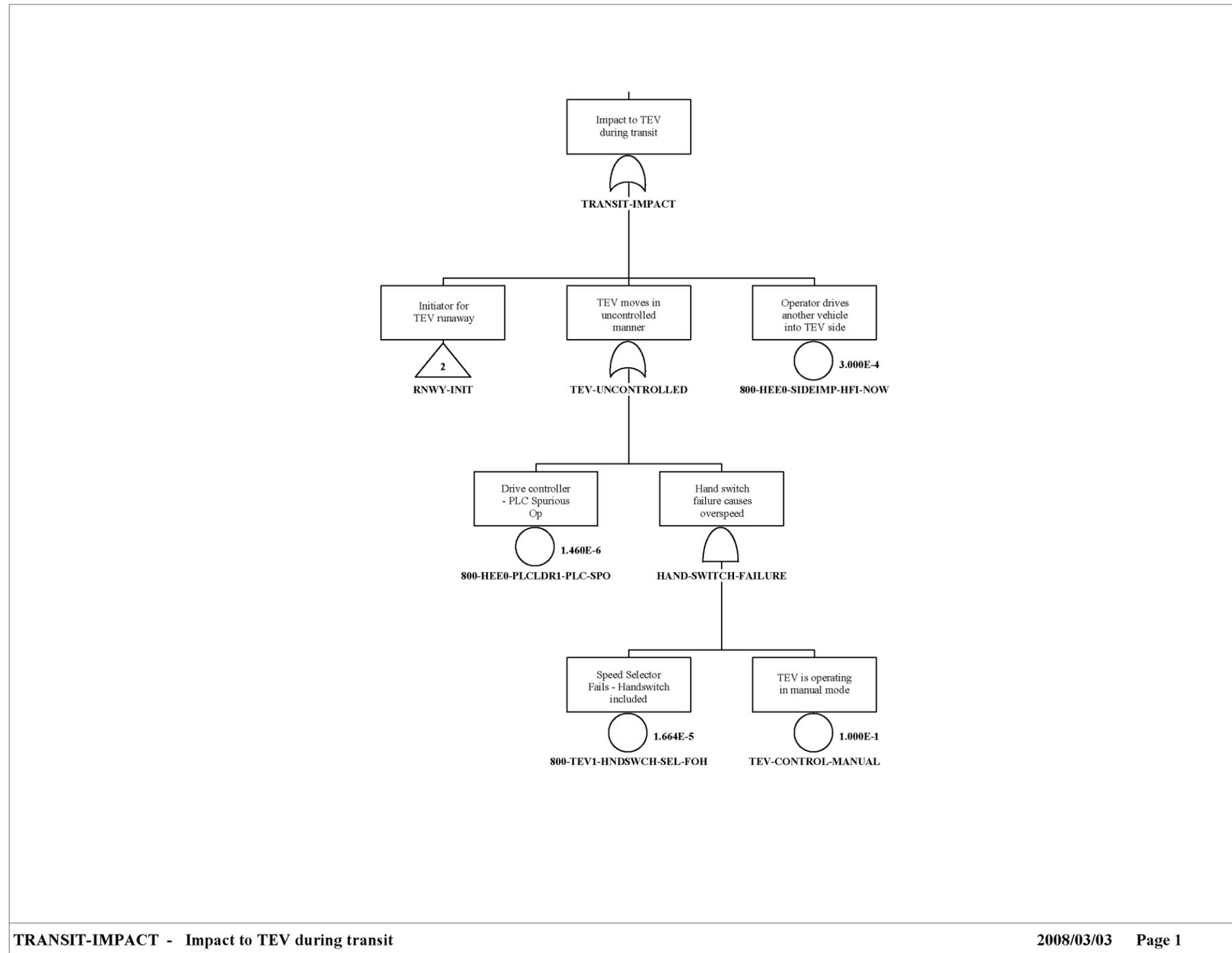
Source: Original

Figure B1.4-24. DRIFT-TEV-IMPACT (Page 2 of 3) –  
Subtree: DRIFT-DETRAIL – TEV Derails  
in Emplacement Drift



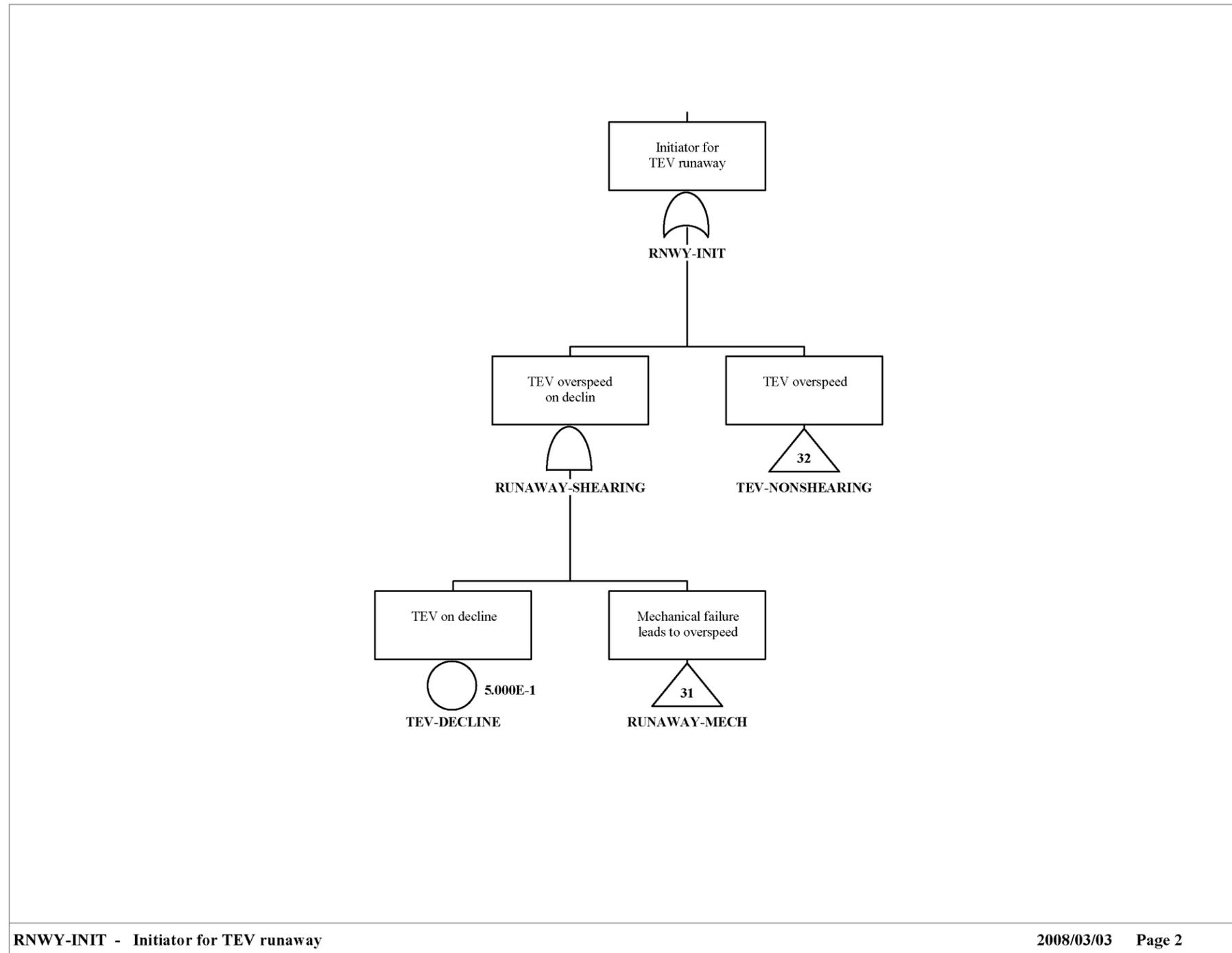
NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.  
Source: Original

Figure B1.4-25. DRIFT-TEV-IMPACT (Page 3 of 3) –  
Impact to TEV during Transit



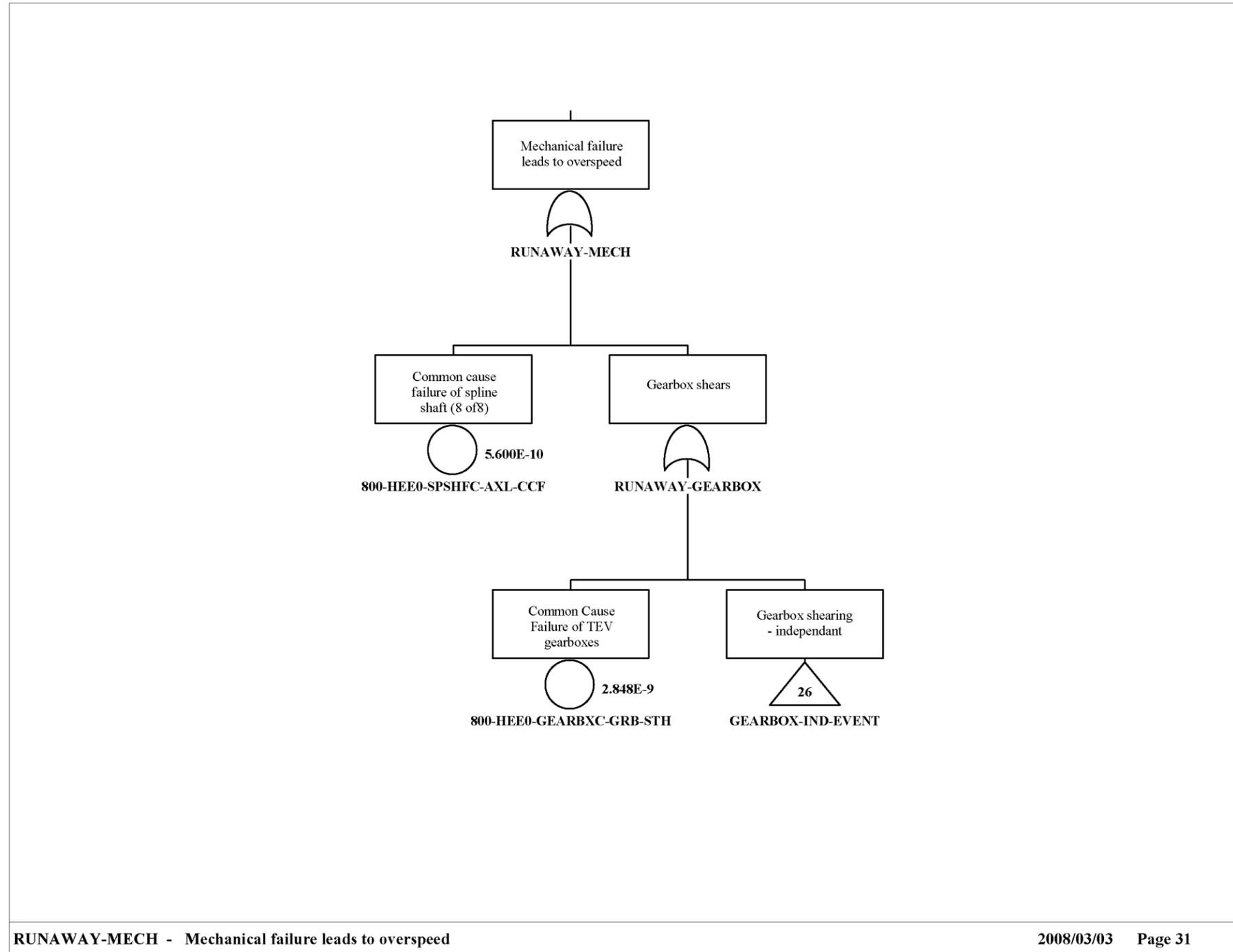
NOTE: TEV = transport and emplacement vehicle.  
Source: Original

Figure B1.4-26. TRANSIT-IMPACT (Page 1 of 9) –  
Impact to TEV during Transit



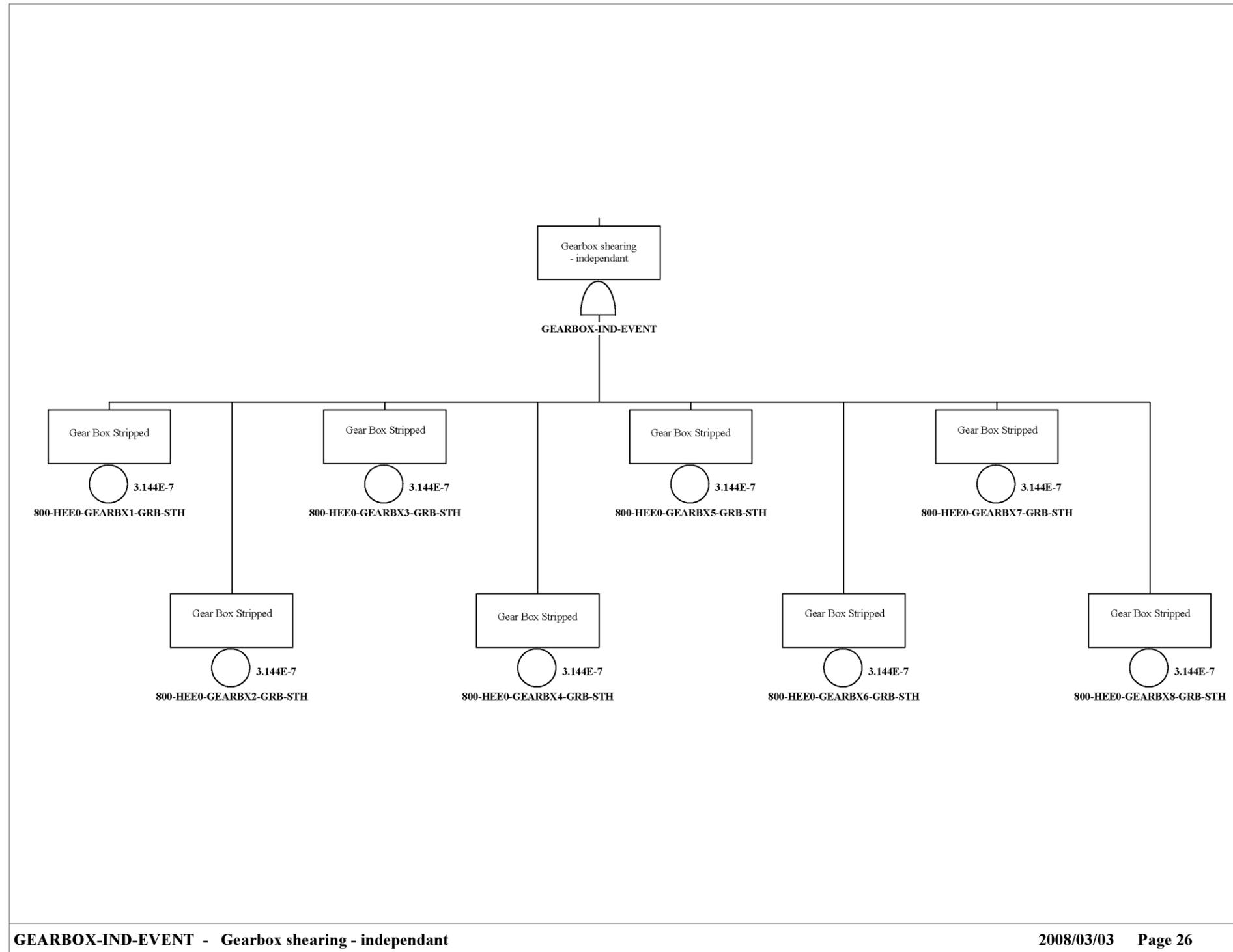
NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle.  
Source: Original

Figure B1.4-27. TRANSIT-IMPACT (Page 2 of 9) –  
Impact to TEV during Transit



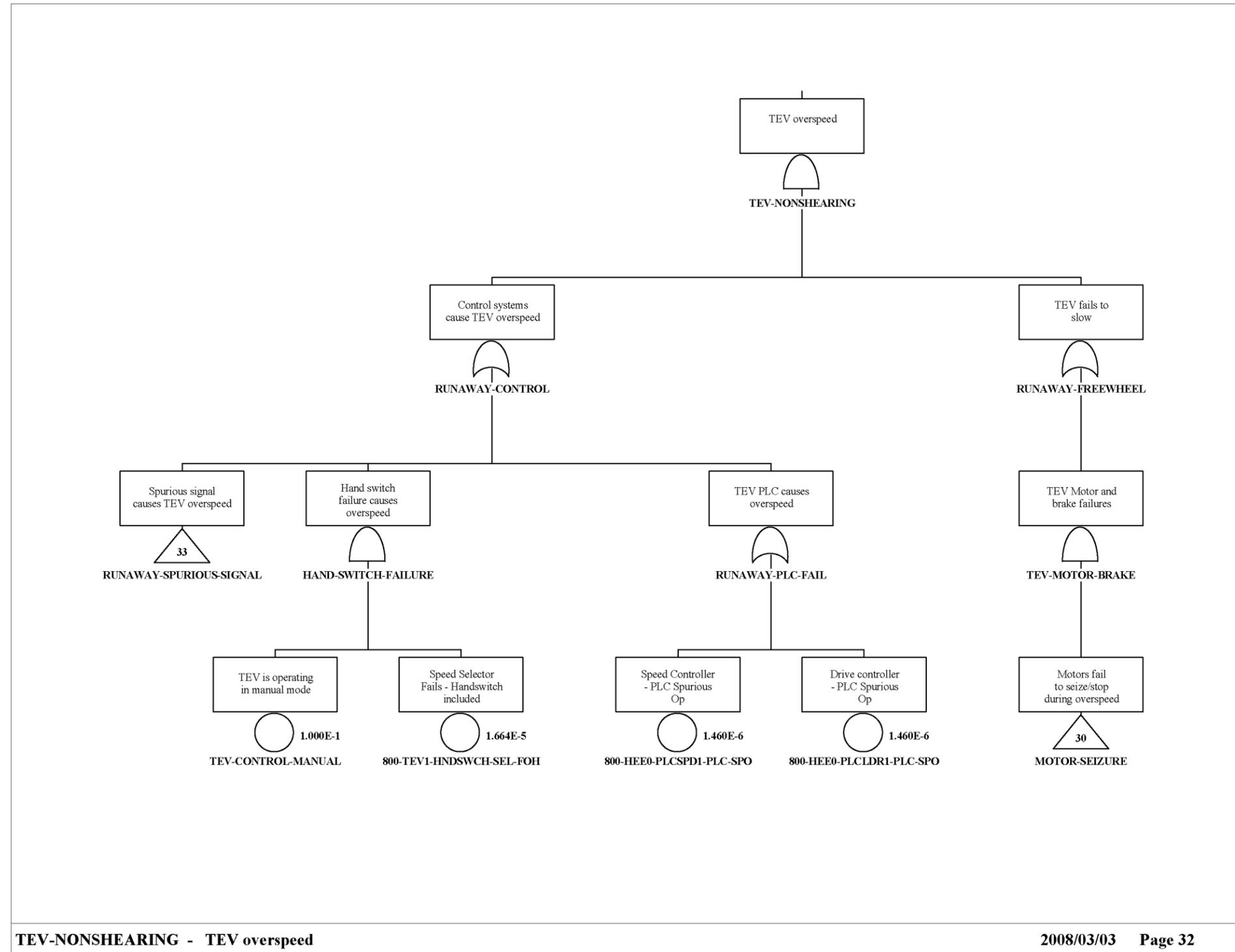
NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.  
Source: Original

Figure B1.4-28. TRANSIT-IMPACT (Page 3 of 9) –  
Impact to TEV during Transit



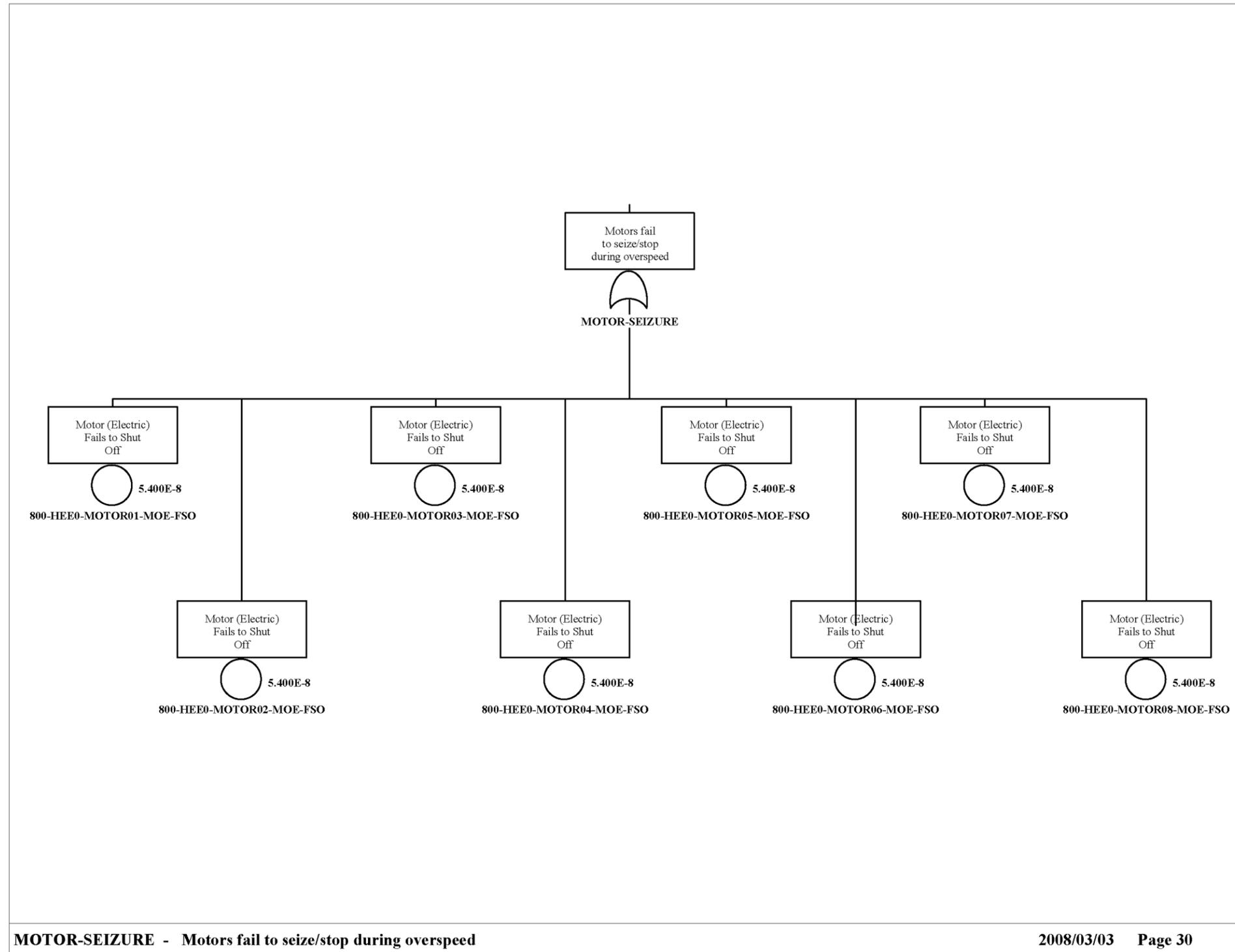
Source: Original

Figure B1.4-29. TRANSIT-IMPACT (Page 4 of 9) –  
Impact to TEV during Transit



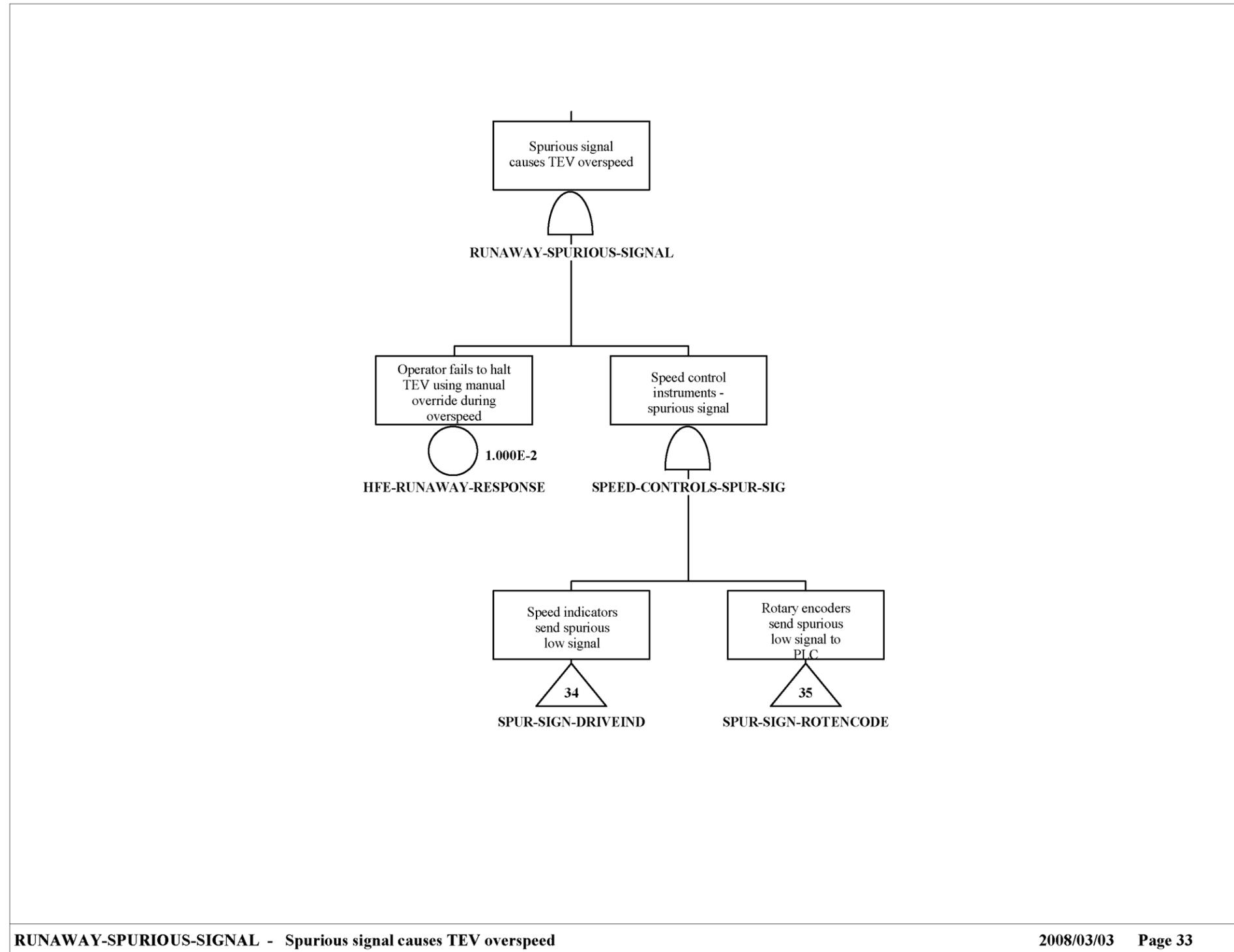
Source: Original

Figure B1.4-30. TRANSIT-IMPACT (Page 5 of 9) –  
Impact to TEV during Transit



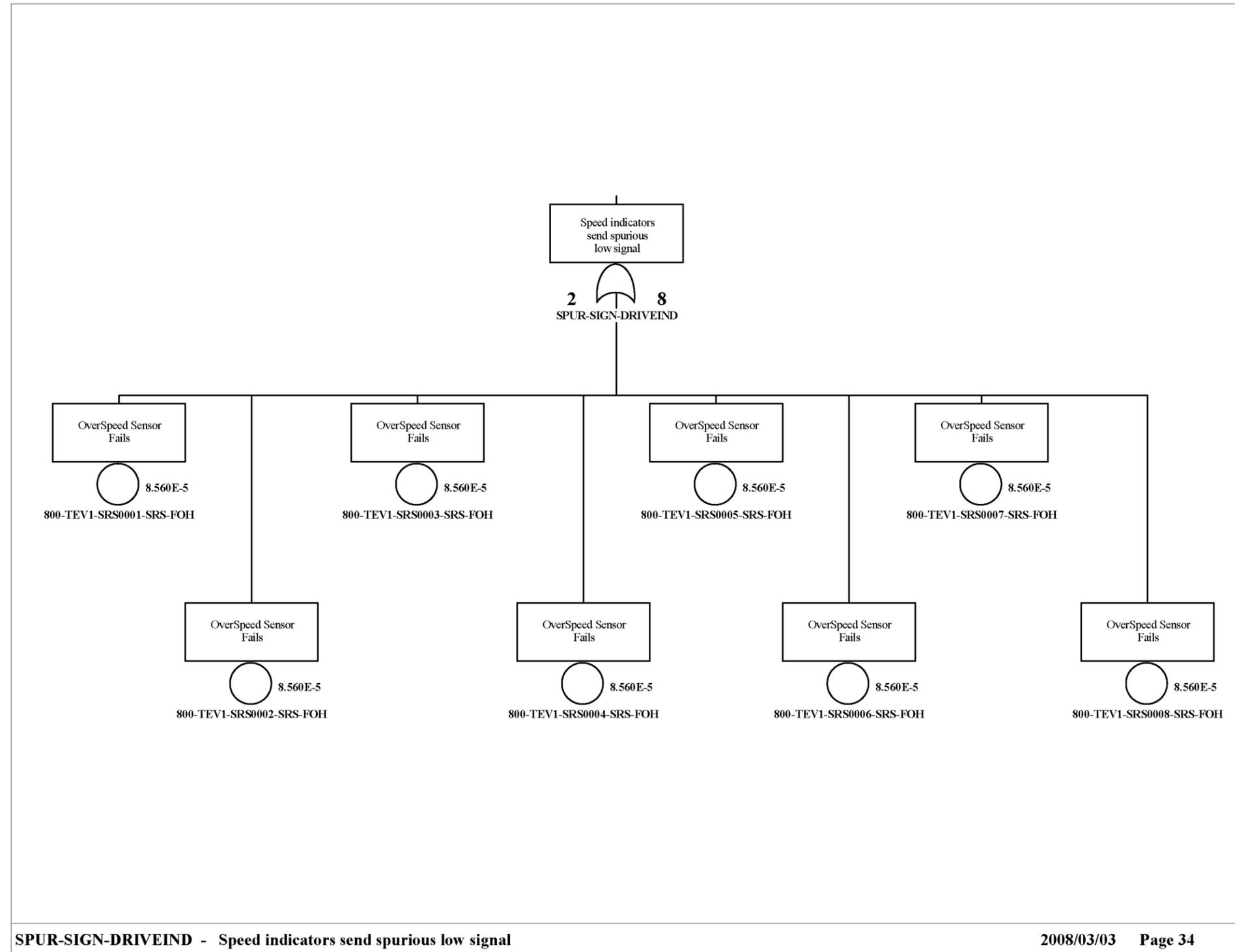
Source: Original

Figure B1.4-31. TRANSIT-IMPACT (Page 6 of 9) –  
Impact to TEV during Transit



Source: Original

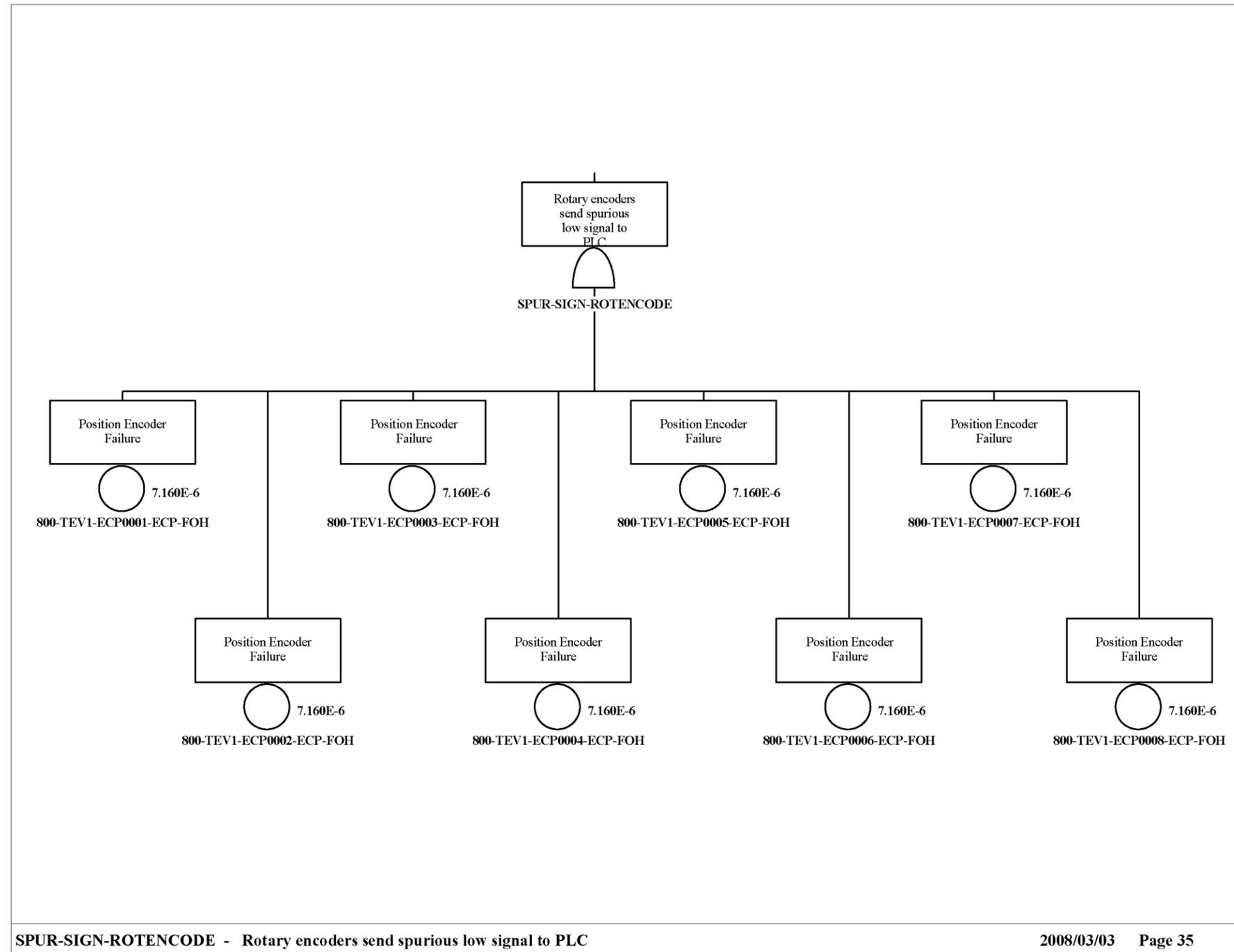
Figure B1.4-32. TRANSIT-IMPACT (Page 7 of 9) –  
Impact to TEV during Transit



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

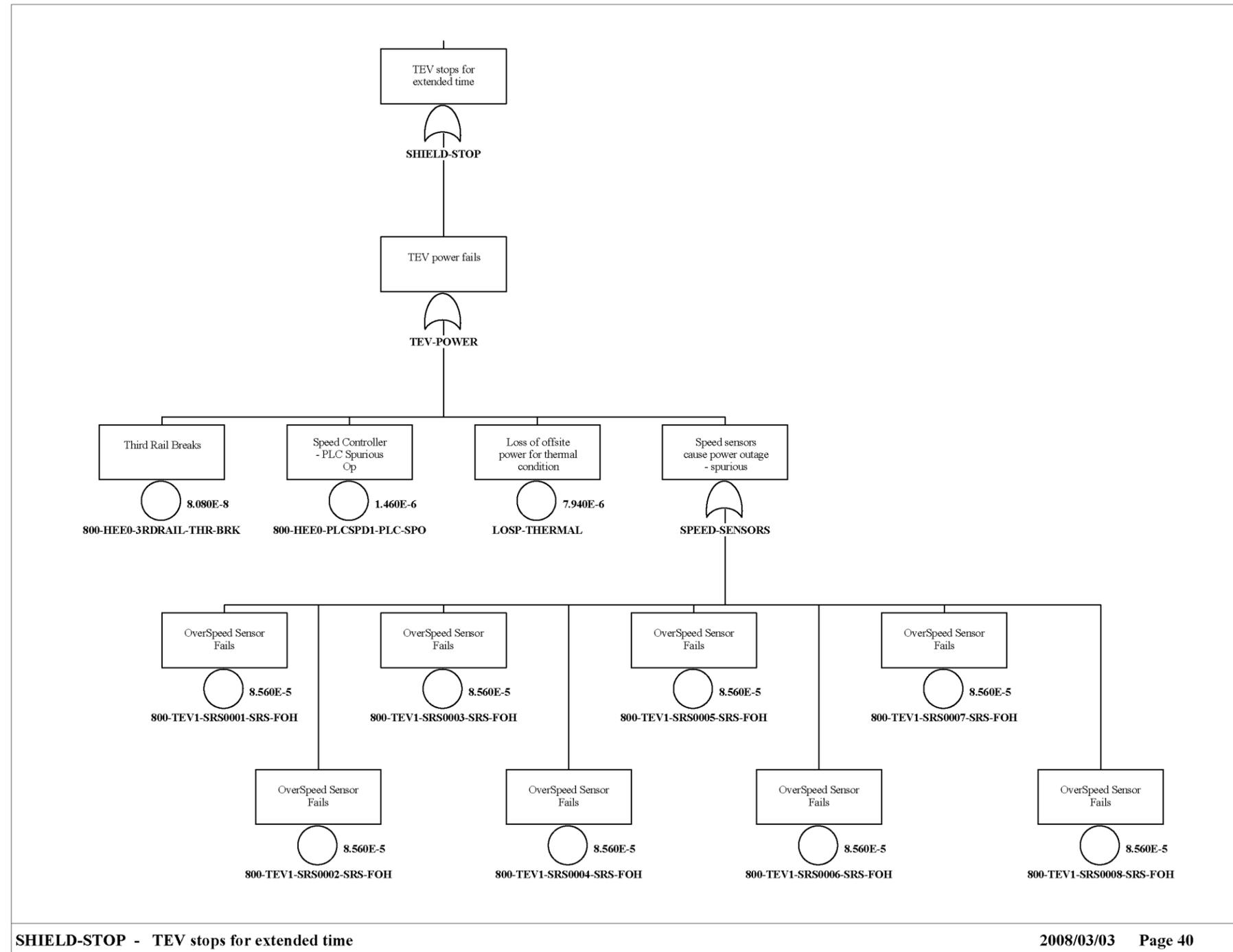
Figure B1.4-33. TRANSIT IMPACT (Page 8 of 9)  
Impact to TEV during Transit



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

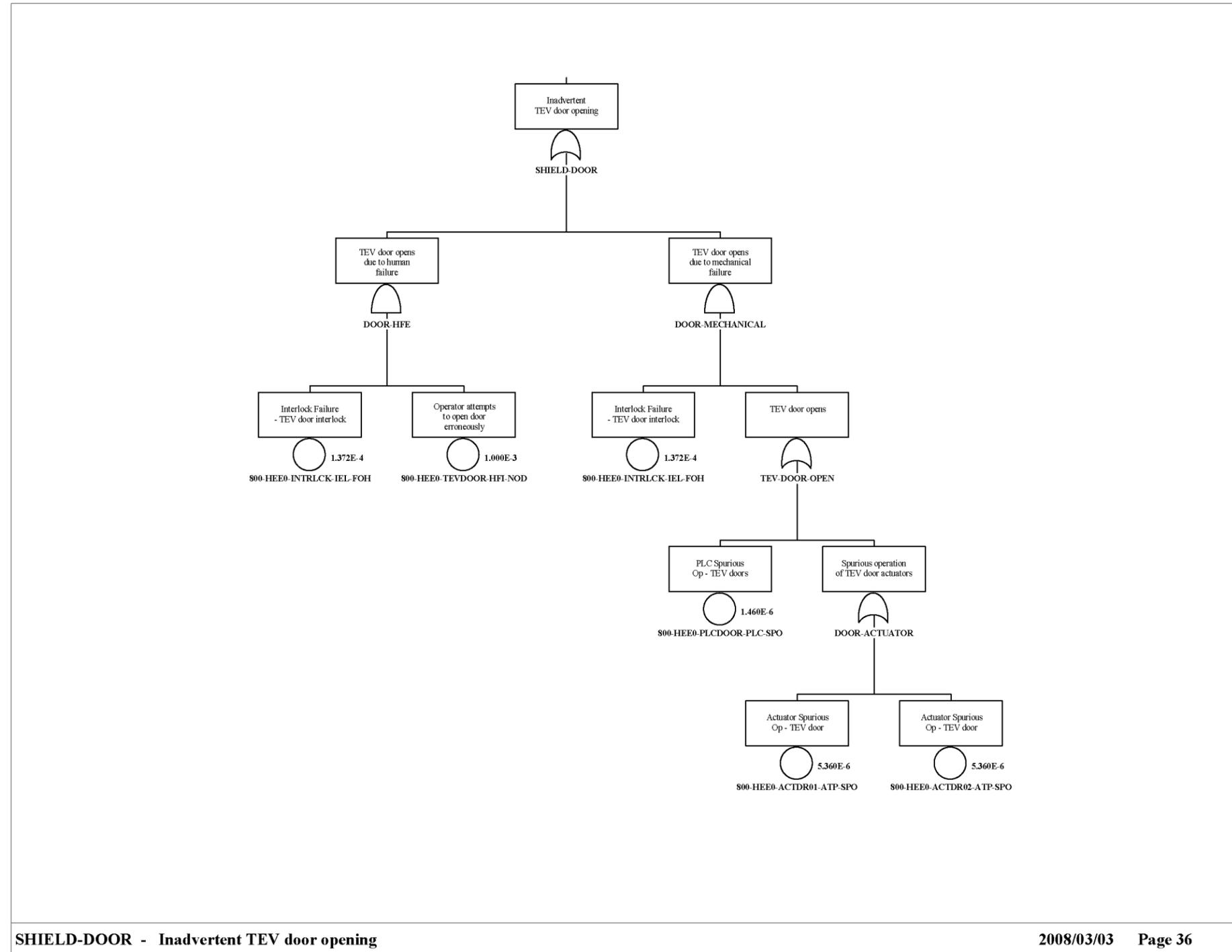
Figure B1.4-34. TRANSIT IMPACT (Page 9 of 9)  
Impact to TEV during Transit



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

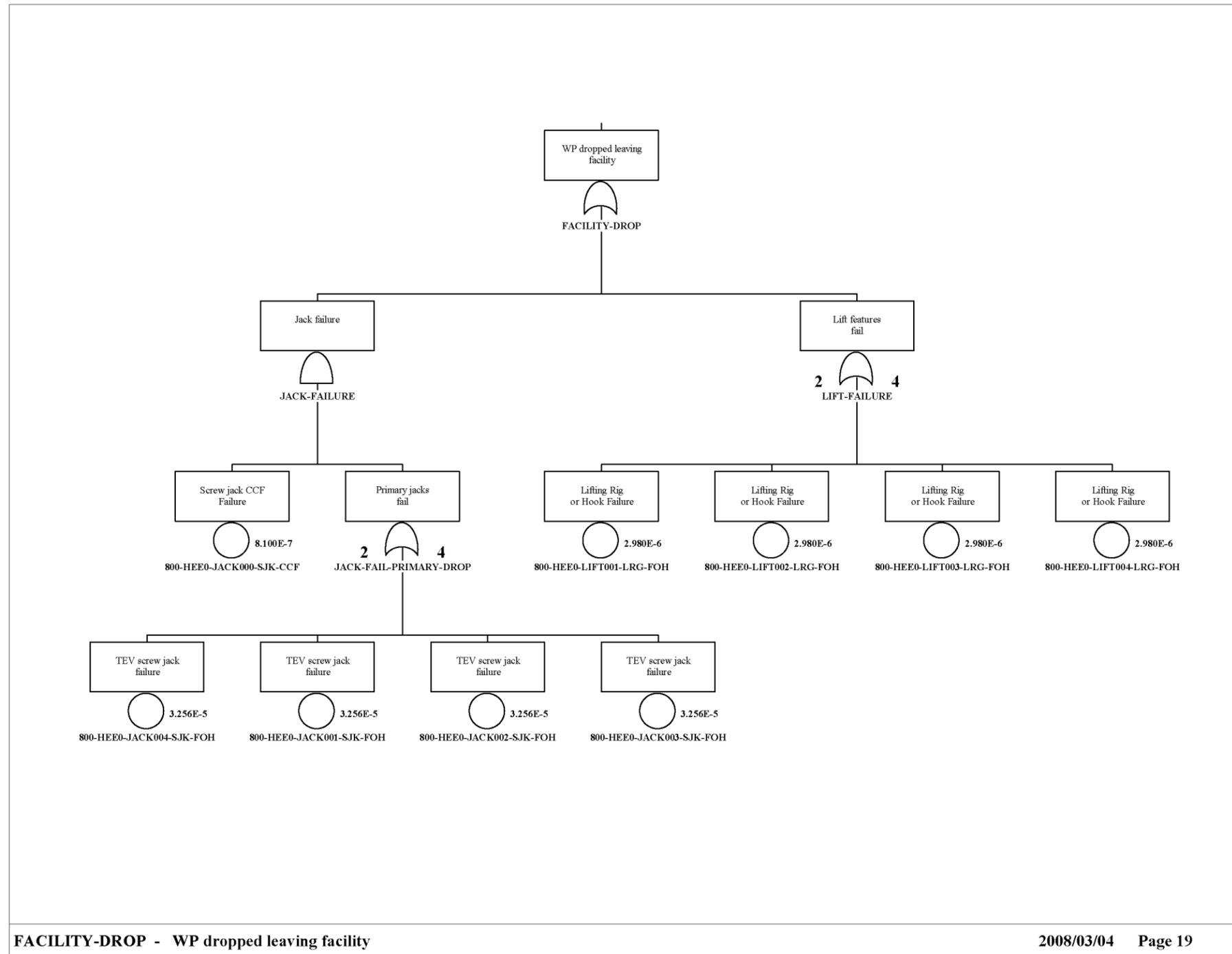
Figure B1.4-35. SHIELD-STOP – TEV Stops for Extended Time



NOTE: TEV = transport and emplacement vehicle.

Source: Original

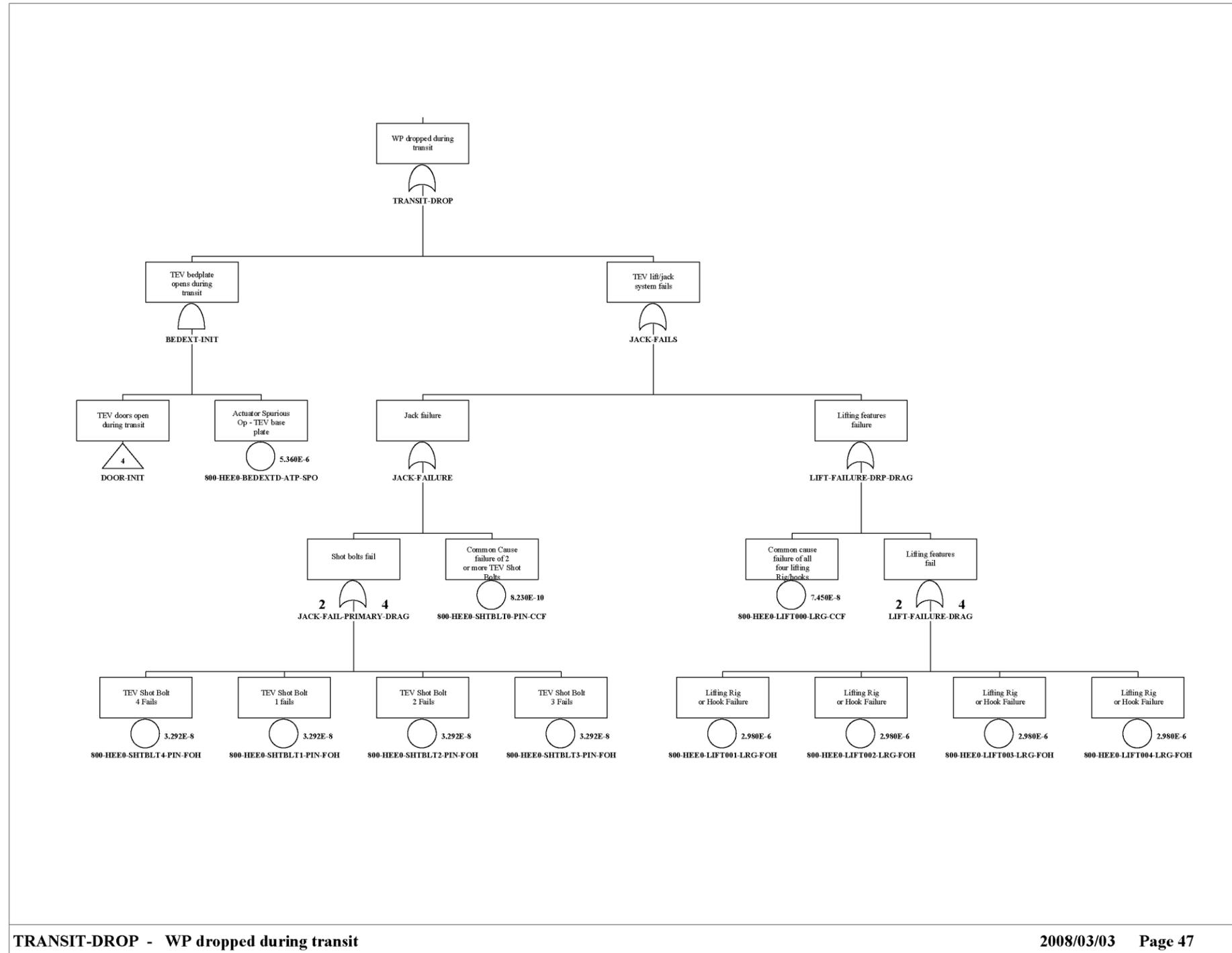
Figure B1.4-36. SHIELD-DOOR – Inadvertent TEV Door Opening



NOTE: Op = operation; TEV = transport and emplacement vehicle; WP = waste package.

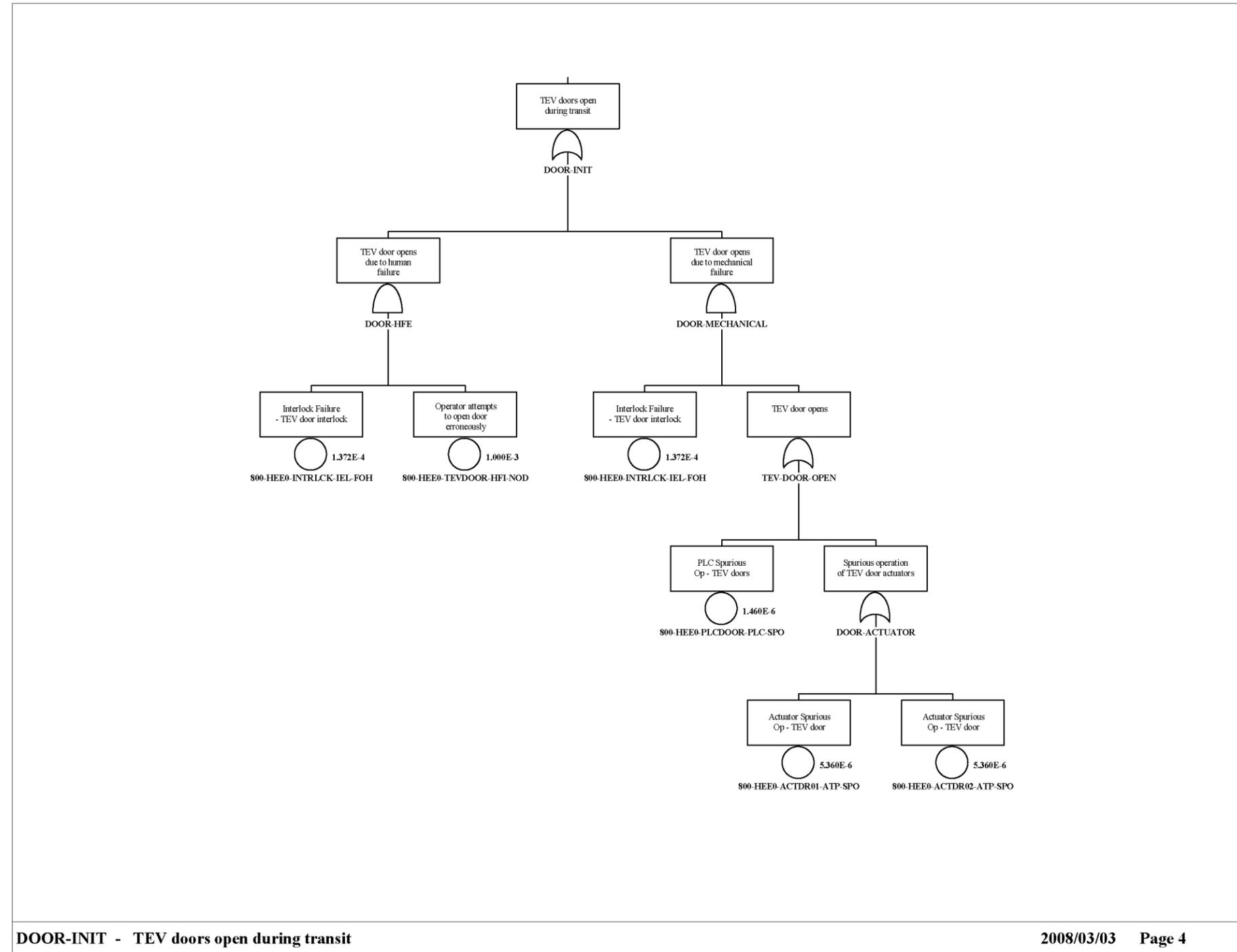
Source: Original

Figure B1.4-37. FACILITY-DROP – WP Dropped While Leaving Facility



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.  
Source: Original

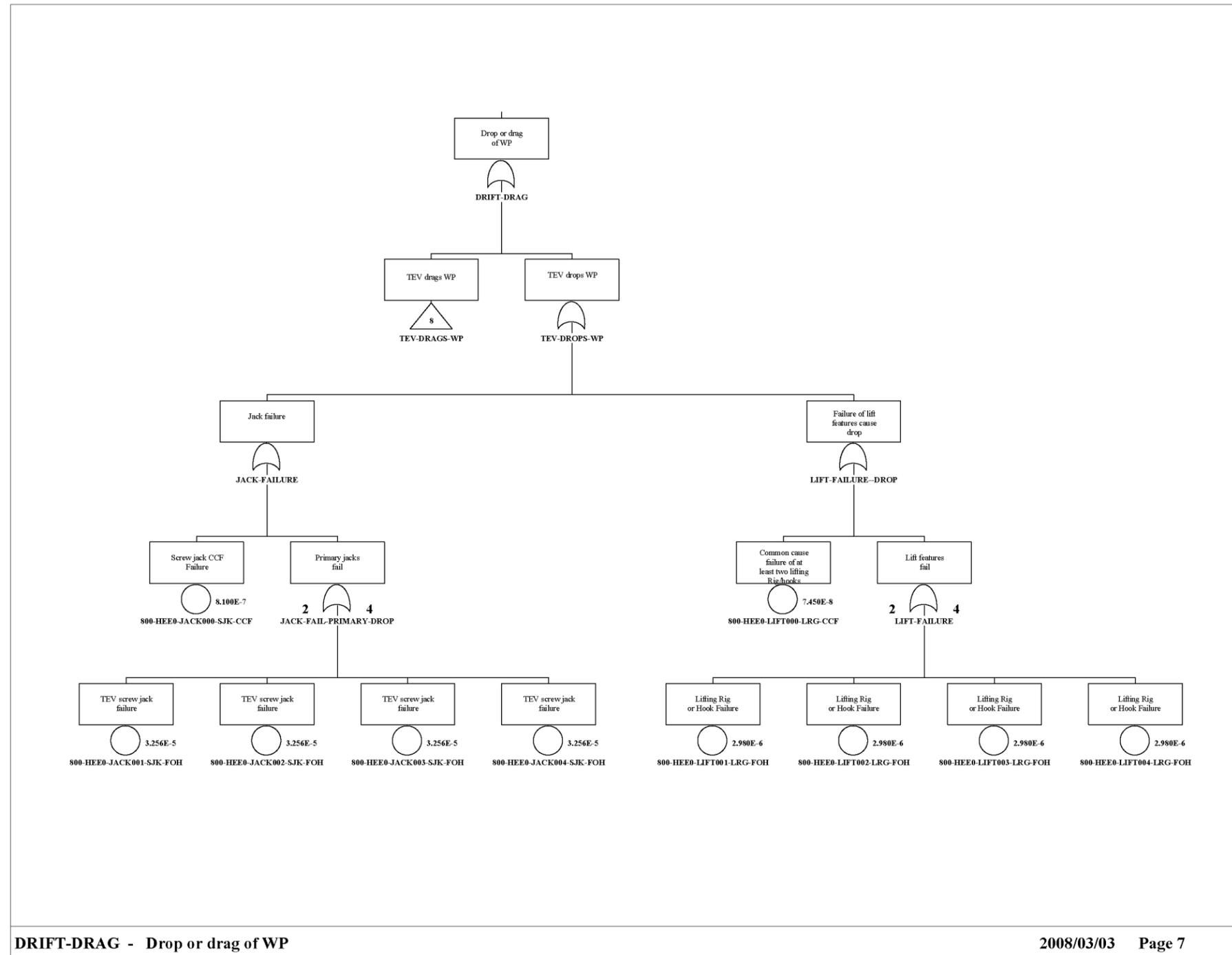
Figure B1.4-38. TRANSIT- DROP (1 of 2) Waste Package Dropped During Transit



NOTE: Op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

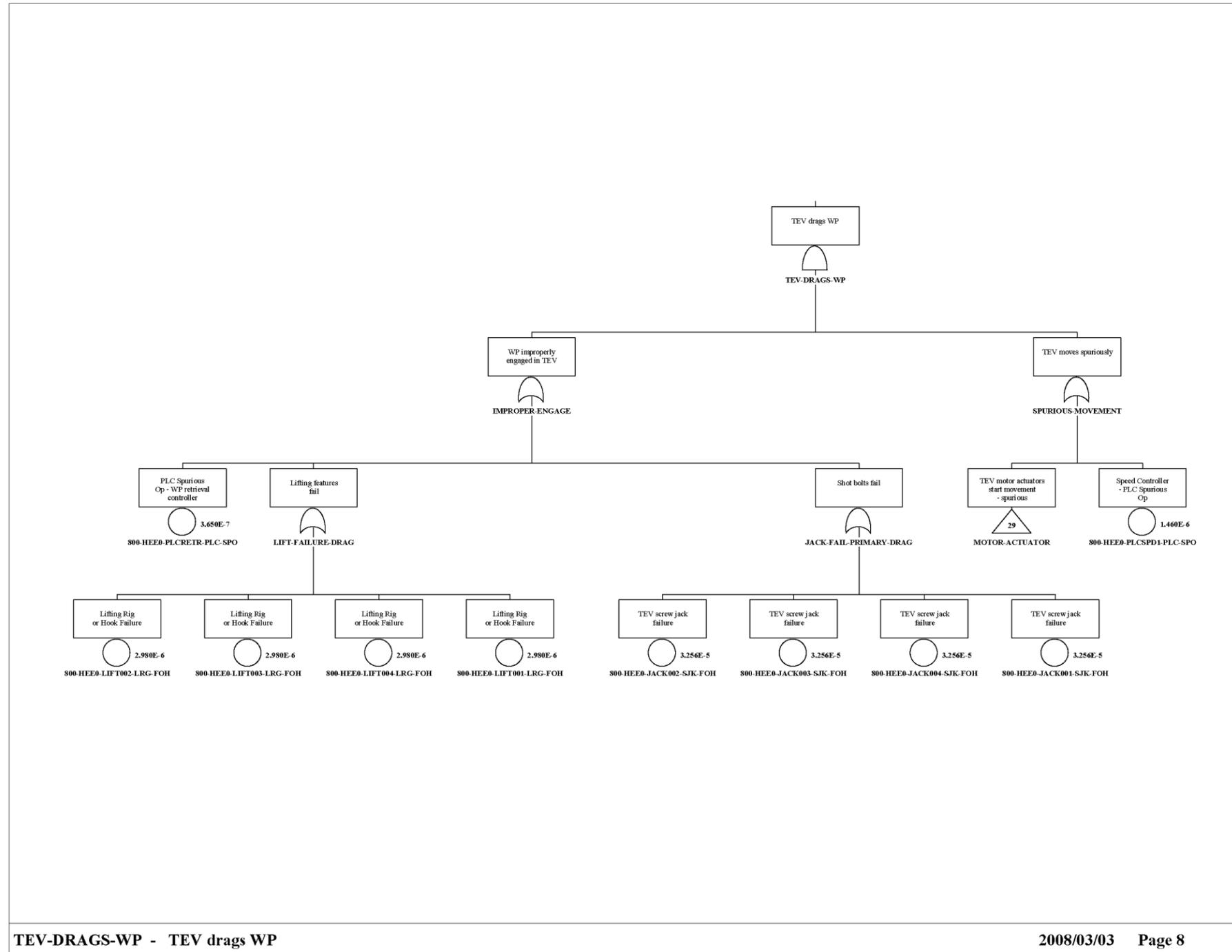
Figure B1.4-39. TRANSIT- DROP (2 of 2) Waste Package Dropped During Transit



NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

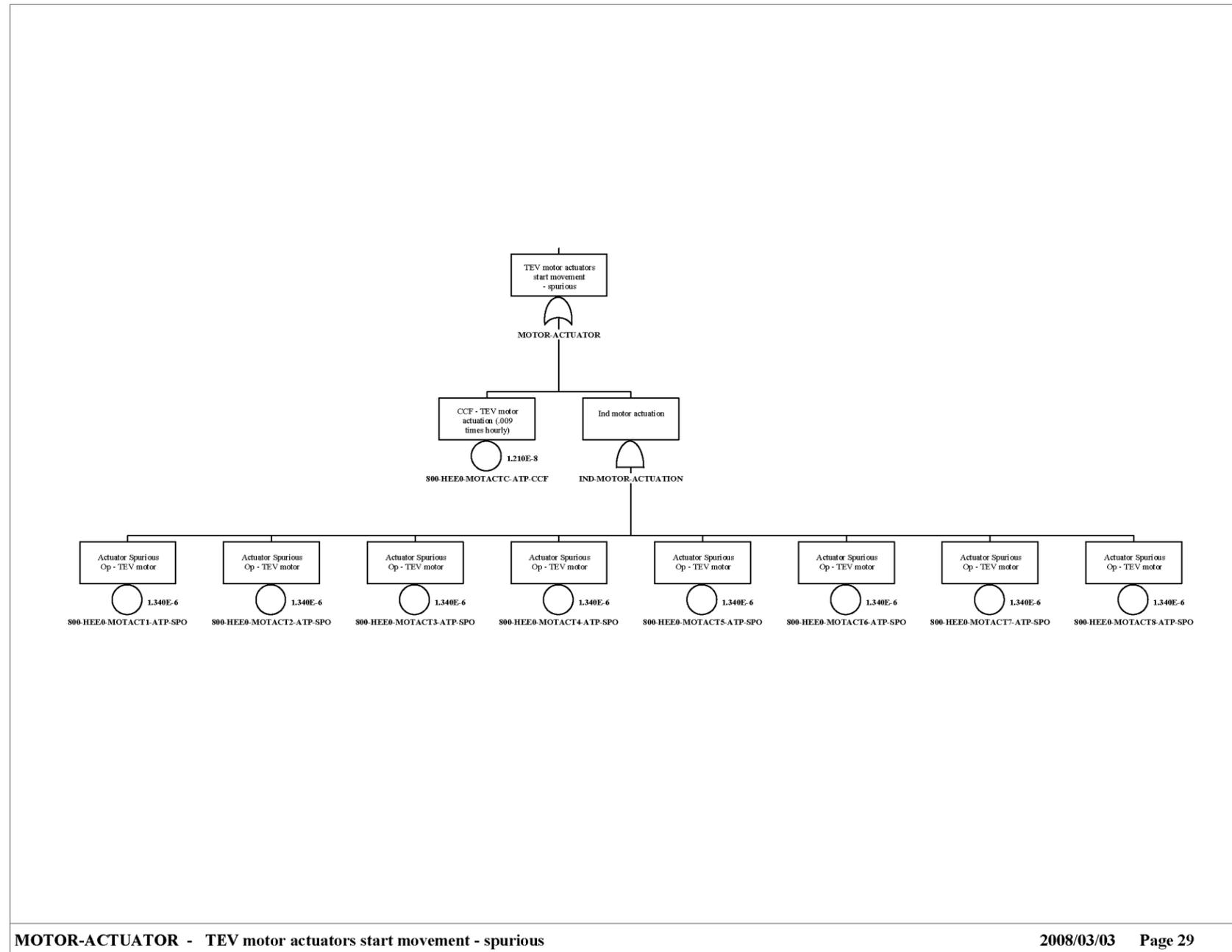
Figure B1.4-40. DRIFT-DRAG (1 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift



NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

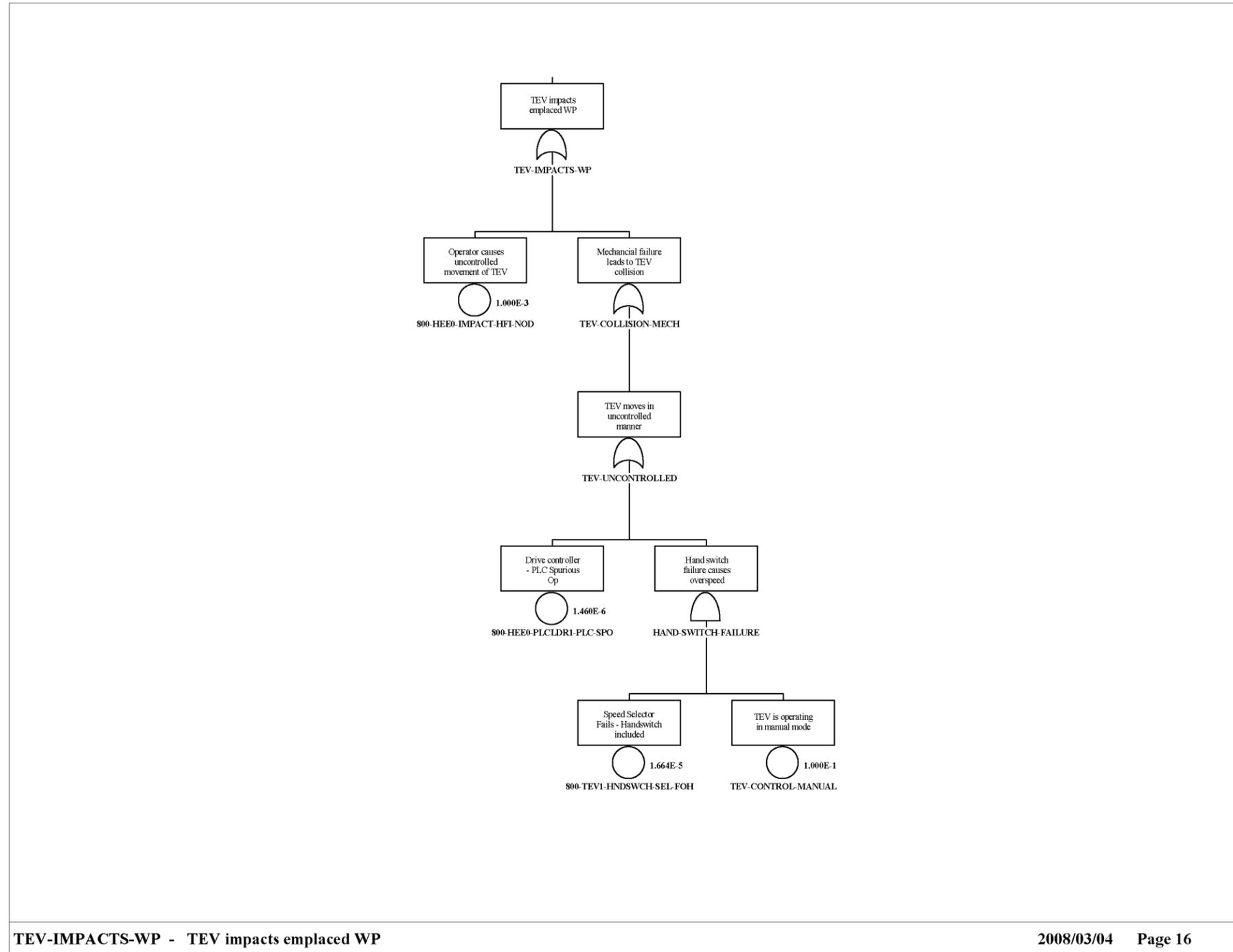
Figure B1.4-41. DRIFT-DRAG (2 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift



NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Figure B1.4-42. DRIFT-DRAG (3 of 3) – Drop or Drag of Waste Package by TEV in Emplacement Drift



NOTE: PLC = programmable logic controller; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

Figure B1.4-43. TEV-IMPACTS-WP – TEV Impacts Waste Package in Emplacement Drift

## **B2 HEATING VENTILATION AND AIR CONDITIONING FAULT TREE ANALYSIS**

### **B2.1 REFERENCES**

#### **Design Inputs**

The PCSA is a safety analysis 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, paragraph 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

B2.1.1 Not Used.

B2.1.2 Not Used.

B2.1.3 BSC 2007. *CRCF 1 Composite Vent Flow Diagram Tertiary Conf ITS Exhaust & Non-ITS HVAC Supply Systems*. 060-M50-VCT0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071227.0013.

B2.1.4 BSC 2007. *CRCF 1 ITS Confinement Areas HEPA Exhaust System—Train A Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00103-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0005.

B2.1.5 BSC 2007. *CRCF 1 ITS Confinement Areas HEPA Exhaust System—Train B Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00104-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0006.

B2.1.6 BSC 2007. *CRCF 1 Equipment Sizing and Selection Calculation (ITS)*. 060-M8C-VCT0-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0032.

#### **Design Constraints**

B2.1.7 NRC (Nuclear Regulatory Commission) 2007. *Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program*. HLWRS-ISG-03. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20070918.0096.

### **B2.2 ITS HVAC DESCRIPTION**

#### **B2.2.1 Overview**

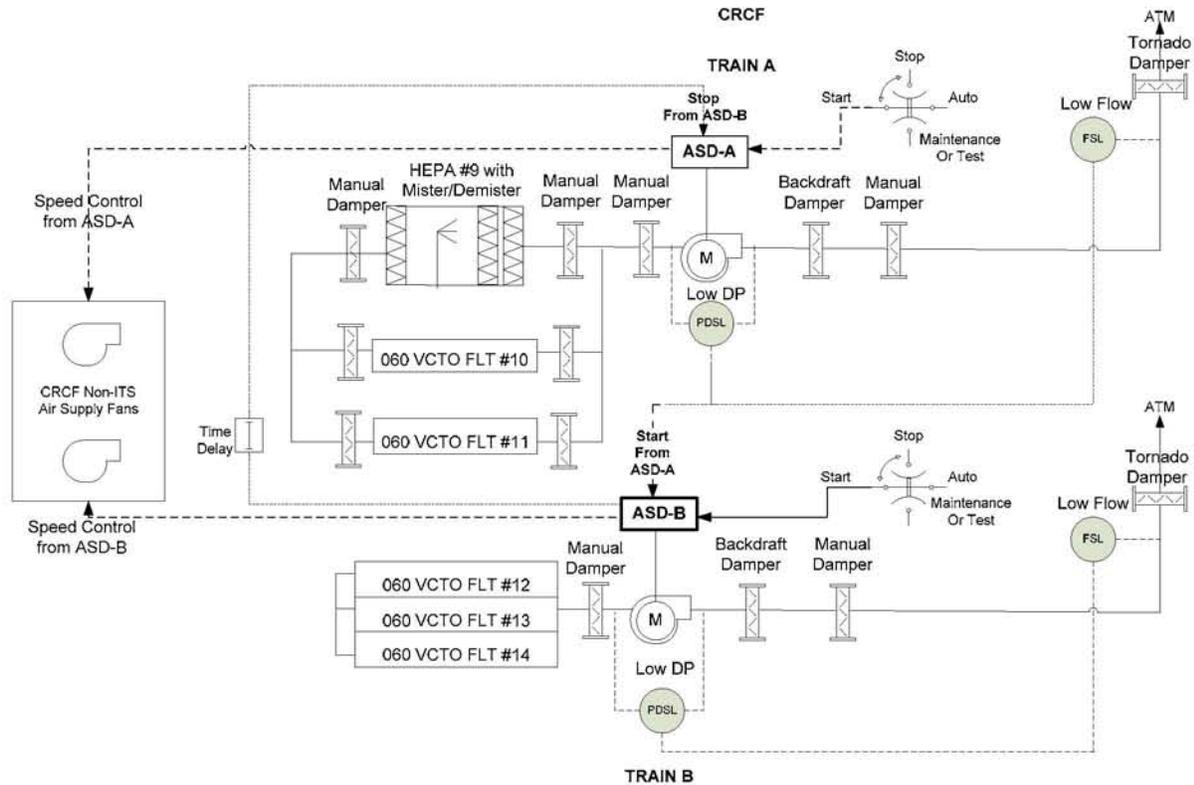
The ITS HVAC is a two train system of identical components. One train is always operational while the other train is in standby mode. This system is not configured to run both trains at the same time without bypassing relevant control circuitry. An operational two-train configuration is not addressed in this analysis.

Figure B2.2-1 shows the locations of the various pieces of ITS HVAC equipment described in the following sections. Sizing of the ITS HVAC in the CRCF (Ref. B2.1.6, Section 6.1) was performed to ensure desired air distribution, ventilation rates, and transport velocities were attainable to maintain the required negative delta pressure within the tertiary confinement (C2) zones in this facility.

In the CRCF, the train A HVAC equipment is located in Room 1011 and the train B HVAC equipment is on the opposite end of the building in Room 1032. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. Although these trains are interconnected through interior duct work, the trains are independent. A backdraft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

This HVAC system is composed of four subsystems:

- A series of dampers are used to control pressure, flow, and flow direction
- Three HEPA filter units, each consisting of one medium-efficiency roughing filter (60-90% efficiency), two high-efficiency filters for particulate removal (99.97% efficiency) (Ref. B2.1.6, Appendix B) and a mister/demister for maintaining proper humidity levels. (There is a water deluge system in each HEPA filter which is used in fire scenarios. Refer to the facility fire analysis for information regarding these pieces of equipment)
- One exhaust fan per train
- Control circuitry with logic contained in an erasable programmable read-only memory (EPROM) located in the adjustable speed drive (ASD) controller used for controlling the speed of the operating fan and on fault detection ((Ref. B2.1.6, Section 3.2.3). For off-normal conditions, uncorrectable delta pressures is either too high or too low, as defined in Table B2.2-1, the ASD, shuts down the operating train and starts the standby train. The ASD also controls non-ITS supply fans that are adjusted to maintain airflow in the facility.



NOTE: It should be noted that, the diagram has been simplified with respect to the HEPA filter equipment shown for train A and B. The equipment configuration for HEPA Filters identified as 060 VCTO FLT 10, 11, 12, 13 and 14 are identical to the HEPA FLT 9. In addition, train B has the same input/output dampers shown for train A. Train A is always defined as the operating train and train B is always designated as the standby train.

ASD = adjustable speed drive; ATM = atmosphere; CRCF = Canister Receipt and Closure Facility; DP = delta pressure; FSL = flow sensor low; ITS = important to safety; HEPA = high=efficiency particulate air (filter); PDSL = pressure differential sensor low.

Source: Original

Figure B2.2-1. Block Diagram of the CRCF ITS HVAC System

### B2.2.2 Damper Subsystem Description

The ITS HVAC system uses manual, backdraft and tornado dampers to control the delta pressure inside the containment area or to isolate the standby system from the outside atmosphere.

Manual dampers are located on the input and output sides of the HEPA filter. These filters are used to isolate the HEPA filter, if required, during maintenance. There is a manual damper on the input side of the exhaust fan that is used to isolate the entire HEPA filter subsystem for maintenance on the HEPA filters or the exhaust fan. One additional manual damper is located between the backdraft and the tornado damper which can be used to isolate the entire train.

A backdraft damper is located on the exhaust side of the fan. This damper is normally open for the operating train and closed on the standby train. This damper prevents a reverse airflow through the standby system as a result of the negative delta pressure in the containment C2 areas.

A tornado damper is used to control airflow automatically to prevent the transmission of tornado pressure surges from outside the facility.

### **B2.2.3 HEPA Filters**

The three HEPA filter units are identical consisting of a  $3 \times 3$  array of medium (nine filters) and two banks of HEPAs (18 filters). A bag-in/bag-out procedure is used to replace the HEPA filters. Each filter is sized for a maximum flow of 1,500 cfm (Ref. B2.1.6, Section 3.2.2). The failure analysis includes the HEPA filter bank for plugs and leaks, mister/demister for humidity control, and the medium roughing filter.

The HEPA subsystem also contains the following components that are not modeled in the analysis: Inlet test section, combination test section, the outlet test section, and the deluge system during fire scenarios.

### **B2.2.4 Direct Drive Exhaust Fan and Motor**

The exhaust fan and motor are sized to provide a maximum airflow rate of 40,500 cfm. To meet delta pressure requirements for the CRCF, the exhaust system must provide an airflow rate of 35,010 cfm (Ref. B2.1.6, Appendix A, Table A-1). At this airflow rate, the exhaust system provides for a total of 14.2 inches of water column required to maintain delta pressure in the facility (Ref. B2.1.6, Section 3.1.4).

The exhaust fan motor is rated at 1800 rpm (Ref. B2.1.6, Section 3.1.5) but the actual speed is controlled by the ASD. The ASD adjusts the speed to maintain delta pressure when facility doors are opened, HEPA filters lose efficiency, or outside wind speeds.

### **B2.2.5 Control Circuitry**

The ITS HVAC system is controlled by EPROM (although there are programmable logic controls in various locations throughout the CRCF, none of these are ITS) logic. This control logic is contained in the ASD control panel which is used to monitor the delta pressure across the exhaust fan and airflow rate exhausting to the atmosphere. Changes in air pressure cause the ASD to change the speed of the exhaust fan motor. The ASD also controls the rpm of the non-ITS supply fans (Ref. B2.1.4), (Ref. B2.1.5), and (Ref. B2.1.3). The supply fans are used to stabilize the airflow within the CRCF. These fans are non-ITS so they are not accounted for in this analysis except in a degraded mode of operation.

At any time the ASD can not return the delta pressure to normal operating conditions, the ADS shuts down the operating train and sends a signal to the standby train to start up. When the standby ASD receives this signal, it starts the standby system and sends a signal to the operational train to shutdown. There is an interlock to preclude the operation of both trains at the same time. Time delays are built-into the ASD processing system to preclude spurious signals received from the sensors triggering a false transfer.

### B2.2.6 ITS HVAC Normal Operations

In normal operations, train A is operational and train B is in standby. EPROM logic within the ASD monitor the pressure differential across the exhaust fan and the flow rate of the exhaust to the atmosphere. There are no programmable logic controllers used in the ITS HVAC control system and all interlocks are hardwired for ITS operations. Table B2.2-1 shows the ASD operational response to various delta pressure conditions inside the facility.

Table B2.2-1. ASD Response to Variations in Delta Pressure

DP Pressure Sensor	Low Flow Sensor	ASD Response
High DP (Plugged HEPA)	Low Flow	Switch trains
High DP	High Flow	Decrease RPM of Exhaust Fan
High DP	Nominal Flow	Increase RPM of Supply Fans
Low DP (HEPA Leak)	High Flow	Switch trains
Low DP	Nominal Flow	Decrease RPM of Supply Fans
Low DP	Low Flow	Increase RPM of Exhaust Fan

NOTE: ASD = adjustable speed drive; DP = delta pressure; HEPA = high-efficiency particulate air (filter); RPM = revolutions per minute.

Source: Original

If the ASD-A response does not return the delta pressure and/or flow rates to a nominal state, then ASD-A issues the command to the ASD-B to startup train B. ASD-B commands the startup of train B and, after a time delay, send a signal back to ASD-A to shut down. An interlock prevents both trains from operating at the same time.

Under normal operations with non-ITS supply fans working, all three HEPA filter assemblies in the train must be working to achieve the exhaust flow rate of 35,010 cfm (Ref. B2.1.6, Section 6.1.1 item 1). Each HEPA filter array can filter 13,500 cfm at maximum efficiency (Ref. B2.1.6 Section 6.1.1 item 2). The design has some reserve capacity but not enough to maintain the required delta pressure if one of the HEPA filters fail. Under normal operations, the only redundancy in the design is the second train.

Misters/demisters are included as part of the HEPA filters to control the temperature and relative humidity of the air passing through the filters. The water deluge system is not considered to be normal operations and is handled in the fire suppression analyses.

During receipt of a transportation cask or aging overpack or during the export of a waste package or aging overpack, delta pressure is lost for a period of time not to exceed seven minutes per event (this is a conservative estimate of the time it will take for the HVAC system to return the vestibule to a negative pressure). This occurs when the vestibule doors are opened to allow the site transporter, site prime mover or the transport and emplacement vehicle to enter or leave the CRCF.

### **B2.2.7 ITS HVAC Off-Normal Operations**

The ITS HVAC system maintains proper delta pressure throughout Class C2 designated containment areas. Exhausted air from the CRCF is made-up from opening/closing doors to the outside, leaks in the structure and from one of two supply fans which are controlled by the ASD on the operating train. One of these fans in conjunction with other air makeup sources can provide sufficient airflow through the C2 containment areas for the HVAC to maintain delta pressure. These supply fans are not ITS and therefore, they are not connected to the ITS power system for the CRCF. Should there be a loss of non-ITS site power, or for a mechanical reason, these fans shut down, the HVAC system can be operated in a degraded mode. Since there is less air to exhaust, train A no longer has to exhaust 35,010 cfm. It then becomes possible to maintain delta pressure with two of three HEPA filters. This special case has been added to the fault trees for the failure to maintain delta pressure in the CRCF. In this case, there is redundancy within the train and a common-cause failure mode has been added to the fault tree.

### **B2.2.8 ITS HVAC Testing and Maintenance**

Under normal operations train A continues to operate until a failure is detected or the train is shut down for maintenance. Normal maintenance renders train B unavailable 40 hours per year (the majority of operational-level maintenance can be performed on the operational train and therefore does not affect the overall availability of the standby train). During maintenance, the train B “start/stop/auto/maintenance” switch is placed in the maintenance position. When maintenance is completed, the standby system (train B) is started and operational system (train A) is shut down and is now considered to be the standby train (train A). Maintenance may be scheduled consecutively for this train or at some future date. Under normal operations, maintenance does not result in the loss of/or the inability of the operating train to perform its intended function.

Testing is considered part of routine maintenance. When the maintenance has been completed, maintenance personnel turn on the standby train and check for normal operations including delta pressure, flow rate, and that all failure indicators are reset/off. Maintenance personnel also observe the forced shutdown of the operating system as the standby train is turned on.

Flow rates are monitored as part of testing to ensure that the manual dampers for the active train are in the proper position to achieve a balanced airflow across the three HEPA filters. Once the dampers have been adjusted, they do not require further adjustment unless a damper or combination of dampers must be closed to isolate a component in the train or the entire train.

## **B2.3 DEPENDENCIES AND INTERACTIONS**

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table 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

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
ASD	Flow and pressure sensors	—	—	—	—
	Speed control for fan/motor	—	—	—	—
DP Exhaust Fans	—	Wind speed	—	—	—
Stop/Start/Auto Switch Position	—	—	—	Wrong position	—
Dampers	—	—	—	Wrong position	—
ITS Power	HVAC shuts down	—	—	—	—
Non-ITS Power	—	—	—	—	Supply fans stop
HEPA	—	—	—	Failure to notice leak	—
HVAC Maintenance	—	—	—	Trains can not switch	—
Vestibule Doors	Open only one door at a time	—	—	—	—
Alarm Panel (Non-ITS)	—	—	—	Failure to Respond to HVAC Alarm	—

NOTE: ASD = adjustable speed drive; DP = delta pressure; HEPA = high-efficiency particulate air (filter); HVAC = heating, ventilation, and air-conditioning; ITS = important to safety.

Source: Original

## B2.4 HVAC RELATED FAILURE SCENARIO

### B2.4.1 Failure to Maintain Delta Pressure

#### B2.4.1.1 Description

There is a single failure scenario used in this analysis. The components of the HVAC system used inside buildings to maintain C2 in areas that are normally clean and where airborne contamination is not expected during normal facility operations. The ITS HVAC equipment maintains a positive airflow from outer confinement areas, through the HEPA filters, and into the atmosphere (Ref. B2.1.3).

This model is also applicable to CRCF 2 and 3, RF and WHF with only minor differences that are addressed in these facility specific appendices.

### **B2.4.1.2 Success Criteria**

Success criteria for maintaining delta pressure in the CRCF requires that one of two HVAC trains is operational. The sizing of the exhaust motor and fan assembly maintains the delta pressure in sustained winds of 40 mph with less than 3 second gusts up to 90 mph. In addition, delta pressure is lost for a period of time not to exceed 7 minutes in the CRCF if and only if one of the four vestibule doors is open. These doors are interlocked to ensure only one door is open at a time during normal operations.

Switching between the active and standby trains is controlled by ASD-A (“active train”) which continually monitors the pressure across the exhaust fan and the air flow rate exhausting from the CRCF. These sensors are in a one-of-two configuration which means that the ASD initiates the transfer of operations from the “active train” to the “standby train” when either one of these sensors can not be returned to a normal operating range by the ASD, by controlling, in some combination, the speed of the supply and exhaust fans.

ASD-A must be able to recognize an uncorrectable airflow rate in train A and transmit a signal to ASD-B to start. Having received the start command, ASD-B must send a signal back to ASD-A, commanding a stop.

Maintaining delta pressure during/after the switchover requires the “start/stop/auto or test/maintenance” switch be in the auto position, the train B exhausts fan and motor start, and the airflow across the HEPA filters adjusted by ASD-B to maintain delta pressure.

With the exception of the tornado and backdraft dampers, all control dampers in the ITS HVAC system are manual dampers. These dampers are typically set once for air balancing. These dampers may be adjusted or closed when maintenance is required on the “standby train.” Should the damper setting be changed, it would require the maintenance personnel to return the damper to its proper position to ensure balanced airflow.

### **B2.4.1.3 Design Requirements and Features**

#### **Requirements**

There is only one HVAC train in operation at anytime. The second train is always on standby (exception—when train B is off-line for maintenance).

Alarms are on a panel in the continuously manned central control station and responded to by operators. Alarm conditions are: ASD trouble, fan failure, motor running/stop, and flow rate problem. Operators are not required to respond to the alarm (ITS-HVAC trains are switch automatically); however, operators are expected to notify maintenance that a switch has occurred and maintenance is required to determine the cause of the failure and correct it.

#### **Features**

ITS HVAC system is in normal operation with three, 3 HEPA filter units. Each HEPA filter unit consists of one 3 × 3 medium filter array and two 3 × 3 high-efficiency arrays.

The only difference between the ITS HVAC in the various facilities is the number of non-ITS fans operating in the facility.

## **Testing and Maintenance**

### **Requirements**

HVAC maintenance personnel are notified when an alarm condition exists. Repairs are performed as soon as possible to return train to standby status.

While a HVAC train is undergoing maintenance, the train is not available for service.

Testing that requires the exhaust fan to run is performed on the active HVAC system.

### **Features**

Normal maintenance is performed in accordance with manufacture's recommendations; however, the majority of preventative maintenance do not require shutting down the active system.

#### **B2.4.1.4 Fault Tree Model**

The top event in this fault tree is "Failure to Maintain Delta Pressure" in CRCF . This is defined as the inability of the ITS HVAC system to maintain proper delta pressure within the facility. The ITS HVAC system is a two train system. The configuration of the ITS HVAC systems in these facilities is essentially identical. The only variations are the number of non-ITS supply fans used to stability the airflow within these buildings.

- The fault tree model for the loss of delta pressure in the facility includes those components that have been designated as ITS. There is only one exception and that is the inclusion of two non-ITS supply fans. The fans were added to stabilize air pressure differentials in the facility during normal operations and provide a capability for operating in a degraded mode.
- There are two interlocks in the ITS HVAC system. The first addresses the potential for opening two or more of the entrance/exit vestibule doors. (Note: There is no physical connection between this door interlock and the HVAC system.) The second interlock prevents two HVAC trains from operating at the same time.
- The mission time for the ITS HVAC system is currently set to 720 hours (Ref. B2.1.7). To take into account the differences in failure rates for active and standby systems, all basic events in the standby train are set to half that of the active system. For ease of implementation in SAPHIRE, the rate data is maintained constant and the mission time is set to 1/2 the mission time or 360 hours.

### B2.4.1.5 Basic Event Data

Table B2.4-1 contains a list of basic events used in the loss of delta pressure in the CRCF. The model contains undeveloped transfers to ITS power systems. These failures are addressed in Attachment B3. Reliability data for basic events is detailed in Attachment C with the following exceptions:

- A. Three are associated with human error. HFE detailed analysis is in Section 6.4 and Attachment E:
  - 1. Opening two or more vestibule doors.
  - 2. Failure to properly restore system after maintenance.
  - 3. Failure to notice HEPA filter leak.
- B. Unavailability of the standby train due to scheduled maintenance which is based on a conservative estimate.
- C. Loss of delta pressure as a direct result of opening a vestibule door and the time it takes for the HVAC exhaust fans to re-establish delta pressure.
- D. Two CCFs:
  - 1. CCFs of the HEPA filters in the degraded mode.
  - 2. CCFs of the non-ITS supply fans.

Table B2.4-1. Basic Event Probability for the HVAC Failure to Maintain Delta Pressure in the CRCF

Name	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-EXCESSIVE-WIND-SPEED	1	4.700E-003	4.700E-003	0.000E+000	0.000E+000
060-VCT0-SUPPLY-FAN-CCF	3	1.200E-003	3.760E-006	1.667E-006	0.000E+000
060-VCOO-NITS-PWR-FAILS	3	3.536E-002	1.000E+000	5.000E-005	0.000E+000
060-VCOO-SFAN001-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	0.000E+000
060-VCOO-SFAN002-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	0.000E+000
060-VCTO--B-FAIL-START	1	2.020E-003	2.020E-003	0.000E+000	0.000E+000
060-VCTO-CONTDOORS-OPEN	T	1.000E+000	1.000E+000	0.000E+000	0.000E+000
060-VCTO-DMP000A-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP000B-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP001A-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP001B-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP009I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP009O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP010I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP010O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP011I-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP011O-DMP-FRO	3	6.033E-005	0.000E+000	8.380E-008	0.000E+000
060-VCTO-DMP012I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002

Table B2.4-1. Basic Event Probability for the HVAC Failure to Maintain Delta Pressure in the CRCF (Continued)

Name	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-VCTO-DMP012O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP013I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP013O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP014I-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DMP014O-DMP-FRO	3	3.017E-005	0.000E+000	8.380E-008	3.600E+002
060-VCTO-DR00001-HFI-NOD	1	1.000E-002	1.000E-002	0.000E+000	0.000E+000
060-VCTO-DRS0000-DRS-OPN	1	1.600E-004	1.600E-004	0.000E+000	0.000E+000
060-VCTO-DTC0A-DTC-RUP	3	2.675E-003	0.000E+000	3.720E-006	0.000E+000
060-VCTO-DTC0B-DTC-RUP	3	1.338E-003	0.000E+000	3.720E-006	3.600E+002
060-VCTO-FAN00A-FAN-FTR	3	5.059E-002	0.000E+000	7.210E-005	0.000E+000
060-VCTO-FAN00B-FAN-FTR	3	2.562E-002	0.000E+000	7.210E-005	3.600E+002
060-VCTO-FAN00B-FAN-FTS	1	2.020E-003	2.020E-003	0.000E+000	0.000E+000
060-VCTO-FANA-PRM-FOH	3	3.873E-004	0.000E+000	5.380E-007	0.000E+000
060-VCTO-FANB-PRM-FOH	3	1.937E-004	0.000E+000	5.380E-007	3.600E+002
060-VCTO-FSLAB0-SRF-FOH	3	7.701E-004	0.000E+000	1.070E-006	0.000E+000
060-VCTO-HEPA-CCF	3	7.682E-005	0.000E+000	1.067E-007	7.2000E+02
060-VCTO-HEPA09-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	0.000E+000
060-VCTO-HEPA0A9-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	0.000E+000
060-VCTO-HEPA10-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	0.000E+000
060-VCTO-HEPA11-DMS-FOH	3	6.545E-003	0.000E+000	9.120E-006	0.000E+000
060-VCTO-HEPA12-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
060-VCTO-HEPA13-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
060-VCTO-HEPA14-DMS-FOH	3	3.278E-003	0.000E+000	9.120E-006	3.600E+002
060-VCTO-HEPAA09-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	0.000E+000
060-VCTO-HEPAA09-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	0.000E+000
060-VCTO-HEPAA10-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	0.000E+000
060-VCTO-HEPAA10-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	0.000E+000
060-VCTO-HEPAA11-HEP-LEK	3	2.158E-003	0.000E+000	3.000E-006	0.000E+000
060-VCTO-HEPAA11-HEP-PLG	3	3.070E-003	0.000E+000	4.270E-006	0.000E+000
060-VCTO-HEPAB-CCF	3	3.841E-005	1.000E+000	1.067E-007	3.600E+002
060-VCTO-HEPAB12-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002
060-VCTO-HEPAB12-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
060-VCTO-HEPAB13-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002
060-VCTO-HEPAB13-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
060-VCTO-HEPAB14-HEP-LEK	3	1.079E-003	0.000E+000	3.000E-006	3.600E+002
060-VCTO-HEPAB14-HEP-PLG	3	1.536E-003	0.000E+000	4.270E-006	3.600E+002
060-VCTO-HEPALK-HFI-NOD	1	1.000E+000	1.000E+000	0.000E+000	0.000E+000
060-VCTO-HFIA000-HFI-NOM	1	1.000E-001	1.000E-001	0.000E+000	0.000E+000
060-VCTO-IEL0001-IEL-FOD	1	2.750E-005	2.750E-005	0.000E+000	0.000E+000
060-VCTO-PDSLA0B-SRP-FOD	1	3.990E-003	3.990E-003	0.000E+000	0.000E+000

Table B2.4-1. Basic Event Probability for the HVAC Failure to Maintain Delta Pressure in the CRCF (Continued)

Name	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-VCTO-TDMP00A-DTM-FOD	1	8.710E-004	8.710E-004	0.000E+000	0.000E+000
060-VCTO-TDMP00B-DTM-FOD	1	8.710E-004	8.710E-004	0.000E+000	3.600E+002
060-VCTO-TDMP00B-DTM-FOH	3	8.103E-003	0.000E+000	2.260E-005	3.600E+002
060-VCTO-TRAINB-MAINT	1	4.570E-003	4.570E-003	0.000E+000	0.000E+000
060-VCTO-UDMP000-UDM-FOH	3	8.103E-003	0.000E+000	2.260E-005	3.600E+002

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time

Calc. = calculation; CRCF = Canister Receipt and Closure Facility; DP = delta pressure; Fail. = failure; Miss. = mission; P = pressure; Prob. = probability.

Source: Original

### B2.4.1.5.1 Human Failure Events

There are three basic human failure events (HFE) associated with human error listed in Table B2.4-2. They are for inadvertently opening two or more vestibule doors at the same time, failure to notice that there is a HEPA leak and leaving the start/stop/auto switch on the standby train in the wrong position.

Table B2.4-2. Human Failure Events

Basic Event Name	Basic Event Description
060-VCTO-DR00001-HFI-NOD	Operators open 2 or more vestibule doors in CRCF
060-VCTO-HEPALK-HFI-NOD	Operator fails to notice HEPA filter leak in Train A (or Train B)
060-VCTO-HFIA000-HFI-NOM	Human error exhaust fan switch wrong position

NOTE: CRCF = Canister Receipt and Closure Facility; HEPA = high-efficiency particulate air (filter)

Source: Original

### B2.4.1.5.2 Common-Cause Failures

There are three common-cause failures (CCFs) identified in the HVAC model. Two of the CCFs are associated with the potential of a HEPA filter failure in the degraded mode for HEPA filters in the degraded mode where there is a two-of-three success situation. An alpha factor of 0.025 is used (Table C3-1, CCCG=3). The third common-cause is applied to the non-ITS supply fans where success is one-of-two in the degraded mode of operation. An alpha factor of 0.0235 is used (Table C3-1, CCCG=2).

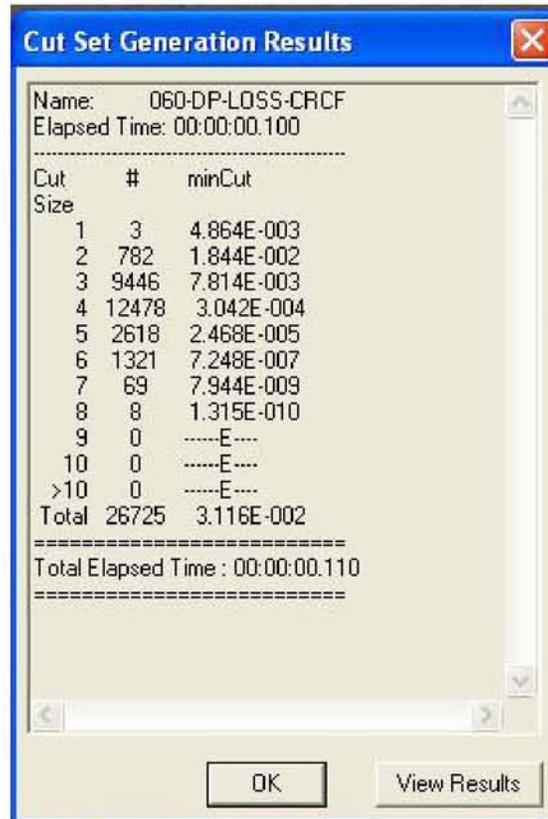
### B2.4.1.6 Uncertainty and Cut Set Generation

Figure B2.4-1 contains the uncertainty results obtained from running the fault trees for “Failure to Maintain Delta Pressure” using a cutoff probability of 1E-12. Figure B2.4-2 provides the cut set generation results for the “Failure to Maintain Delta Pressure” fault tree. These results are for the HVAC system coupled with loss of electrical power, which is discussed separately in Section B3. If loss of electrical power is not included in the HVAC tree, the mean failure probability and standard deviation of the HVAC system alone is 3.3E-02 and 9.3E-02.

Uncertainty Results	
Name	060-DP-LOSS-CRCF
Random Seed	1234
Events	180
Sample Size	10000
Cut Sets	26725
Point estimate	3.116E-002
Mean Value	3.470E-002
5th Percentile Value	4.594E-003
Median Value	1.448E-002
95th Percentile Value	9.814E-002
Minimum Sample Value	1.245E-003
Maximum Sample Value	1.000E+000
Standard Deviation	9.386E-002
Skewness	7.465E+000
Kurtosis	6.576E+001
Elapsed Time	00:00:35.660
OK	

Source: Original

Figure B2.4-1. Uncertainty Results of the CRCF Failure to Maintain Delta Pressure Fault Tree



Source: Original

Figure B2.4-2. Cut Set Generation Results for the CRCF Failure to Maintain Delta Pressure Fault Tree

### B2.4.1.7 Cut Sets

Table B2.4-3 contains the top 35 cut sets for the “Failure to Maintain Delta Pressure” fault tree.

### B2.4.1.8 HVAC Fault Trees

For purposes of this report, the transfers to the ITS electrical system for the HVAC equipment is ignored. For specifics on the electrical system, refer to the “AC Power System Fault Tree Analysis” in Attachment B3.

Table B2.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure in the CRCF

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
060-DP- LOSS-CRCF	16.23	5.059E-003	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	15.08	4.700E-003	060-EXCESSIVE-WIND-SPEED	Sustained Wind Exceeds 40 MPH & Gust to 90 MPH	4.7E-003
	5.69	1.772E-003	LOSP	Loss of offsite power	3.0E-003
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.7E-001
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.7E-001
	4.16	1.296E-003	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
	2.10	6.545E-004	060-VCTO-HEPA09-DMS-FOH	Moisture Separator/Demister HEPA 09 Fails	6.5E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	2.10	6.545E-004	060-VCTO-HEPA10-DMS-FOH	Moisture Separator/Demister HEPA 10 Fails	6.5E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	2.10	6.545E-004	060-VCTO-HEPA11-DMS-FOH	Moisture Separator/Demister HEPA 11 Fails	6.5E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.73	5.378E-004	060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	5.4E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.32	4.099E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-TDMP00B-DTM-FOH	Tornado damper Train B Fails	8.1E-003
	1.32	4.099E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-UDMP000-UDM-FOH	Backdraft Damper for Train B exhaust Fails	8.1E-003
	1.22	3.816E-004	060-#EEE-LDCNTRA-C52-SPO	Load Center A Feed Circuit Breaker (AC) Spurious Operation	3.8E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	1.22	3.816E-004	060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 Feed Breaker Spurious Operation	3.8E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.99	3.070E-004	060-VCTO-HEPAA09-HEP-PLG	HEPA #A09 Train A Plugged	3.1E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.99	3.070E-004	060-VCTO-HEPAA10-HEP-PLG	HEPA #A10 Train A Plugged	3.1E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001

B2-15

March 2008

Table B2.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
	0.99	3.070E-004	060-VCTO-HEPAA11-HEP-PLG	HEPA #A11 Train A Plugged	3.1E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.94	2.938E-004	060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.7E-001
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.8E-003
	0.94	2.938E-004	060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.7E-001
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.8E-003
	0.87	2.721E-004	060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 Failure	5.4E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
	0.86	2.675E-004	060-VCTO-DTC0A-DTC-RUP	Duct Fails between HEPA and Exhaust Fan (10 feet)	2.7E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.85	2.646E-004	060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
			26D-#EEESWGRDGA-AHU-FTR	13.8 kV ITS Switchgear room Air Handling Unit Fails	2.6E-003
	0.82	2.559E-004	060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	5.1E-002
			060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	5.1E-002
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.74	2.312E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-TRAINB-MAINT	Train B HVAC is Off-Line for Maintenance	4.6E-003
	0.74	2.302E-004	LOSP	Loss of offsite power	3.0E-003
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
			26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.7E-001
	0.69	2.158E-004	060-VCTO-HEPA0A9-HEP-LEK	HEPA #09 Train A Leaks	2.2E-003
			060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.69	2.158E-004	060-VCTO-HEPAA10-HEP-LEK	HEPA #10 Train A Leaks	2.2E-003
			060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001
	0.69	2.158E-004	060-VCTO-HEPAA11-HEP-LEK	HEPA #11 Train A Leaks	2.2E-003
			060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0E+000
			060-VCTO-HFIA000-HFI-NOM	Human Error Exhaust Fan Switch Wrong Position	1.0E-001

B2-16

March 2008

Table B2.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
	0.62	1.930E-004	060-#EEE-LDCNTRB-C52-SPO	CRCF ITS Load Center Circuit Breaker (AC) Spur Op	3.8E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
	0.62	1.930E-004	060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 Feed Breaker Spurious Operation	3.8E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
	0.54	1.677E-004	060-VCTO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			060-VCTO-HEPA09-DMS-FOH	Moisture Separator/Demister HEPA 09 Fails	6.5E-003
	0.54	1.677E-004	060-VCTO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			060-VCTO-HEPA10-DMS-FOH	Moisture Separator/Demister HEPA 10 Fails	6.5E-003
	0.54	1.677E-004	060-VCTO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
			060-VCTO-HEPA11-DMS-FOH	Moisture Separator/Demister HEPA 11 Fails	6.5E-003
	0.53	1.658E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-HEPA12-DMS-FOH	Moisture Separator/Demister HEPA 12 Fails	3.3E-003
	0.53	1.658E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-HEPA13-DMS-FOH	Moisture Separator/Demister HEPA 13 Fails	3.3E-003
	0.53	1.658E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-HEPA14-DMS-FOH	Moisture Separator/Demister HEPA 14 Fails	3.3E-003
	0.51	1.600E-004	060-VCTO-DRS0000-DRS-OPN	Vestibule Door Open During Receipt/Export	1.6E-004
	0.48	1.486E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.7E-001
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.8E-003
	0.48	1.486E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.7E-001
			27A-#EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.8E-003
	0.44	1.378E-004	060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	5.4E-003
			060-VCTO-FAN00B-FAN-FTR	Exhaust Fan in Train B Fails	2.6E-002
	0.43	1.339E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			26D-#EEE-SWGRDGB-AHU-FTR	EDGF Switchgear Room Air Handling Unit Failure to Run	2.6E-003
	0.42	1.295E-004	060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	5.1E-002
			060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh. Fan 8 Fails to Run	5.1E-002
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002

B2-17

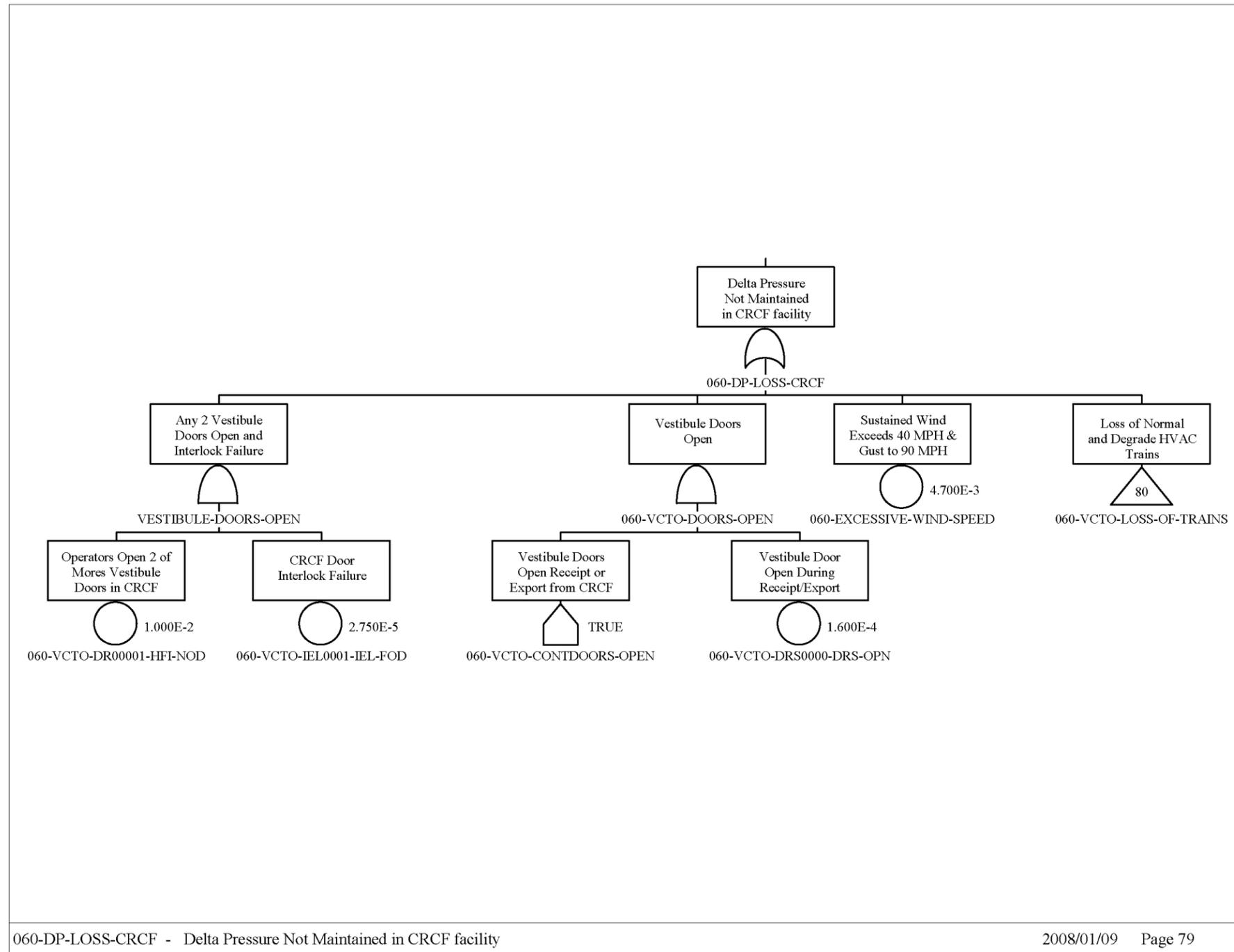
March 2008

Table B2.4-3. Dominant Cut Sets for the Failure to Maintain Delta Pressure in the CRCF (Continued)

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
	0.37	1.164E-004	LOSP	Loss of offsite power	3.0E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.7E-001
	0.33	1.022E-004	060-VCTO--B-FAIL-START	Train B Fails to Start	2.0E-003
			060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
	0.33	1.022E-004	060-VCTO-FAN00A-FAN-FTR	Exhaust Fan in Train A Fails	5.1E-002
			060-VCTO-FAN00B-FAN-FTS	Exhaust Fan in Train B Fails to Start	2.0E-003
		3.116E-002	= Total		

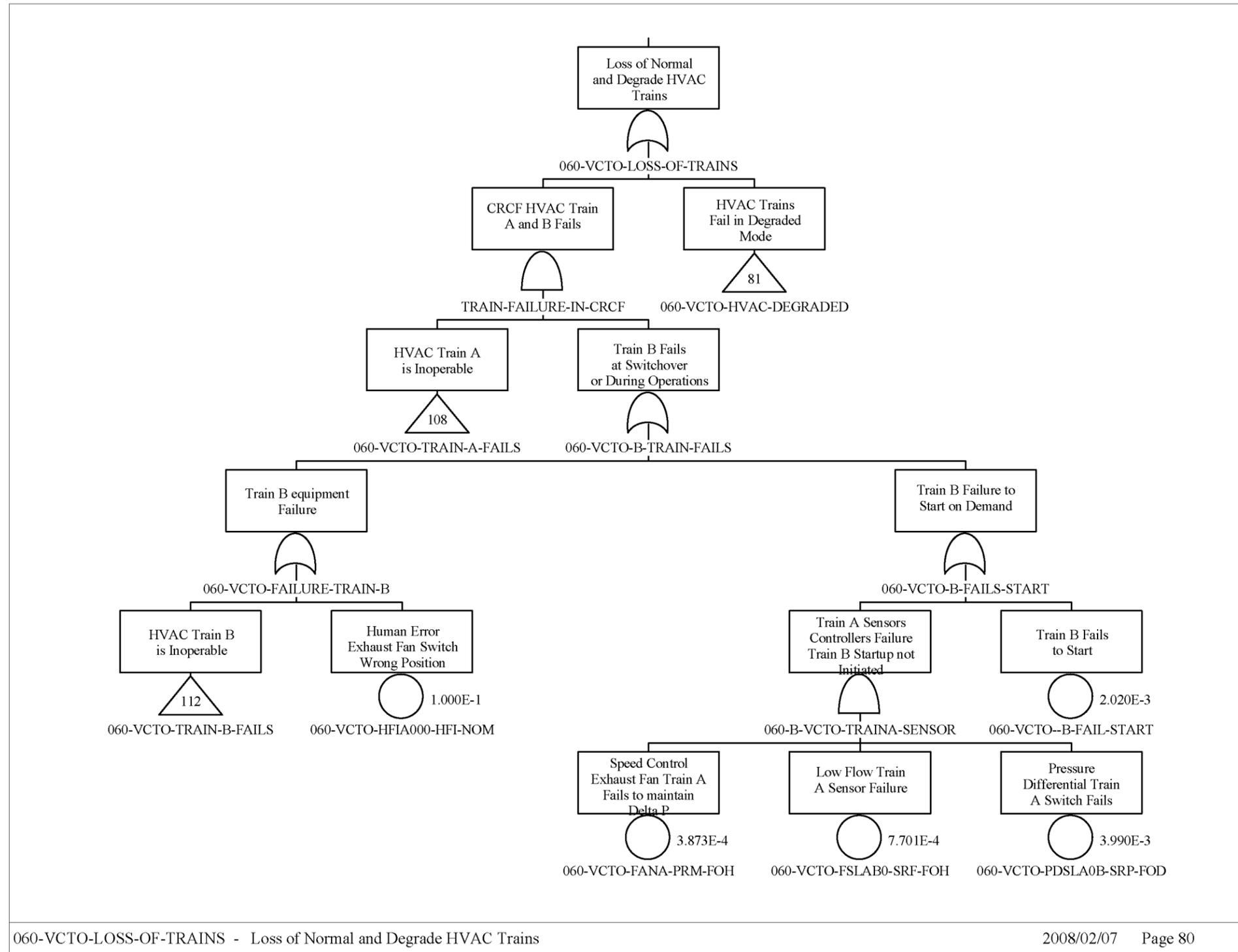
NOTE: AC = alternating current; CRCF = canister receipt and closure facility; DG = diesel generator; Elec = electrical; Exh = exhaust; Freq. = frequency; HEPA = high efficiency particulate air; ITS = important-to-safety; MCC = motor control center; Prob. = probability; SWGR = switchgear

Source: Original



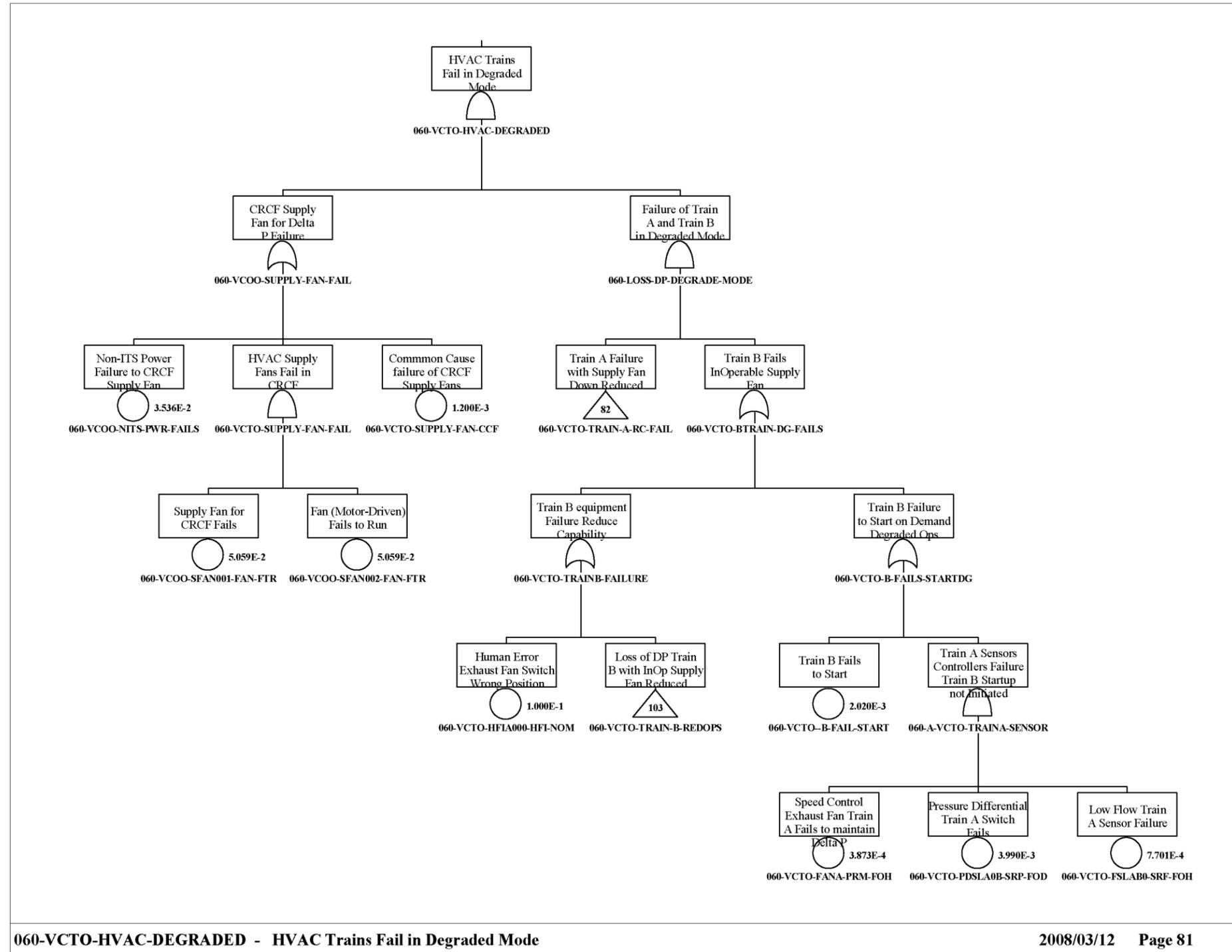
Source: Original

Figure B2.4-3. Delta Pressure not Maintained in CRCF Facility



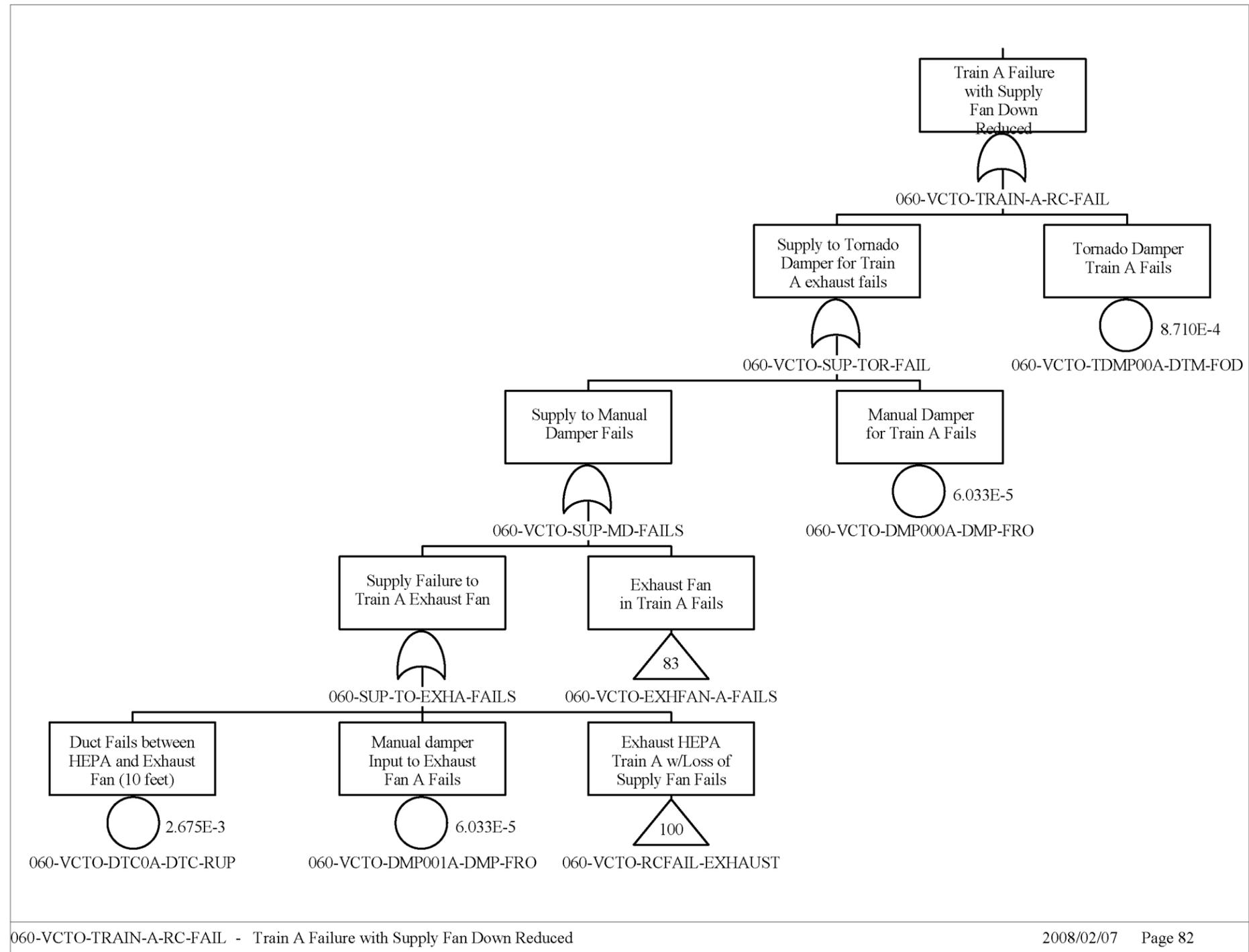
Source: Original

Figure B2.4-4. Loss of Normal and Degrade HVAC Trains



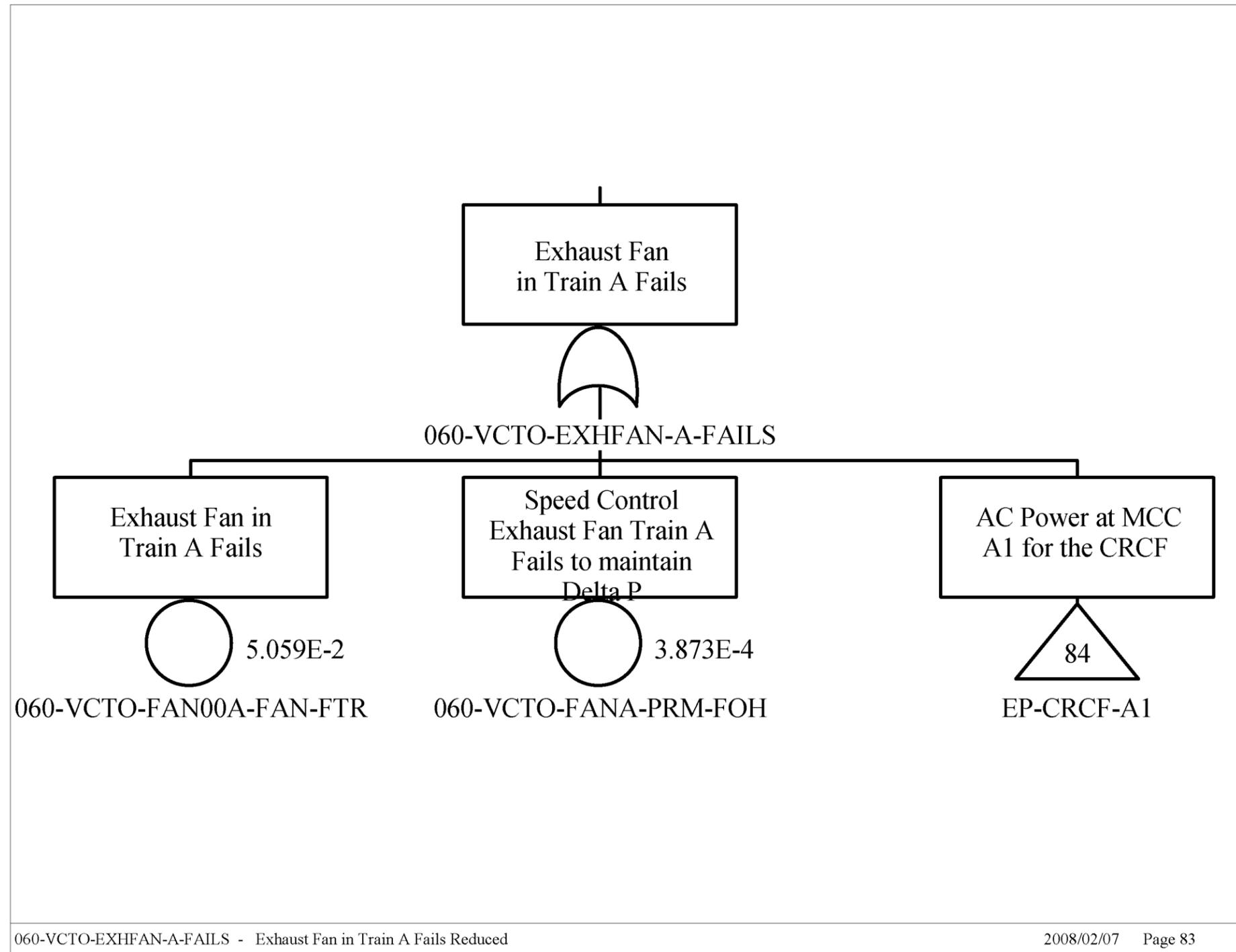
Source: Original

Figure B2.4-5. HVAC Trains Fail in Degraded Mode



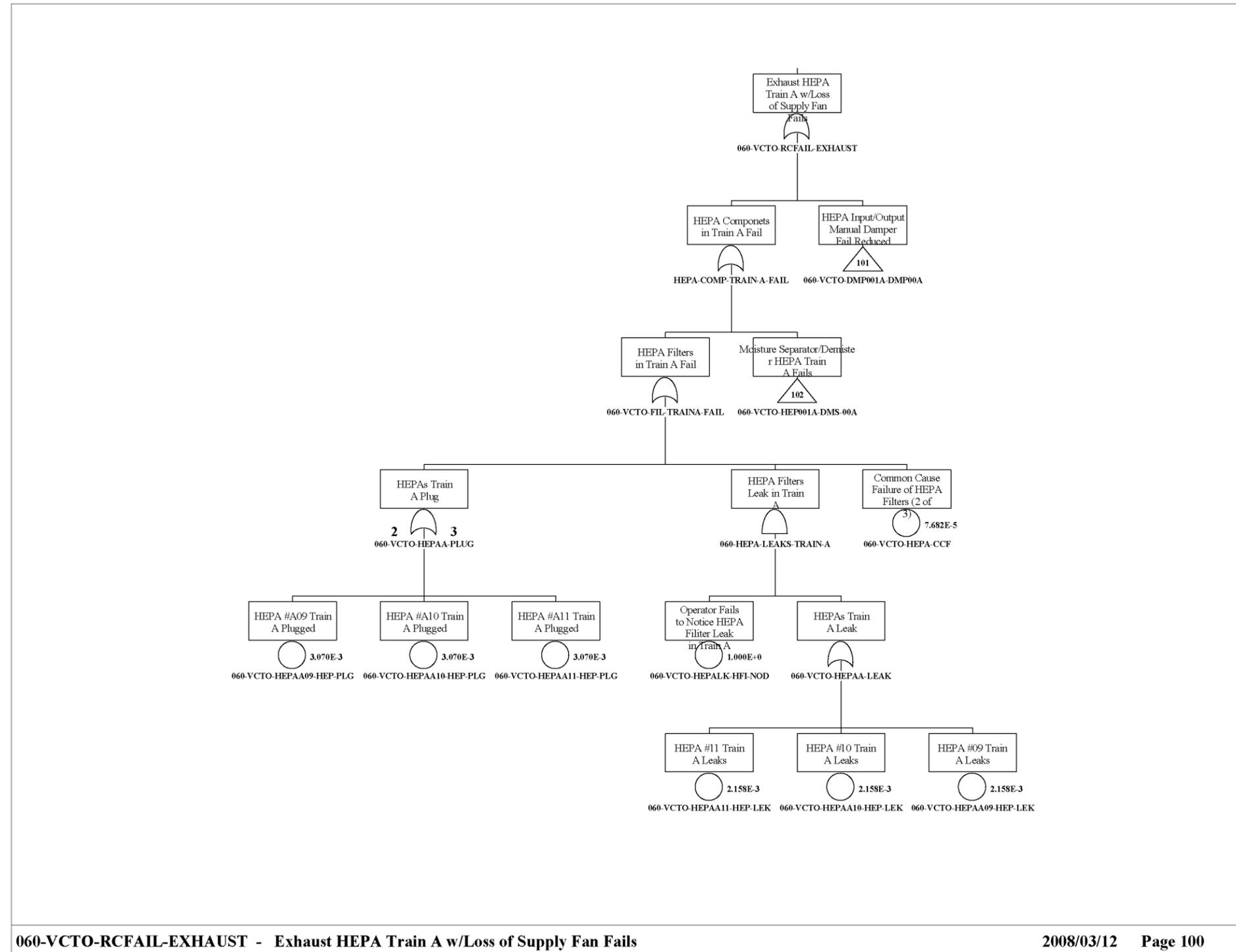
Source: Original

Figure B2.4-6. Train A Failure with Supply Fan Down Reduced



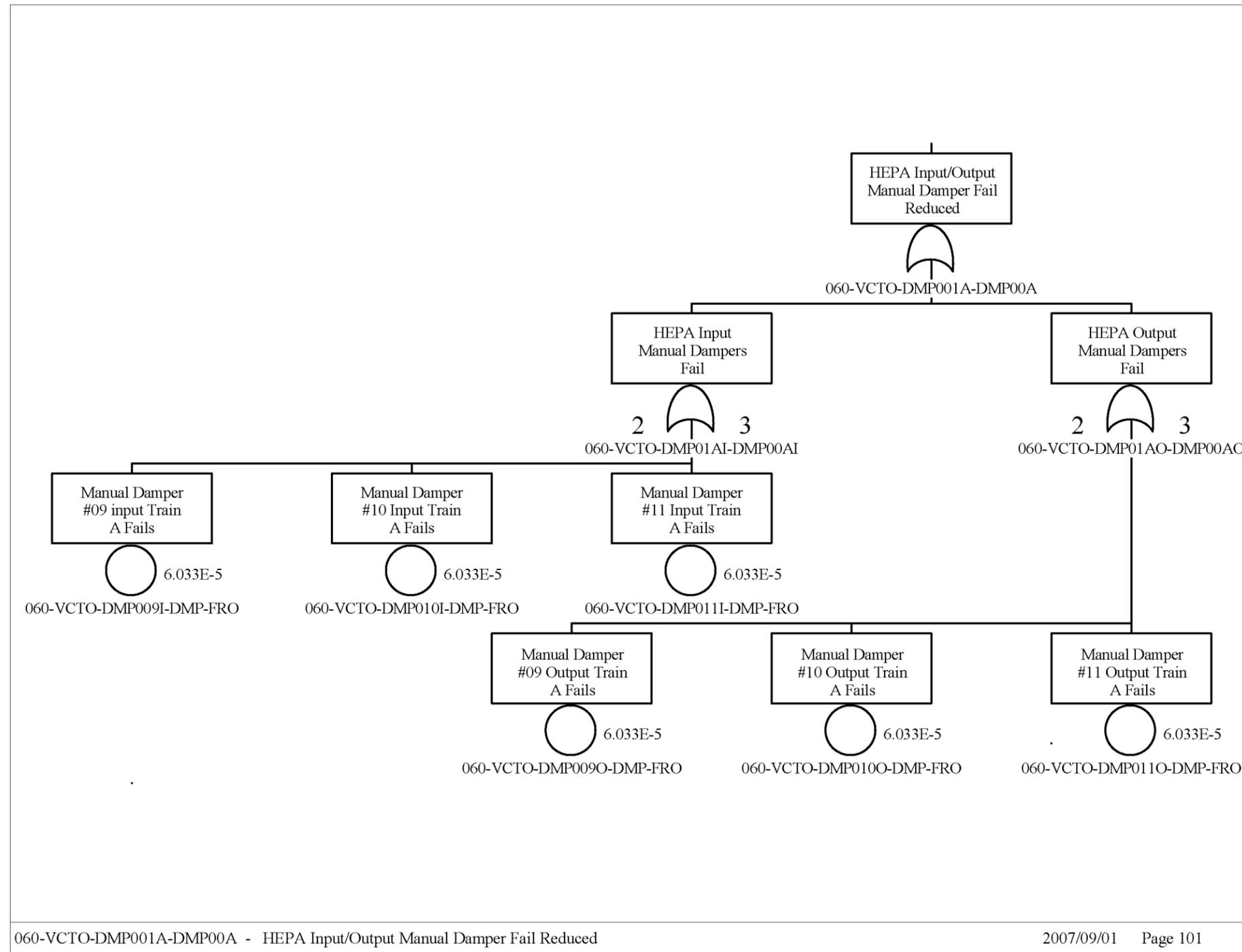
Source: Original

Figure B2.4-7. Exhaust Fan in Train A Fails Reduced



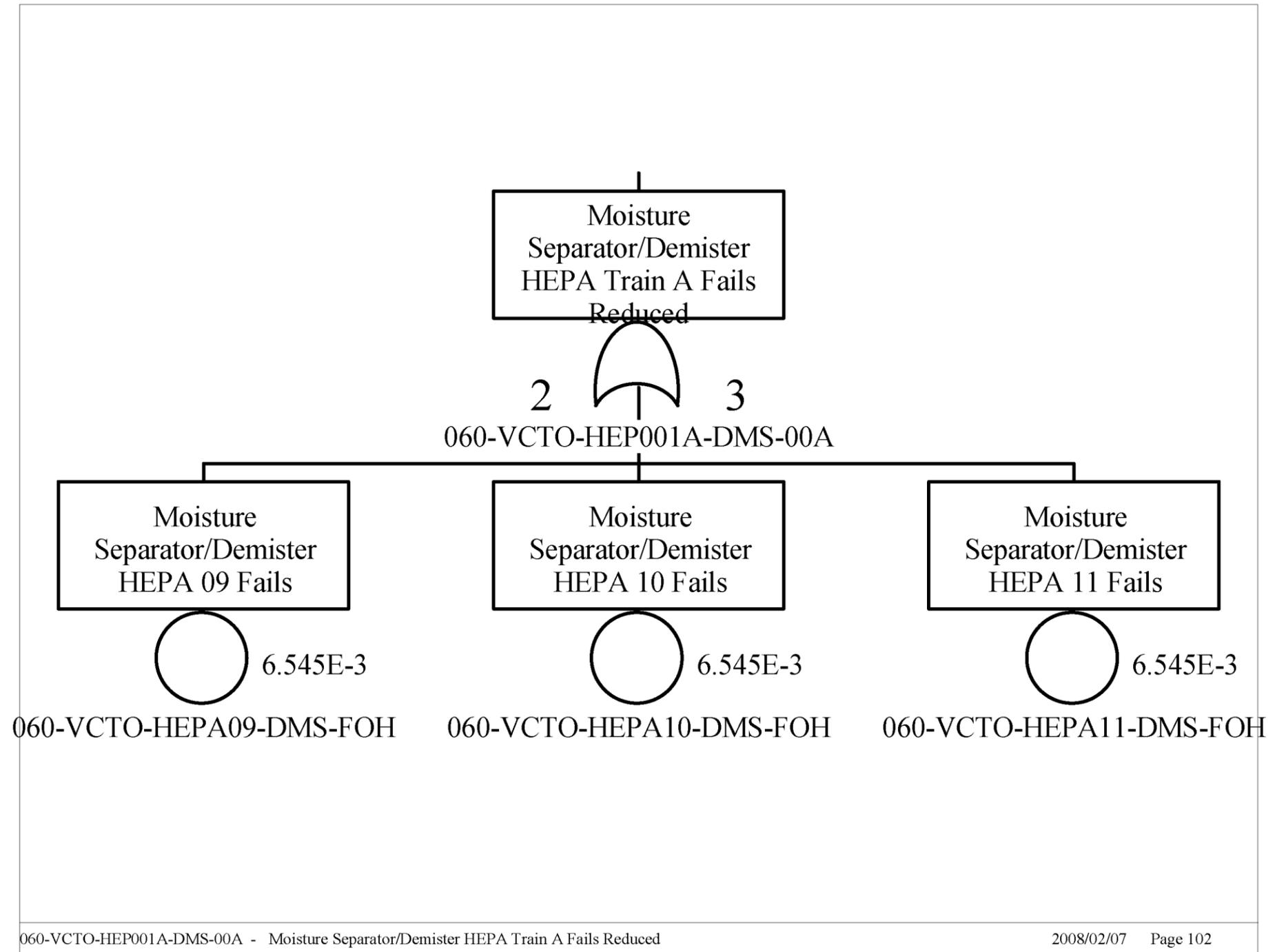
Source: Original

Figure B2.4-8. Exhaust HEPA Train A with Loss of Supply Fan Fails



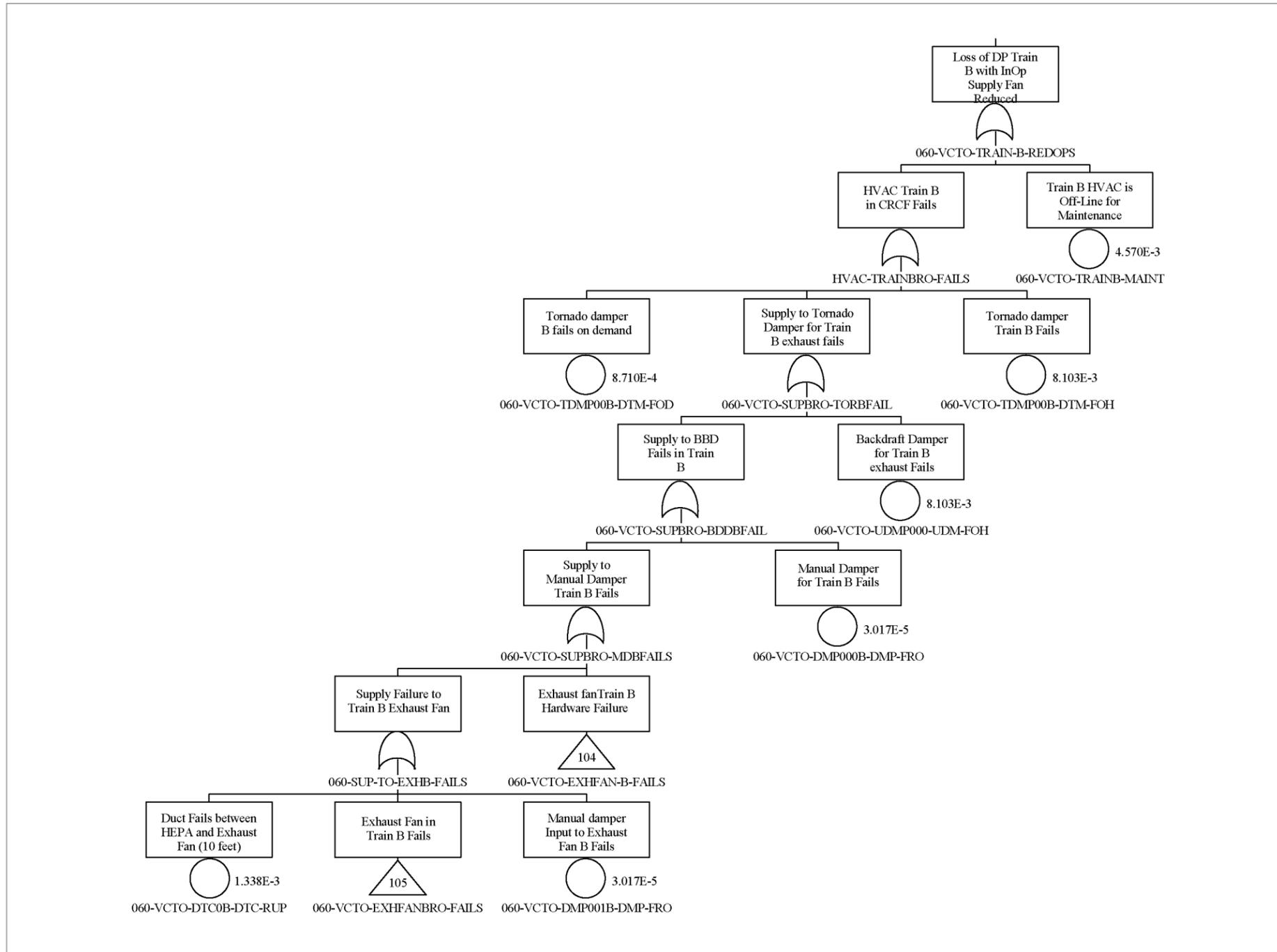
Source: Original

Figure B2.4-9. HEPA Input/Output Manual Damper Fail Reduced



Source: Original

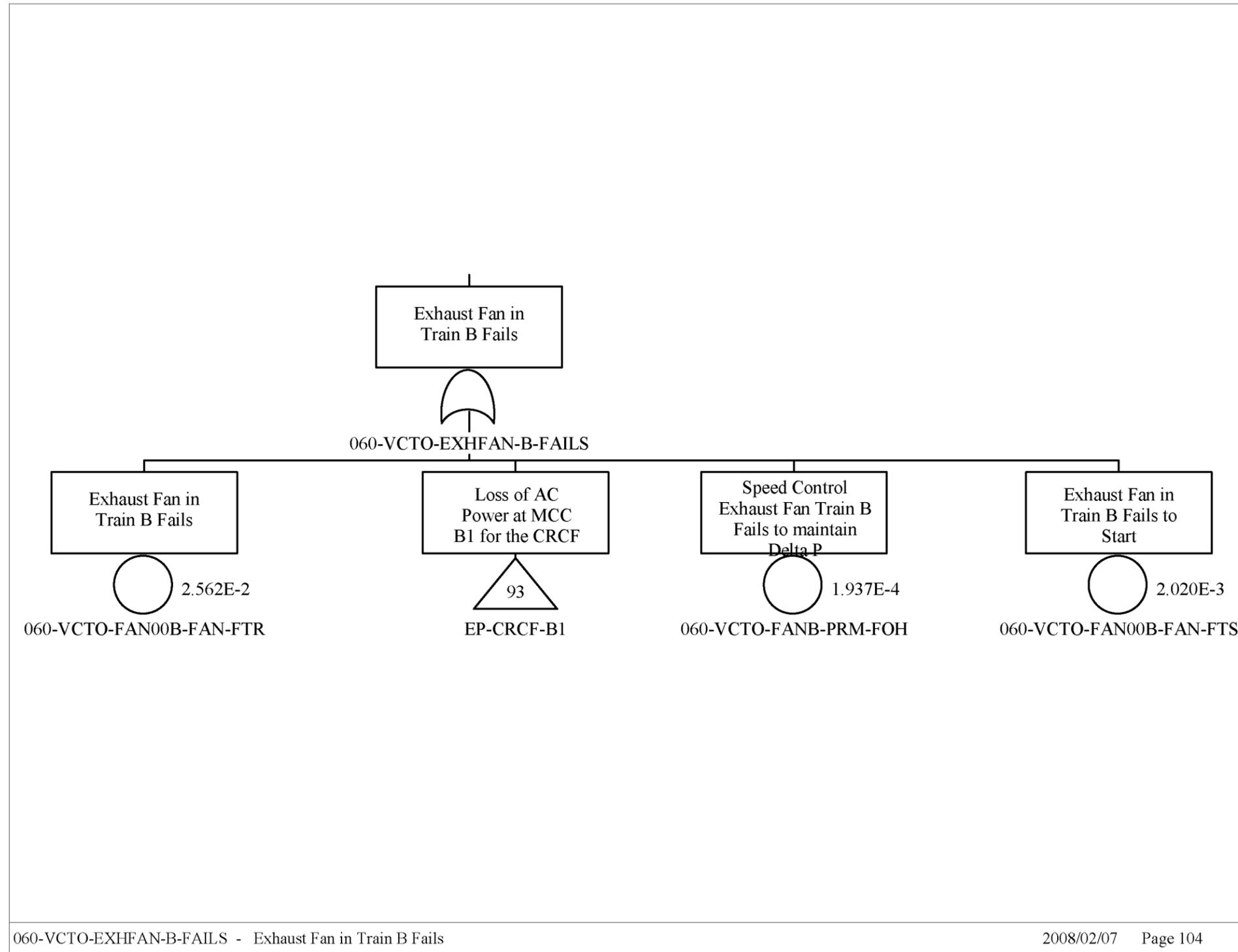
Figure B2.4-10. Moisture Separator/Demister HEPA Train A Fails Reduced



060-VCTO-TRAIN-B-REDOPS - Loss of DP Train B with InOp Supply Fan Reduced

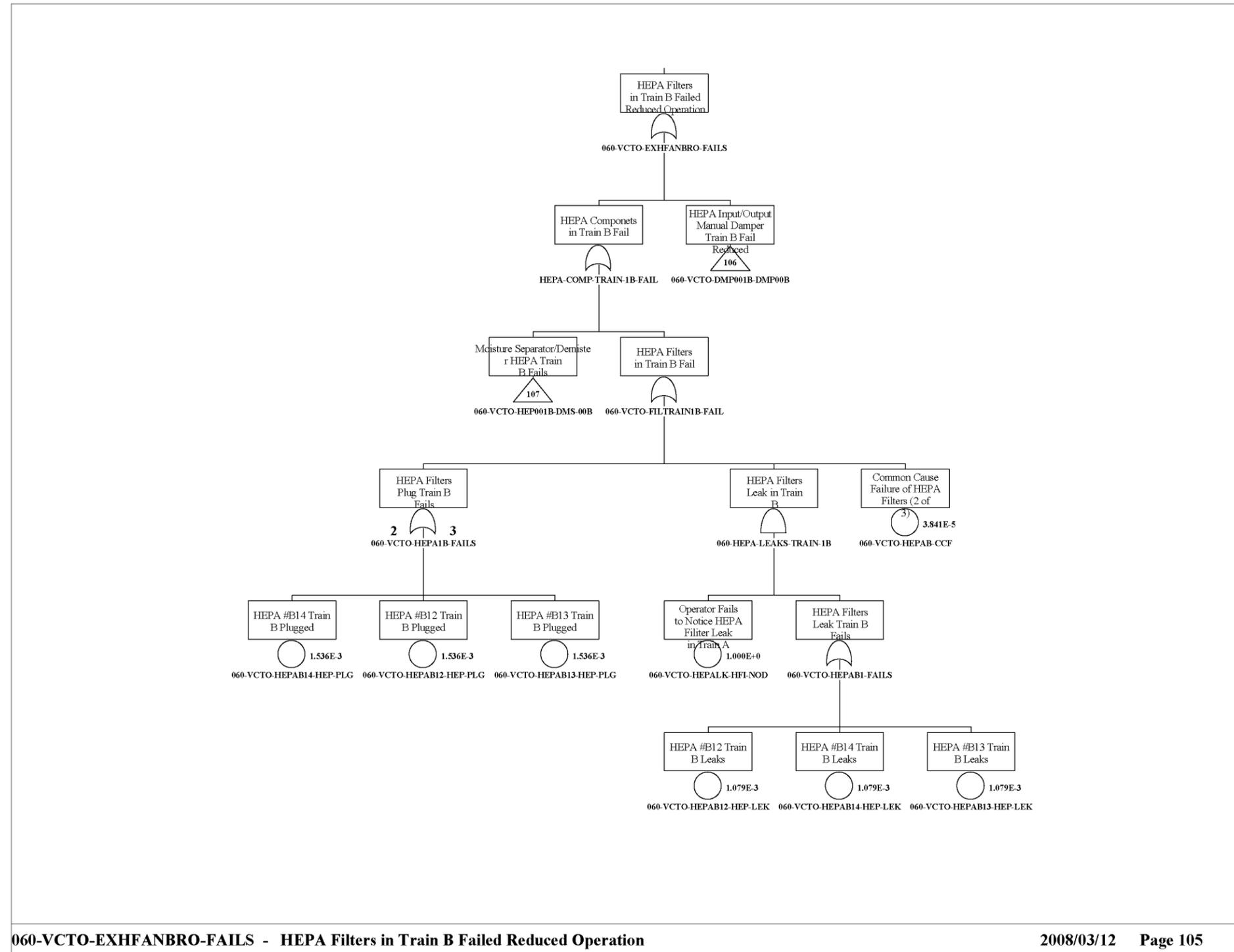
Source: Original

Figure B2.4-11. Loss of Delta Pressure Train B with Inoperative Supply Fan Reduced



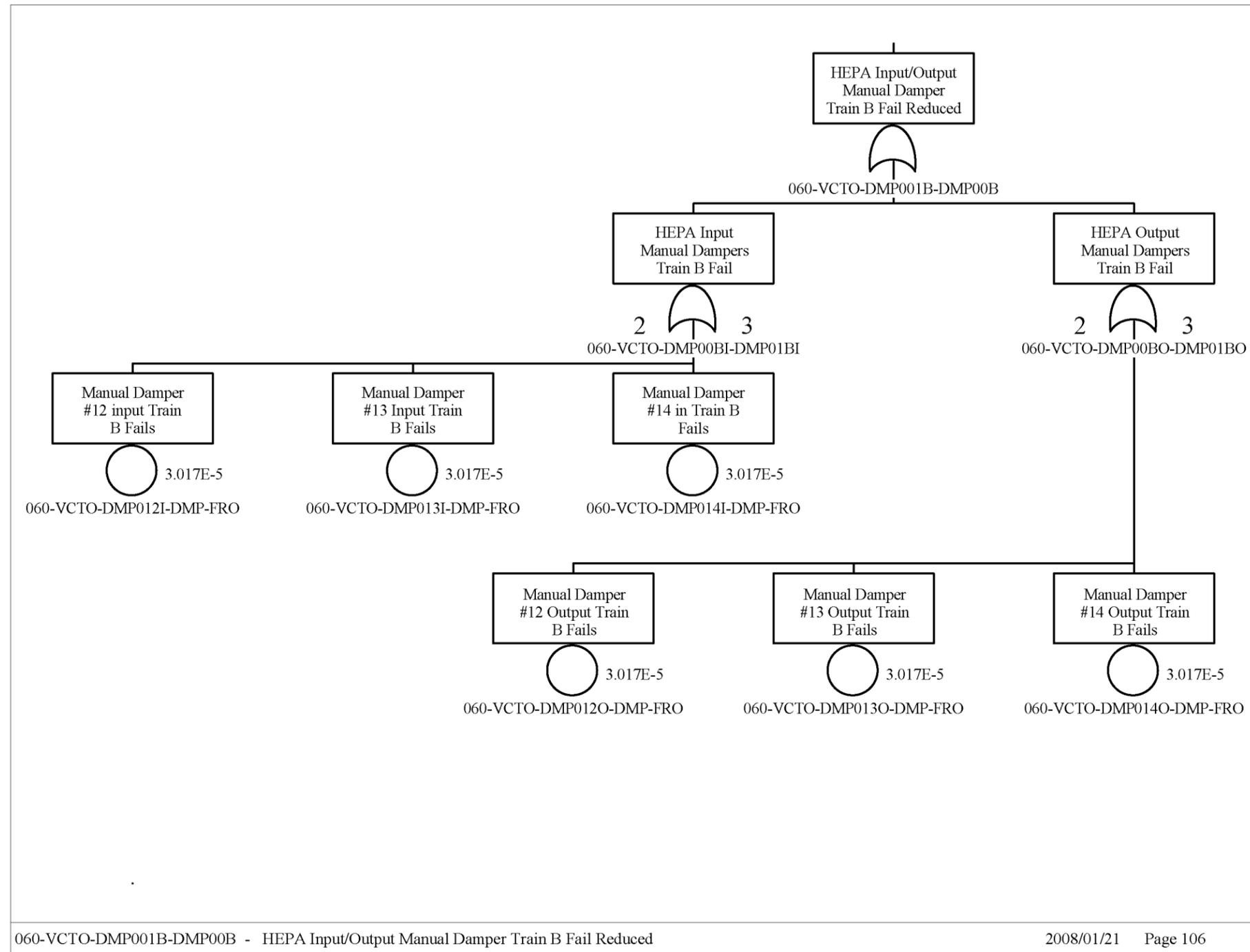
Source: Original

Figure B2.4-12. Exhaust Fan in Train B Fails



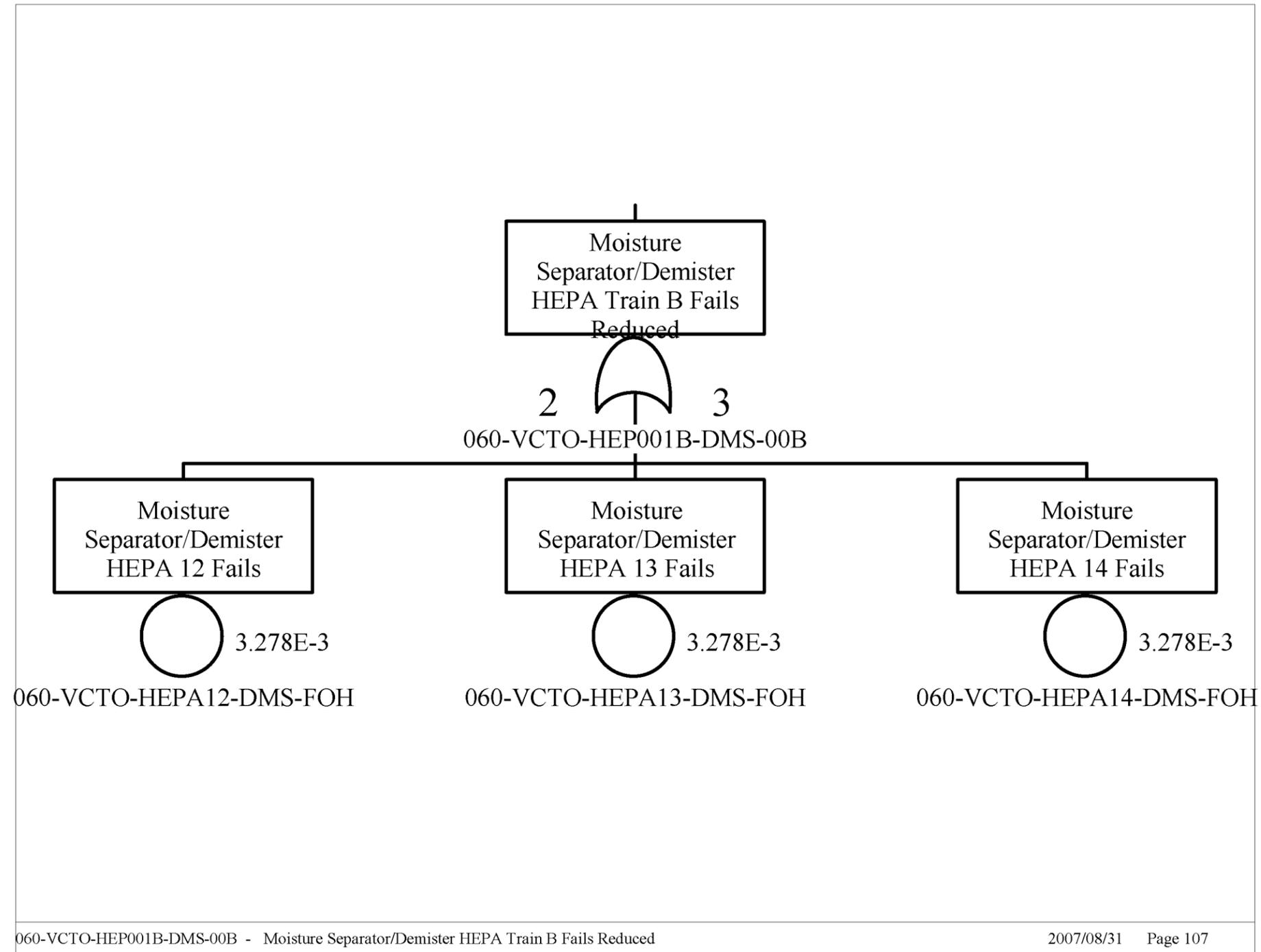
Source: Original

Figure B2.4-13. HEPA Filters in Train B Failed Reduced Operation



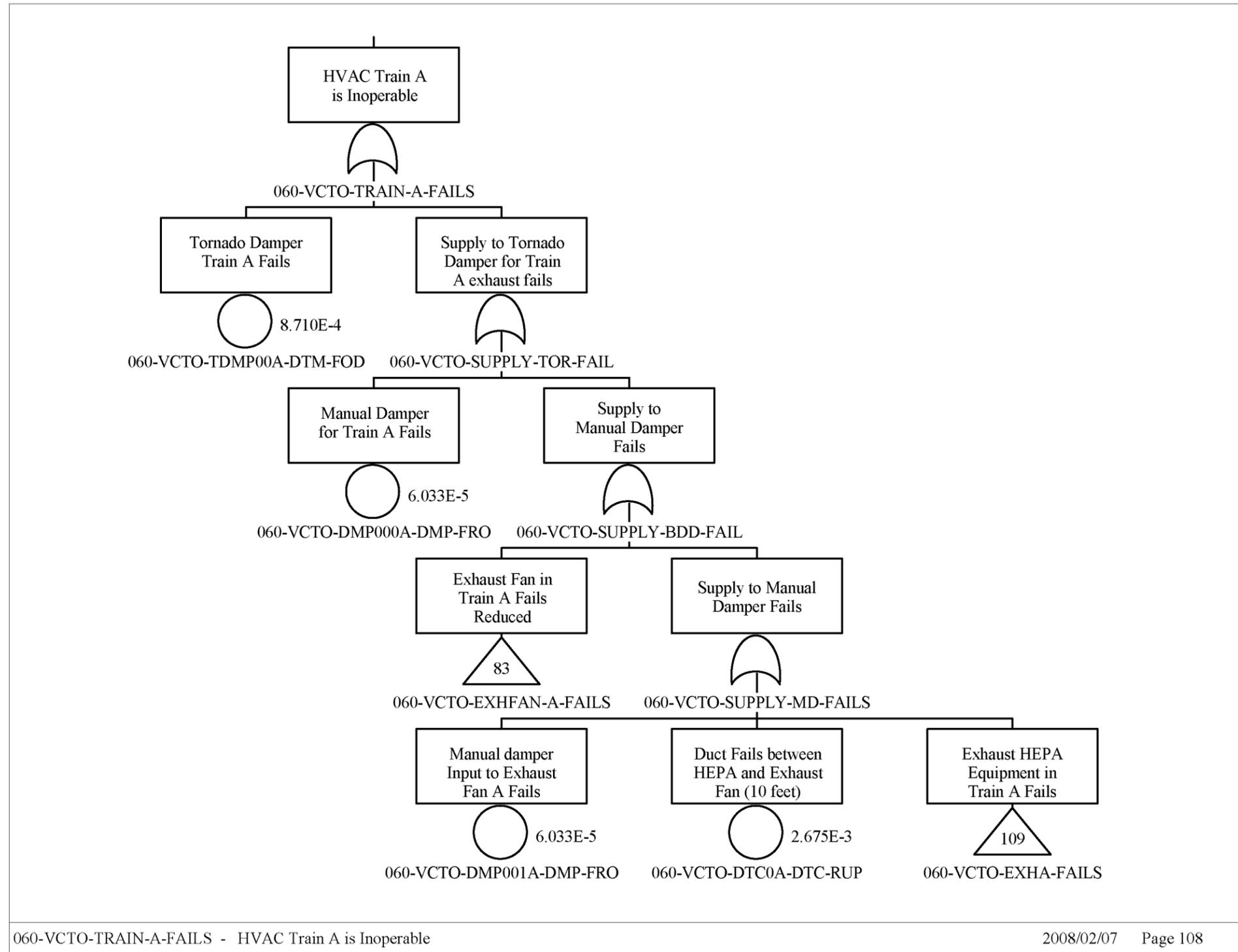
Source: Original

Figure B2.4-14. HEPA Input/Output Manual  
Damper Train B Fail Reduced



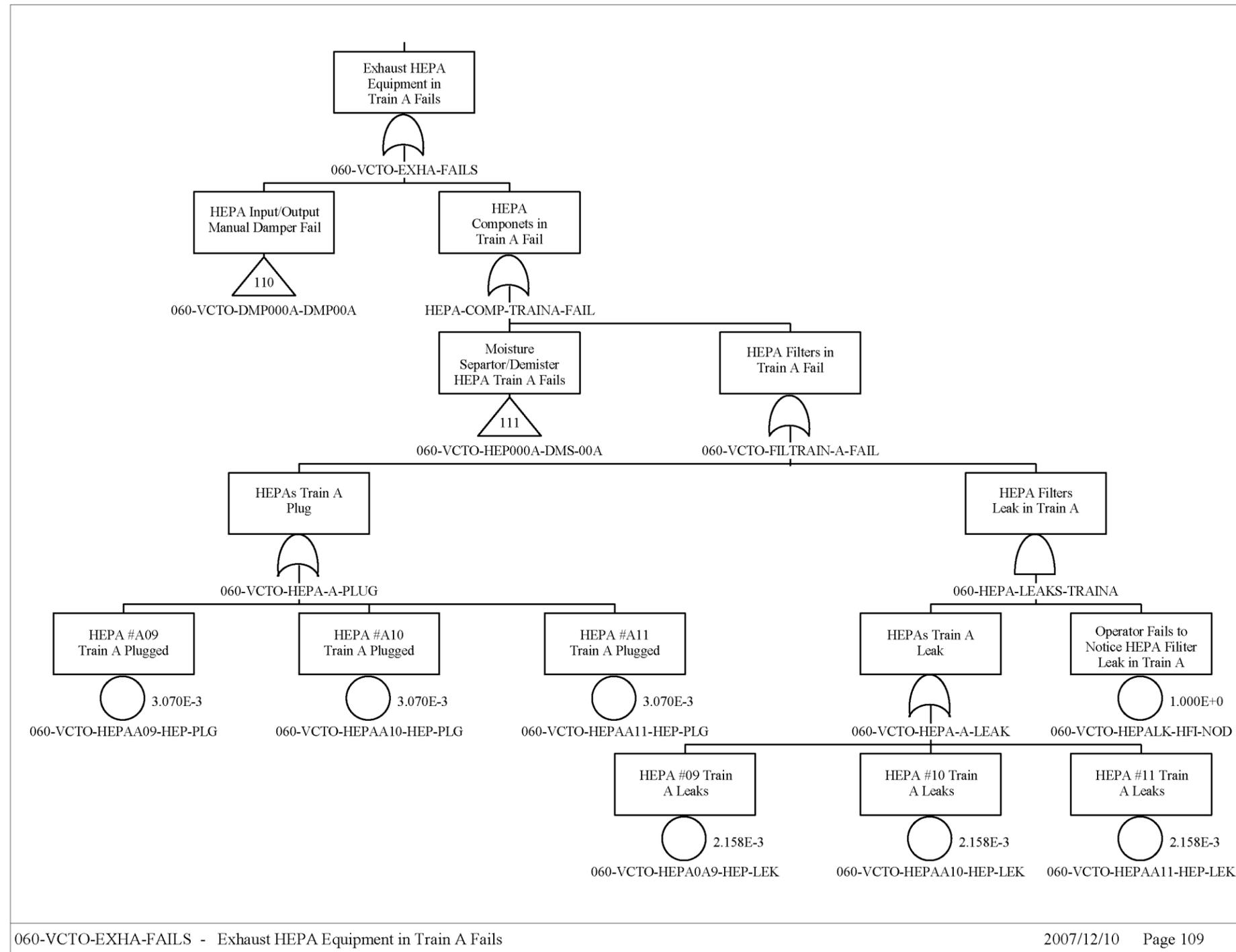
Source: Original

Figure B2.4-15. HEPA Input/Output Manual Damper Train B Fail Reduced



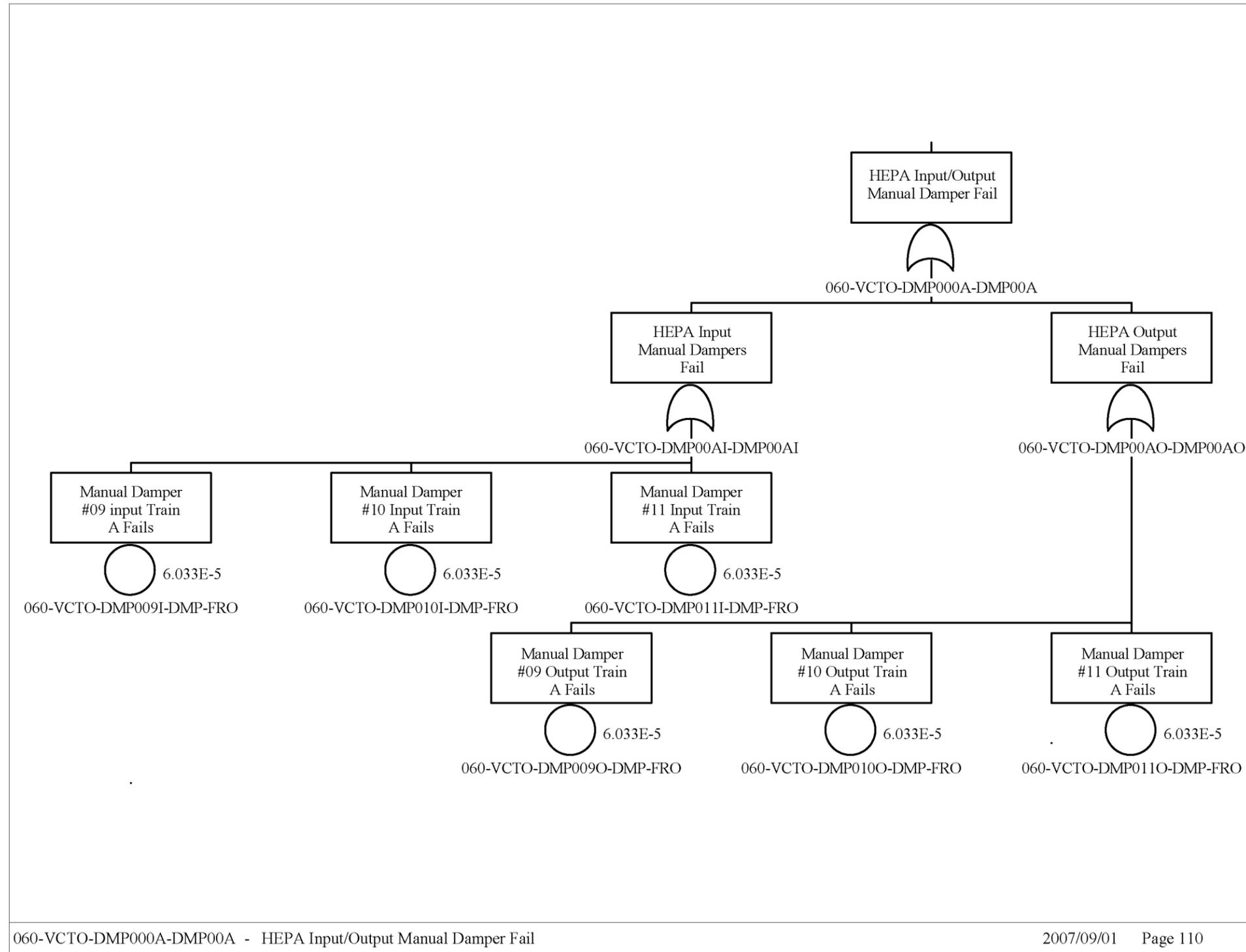
Source: Original

Figure B2.4-16. HVAC Train A is Inoperable



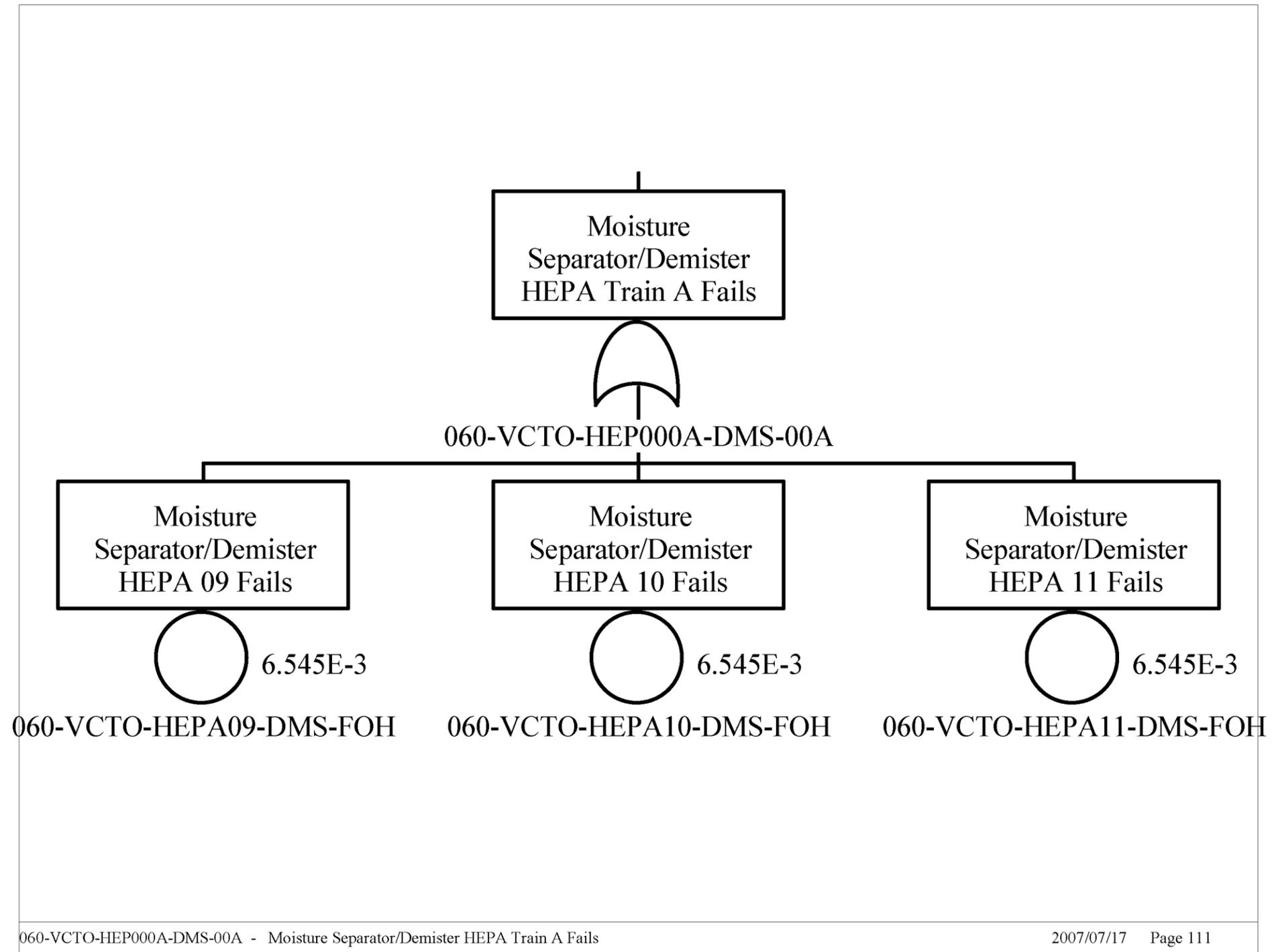
Source: Original

Figure B2.4-17. Exhaust HEPA Equipment in Train A Fails



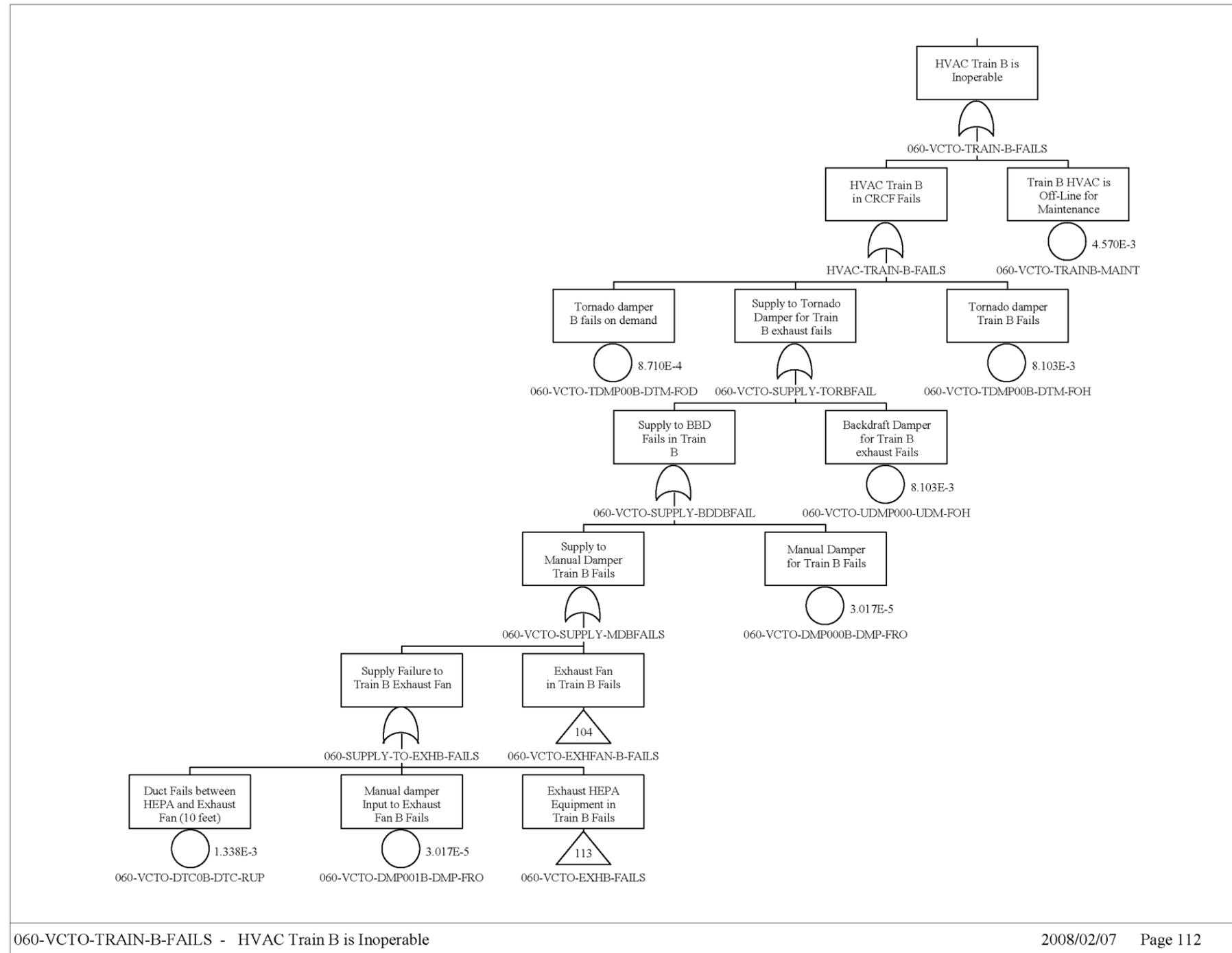
Source: Original

Figure B2.4-18. HEPA Input/Output Manual Damper Fail



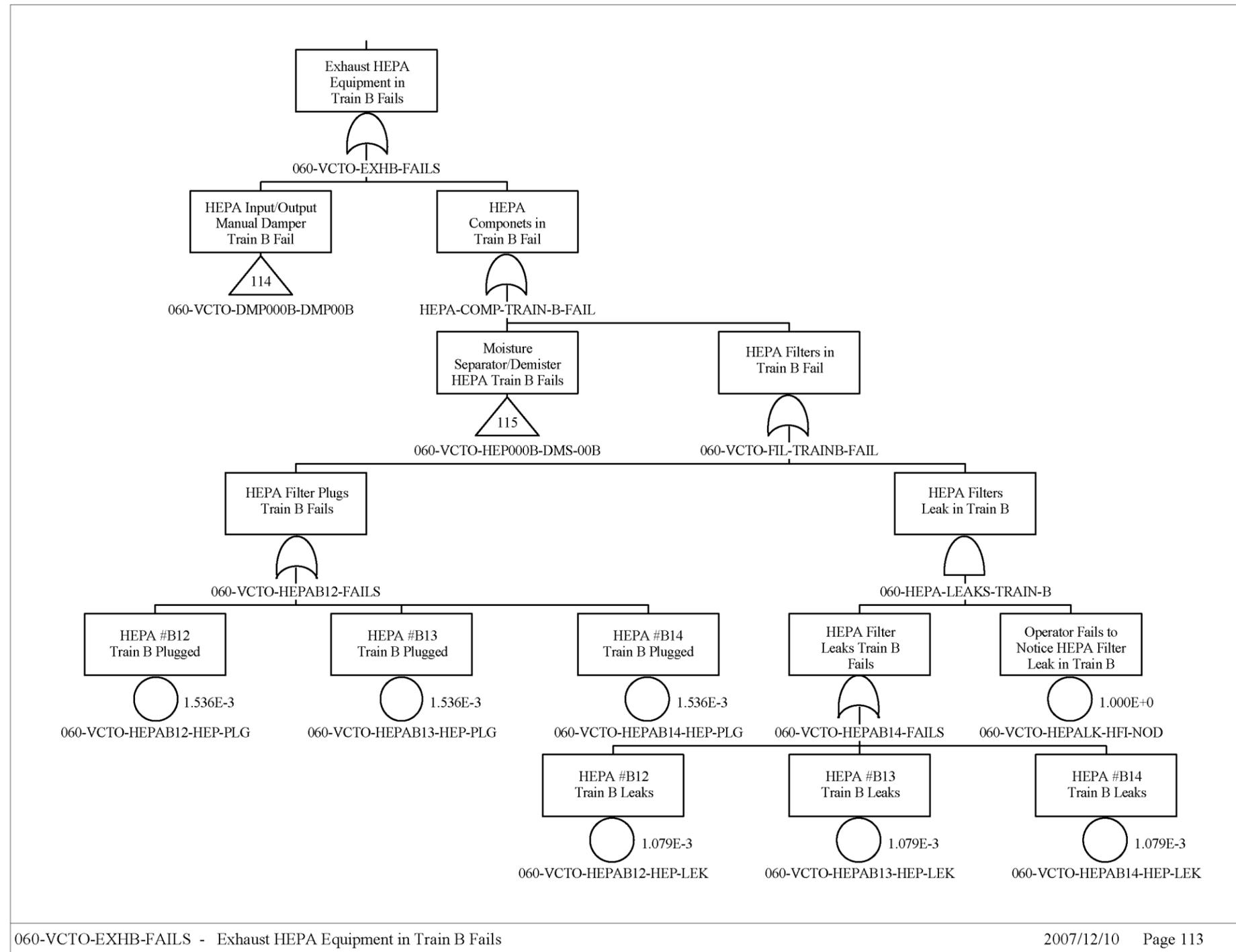
Source: Original

Figure B2.4-19. Moisture Separator/Demister HEPA Train A Fails



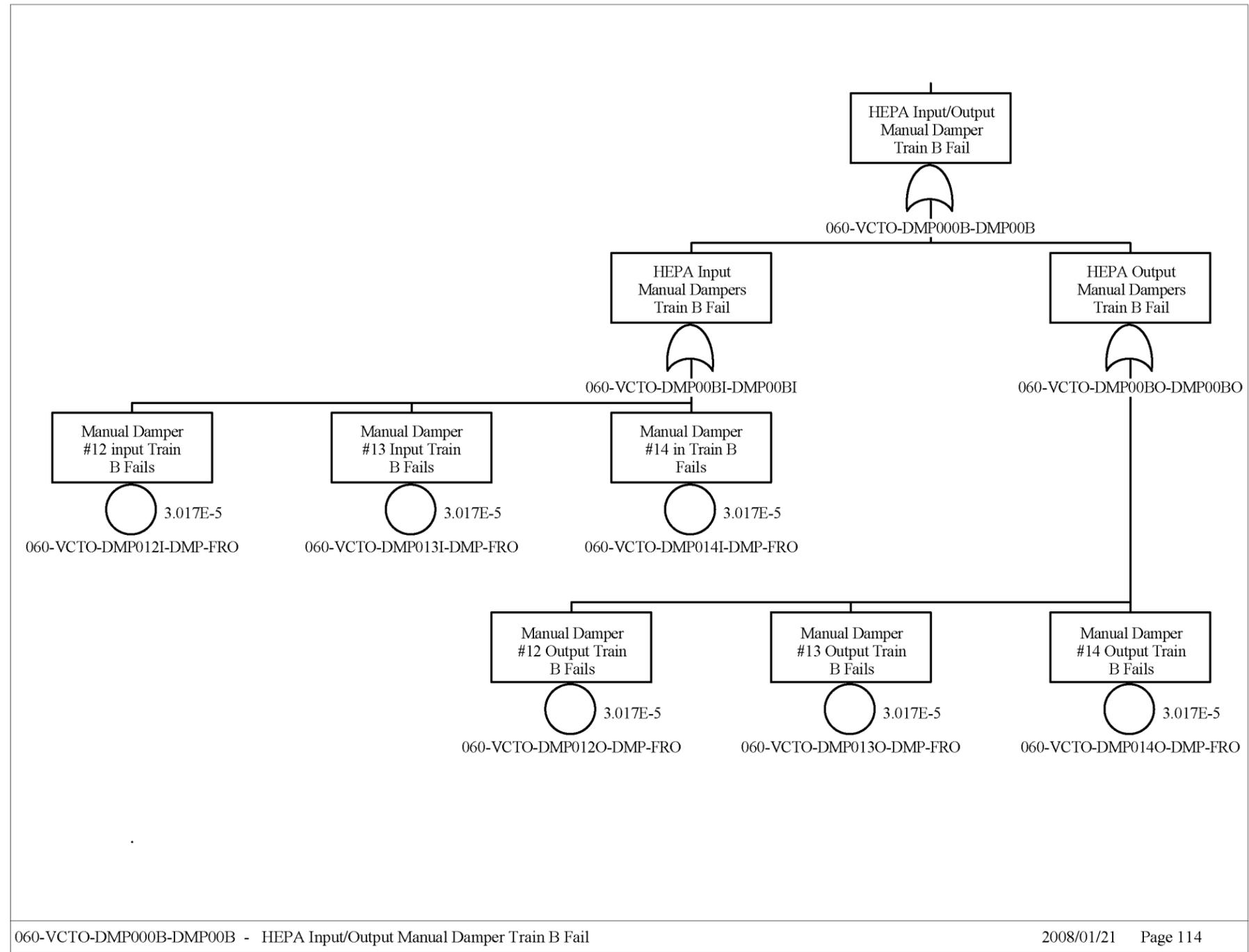
Source: Original

Figure B2.4-20. HVAC Train B is Inoperable



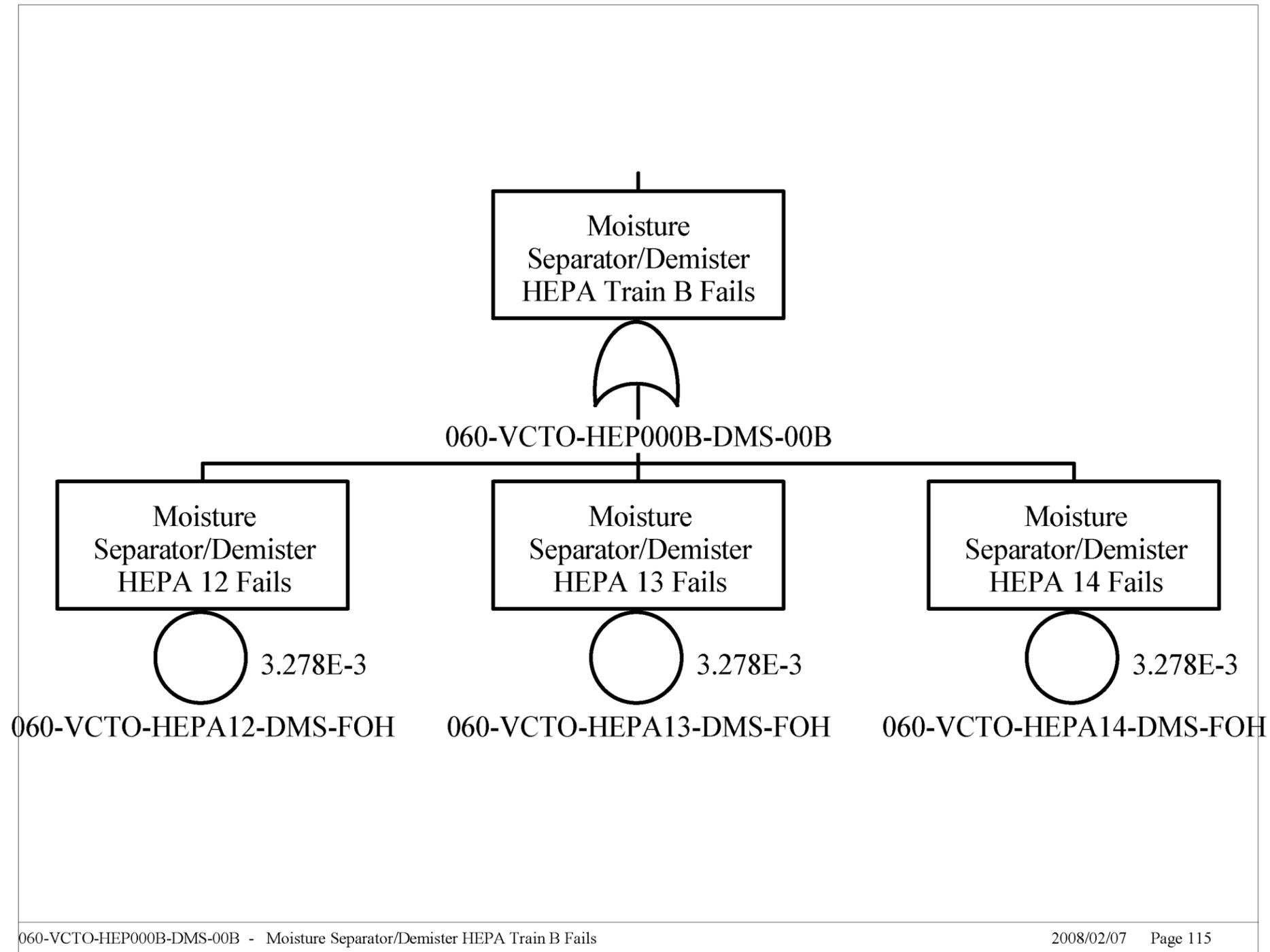
Source: Original

Figure B2.4-21. Exhaust HEPA Equipment in Train B Fails



Source: Original

Figure B2.4-22. HEPA Input/Output Manual Damper Train B Fail



Source: Original

Figure B2.4-23. Moisture Separator/Demister

## B3 IMPORTANT TO SAFETY AC POWER FAULT TREE ANALYSIS

### B3.1 REFERENCES

#### Design Inputs

The PCSA is a safety analysis 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), paragraph 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.

- B3.1.1 BSC (Bechtel SAIC Company) 2007. *CRCF 1 480V ITS LC – Train A 060-EEE0-LC-00001 Single Line Diagram*. 060-E10-EEE0-00301-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0004.
- B3.1.2 BSC 2007. *CRCF 1 480V ITS LC – Train B 060-EEE0-LC-00002 Single Line Diagram*. 060-E10-EEE0-00401-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0005.
- B3.1.3 BSC 2007. *CRCF 1 480V ITS MCC – Train A 060-EEE0-MCC-0001 Single Line Diagram*. 060-E10-EEE0-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0002.
- B3.1.4 BSC 2007. *CRCF 1 480V ITS MCC – Train B 060-EEE0-MCO-00002 Single Line Diagram*. 060-E10-EEE0-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071129.0003.
- B3.1.5 BSC 2007. *CRCF 1 Confinement ITS Battery Room Exhaust System – Train A Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00402-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG. 20071227.0011.
- B3.1.6 BSC 2007. *CRCF 1 Confinement ITS Battery Room Exhaust System – Train B Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00404-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG. 20071227.0012.
- B3.1.7 BSC 2007. *CRCF 1 Confinement ITS Electrical Room HVAC System – Train A Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00401-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071119.0023.
- B3.1.8 BSC 2007. *CRCF 1 Confinement ITS Electrical Room HVAC System – Train B Ventilation & Instrumentation Diagram*. 060-M80-VCT0-00403-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071119.0025.

- B3.1.9 BSC 2007. *Emergency Diesel Generator Facility – 480V ITS MCC 26D-EEE0-MCC-00001 Single Line Diagram (Train A)*. 26D-E10-EEE0-00301-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0026.
- B3.1.10 BSC 2007. *Emergency Diesel Generator Facility – 480V ITS MCC 26D-EEE0-MCC-00002 Single Line Diagram (Train B)*. 26D-E10-EEE0-00401-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071130.0027.
- B3.1.11 BSC 2007. *Emergency Diesel Generator Facility – Fuel Oil System Calculation*. 26D-M6C-EG00-00200-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071025.0001.
- B3.1.12 BSC 2007. *Emergency Diesel Generator Facility – Generator Room Ventilation System Calculation*. 26D-M5C-VNI0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071015.0018.
- B3.1.13 BSC 2007. *Emergency Diesel Generator Facility – ITS 125V DC System Single Line Diagram (Train A)*. 26D-E10-EED0-00101-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0015.
- B3.1.14 BSC 2007. *Emergency Diesel Generator Facility – ITS 125V DC System Single Line Diagram (Train B)*. 26D-E10-EED0-00201-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0016.
- B3.1.15 BSC 2007. *Emergency Diesel Generator Facility – Switchgear and Battery Rooms Ventilation System Calculation*. 26D-M5C-VNI0-00200-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071022.0001.
- B3.1.16 BSC 2008. *Normal Power System 13.8kV Site Distribution Overall Single Line Diagram*. 000-E10-EEN0-00202-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080206.0078.
- B3.1.17 BSC 2008. *Emergency Diesel Generator Facility – 13.8kV ITS Switchgear 26D-EEE0-SWGR-00001 Single Line Diagram (Train A)*. 26D-E10-EEE0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080204.0001.
- B3.1.18 BSC 2008. *Emergency Diesel Generator Facility – 13.8kV ITS Switchgear 26D-EEE0-SWGR-00002 Single Line Diagram (Train B)*. 26D-E10-EEE0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080204.0002.
- B3.1.19 \*Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Loss of Offsite Power Events: 1986-2004*. Volume 1 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0164.

## **B3.2 ITS AC POWER DESCRIPTION**

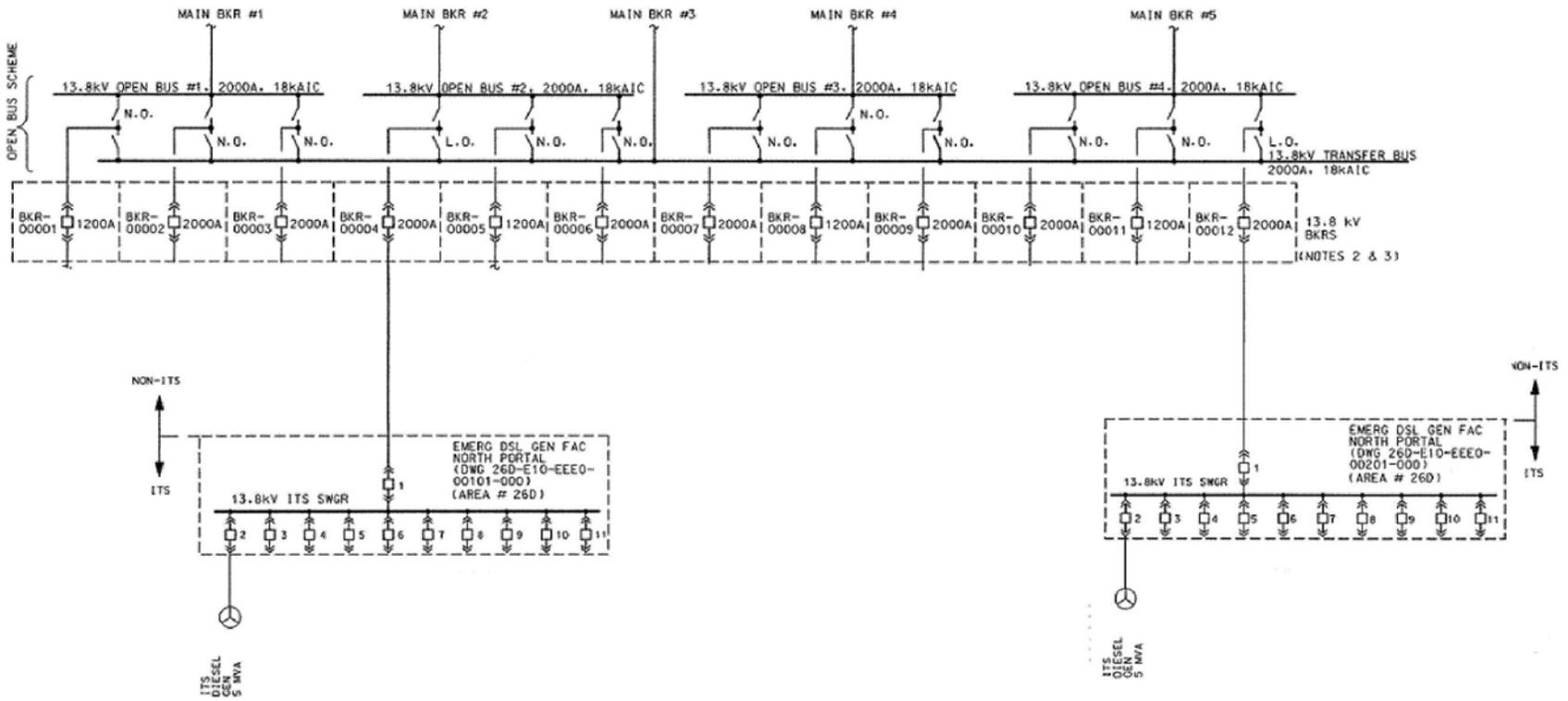
The ITS AC power system supplies power to the ITS HVAC systems in the CRCF, WHF and RF. The ITS power system makes use of two elements: (1) the onsite ITS power supply and (2) the ITS equipment needed to supply power from the onsite ITS power supply to the ITS loads in each of the site facilities. During normal operations AC power is supplied from two offsite 138 kV power lines through the 138 kV – 13.8 kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site. Off-normal conditions for the distribution of AC power occur during a loss of offsite power (LOSP). A LOSP may be the result of problems on the power grid, or the result of failures within the plant AC power systems (most likely within the 138 kV – 13.8 kV switchyard). Under these conditions, the AC power source for the CRCF ITS equipment is two onsite ITS diesel generators. There are several diesel generators located onsite. However there are only two generators designated as ITS; the two that support each division of ITS equipment (A or B) in the three CRCFs, the WHF and the RF. Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each ITS diesel generator supplies power to one division (A or B) of ITS systems. Each ITS diesel generator, its associate support systems and the power distribution system is independent, and electrically isolated, of the other diesel generator, its support systems and power distribution system.

There are three CRCFs on site. The same ITS diesel generators, 13.8 kV ITS switchgear, and associated equipment and support systems are used to support all three facilities. The AC power distribution equipment from the 13.8 kV ITS switchgear to each CRCF's set of ITS equipment are separate but identical for all three facilities. Only one set of CRCF ITS AC power fault trees have been developed, and are applicable for all three CRCFs.

### **B3.2.1 Normal AC Power Distribution**

Normal AC power to the CRCF ITS equipment is provided via two 13.8 kV ITS Switchgears (A and B), one supplying CRCF train A ITS loads and the second supplying power to CRCF train B ITS loads. These two 13.8 kV ITS switchgears (Figures B3.2-1 through B3.2-3) are normally aligned to receive power from the site 138 kV - 13.8 kV switchyard through open buses 2 and 4.

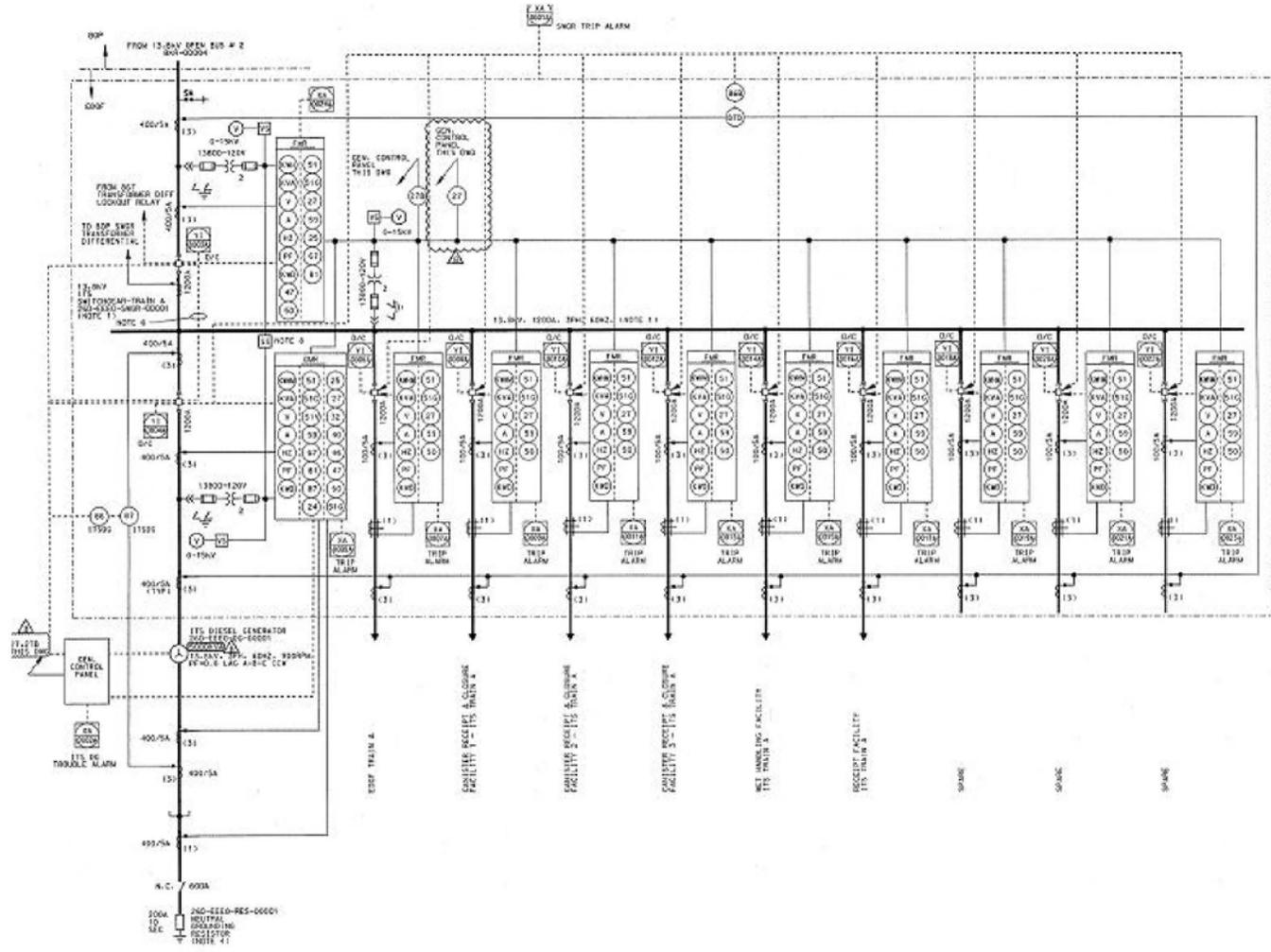
In addition to supplying power to the ITS loads in the CRCF, the 13.8 kV ITS switchgear supplies power to equipment in the EDGF required to support ITS diesel generator operation. These loads include the diesel generator room fans, 13.8 kV ITS switchgear room and battery room air handling unit, the ITS diesel generator fuel oil pumps, and DC power (via a battery charger) to operate the ITS switchgear circuit breakers. (Figures B3.2-4 and B3.2-5 for ITS diesel generator train A and Figures B3.2-6 and B3.2-7 for ITS diesel generator train B).



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: (Ref. B3.1.16)

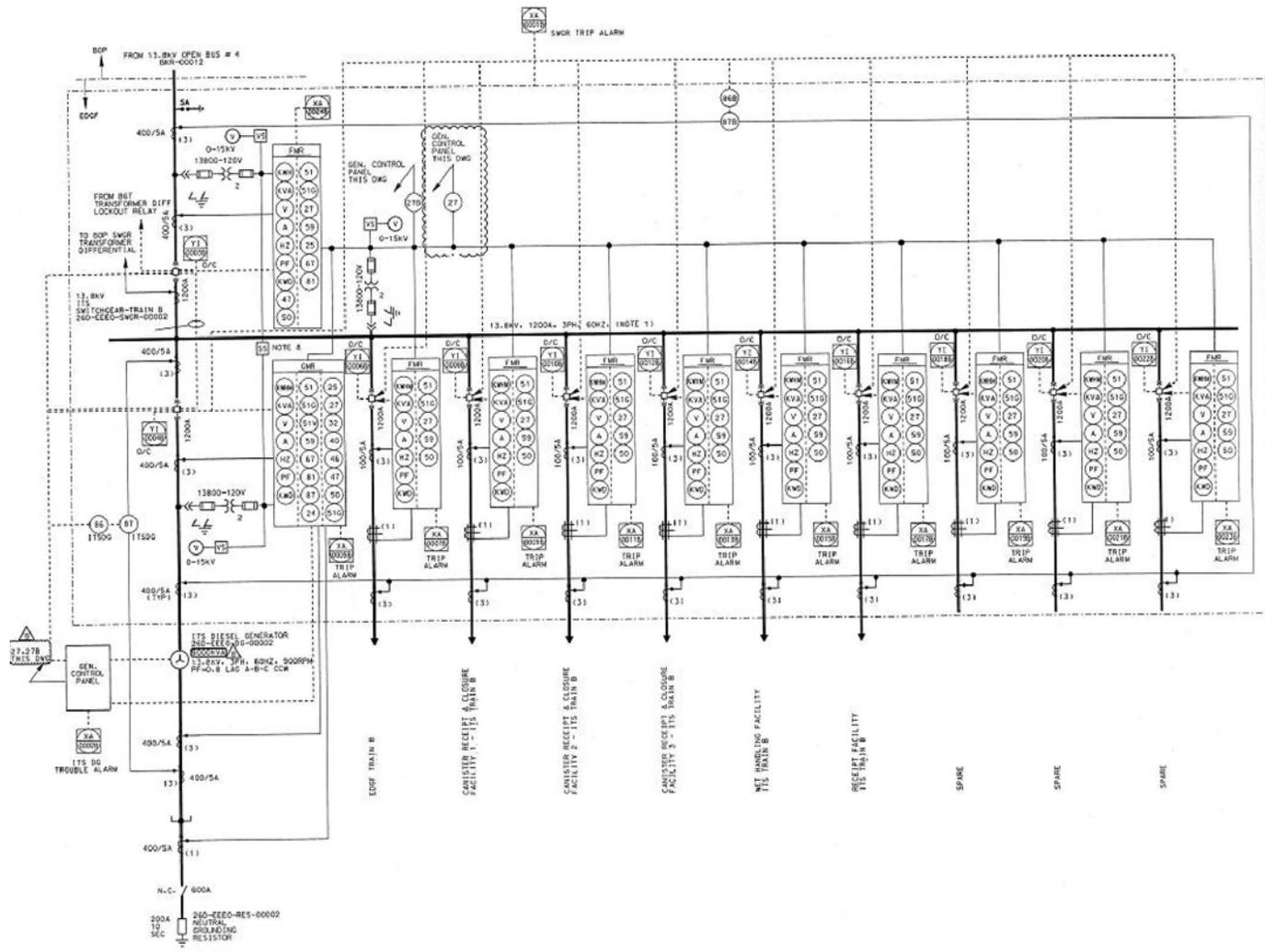
Figure B3.2-1. AC Power – Main Electrical Distribution



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

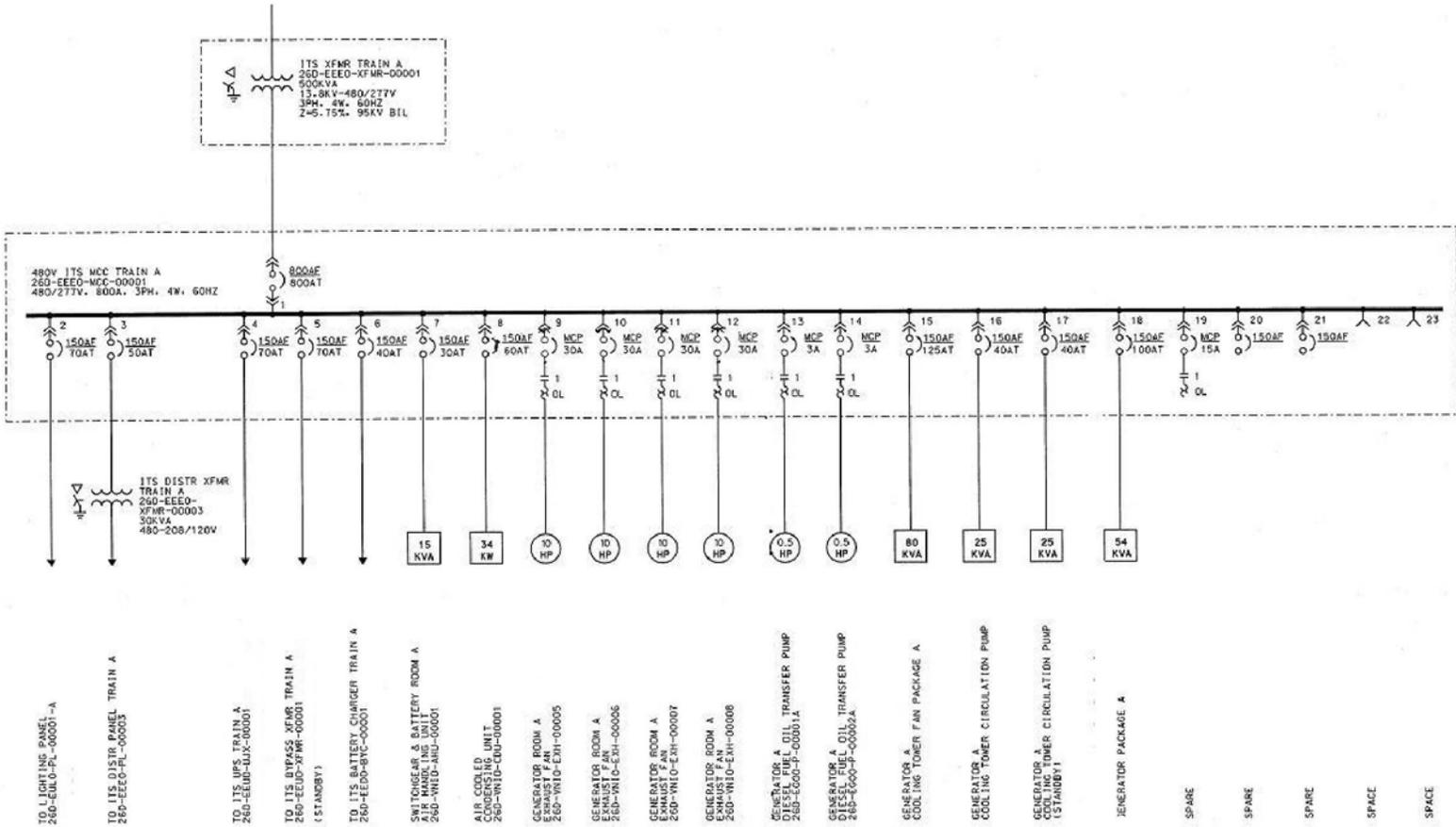
Source: (Ref. B3.1.17)

Figure B3.2-2. AC Power – 13.8 kV ITS Switchgear Train A



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.  
Source: (Ref. B3.1.18)

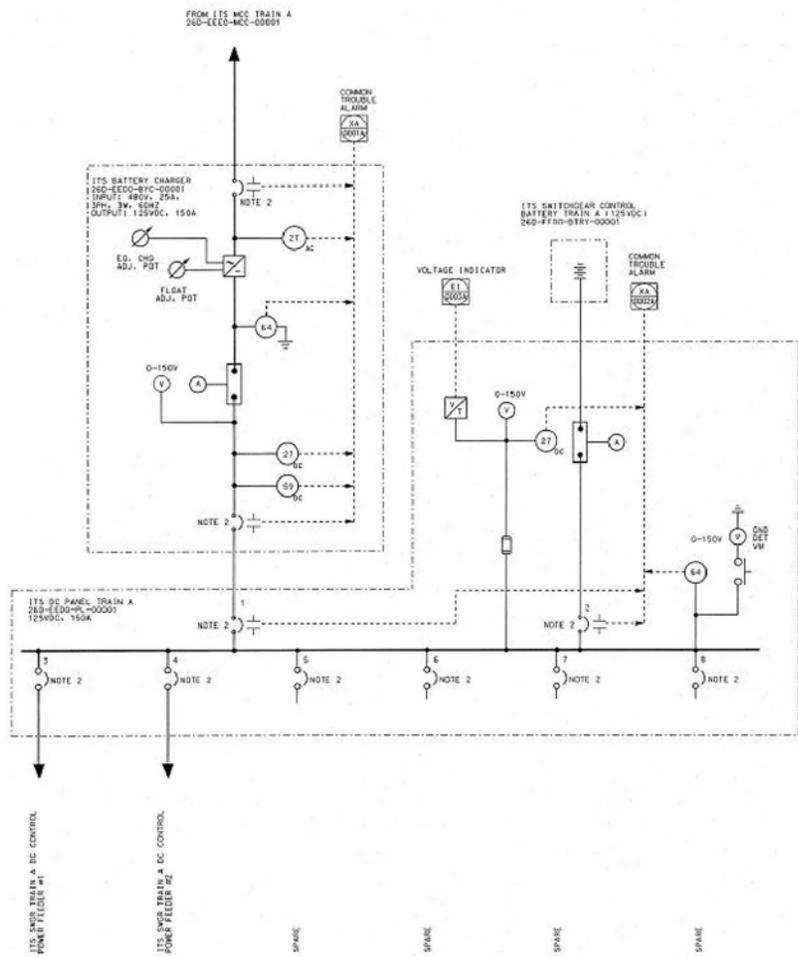
Figure B3.2-3. AC Power – 13.8 kV ITS Switchgear Train B



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: (Ref. B3.1.9)

Figure B3.2-4. Emergency Diesel Generator Facility – 480 V ITS Motor Control Center Train A



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.  
Source: (Ref. B3.1.13)

Figure B3.2-5. ITS 125 V DC System Train A

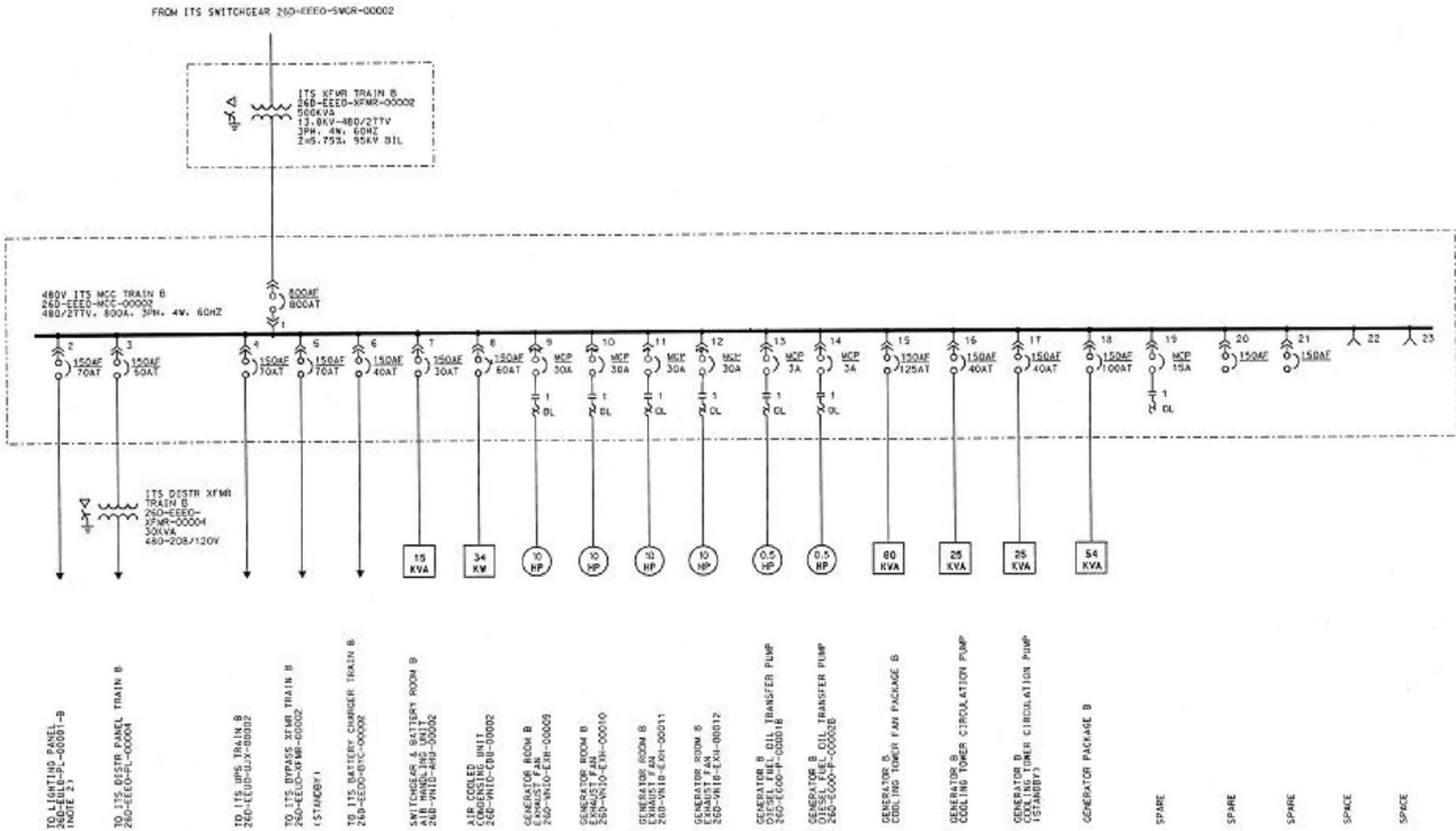


Figure B3.2-6. Emergency Diesel Generator facility – 480V ITS Motor Control Center Train B

NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: ( Ref. B3.1.10)

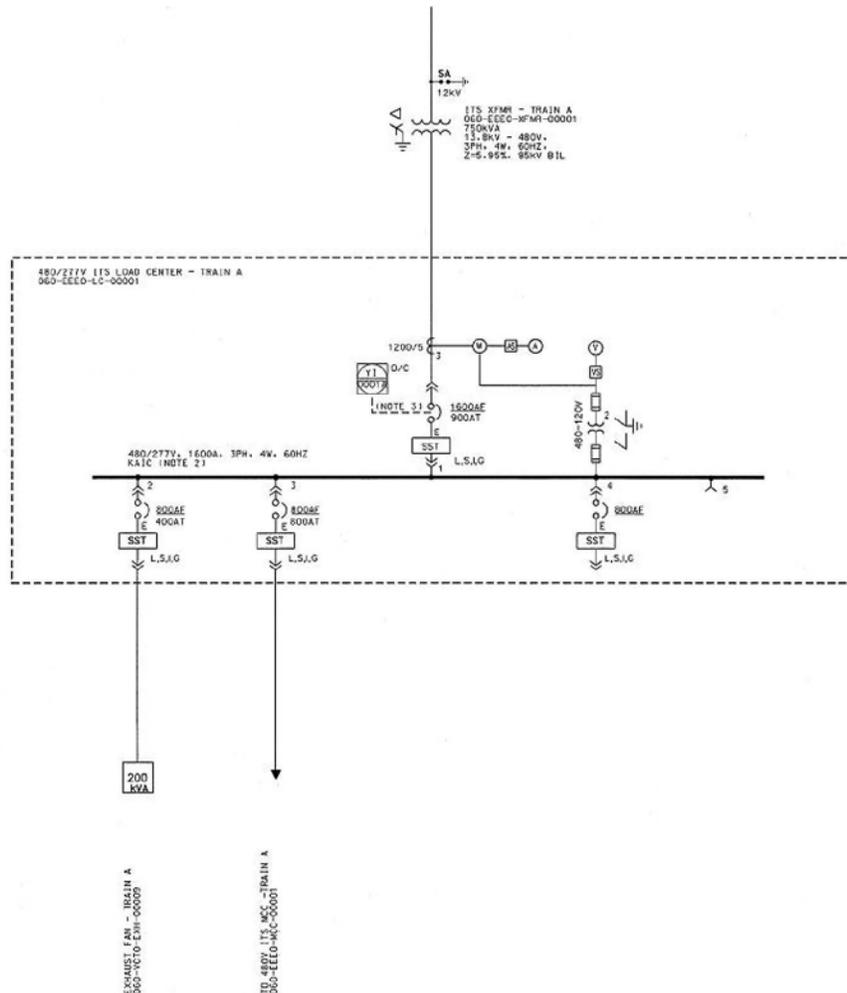


The ITS loads within the CRCF are powered via two ITS 480/277 V load centers and ITS 480/277 V motor control centers (MCC) located within separate areas in the CRCF. The ITS 480/277 V load center train A (Figure B3.2-8) and ITS 480/277V MCC train A (Figure B3.2-10) support train A of the CRCF ITS HVAC.

For the remainder of this attachment, these are referred to as ITS load center train A and ITS MCC train A.

The ITS 480/277 V load center train B (Figure B3.2-9) and ITS 480/277 V MCC train B (Figure B3.2-11) support train B of the CRCF ITS HVAC.

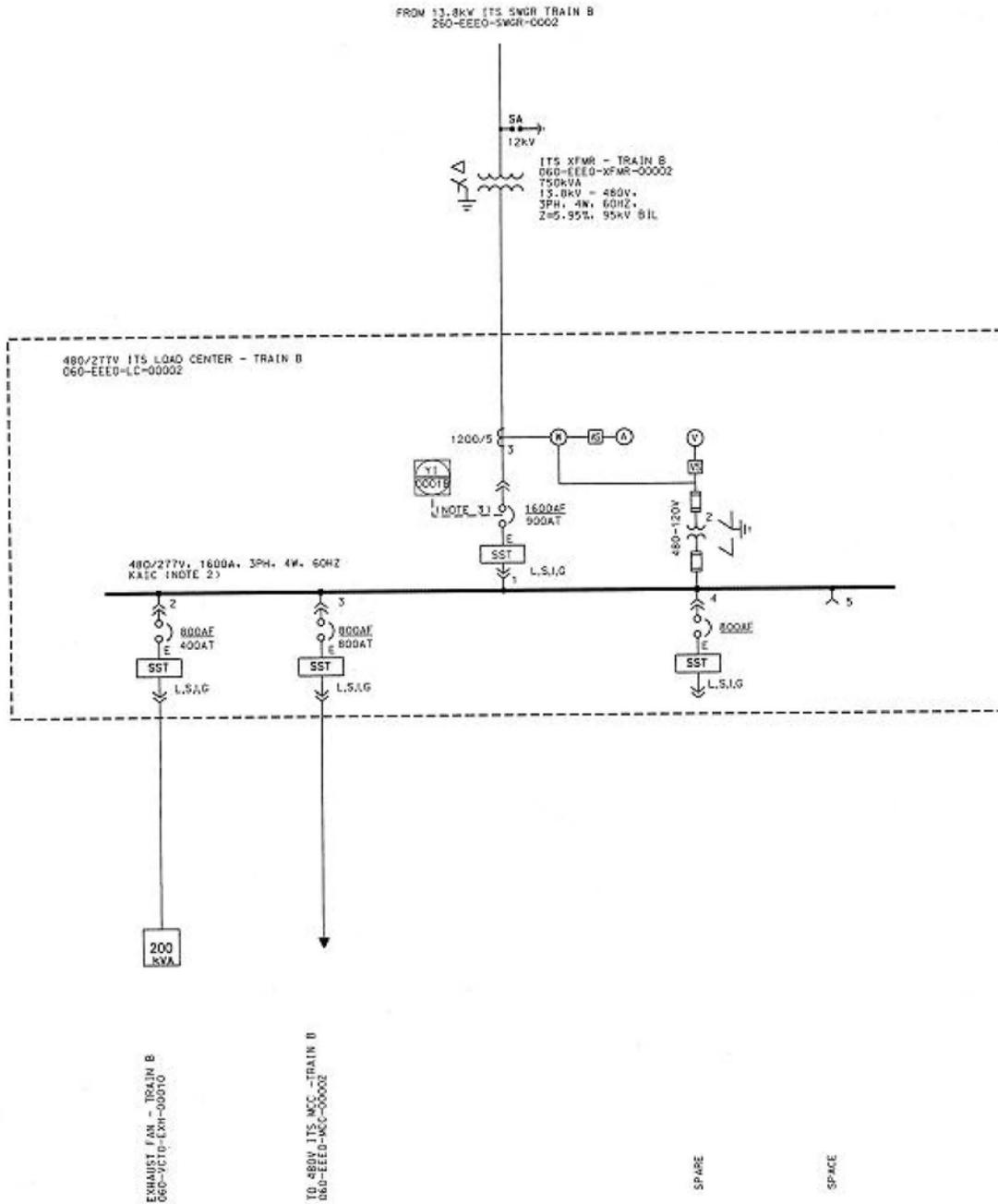
For the remainder of this attachment these are referred to as ITS load center train B and ITS MCC train B. Each division of the AC power supply from the 13.8 kV ITS switchgears to the CRCF passes through a 13.8 kV to a 480 V transformer (Figures B3.2-8 through B3.2-11).



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: (Ref. B3.1.1)

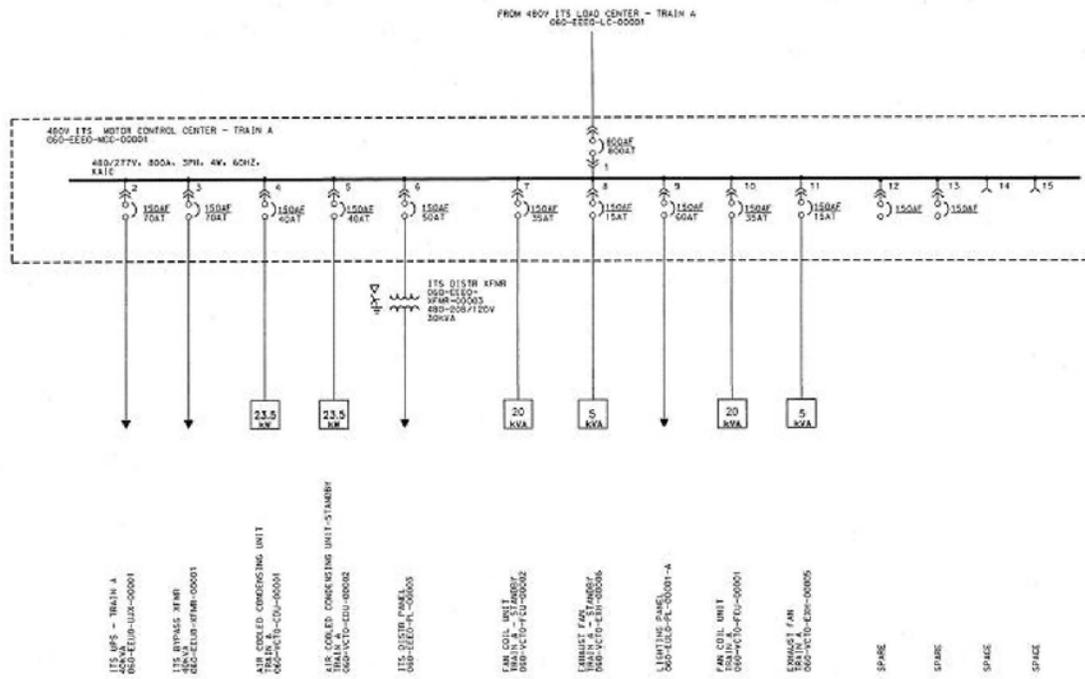
Figure B3.2-8. CRCF ITS Load Center Train A



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

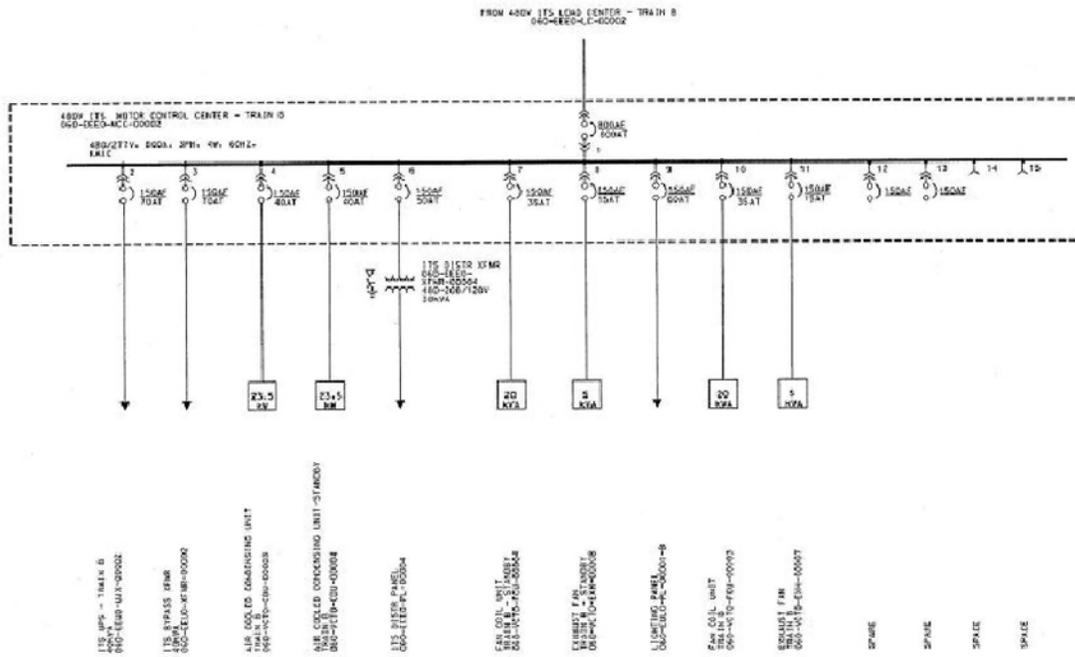
Source: (Ref. B3.1.2)

Figure B3.2-9. CRCF ITS Load Center Train B



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.  
Source: (Ref. B3.1.3)

Figure B3.2-10. CRCF ITS MCC Train A



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: (Ref. B3.1.4)

Figure B3.2-11. CRCF ITS MCC Train B

### B3.2.2 ITS Onsite AC Power

The ITS power supply system is intended to provide back-up power to selected buildings and operations in the event of LOSP. A LOSP could result from a loss of power on the offsite power grid or a failure within the site 138 kV to 13.8 kV switchyard. This portion of the ITS power supply system consists of two identical divisions of diesel generator supplied AC power. The primary components in each division include: a diesel generator, support systems for the diesel generator, and a load sequencer.

Both ITS diesel generators are located in the Emergency Diesel Generator Facility (EDGF). Each is sized to provide sufficient 13.8 kV power to support all of the ITS loads in one ITS switchgear (A or B) in six facilities (three CRCFs, the WHF, the RF, and the EDGF). The ITS diesel generator starts upon detection of an under voltage condition via an under voltage relay of the 13.8 kV ITS switchgear. (The switchyard to switchgear feeder breaker also trips open upon

detection of this under voltage condition.) Each ITS diesel generator is equipped with a complete set of support systems including HVAC systems, UPS and DC power systems, a fuel oil system, diesel generator start subsystem, diesel generator cooling subsystem and lube oil subsystem that are separate and independent from the support system for the other ITS diesel generator.

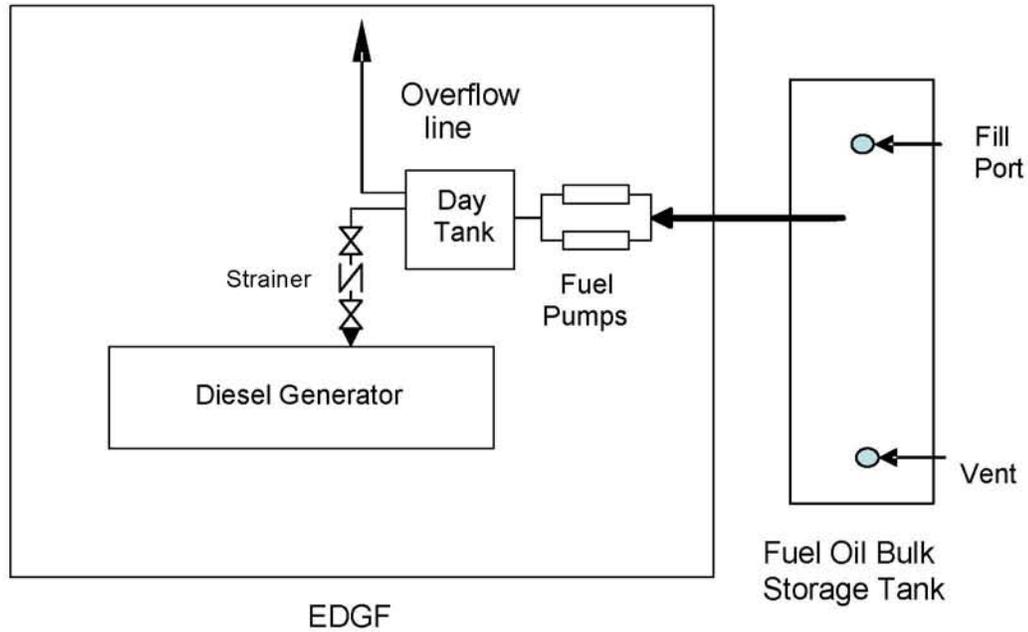
The EDGF is divided into several areas/rooms supporting the two trains of ITS AC power. Separate HVAC systems are provided for each room. The 125 V DC power system (one for each ITS division) provides the necessary power to operate (open/close) the medium voltage circuit breakers on the ITS switchgears. The uninterruptible power system (UPS) supports the ITS diesel generator control system. The UPS is not included in the ITS AC Power model. A UPS is generally very reliable and inclusion of this support system would not noticeably impact the ITS AC Power System failure probability. The HVAC for the 13.8 kV ITS Switchgear Room and Battery Room for each train of the ITS power system, includes an air handling unit and two exhaust fans for each battery room for both air flow and temperature control (Ref. B3.1.15). The system for each of the ITS diesel generator rooms consists of four exhaust fans, as maintaining air flow is sufficient to maintain room temperature within the ITS diesel generator operational limits. All four fans must operate to maintain an acceptable temperature within the ITS Diesel Generator Room (Ref. B3.1.12).

The 125 V DC power system (one for each ITS diesel generator) provides essential power needed to start and load the diesel generator upon a LOSP. DC power for each division of the ITS power supply in the EDGF is supplied by a single battery. The battery is continuously charged through a single battery charger powered (through a transformer and the 480 V ITS MCC, 26D-EEE0-MCC-00001) from the 13.8 kV ITS switchgear (Figures B3.2-5 and B3.2-7).

Each ITS diesel generator fuel oil system consists primarily of a bulk storage tank, two fuel pumps, and a day tank (Figure B3.2-12). The bulk storage tank, located outside of the EDGF, has a capacity sufficient to operate the ITS diesel generator for two weeks. Each fuel pump is sized to be capable of providing sufficient makeup flow to the day tank once the level in the day tank has dropped to a one hour supply for the ITS diesel generator, and to refill the tank while the ITS diesel generator is running. The day tank, located within the EDGF, has a capacity to support four hours of ITS diesel generator operation (Ref. B3.1.11).

The lube oil subsystem, the diesel generator cooling subsystem, and the starting subsystem are considered to be part of the diesel generator and their failures are not modeled as separate events in the fault trees.

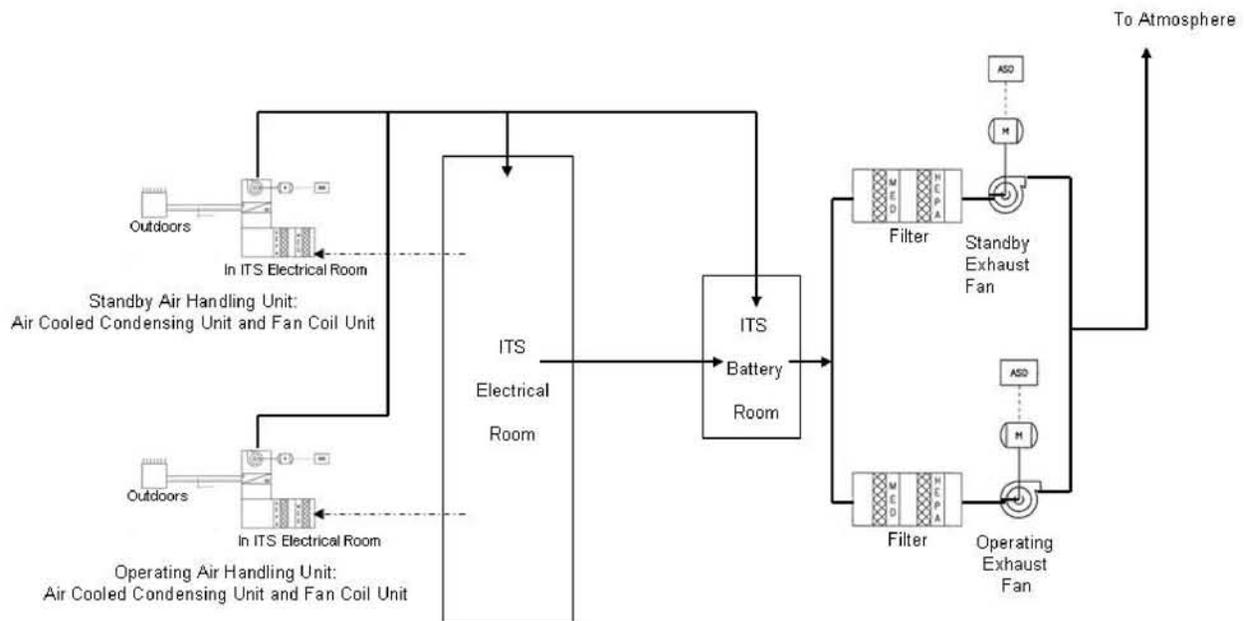
The load sequencer controls the sequence of events that occur after a LOSP and the diesel generator starts. Upon a LOSP, and after the diesel generator starts and reaches its rated capacity, the load sequencer connects the diesel generator to the 13.8 kV ITS Switchgear and then reconnects all division ITS loads, including the CRCF ITS loads.



Source: Modified from (Ref. B3.1.11)

Figure B3.2-12. ITS Diesel Generator Fuel Oil System

Within the CRCF, ventilation and cooling for the ITS Electrical Rooms and ITS Battery Rooms is provided by a dedicated ventilation system. A separate ventilation train is provided for each train of ITS Electrical/Battery Rooms. Each train consists of two air handling units (each consisting of an air cooled condensing unit and a fan coil unit), two exhaust fans and associated ducting and instrumentation. (Figure B3.2-13) Each air handling unit and exhaust fan is rated at 100% capacity. Two air handling Units, one in each train (air cooled condensing units 060-VCT0-CDU-00001 and 060-VCT0-CDU-00003 and fan coil units 060-VCT0-FCU-00001 and 060-VCT0-FCU-00003) are normally operating while the second one in each train (air cooled condensing units 060-VCT0-CDU-00002 and 060-VCT0-CDU-00004 and fan coil units 060-VCT0-FCU-00002 and 060-VCT0-FCU-00004) is normally in standby. Similarly, two exhaust fans, one in each train, (exhaust fan 060-VCT0-EXH-00005 and 060-VCT0-EXH-00007) are normally operating while the second one in each train (exhaust fan 060-VCT0-EXH-00006 and 060-VCT0-EXH-00008) is normally in standby (Ref. B3.1.7), (Ref. B3.1.5), (Ref. B3.1.8), and (Ref. B3.1.6).



NOTE: Legibility of figure does not affect technical content of the document. See source for detail.

Source: (Ref. B3.1.5) through (Ref. B3.1.8)

Figure B3.2-13. Simplified Diagram of Representative Train of CRCF ITS Electrical and ITS Battery Rooms Ventilation System

### B3.2.3 ITS AC Power Normal Operations

Under normal operating conditions, AC power is supplied from two 138 kV offsite power lines. Power is passed through the 138 kV – 13.8 kV switchyard to the two independent 13.8 kV ITS switchgears. From there, power is transmitted to two 13.8 kV – 480 V transformers, one supporting division A and one supporting division B of the CRCF. Power to individual ITS equipment within each facility is provided via the ITS load centers and ITS MCCs (one of each for division A and division B).

The AC power system is normally operating, but one division at a time may be taken out of service for maintenance. With one division out of service, only one division of the supported ITS systems can be considered to be operable.

### B3.2.4 ITS AC Power Off-Normal Operations

The off-nominal condition of interest for the ITS AC power system is a LOSP. During a LOSP, both ITS diesel generators are required to start and accept loads in a timely manner. Upon a LOSP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8 kV ITS switchgear and the switchyard in each division automatically opens. Both diesel generators start automatically and are connected to the 13.8kV ITS switchgear when the connecting breaker is closed by the load sequencer. The load

sequencer then reconnects the CRCF loads to the 13.8 kV ITS switchgear. Both diesel generators continue to supply AC power until normal power is restored.

### **B3.2.5 ITS AC Power Testing and Maintenance**

The normal AC power system is operated continuously. Maintenance would be performed on an as needed basis. The diesel generators and supporting subsystems are normally in a standby mode. Routine tests are performed to ensure that the ITS diesel generator can start and load, in the event of a loss of normal power, including during a LOSP event.

#### **Requirements**

The ITS diesel generators and their associated support components (start systems, lube oil, HVAC) are tested monthly on a staggered basis.

#### **Features**

Normal maintenance is performed in accordance with manufacturer's recommendations.

Maintenance outages that remove a division of ITS AC power from operation is limited to one week per maintenance outage.

#### **B3.2.5.1 Fault Trees**

##### **Requirements**

The fault tree model for the ITS AC power system includes: (1) those components that have been declared as ITS and (2) those AC power distribution system components whose failure would require the ITS AC power system to perform. The ITS power system includes components that are normally in standby (e.g., the diesel generator) and components that are normally in operation. The portions of the normal AC power distribution system modeled include the AC power distribution system from the 13.8 kV ITS Switchgear to the facility ITS load centers.

The mission time for the ITS AC power system is set to 720 hours. This is based on the mission time requirement for the CRCF HVAC system following the potential breach of a waste canister.

##### **Features**

CCFs have been included for fourteen events. Six are associated with ITS diesel generator operation: two for the ITS diesel generators (failure to start or run) themselves and four for the pair of fuel pumps (failure to start and run for each pair) that support each ITS diesel generator. Three more are associated with the failure to open/close of the breakers that disconnect the 13.8 kV ITS switchgear from the normal offsite power supply, the ITS load center feed breakers, and the breakers that connect the ITS diesel generators to the 13.8 kV ITS switchgear. Four are associated with the CRCF confinement ITS electrical and battery rooms ventilation system: one for the failure to start and run of the system standby exhaust fans, one for the failure to run of the operating exhaust fans, one for the failure to start and run of the standby air handling units, and one for the failure to run of the operating air handling units. The final CCF event modeled is

associated with the CRCF 13.8 kV - 480 V ITS transformers. Additional detail about the treatment of CCF failures can be found in Attachment C.

Four human error conditions are incorporated into the model, details are provided in Section B3.4 of this attachment. All four address the failure to properly restore portions of the system to operable status following maintenance.

The ITS diesel generator lube oil, cooling systems, and start subsystems are considered to be part of the diesel generator and are not modeled as separate systems.

### B3.3 Dependencies and Interactions

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B3.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B3.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
ITS diesel generators	Start systems, load sequencer	EDGF diesel generator room HVAC	—	Test and maintenance	—
13.8 kV ITS Switchgear	ITS Diesel generator, CRCF 13.8 – 480V ITS transformers	EDGF Switchgear room HVAC	—	Test and maintenance	Offsite power
ITS Load Centers and ITS MCCs	ITS diesel generator, 13.8 kV ITS switchgear	CRCF ITS AC Power Room Ventilation	—	Test and maintenance	Offsite power
AC load breakers	EDGF DC power system	—	—	Test and maintenance	—
CRCF 13.8 kV to 480V ITS transformers	ITS diesel generator, 13.8 kV ITS switchgear	—	—	Test and maintenance	Offsite power
CRCF ITS AC Power Room Ventilation	CRCF ITS MCCs	—	—	Test and maintenance	—

NOTE: CRCF = Canister Receipt and Closure Facility; EDGF = Emergency Diesel Generator Facility; HVAC = heating, ventilation, and air conditioning; ITS = important to safety; kV = kilovolt; MCC = motor control centers.

Source: Original

### **B3.4 ITS AC Power Failure Scenarios**

For the CRCF the ITS AC power system has two credible failure scenarios:

1. Loss of AC power to CRCF ITS load center train A. Failure to provide power to the CRCF ITS HVAC system train A.
2. Loss of AC power to CRCF ITS load center train B. Failure to provide power to the CRCF ITS HVAC system train B.

These two scenarios apply to operations in all three CRCFs. The facilities and operations within each of these facilities are identical, therefore, only one set of fault trees have been developed to address operations within all three facilities.

#### **B3.4.1 Loss of AC Power to CRCF ITS Load Center Train A**

##### **B3.4.1.1 Description**

CRCF confinement following the potential breach of a waste canister is provided, in part, by the CRCF ITS HVAC system. The ITS AC power system provides the power needed to operate the ITS HVAC system equipment. This fault tree models the components that are required to provide AC power from either the normal offsite power supplies or from ITS diesel generator A to ITS load center train A.

##### **B3.4.1.2 Success Criteria**

Success criteria for this train of the ITS AC power system is providing AC power from either the normal power system, or from the ITS diesel generator (DG A) to the ITS HVAC division powered through CRCF ITS load center train A. The AC power system must operate in support of the ITS HVAC system for as long as necessary to successfully provide confinement after the potential release of material from a breached canister. Therefore, the mission time (the period for which ITS AC power must be supplied to the ITS HVAC system) is the same for the ITS AC power system as it is for the ITS HVAC system, 720 hours.

##### **B3.4.1.3 Design Requirements and Features**

###### **Requirements**

Each ITS diesel generator has support systems that are independent from the support system for the other diesel generator. Independent support systems include:

- Fuel oil systems
- HVAC systems to include the ITS diesel generator room and 13.8 kV ITS switchgear room systems

- Lube oil system
- ITS diesel generator cooling systems
- Diesel generator start system.

## Features

The 13.8 kV ITS switchgear is isolated from the main switchyard upon a loss of power in the switchyard, either due to a LOSP or from failures within the switchyard.

The CRCF load is shed from the 13.8 kV ITS switchgear upon a loss of power indication.

A load sequencer controls the loading of the diesel generator onto the 13.8 kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the CRCF loads onto the ITS AC power system.

Environmental systems are provided to maintain the temperature in the various EDGF rooms within acceptable levels. This includes a fan system for the diesel generator room and an air handling unit for the 13.8 kV ITS switchgear and battery room.

### B3.4.1.4 Fault Tree Model

The top event in this fault tree is “Loss of AC Power to CRCF ITS Load Center Train A.” This is defined as a failure of normal and ITS on-site power to provide power to ITS load center train A. Faults considered in the evaluation of this top event include: failure of components in the normal AC power system, failure of the ITS diesel generator, human events that can contribute to onsite system failures resulting in a power loss at the CRCF and a LOSP. In this fault tree offsite power is not modeled as an initiating event, but as a system failure. The value used for this event represents the probability that offsite power would be lost in the 720 hours following a possible radioactive release from a damaged canister.

### B3.4.1.5 Basic Event Data

Table B3.4-1 contains a list of basic events used in the “Loss of AC Power to CRCF ITS Load Center Train A” fault tree. Included are component failures, maintenance errors and the human and CCF events identified in the previous two sections. The data, for both random and CCF failures) used to develop the failure probabilities associated with these basic events comes from the component reliability data analysis (Attachment C). Human reliability analyses (Attachment E) provide the probabilities for the human events.

Mission times for the various components are based on the following:

- Fault exposure time (168 hours) for events limited to one week maintenance outages (train OOS for maintenance).
- Mission time (360 hours) for operation of standby equipment that would operate after a LOSP (distribution of the occurrence of an LOSP is evenly distributed over the 720 hours, after a potential radiological release, average mission time is therefore 360 hours), average fault exposure time for standby components tested monthly.
- Mission time (720) hours for operating components.

While some of the components are normally in operation, it is possible for any of the components to be out of service (OOS) for maintenance. With train A of AC power OOS (resulting in train A of the facility ITS HVAC being OOS), train B provides support to an operable ITS HVAC train B. The intent of the maintenance events modeled is for the events to address maintenance on any component in that AC power division. This is true for the components normally in operation and the standby components. The maintenance unavailability represented by the ITS load center maintenance events model the unavailability of any component from the 13.8 kV ITS switchgear through the ITS load center. The maintenance unavailability represented by the ITS diesel generator maintenance events represent the unavailability of any of the components or systems that would prevent the ITS diesel generator from starting and loading onto the 13.8 kV ITS switchgear. As noted earlier all of the human events are associated with the failure to restore a component to operable or standby status after maintenance. The operator-related events shown in the following table are combinations events: they include the probability that the component has been taken OOS for maintenance and that site personnel have not restored the component to operable or standby status. A screening value of 0.1 has been used for the HEP in all cases.

Table B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS Transformers CCF	1	4.920E-06	4.920E-06	0.000E+00	0.000E+00
060-#EEE-CRCF1-A-XMR-FOH	CRCF ITS Train A Transformer Failure	3	2.095E-04	0.000E+00	2.910E-07	7.200E+02
060-#EEE-LDCNTRA-BUA-FOH	CRCF ITS Load Center A Fails	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
060-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
060-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post maintenance	1	1.025E-05	1.025E-05	0.000E+00	0.000E+00
060-#EEE-LDCNTRA-C52-FOD	ITS Load Center A feed breaker (AC) Fails to reclose	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
060-#EEE-LDCNTRA-C52-SPO	ITS Load Center A Feed Circuit Breaker (AC) Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
060-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
060-#EEE-LDCNTRB-BUA-ROE	ITS Failure to Restore Load Center Train B post maintenance	1	1.025E-05	1.025E-05	0.000E+00	0.000E+00
060-#EEE-LDCNTRS-C52-CCF	Common-cause failure of the ITS Load Center feed breakers to reclose	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 Feed Breaker Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	3	5.378E-03	0.000E+00	7.490E-06	7.200E+02
060-VCT0-AHU0001-AHU-FTR	CRCF ITS Elec AHU 00001 Fails to run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
060-VCT0-AHU0001-CTL-FOD	CRCF ITS Elec AHU 00001 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-AHU0002-AHU-FTR	CRCF ITS ELec AHU 00002 Fails to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
060-VCT0-AHU0002-CTL-FOD	CRCF ITS Elec AHU 00002 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-AHU0002-FAN-FTS	CRCF ITS Elec AHU 00002 Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
060-VCT0-AHU0103-AHU-CCR	CCF of the running CRCF ITS Elec AHUs to continue to run	1	6.200E-05	6.200E-05	0.000E+00	0.000E+00
060-VCT0-AHU0202-AHU-CCR	CCF of standby CRCF ITS Elec AHUs to start/run	1	1.600E-04	1.600E-04	0.000E+00	0.000E+00
060-VCT0-EXH-005-CTL-FOD	CRCF ITS Elec Exh fan 00005 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCT0-EXH-006-FAN-FTS	CRCF ITS Elec Exh fan 00006 Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00

Table B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-VCT0-EXH006-CTL-FOD	CRCF ITS Elec Exh Fan 0006 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-EXH0507-FAN-CCR	CCF of running Exh fans for CRCF ITS Elec.	1	1.200E-03	1.200E-03	0.000E+00	0.000E+00
060-VCT0-EXH0608-FAN-CCF	CCF to start/run: standby Exh fans for the CRCF ITS Elec	1	1.300E-03	1.300E-03	0.000E+00	0.000E+00
26D-##EG-DAYTNKA-TKF-FOH	ITS DG A Day Tank (00002A) Fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EG-FLITLKA-IEL-FOD	ITS DG A fuel transfer pumps Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
26D-##EG-FTP1DGA-PMD-FTR	ITS DG A Fuel Transfer Pump Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP1DGA-PMD-FTS	ITS DG A Fuel Pump 1A Fails to Start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FTP2DGA-PMD-FTR	ITS DG A Fuel Transfer Pump 2A Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP2DGA-PMD-FTS	ITS DG A Fuel Transfer pump 2A Fails to Start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FULPMPA-PMD-CCR	Common-cause failure of ITS DG A fuel pumps to run	1	2.900E-04	2.900E-04	0.000E+00	0.000E+00
26D-##EG-FULPMPA-PMD-CCS	Common-cause failure of ITS DG A fuel pumps to start	1	1.200E-04	1.200E-04	0.000E+00	0.000E+00
26D-##EG-STRTDGA-C72-SPO	ITS Switchgear A Battery Circuit Breaker (DC) Spur Op	3	3.851E-04	0.000E+00	1.070E-06	3.600E+02 <sup>d</sup>
26D-##EG-WKTNK_A-TKF-FOH	ITS DG A Bulk Fuel Tank (00001A) Fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EGBATCHRGA-BYC-FOH	ITS Switchgear A Battery: Battery Charger failure	3	1.276E-03	0.000E+00	7.600E-06	1.680E+02 <sup>c</sup>
26D-##EEE-SWGRDGA-BUA-FOH	13.8 kV ITS Switchgear A Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
26D-##EEESWGRDGA-AHU-FTR	13.8 kV ITS Switchgear room Air Handling Unit Fails	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
26D-##EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EEG-HVACFA1-FAN-FTS	ITS DG A room Fan 1 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EEG-HVACFA2-FAN-FTR	ITS DG A room Fan 2 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EEG-HVACFA2-FAN-FTS	ITS DG A room Fan 2 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EEG-HVACFA3-FAN-FTR	ITS DG A room Fan 3 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EEG-HVACFA3-FAN-FTS	ITS DG A room Fan 3 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EEG-HVACFA4-FAN-FTR	ITS DG A room Fan 4 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EEG-HVACFA4-FAN-FTS	ITS DG A room Fan 4 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EEU-208_DGA-BUD-FOH	ITS DC Panel A DC Bus Failure	3	8.640E-05	0.000E+00	2.400E-07	3.600E+02 <sup>d</sup>
26D-##EEY-DGALOAD-C52-FOD	DG A Load Breaker (AC) Fails to Close	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00

B3-24

March 2008

Subsurface Operations Reliability and Event Sequence Categorization Analysis

000-PSA-MGR0-00500-000-00A

Table B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
26D-#EEY-DGLOADS-C52-CCF	Common-cause failure of ITS DG Load Breakers to close	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	3	7.698E-01	0.000E+00	4.080E-03	3.600E+02
26D-#EEY-ITSDG-A-#DG-FTS	Diesel Generator Fails to Start	1	8.380E-03	8.380E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly restore ITS DG-B to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B Fail to Run	1	1.800E-02	1.800E-02	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to Start	1	3.900E-04	3.900E-04	0.000E+00	0.000E+00
26D-#EEY-OB-SWGA-C52-FOD	13.8 kV ITS SWGR feed breaker (AC) Fails to open	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
26D-#EEY-OB-SWGS-C52-CCF	Common-cause failure of 13.8kV ITS SWGR feed breakers to open	1	1.040E-04	1.040E-04	0.000E+00	0.000E+00
26D-#EG-LCKOUTRL-RLY-FTP	13.8 kV ITS Switchgear Feed breaker lock out relay fails to Open CB	3	3.152E-03	0.000E+00	8.770E-06	3.600E+02
26D-#EGLDSQNCRA-SEQ-FOD	ITS DG A Load Sequencer Fails	1	2.670E-03	2.670E-03	0.000E+00	0.000E+00
26D-EG-BATTERYA-BTR-FOD	ITS Switchgear A Battery No Output Given Challenge	1	8.200E-03	8.200E-03	0.000E+00	0.000E+00
27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02

B3-25

March 2008

Table B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
27A-#EEN-OPENBS2-BUA-FOH	13.8 kV Open Bus 2 Bus Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
27A-#EEN-OPNBS1A-SWP-SPO	13.8 kV Open Bus 2 to ITS Div A Electric Power Switch Spur. Xfer	3	1.116E-04	0.000E+00	1.550E-07	7.200E+02
LOSP*	Loss of Offsite Power	1	2.99E-03	2.99E-03	0.000E+00	0.000E+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> The designation of a circuit breaker as AC or DC refers to the system designation for the circuit breaker, it is not representative of the motive power for the circuit breaker.

<sup>c</sup> The failure of the battery charger would result in eventual depletion of the battery and a low power indication on both the battery and the DC bus. The 168 hr mission time was selected as a conservative estimation for the detection time of this failure.

<sup>d</sup> The mission times for the DC bus related failure rates do not take credit for any monitoring of bus status, which would provide nearly instantaneous indication of a bus failure or loss of power to the bus. The standby component mission time was used conservatively.

LOSP\* represents the probability of losing offsite power during the 720 hours HVAC is required after any breach of a container releases radioactive material. It is based on a loss of offsite power frequency of 3.59E-02/year from NUREG/CR6890 Vol. 1 (Ref. B3.1.19).

AC = alternating current; AHU = air handling unit; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator; Div = division; elec = electrical EXH = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation; Prob. = probability; Spur. = spurious; SWGR = switch gear; Xfer = transfer.

Source: Original

### B3.4.1.5.1 Human Failure Events

Four basic HFEs (Table B3.4-2) are associated with human error. All of the HFEs are associated with the failure to properly restore components to operable status following maintenance. The first two shown in Table B3.4-2 are associated with the failure to restore the normal power supply to the CRCF ITS load centers after maintenance. The last two are representative of the failure to restore the ITS diesel generators (and any other components that would prevent the ITS diesel generator from starting or loading) to service after maintenance. These events are combination events consisting of the probability that a component was removed for maintenance and the failure of plant operators (assigned a screening value of 0.1) to restore the component after maintenance.

Table B3.4-2. Human Failure Events

Name	Description
060-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post maintenance
060-#EEE-LDCNTRB-BUA-ROE	Failure to Restore ITS Load Center Train B post maintenance
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly return ITS DG-B to service

NOTE: DG = diesel generator; ITS = important to safety.

Source: Original

### B3.4.1.5.2 Common-Cause Failures

Twelve of the fourteen CCF failures identified earlier (Section B3.2.5.1) have been included in the analysis of the loss of ITS AC power to the ITS load center train A. Ten of the CCF events affect both trains of ITS AC Power. Two affect only this train of the system. The remaining two affect only the other train of the system. Two are associated with the ITS diesel generators: CCF failure of the ITS diesel generators to start and CCF failure of the ITS diesel generators to run. The CCF failure of the ITS diesel generator fuel oil system incorporates two CCF failures: CCF failure of the two fuel oil pumps to start and the CCF failure of the pumps to run. Three circuit breaker CCF events were considered. These are the CCF failure of the (1) 13.8 kV ITS switchgear feed breakers (from 13.8 kV open buses) to open on loss of offsite power, (2) ITS diesel generator load breakers to close when commanded by the load sequencer and (3) ITS load center feed breakers to close when commanded by the load sequencer. Four CCFs are associated with the CRCF ITS Electrical and Battery Rooms Ventilation System, two for the common cause failure of exhaust fans to start and run, and two for the common-cause failure of the air handling units to start and run. The last CCF event considered is the CCF failure of the 13.8 kV – 480 V ITS transformers.

Table B3.4-3. Common-Cause Basic Events

Name	Description	Alpha-factor
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS Transformers CCF	0.0235
060-#EEE-LDCNTRS-C52-CCF	CCF of the ITS Load Center feed breakers to reclose	0.047
26D-##EG-FULPMPA-PMD-CCR	CCF of ITS DG A fuel pumps to run	0.0235
26D-##EG-FULPMPA-PMD-CCS	CCF of ITS DG A fuel pumps to start	0.047
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG Load Breakers to close	0.047
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B Fail to Run	0.0235
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to Start	0.047
26D-#EEY-OB-SWGS-C52-CCF	Common-cause failure of 13.8 kV ITS SWGR feed breakers to open	0.047
060-VCT0-AHU0103-AHU-CCR	CCF of the running CRCF ITS Elec AHUs to continue to run	0.0235
060-VCT0-AHU0202-AHU-CCR	CCF of standby CRCF ITS Elec AHUs to start/run	0.047 start 0.0235 run
060-VCT0-EXH0507-FAN-CCR	CCF of running Exh fans for CRCF ITS Elec.	0.0235
060-VCT0-EXH0608-FAN-CCF	CCF to start/run: standby Exh fans for the CRCF ITS Elec	0.047 start 0.0235 run

NOTE: AHU = air handling unit; CCF = common-cause failure, CRCF = Canister Receipt and Closure Facility; DG = diesel generator; elec = electrical; Exh = exhaust; ITS = important to safety; SWGR = switch gear.

Source: Original

All of the CCFs modeled are used on pairs of components with one of two success criteria (i.e., two of two failure criteria). Alpha-factors used to determine the CCF probability are 0.047 for demand failures and 0.0235 for time dependent failures (Table C3-1, CCCG=2, and the associated text). Two CCF in Table B3.4-3 are used to represent the CCF associated with the failure to start and failure to run for components. For these two CCFs, the appropriate alpha-factors were applied to the start and run portions of the random failure probability to develop a single CCF probability for the components.

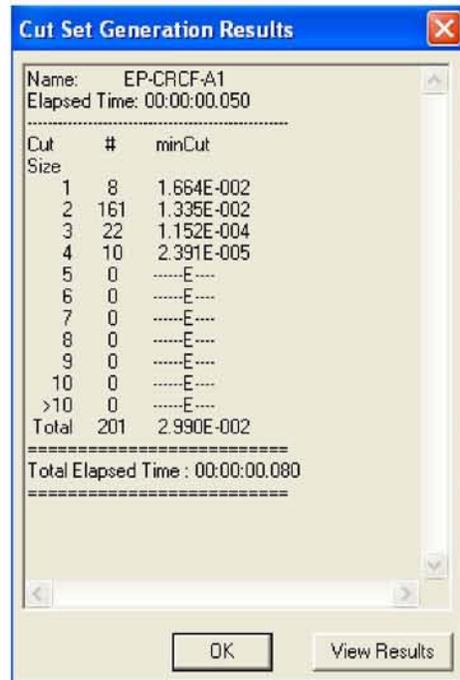
#### B3.4.1.6 Uncertainty and Cut Set Generation

Figure B3.4-1 contains the uncertainty results obtained from running the fault trees for the “Loss of AC Power to CRCF ITS Load Center Train A”. Figure B3.4-2 provides the cut set generation results for the “Loss of AC Power to CRCF ITS Load Center Train A” fault tree.



Source: Original

Figure B3.4-1. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree



Source: Original

Figure B3.4-2. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train A

### B3.4.1.7 Cut Sets

Table B3.4-4 contains the top 25 cut sets accounting for 97% of the system failure probability for the “Loss of AC Power to CRCF ITS Load Center Train A” fault tree.

Table B3.4-4. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train A

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
17.99	17.99	5.378E-03	060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 Fails	5.378E-03
30.75	12.76	3.816E-03	060-#EEE-LDCNTRA-C52-SPO	ITS Load Center A Feed Circuit Breaker (AC) Spurious Operation	3.816E-03
43.51	12.76	3.816E-03	060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 Feed Breaker Spurious Operation	3.816E-03
53.33	9.82	2.937E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
63.15	9.82	2.937E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
72.00	8.85	2.646E-03	26D-#EEESWGRDGA-AHU-FTR	13.8 kV ITS Switchgear room Air Handling Unit Fails	2.646E-03
80.56	8.56	2.559E-03	060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-02
			060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	5.059E-02
88.26	7.70	2.302E-03	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			LOSP	Loss of offsite power	2.990E-03
89.73	1.47	4.391E-04	26D-#EEE-SWGRDGA-BUA-FOH	13.8 kV ITS Switchgear A Failure	4.391E-04
91.20	1.47	4.391E-04	060-#EEE-LDCNTRA-BUA-FOH	CRCF ITS Load Center A Fails	4.391E-04
92.33	1.13	3.380E-04	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			27A-#EEN-OPENBS2-BUA-FOH	13.8 kV Open Bus 2 Bus Failure	4.391E-04
93.03	0.70	2.095E-04	060-#EEE-CRCF1-A-XMR-FOH	CRCF ITS Train A Transformer Failure	2.095E-04
93.37	0.34	1.027E-04	060-VCT0-EXH-005-CTL-FOD	CRCF ITS Elec Exh fan 00005 Controller Fails	2.030E-03
			060-VCT0-EXH-006-FAN-FTR	CRCF ITS Elec Exh. Fan Fails to Run	5.059E-02
93.71	0.34	1.027E-04	060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-02

Table B3.4-4. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train A  
(Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
			060-VCT0-EXH006-CTL-FOD	CRCF ITS Elec Exh Fan 0006 Controller Fails	2.030E-03
94.05	0.34	1.025E-04	060-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	1.025E-04
			060-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	9.999E-01
			060-#EEE-LDCNTRB-BUA-ROE	ITS Failure to Restore Load Center Train B post maintenance	1.000E+00 0
94.39	0.34	1.022E-04	060-VCT0-EXH-005-FAN-FTR	CRCF ITS Elec Exhaust Fan 00005 Fails to Run	5.059E-02
			060-VCT0-EXH-006-FAN-FTS	CRCF ITS Elec Exh fan 00006 Fails to Start	2.020E-03
94.72	0.33	9.777E-05	26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
95.05	0.33	9.777E-05	26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
95.38	0.33	9.777E-05	26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
95.71	0.33	9.777E-05	26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS2DGA-C52-SPO	13.8 kV Open Bus 2 ITS Load Breaker Spurious Operation	3.816E-03
96.04	0.33	9.777E-05	26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
96.37	0.33	9.777E-05	26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
96.70	0.33	9.777E-05	26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
97.03	0.33	9.777E-05	26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room Fan 4 (Motor-Driven) Fails to Run	2.562E-02

Table B3.4-4. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train A  
(Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
			26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed Breaker Spurious Operation	3.816E-03
97.32	0.29	8.590E-05	26D-#EEY-ITSDG-A-#DG-FTR	ITS Diesel Generator A Fails to Run	7.698E-01
			27A-#EEN-OPNBS1A-SWP-SPO	13.8 kV Open Bus 2 to ITS Div A Electric Power Switch Spur. Xfer	1.116E-04

NOTE: AC = alternating current; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator; Div = division elec = electrical; exh = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation; Prob. = probability; Spur. = spurious; SWGR = switch gear; Xfer = transfer.

Source: Original

### B3.4.2 Loss of AC Power to CRCF ITS Load Center Train B

#### B3.4.2.1 Description

CRCF confinement following the potential breach of a waste canister is provided, in part, by the CRCF ITS HVAC system. The ITS AC power system provides the AC power needed to operate the ITS HVAC system equipment. This fault tree models the components that are required to provide AC power from either the normal offsite power supplies or from ITS diesel generator B to ITS load center B.

#### B3.4.2.2 Success Criteria

Success criteria for this train of the ITS AC power system is providing AC power from either the normal power system or from the ITS diesel generator (DG train B) to the ITS HVAC division powered through CRCF ITS load center train B. The AC power system must operate in support of the ITS HVAC system for as long as necessary to successfully provide confinement after the potential release of material from a breached canister. Therefore, the mission time (the period for which AC power must be supplied to the ITS HVAC system) is the same for the ITS AC power system as it is for the ITS HVAC system, 720 hours.

#### B3.4.2.3 Design Requirements and Features

##### Requirements

Each ITS diesel generator has support systems that are independent from the support system for the other diesel generator. Independent support systems include:

- Fuel oil systems
- HVAC systems to include the ITS diesel generator room and 13.8 kV ITS switchgear room systems

- Lube oil system
- ITS diesel generator cooling systems
- Diesel generator start system.

## Features

The 13.8 kV ITS switchgear is isolated from the main switchyard upon a loss of power in the switchyard, either due to a LOSP or from failures within the switchyard.

The CRCF load is shed from the 13.8 kV switchgear upon a loss of power indication.

A load sequencer controls the loading of the diesel generator onto the 13.8 kV ITS switchgear upon the ITS diesel generator reaching rated output. The same load sequencer controls reloading the CRCF loads onto the ITS AC power system.

Environmental systems are provided to maintain the temperature in the various EDGF rooms within acceptable levels. This includes a fan system for the diesel generator room and air handling units for the 13.8 kV ITS switchgear and battery room.

### B3.4.2.4 Fault Tree Model

The top event in this fault tree is “Loss of AC Power to CRCF ITS Load Center Train B.” This is defined as a failure of the normal and ITS onsite power supplies to provide power to ITS Load Center B. Faults considered in the evaluation of this top event include: failure of components in the normal AC power system, failure of the ITS diesel generator subsystem, human events that can contribute to onsite system failures resulting in a power loss at the CRCF and a LOSP. In this fault tree offsite power is not modeled as an initiating event, but as a system failure. The value used for this event represents the probability that offsite power would be lost in the 720 hours following a possible radioactive release from a damaged canister.

### B3.4.2.5 Basic Event Data

Table B3.4-5 contains a list of basic events used in the “Loss of AC Power to CRCF ITS Load Center Train B” fault tree. Included are component failures, maintenance errors and the human events and the CCF events identified in the previous two sections. The data, for both random and CCF failures, used to develop the failure probabilities associated with these basic events comes from the component reliability data analysis in Attachment C. The human reliability analyses in Attachment E, provides the human error probabilities (HEP).

Mission times for the various components are based on the following:

- Fault exposure time (168 hours) for events limited to one week maintenance outages (train OOS for maintenance)

- Mission time (360 hours) for operation of standby equipment that would operate after a LOSP. Distribution of the occurrence of an LOSP is evenly distributed over the 720 hours after a potential radiological release; average mission time is therefore 360 hours. Average fault exposure time for standby components tested monthly.
- Mission time (720 hours) for operating components

While some of the components are normally in operation, it is possible for any of the components to be out of service (OOS) for maintenance. With train A of AC power OOS (resulting in train B of the facility TIS HVAC being OOS) train A provides support to an operable ITS HVAC train A. The intent of the maintenance events modeled is for the events to address maintenance on any component in that AC power division. This is true for the components normally in operation and the standby components. The maintenance unavailability represented by the ITS load center maintenance events model the unavailability of any component from the 13.8 kV ITS switchgear through the ITS load center. The maintenance unavailability represented by the ITS diesel generator maintenance events represent the unavailability of any of the components or systems that would prevent the ITS diesel generator from starting and loading onto the 13.8 kV ITS switchgear. As noted earlier, all of the human events are associated with the failure to restore a component to operable or standby status after maintenance. The operator-related events shown in the following table are combination events: they include the probability that the component has been taken OOS for maintenance and that site personnel have not restored the component to operable or standby status. A screening value of 0.1 has been used for the HEP in all cases.

Table B3.4-5. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train B Fault Trees

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS Transformers CCF	1	4.920E-06	4.920E-06	2.910E-07	3.380E+01
060-#EEE-CRCF1-B-XMR-FOH	CRCF ITS Transformer Train B Failure	3	2.095E-04	0.000E+00	2.910E-07	7.200E+02
060-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
060-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
060-#EEE-LDCNTRB-BUA-FOH	CRCF ITS Load Center B Fails	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
060-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	3	1.025E-04	0.000E+00	6.100E-07	1.680E+02
060-#EEE-LDCNTRB-BUA-ROE	ITS Failure to Restore Load Center Train B post maintenance	1	1.025E-05	1.025E-05	7.910E-07	1.680E+01
060-#EEE-LDCNTRB-C52-FOD	13.8 kV ITS SWGR to CRCF ITS LC B Circuit Breaker Fails on Demand	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
060-#EEE-LDCNTRB-C52-SPO	CRCF ITS Load Center Circuit Breaker (AC) Spur Op	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
060-#EEE-LDCNTRS-C52-CCF	Common cause failure of the ITS Load Center feed breakers to reclose	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 Feed Breaker Spurious Operation	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 Failure	3	5.378E-03	0.000E+00	7.490E-06	7.200E+02
060-VCT0-AHU0004-AHU-FTR	CRCF ITS ELec AHU 00004 Fails to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
060-VCT0-AHU0004-CTL-FOD	CRCF ITS Elec AHU 00004 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-AHU0004-FAN-FTS	CRCF ITS Elec AHU 00004 Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
060-VCT0-AHU0202-AHU-CCR	CCF of standby CRCF ITS Elec AHUs to start/run	1	1.600E-04	1.600E-04	0.000E+00	0.000E+00
060-VCT0-EXH-007-CTL-FOD	CRCF ITS Elec Exh fan 00007 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh. Fan 8 Fails to Run	3	5.059E-02	0.000E+00	7.210E-05	7.200E+02
060-VCT0-EXH-008-FAN-FTS	CRCF ITS Elec Exh fan 00008 Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
060-VCT0-EXH008-CTL-FOD	CRCF ITS Elec Exh Fan 0008 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCT0-EXH0507-FAN-CCR	CCF of running Exh fans for CRCF ITS Elec.	1	1.200E-03	1.200E-03	0.000E+00	0.000E+00
060-VCT0-EXH0608-FAN-CCF	CCF to start/run: standby Exh fans for the CRCF ITS Elec	1	1.300E-03	1.300E-03	0.000E+00	0.000E+00
060-VCT0-AHU0003-AHU-FTR	CRCF ITS Elec AHU 00003 Fails to run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02

B3-35

March 2008

Table B3.4-5. Basic Event Probability for The Loss of AC Power to CRCF ITS Load Center Train B Fault Trees (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
060-VCTO-AHU0003-CTL-FOD	CRCF ITS Elec AHU 00003 Controller Fails	1	2.030E-03	2.030E-03	0.000E+00	0.000E+00
060-VCTO-AHU0103-AHU-CCR	CCF of the running CRCF ITS Elec AHUs to continue to run	1	6.200E-05	6.200E-05	0.000E+00	0.000E+00
26D-##EG-DAYTNKB-TKF-FOH	ITS DG B Day fuel tank fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EG-FLITLKB-IEL-FOD	ITS DG B fuel transfer pumps Interlock Failure	1	2.750E-05	2.750E-05	0.000E+00	0.000E+00
26D-##EG-FTP1DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP1DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 1 (Motor Driven) Fails to Start	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FTP2DGB-PMD-FTR	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Run	3	1.234E-02	0.000E+00	3.450E-05	3.600E+02
26D-##EG-FTP2DGB-PMD-FTS	ITS DG B Fuel Transfer Pump 2 (Motor Driven) Fails to Start on Demand	1	2.500E-03	2.500E-03	0.000E+00	0.000E+00
26D-##EG-FULPMPB-PMD-CCR	CCF of ITS DG B fuel pumps to run	1	2.900E-04	2.900E-04	0.000E+00	0.000E+00
26D-##EG-FULPMPB-PMD-CCS	CCF of ITS DG B fuel pumps to start	1	1.200E-04	1.200E-04	0.000E+00	0.000E+00
26D-##EG-HVACFN1-FAN-FTR	ITS DG B room Fan 1 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN1-FAN-FTS	ITS DG B room Fan (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN2-FAN-FTS	ITS DG B Room Fan (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN3-FAN-FTR	ITS DG B room Fan 3 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN3-FAN-FTS	ITS DG B Room Fan 3 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	3	2.562E-02	0.000E+00	7.210E-05	3.600E+02
26D-##EG-HVACFN4-FAN-FTS	ITS DG B Room Fan 4 (Motor-Driven) Fails to Start	1	2.020E-03	2.020E-03	0.000E+00	0.000E+00
26D-##EG-STRTDGB-C72-SPO	13.8 kV ITS SWGR Battery B Circuit Breaker (DC) Spur Op	3	3.851E-04	0.000E+00	1.070E-06	3.600E+02 <sup>d</sup>
26D-##EG-WKTNK_B-TKF-FOH	ITS DG B Bulk Fuel Tank Fails	3	1.584E-04	0.000E+00	4.400E-07	3.600E+02
26D-##EGBATCHRGB-BYC-FOH	ITS DG B Battery Charger failure	3	1.276E-03	0.000E+00	7.600E-06	1.680E+02 <sup>c</sup>
26D-###SWGRDGB-AHU-FTR	EDGF Switchgear Room Air Handling Unit Failure to Run	3	2.646E-03	0.000E+00	3.680E-06	7.200E+02
26D-###SWGRDGB-BUA-FOH	13.8 kV ITS Switchgear B Bus Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02
26D-###E208_DGB-BUD-FOH	ITS DG B DC Panel Failure	3	8.640E-05	0.000E+00	2.400E-07	3.600E+02 <sup>d</sup>
26D-###EY-DGBLOAD-C52-FOD	ITS DG B Load Breaker (AC) Fails to Close	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00

B3-36

March 2008

Table B3.4-5. Basic Event Probability for The Loss of AC Power to CRCF ITS Load Center Train B Fault Trees (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG Load Breakers to close	1	1.050E-04	1.050E-04	0.000E+00	0.000E+00
26D-#EEY-ITS-DGB-#DG-FTS	Diesel Generator Fails to Start	1	8.380E-03	8.380E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-MTN	ITS DG A OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-MTN	ITS DG B OOS Maintenance	1	1.950E-03	1.950E-03	0.000E+00	0.000E+00
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly restore ITS DG-B to service	1	1.950E-04	1.950E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B Fail to Run	1	1.800E-02	1.800E-02	0.000E+00	0.000E+00
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to Start	1	3.900E-04	3.900E-04	0.000E+00	0.000E+00
26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	3	7.698E-01	0.000E+00	4.080E-03	3.600E+02
26D-#EEY-OB-SWGB-C52-FOD	13.8 kV Feed Breaker (from SWYD) Fails on Demand	1	2.240E-03	2.240E-03	0.000E+00	0.000E+00
26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
26D-#EEY-OB-SWGS-C52-CCF	Common cause failure of 13.8 kV ITS SWGR feed breakers to open	1	1.040E-04	1.040E-04	0.000E+00	0.000E+00
26D-#EG-BATTERYB-BTR-FOD	ITS SWGR Control Battery B No Output	1	8.200E-03	8.200E-03	0.000E+00	0.000E+00
26D-#EG-LDSQNCRB-SEQ-FOD	ITS DG B load sequencer fails	1	3.330E-03	3.330E-03	0.000E+00	0.000E+00
26D-#EG-LOCKOUTB-RLY-FTP	13.8 kV ITS SWGR Lockout Relay (Power) Fails to Open CB	3	3.152E-03	0.000E+00	8.770E-06	3.600E+02
27A-#EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3	3.816E-03	0.000E+00	5.310E-06	7.200E+02
27A-#EEN-OPENBS4-BUA-FOH	13.8 kV Open Bus 4 Bus Failure	3	4.391E-04	0.000E+00	6.100E-07	7.200E+02

B3-37

March 2008

Table B3.4-5. Basic Event Probability for The Loss of AC Power to CRCF ITS Load Center Train B Fault Trees (Continued)

Name	Description <sup>b</sup>	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
27A-#EEN-OPNBS3B-SWP-SPO	13.8 kV Open Bus 4 to ITS B Electric Power Switch Spur Xfer	3	1.116E-04	0.000E+00	1.550E-07	7.200E+02
LOSP*	Loss of Offsite Power	1	2.99E-03	2.99E-03	0.000E+00	0.000E+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> The designation of a circuit breaker as AC or DC refers to the system designation for the circuit breaker, it is not representative of the motive power for the circuit breaker.

<sup>c</sup> The failure of the battery charger would result in eventual depletion of the battery and a low power indication on both the battery and the DC bus. The 168 hr mission time was selected as a conservative estimation for the detection time of this failure.

<sup>d</sup> The mission times for the DC bus related failure rates do not take credit for any monitoring of bus status, which would provide nearly instantaneous indication of a bus failure or loss of power to the bus. The standby component mission time was used conservatively.

LOSP\* represents the probability of losing offsite power during the 720 hours HVAC is required after any breach of a container releases radioactive material. It is based on a loss of offsite power frequency of 3.59E-02/year from NUREG/CR6890 Vol. 1 (Ref. B3.1.19).

AC = alternating current; AHU = air handling unit; Calc. = calculation; CCF = common-cause failure; DC = direct current; DG = diesel generator; Div = division; elc = electrical; exh = exhaust; ITS = important to safety; kV = kilovolt; Miss. = mission; OOS = out of service; op = operation; Prob. = probability; Spur. = spurious; SWGR = switch gear; Xfer = transfer.

Source: Original

### B3.4.2.5.1 Human Failure Events

Four basic HFEs (Table B3.4-6) are associated with human error. All of the HFEs are associated with the failure to properly restore components to operable status following maintenance. The first two shown in Table B3.4-6 are associated with the failure to restore the normal power supply to the CRCF ITS load centers after maintenance. The last two are representative of the failure to restore the ITS diesel generators (and any other components that would prevent the ITS diesel generator from starting or loading) to service after maintenance. These events are combination events consisting of the probability that a component was removed for maintenance and the failure of plant operators (assigned a screening value of 0.1) to restore the component after maintenance.

Table B3.4-6. Human Failure Events

Name	Description
060-#EEE-LDCNTRA-BUA-ROE	Failure to restore ITS load center train A post maintenance
060-#EEE-LDCNTRB-BUA-ROE	Failure to restore ITS load center train B post maintenance
26D-#EEY-ITSDG-A-#DG-RSS	Failure to properly return ITS DG A to service
26D-#EEY-ITSDG-B-#DG-RSS	Failure to properly return ITS DG B to service

NOTE: DG = diesel generator; ITS = important to safety.

Source: Original

### B3.4.2.5.2 Common-Cause Failures

Twelve of the fourteen CCF failures identified earlier (Table B3.4-7) have been included in the analysis of the loss of ITS AC power to the ITS load center train A. Ten of the CCF events affect both trains of ITS AC Power. Two affect only this train of the system. The remaining two affect only the other train of the system. Two are associated with the ITS diesel generators: CCF failure of the ITS diesel generators to start and CCF failure of the ITS diesel generators to run.

The CCF failure of the ITS diesel generator fuel oil system incorporates two CCF failures: The CCF failure of the two fuel oil pumps to start and the CCF failure of the pumps to run. Three circuit breaker CCF events were considered. These are the CCF failure of the (1) 13.8 kV ITS switchgear feed breakers, from 13.8 kV open buses to open on loss of offsite power, (2) ITS diesel generator load breakers to close when commanded by the load sequencer, and (3) ITS load center feed breakers to close when commanded by the load sequencer. Four CCFs are associated with the CRCF ITS Electrical and Battery Rooms Ventilation System, two for the CCF of exhaust fans to start and run, and two for the CCF of the air handling units to start and run. The last CCF event considered is the CCF failure of the 13.8 kV - 480 V ITS transformers.

All of the CCFs modeled are used on pairs of components with one of two success criteria (i.e., two of two failure criteria). Alpha-factors used to determine the CCF probability are 0.047 for demand failures and 0.0235 for time dependent failures (Table C3-1, CCCG=2, and the associated text). Two CCFs in Table B3.4-7 are used to represent the CCF associated with the failure to start and failure to run for components. For these two CCFs, the appropriate alpha-factors were applied to the start and run portions of the random failure probability to develop a single common cause failure probability for the components.

Table B3.4-7 Common-Cause Basic Events

Name	Description	Alpha-factor
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS Transformers CCF	0.0235
060-#EEE-LDCNTRS-C52-CCF	Common-cause failure of the ITS load center feed breakers to reclose	0.047
26D-##EG-FULPMPB-PMD-CCR	Common-cause failure of ITS DG B fuel pumps to run	0.0235
26D-##EG-FULPMPB-PMD-CCS	Common-cause failure of ITS DG B fuel pumps to start	0.047
26D-#EEY-DGLOADS-C52-CCF	Common-cause failure of ITS DG load breakers to close	0.047
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B fail to run	0.0235
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to start	0.047
26D-#EEY-OB-SWGS-C52-CCF	Common-cause failure of 13.8 kV ITS SWGR feed breakers to open	0.047
060-VCT0-AHU0202-AHU-CCR	CCF of standby CRCF ITS Elec AHUs to start/run	0.047 start 0.0235 run
060-VCT0-EXH0507-FAN-CCR	CCF of running Exh fans for CRCF ITS Elec.	0.0235
060-VCT0-EXH0608-FAN-CCF	CCF to start/run: standby Exh fans for the CRCF ITS Elec	0.047 start 0.0235 run
060-VCT0-AHU0103-AHU-CCR	CCF of the running CRCF ITS Elec AHUs to continue to run	0.0235

NOTE: AHU = air handling unit; CCF = common-cause failure, CRCF = Canister Receipt and Closure Facility; DG = diesel generator; elec = electrical; exh = exhaust; ITS = important to safety; SWGR = switch gear.

Source: Original

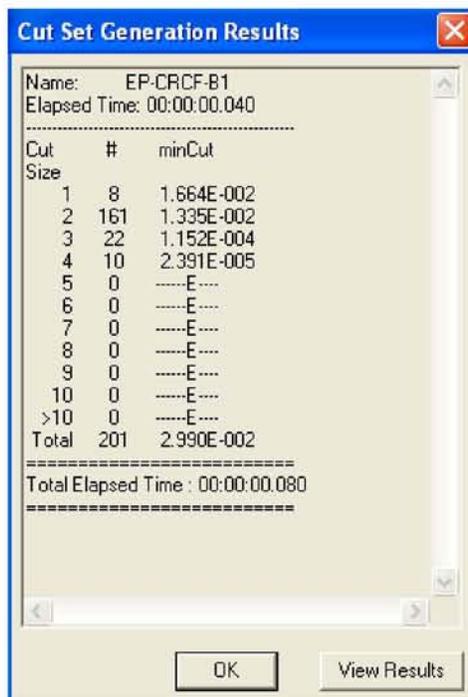
### B3.4.2.6 Uncertainty and Cut Set Generation

Figure B3.4-3 contains the uncertainty results obtained from running the fault tree for “Loss of AC Power to CRCF ITS Load Center Train B”. Figure B3.4-4 provides the cut set generation results for the “Loss of AC Power to CRCF ITS Load Center Train B”.



Source: Original

Figure B3.4-3. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train B Fault Tree



Source: Original

Figure B3.4-4. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train B

### B3.4.2.7 Cut Sets

Table B3.4-8 contains the top 25 cut sets that contribute 97% of the total system failure probability for the “Loss of AC Power to CRCF ITS Load Center Train B” fault tree.

Table B3.4-8. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train B

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
17.99	17.99	5.378E-03	060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 Failure	5.378E-03
30.75	12.76	3.816E-03	060-#EEE-LDCNTRB-C52-SPO	CRCF ITS Load Center Circuit Breaker (AC) Spur Op	3.816E-03
43.51	12.76	3.816E-03	060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 Feed Breaker Spurious Operation	3.816E-03
53.33	9.82	2.937E-03	26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-01
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-03
63.15	9.82	2.937E-03	26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-01
			27A-#EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-03
72.00	8.85	2.646E-03	26D-#EEE-SWGRDGB-AHU-FTR	EDGF Switchgear Room Air Handling Unit Failure to Run	2.646E-03
80.56	8.56	2.559E-03	060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-02
			060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh. Fan 8 Fails to Run	5.059E-02
88.26	7.70	2.302E-03	26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-01
			LOSP	Loss of offsite power	2.990E-03
89.73	1.47	4.391E-04	060-#EEE-LDCNTRB-BUA-FOH	CRCF ITS Load Center B Fails	4.391E-04
91.20	1.47	4.391E-04	26D-#EEE-SWGRDGB-BUA-FOH	13.8 kV ITS Switchgear B Bus Failure	4.391E-04
92.33	1.13	3.380E-04	26D-#EEY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-01
			27A-#EEN-OPENBS4-BUA-FOH	13.8 kV Open Bus 4 Bus Failure	4.391E-04
93.03	0.70	2.095E-04	060-#EEE-CRCF1-B-XMR-FOH	CRCF ITS Transformer Train B Failure	2.095E-04
93.37	0.34	1.027E-04	060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-02
			060-VCT0-EXH008-CTL-FOD	CRCF ITS Elec Exh Fan 0008 Controller Fails	2.030E-03

Table B3.4-8. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train B (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
93.71	0.34	1.027E-04	060-VCT0-EXH-007-CTL-FOD	CRCF ITS Elec Exh fan 00007 Controller Fails	2.030E-03
			060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh. Fan 8 Fails to Run	5.059E-02
94.05	0.34	1.025E-04	060-#EEE-LDCNTRA-BUA-MTN	ITS Load Center Train A OOS for Maintenance	9.999E-01
			060-#EEE-LDCNTRA-BUA-ROE	Failure to Restore ITS Load Center Train A post maintenance	1.000E+00
			060-#EEE-LDCNTRB-BUA-MTN	ITS Load Center Train B OOS for Maintenance	1.025E-04
94.39	0.34	1.022E-04	060-VCT0-EXH-007-FAN-FTR	CRCF ITS Elec Exhaust Fan 00007 Fails to Run	5.059E-02
			060-VCT0-EXH-008-FAN-FTR	CRCF ITS Elec Exh fan 00008 Fails to Start	2.020E-03
94.72	0.33	9.777E-05	26D-##EG-HVACFN1-FAN-FTR	ITS DG B room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-03
95.05	0.33	9.777E-05	26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-03
95.38	0.33	9.777E-05	26D-##EG-HVACFN3-FAN-FTR	ITS DG B room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-03
95.71	0.33	9.777E-05	26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR Feed Breaker (AC) Spurious Op	3.816E-03
96.04	0.33	9.777E-05	26D-##EG-HVACFN1-FAN-FTR	ITS DG B room Fan 1 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-03
96.37	0.33	9.777E-05	26D-##EG-HVACFN2-FAN-FTR	ITS DG B room Fan 2 (Motor-Driven) Fails to Run	2.562E-02
			27A-#EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-03

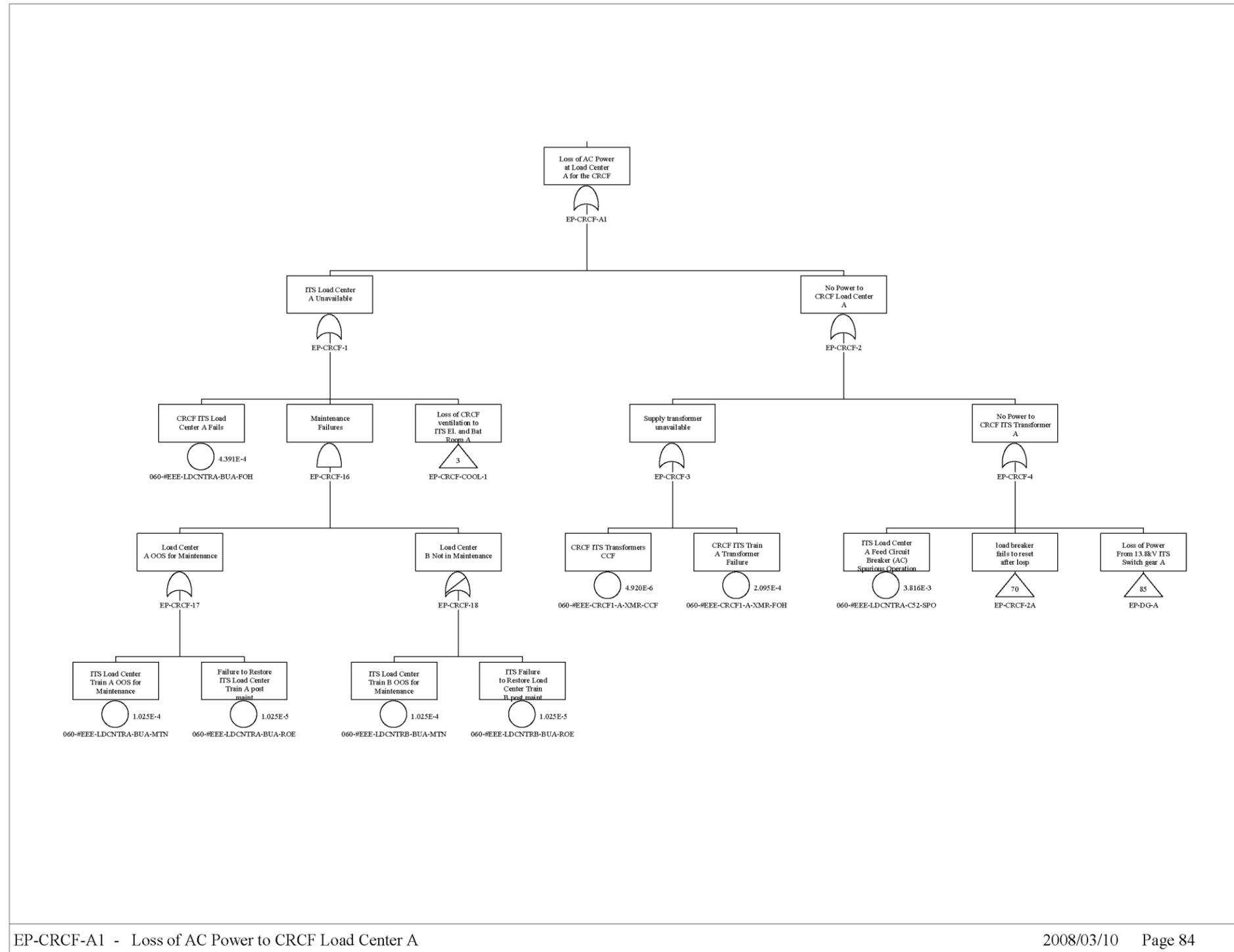
Table B3.4-8. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train B (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
96.70	0.33	9.777E-05	26D-##EG-HVACFN3-FAN-FTR	ITS DG B room Fan 3 (Motor-Driven) Fails to Run	2.562E-02
			27A-###EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-03
97.03	0.33	9.777E-05	26D-##EG-HVACFN4-FAN-FTR	ITS DG B Fan 4 (Motor-Driven) Fails to Run	2.562E-02
			27A-###EEE-BUS3DGB-C52-SPO	13.8 kV Open Bus 4 to ITS B Load Breaker (AC) Spurious Op	3.816E-03
97.32	0.29	8.590E-05	26D-##EY-ITSDGB-#DG-FTR	ITS DG B Fails to Run	7.698E-01
			27A-##EEN-OPNBS3B-SWP-SPO	13.8 kV Open Bus 4 to ITS B Electric Power Switch Spur Xfer	1.116E-04

NOTE: AC = alternating current; CCF = common-cause failure; DG = diesel generator; elec = electrical; exh = exhaust; ITS = important to safety; kV = kilovolt; SWGR = switch gear; Xfer = transfer.

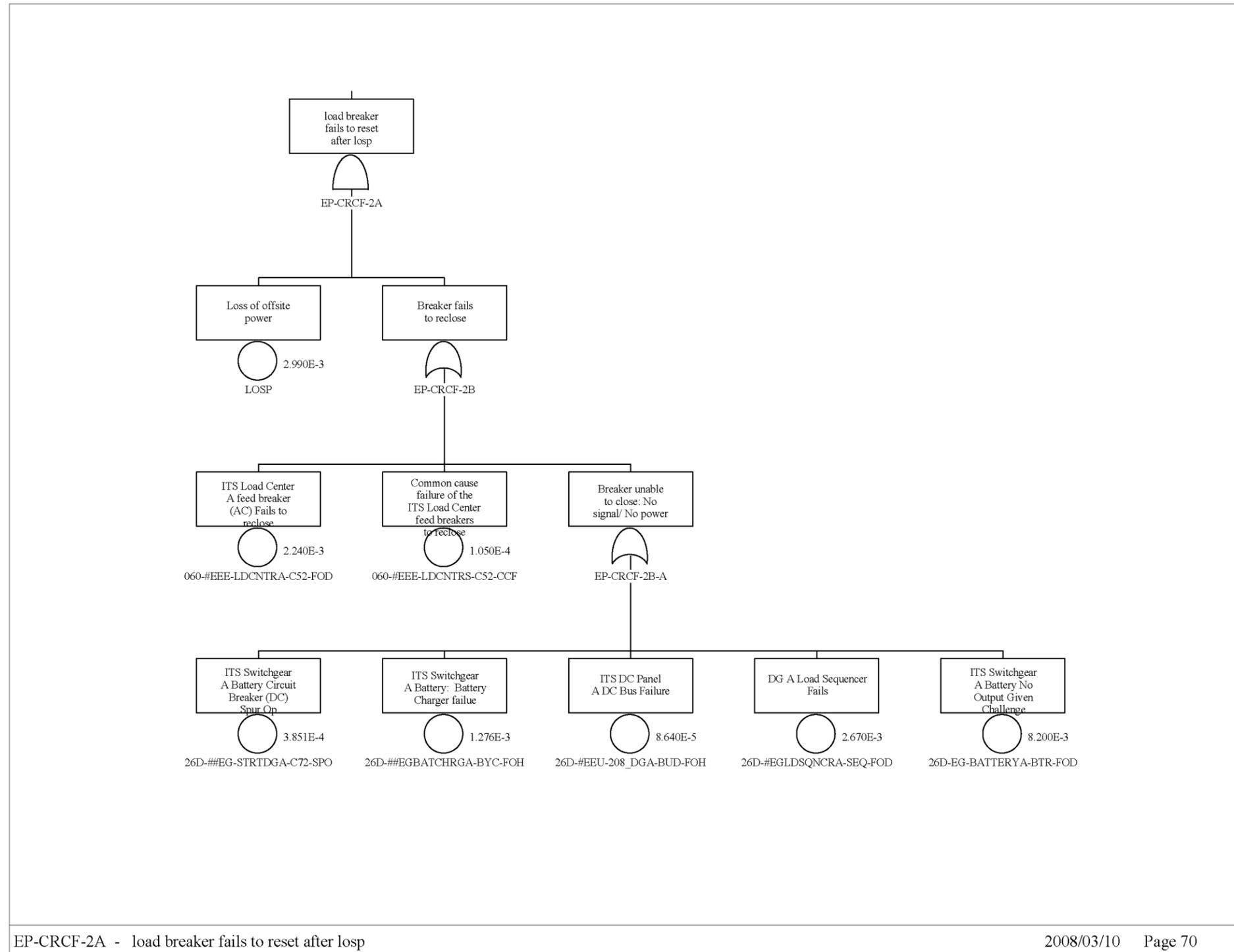
Source: Original

#### B3.4.2.8 AC Power Fault Trees



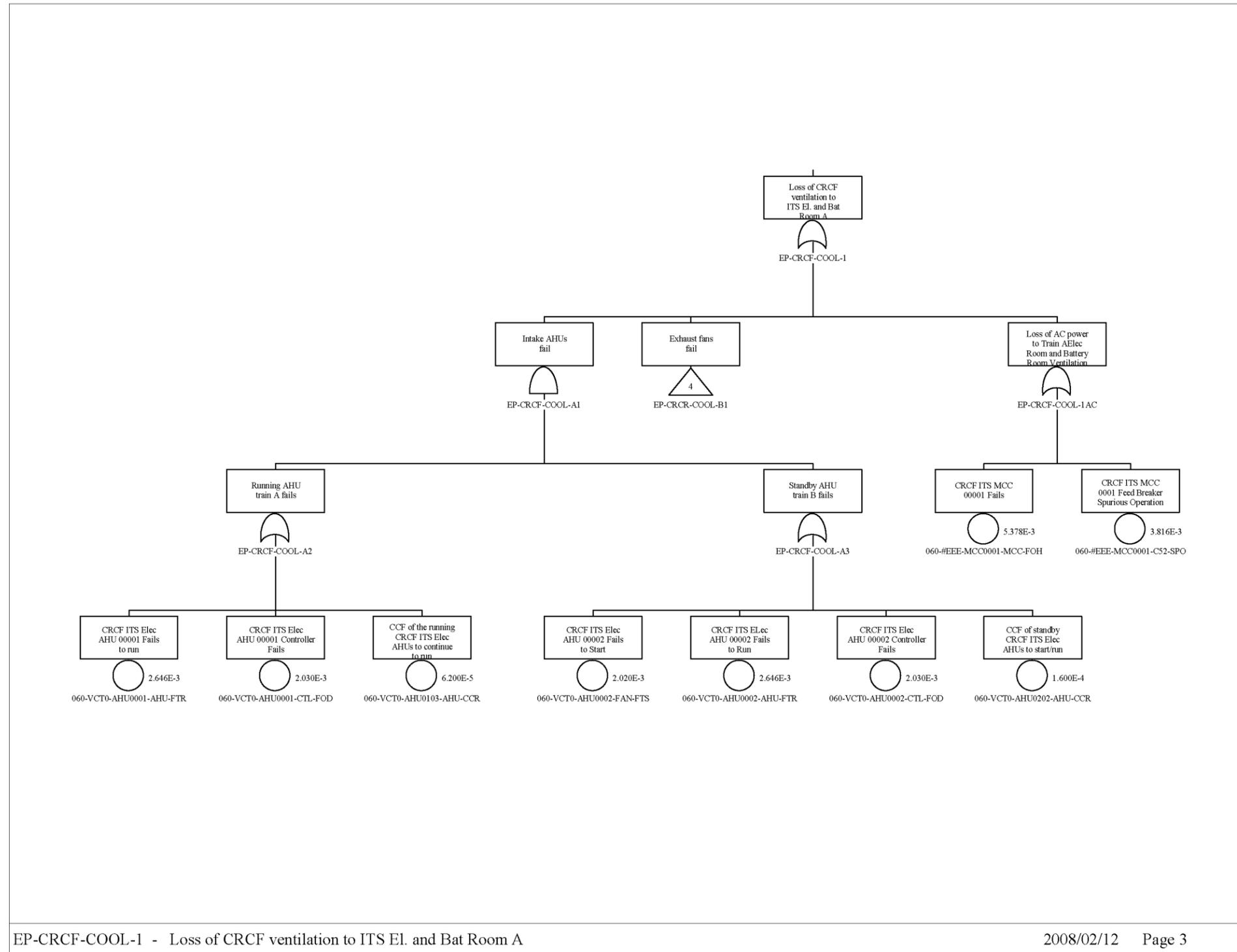
Source: Original

Figure B3.4-5. Loss of Power to CRCF ITS Load Center Train A Sheet 1



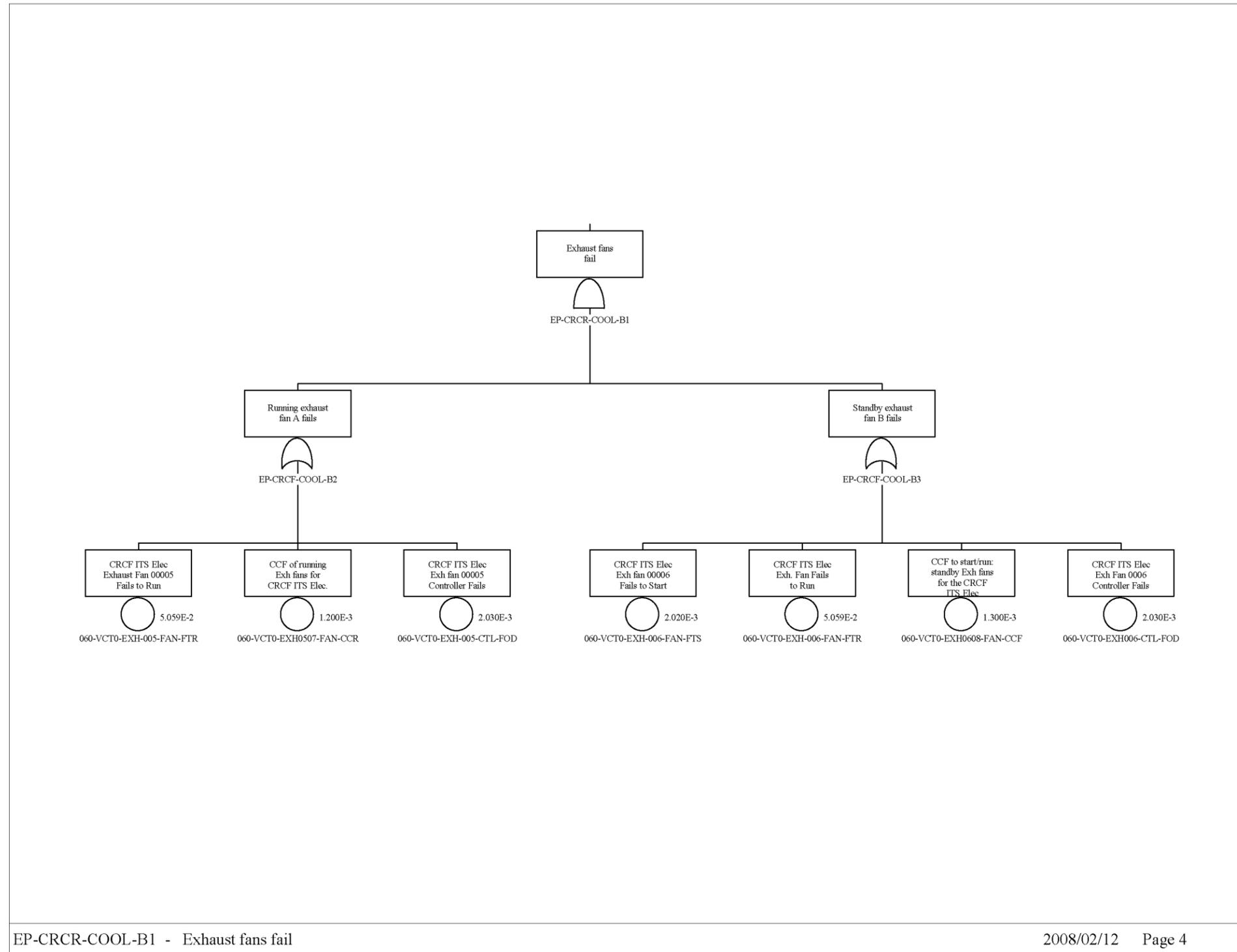
Source: Original

Figure B3.4-6. Loss of Power to CRCF ITS  
Load Center Train A Sheet 2



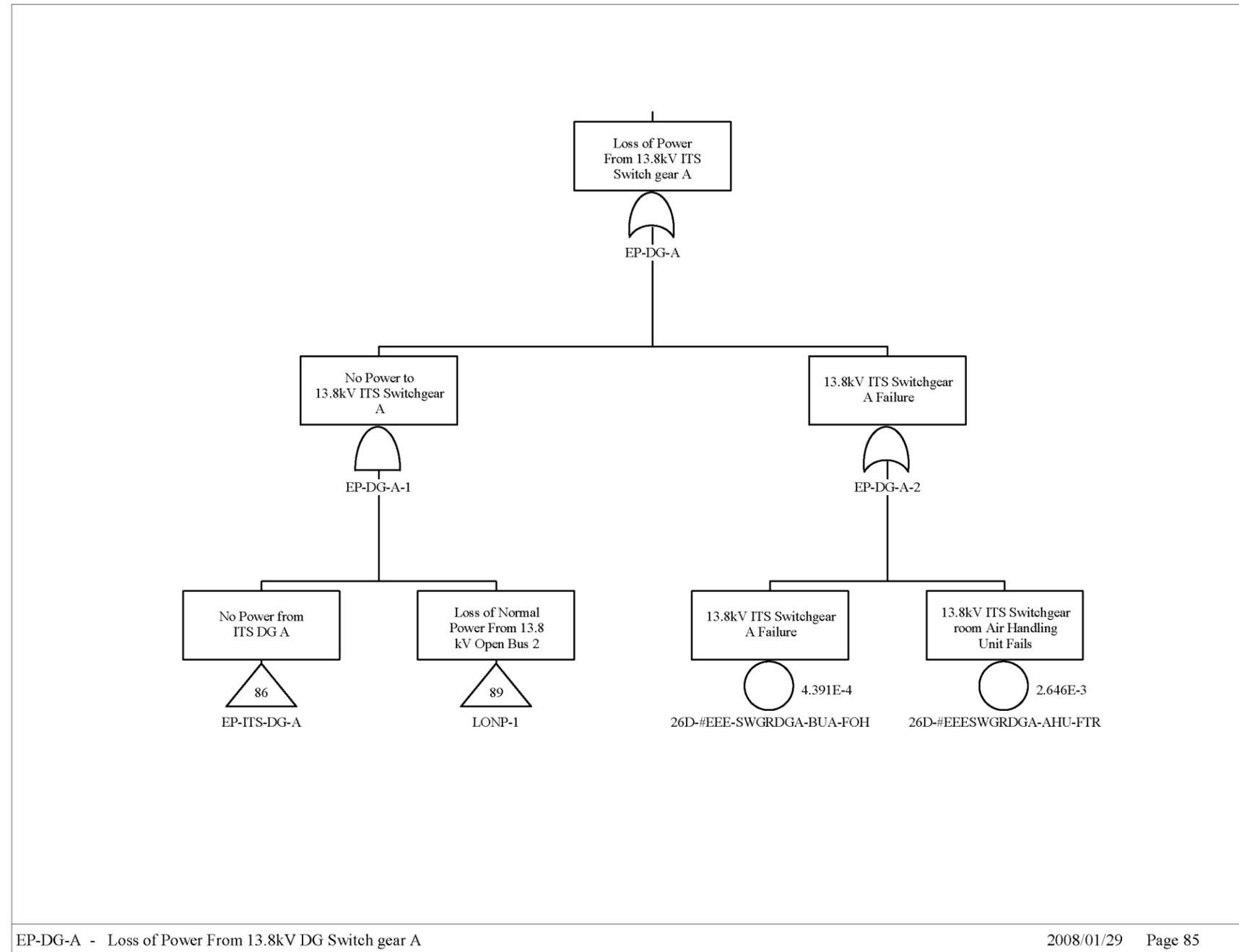
Source: Original

Figure B3.4-7. Loss of Power to CRCF ITS Load Center Train A Sheet 3



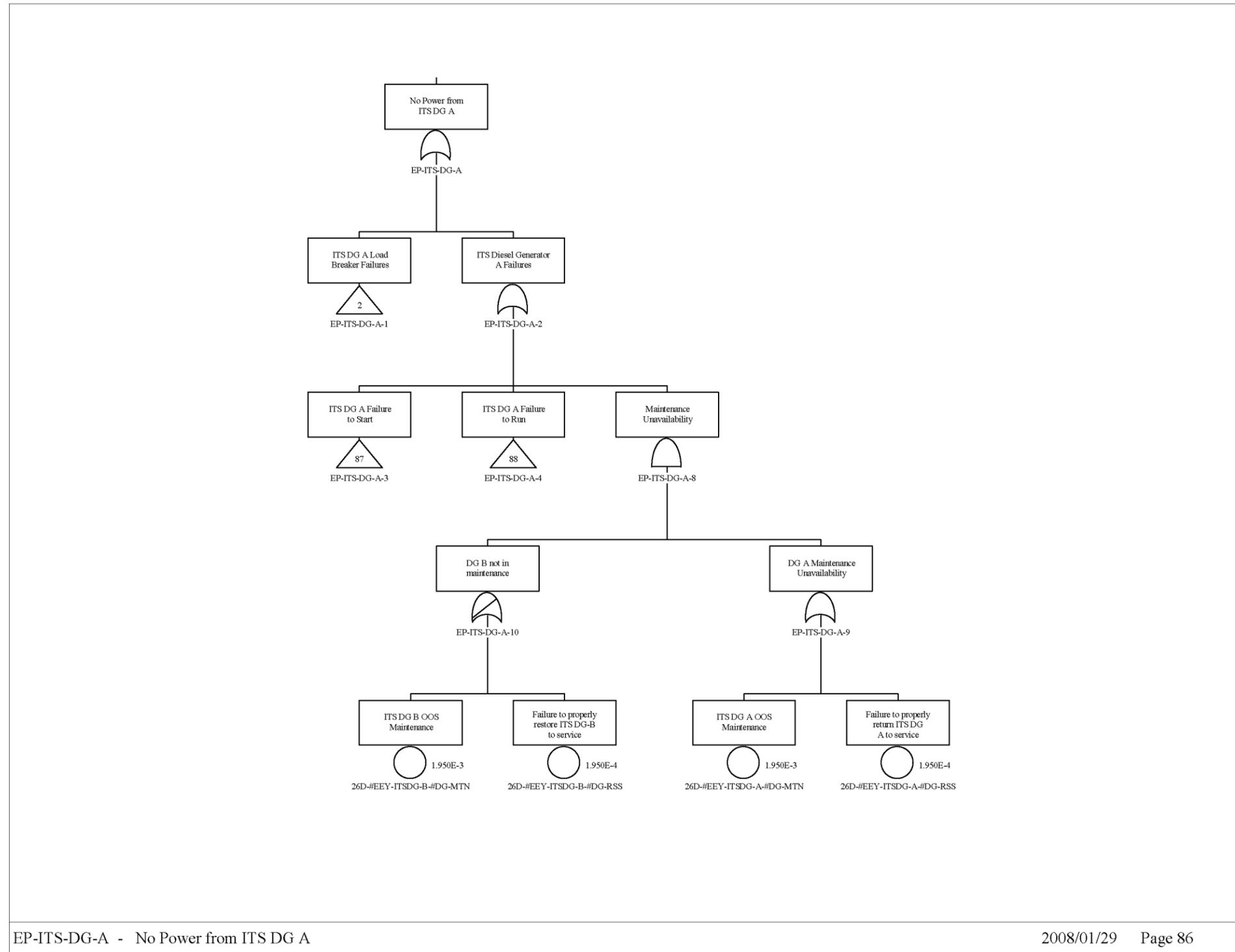
Source: Original

Figure B3.4-8. Loss of Power to CRCF ITS  
Load Center Train A Sheet 4



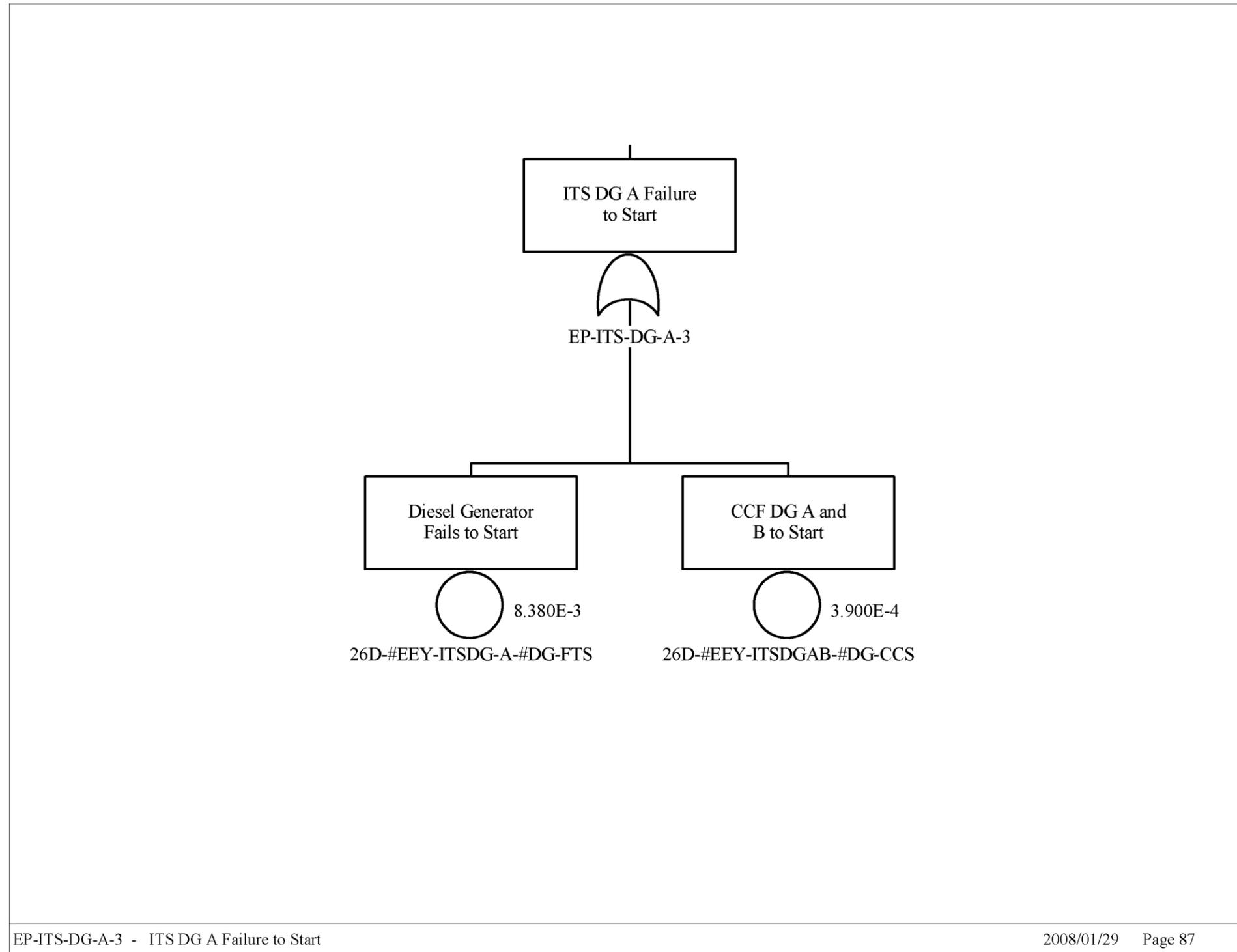
Source: Original

Figure B3.4-9. Loss of Power to CRCF ITS Load Center Train A Sheet 5



Source: Original

Figure B3.4-10. Loss of Power to CRCF ITS Load Center Train A Sheet 6

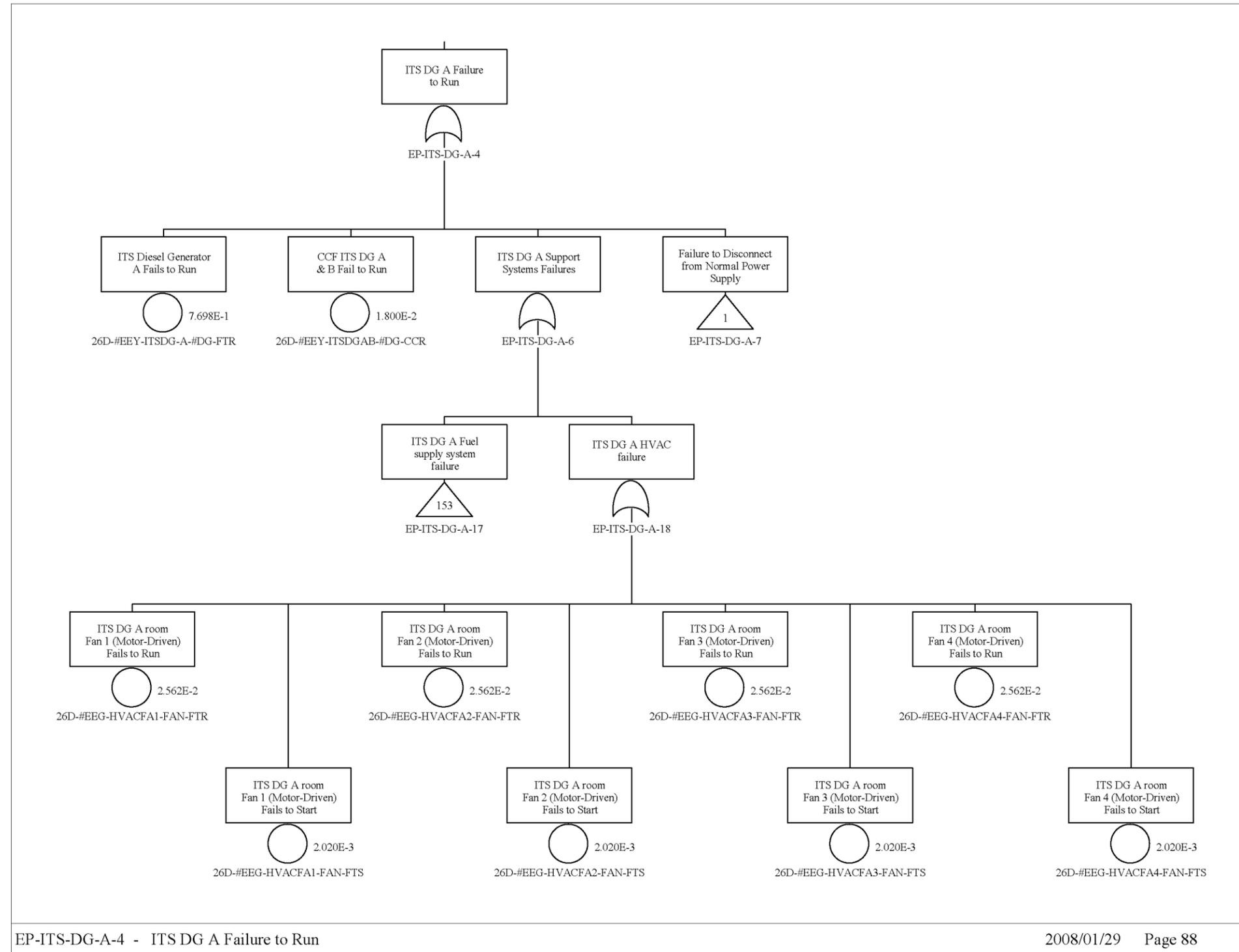


EP-ITS-DG-A-3 - ITS DG A Failure to Start

2008/01/29 Page 87

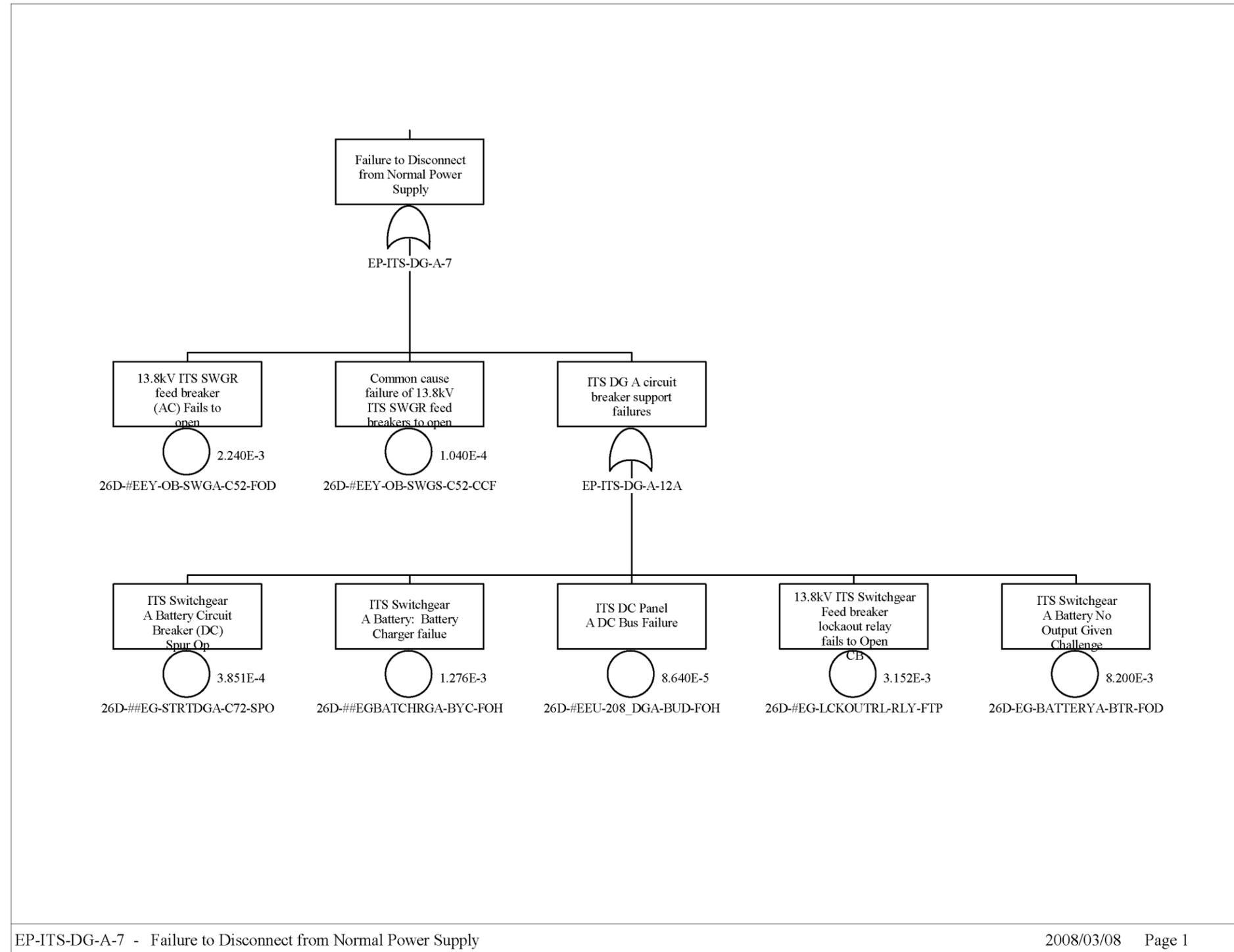
Source: Original

Figure B3.4-11. Loss of Power to CRCF ITS  
Load Center Train A Sheet 7



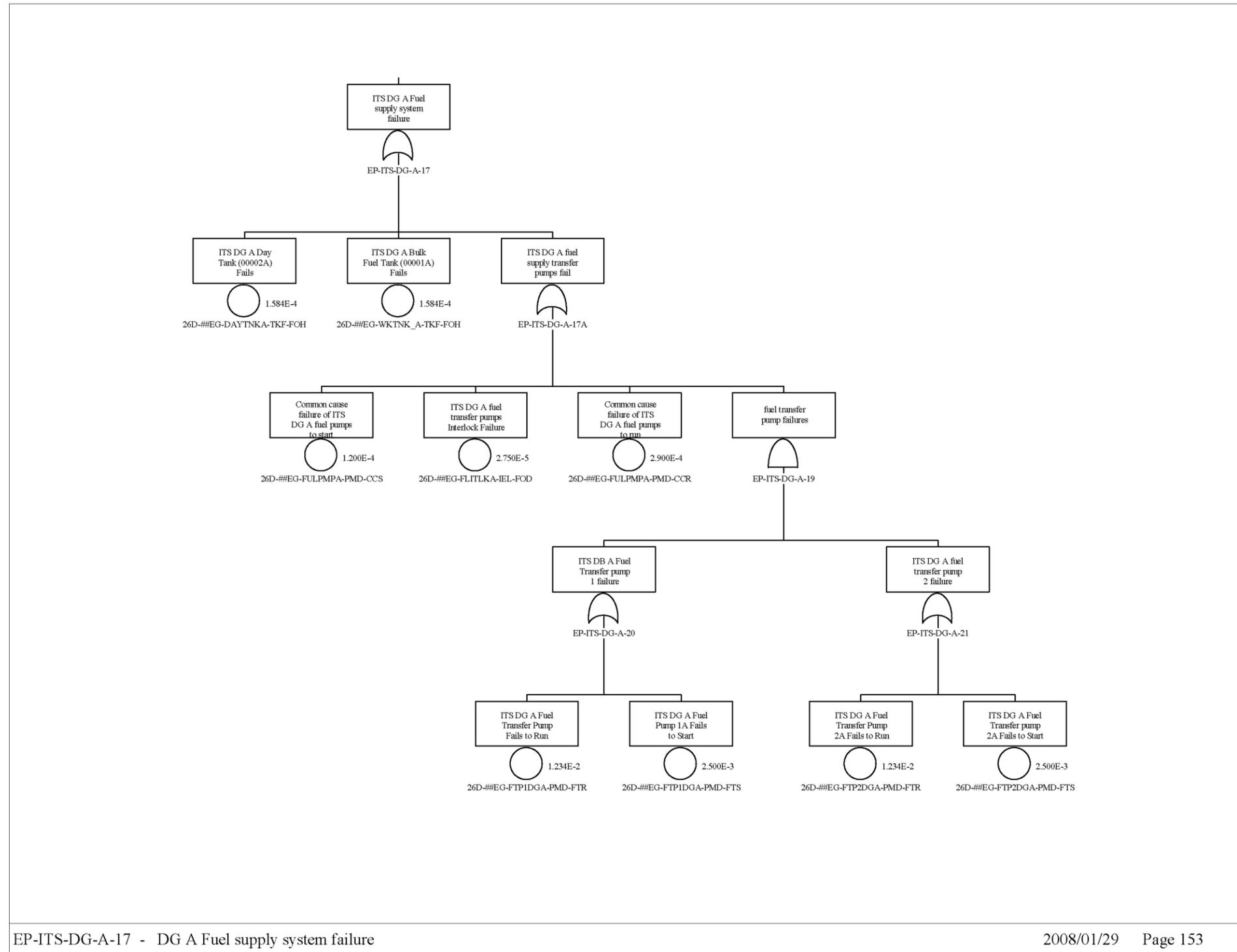
Source: Original

Figure B3.4-12. Loss of Power to CRCF ITS  
Load Center Train A Sheet 8



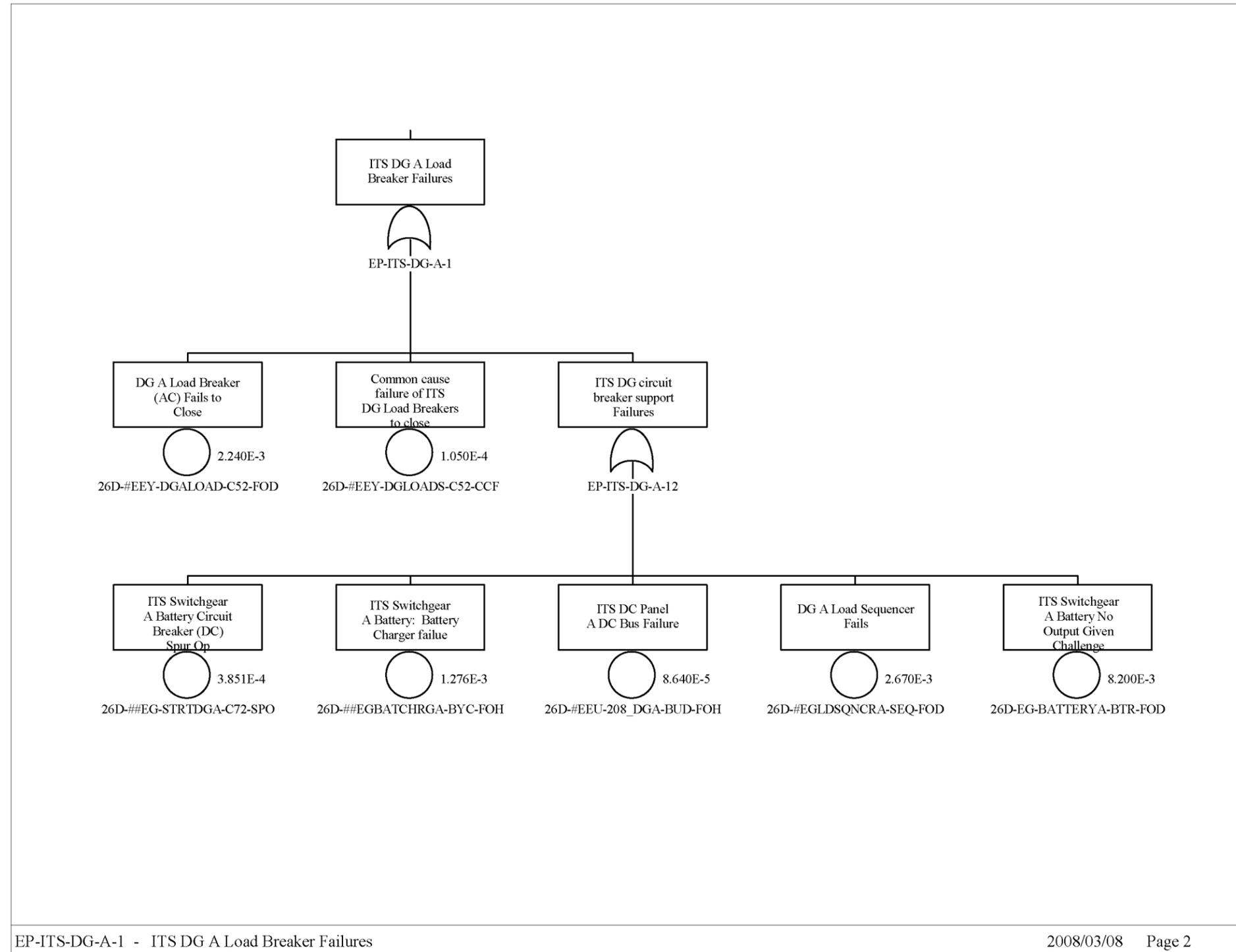
Source: Original

Figure B3.4-13. Loss of Power to CRCF ITS Load Center Train A Sheet 9



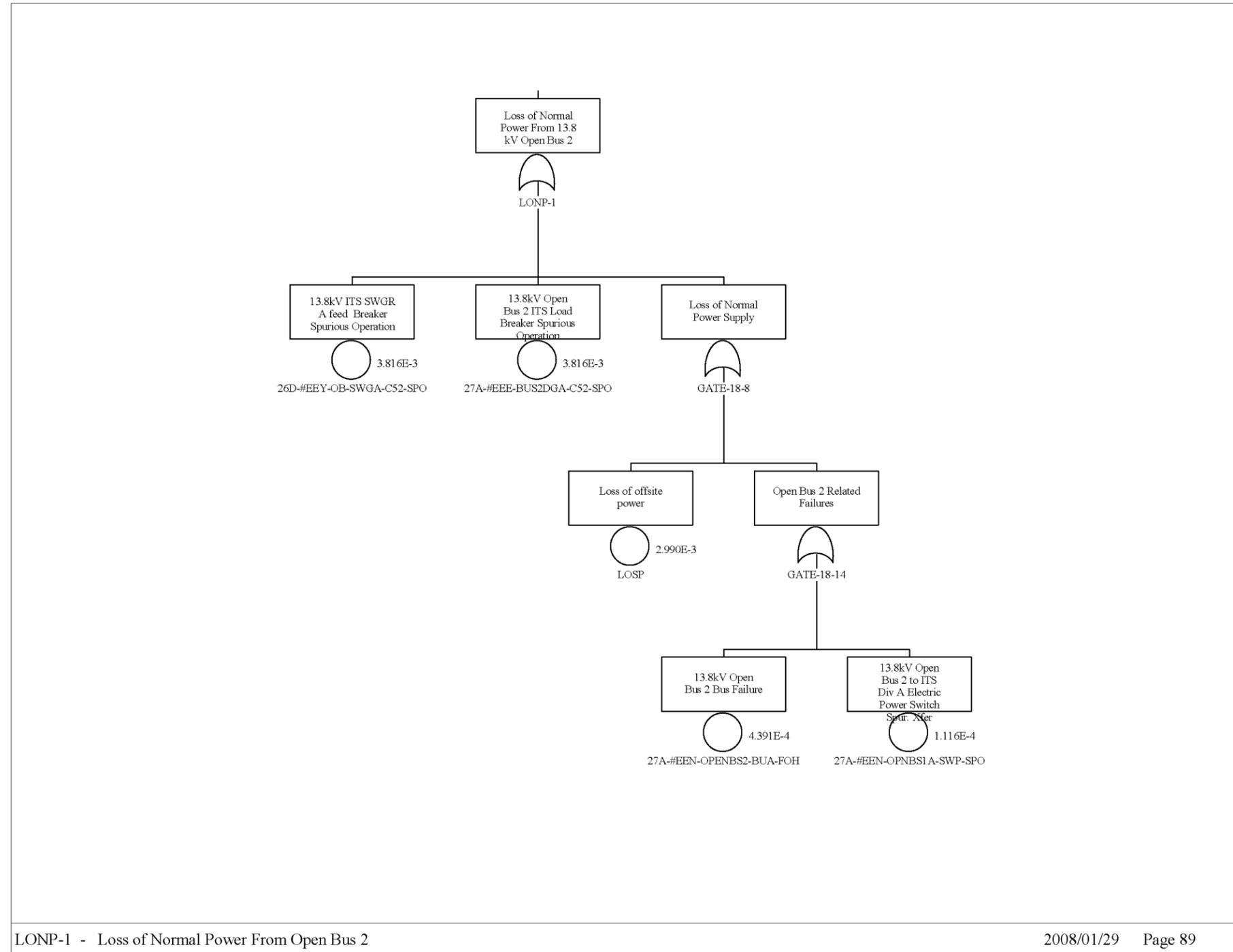
Source: Original

Figure B3.4-14. Loss of Power to CRCF ITS  
Load Center Train A Sheet 10



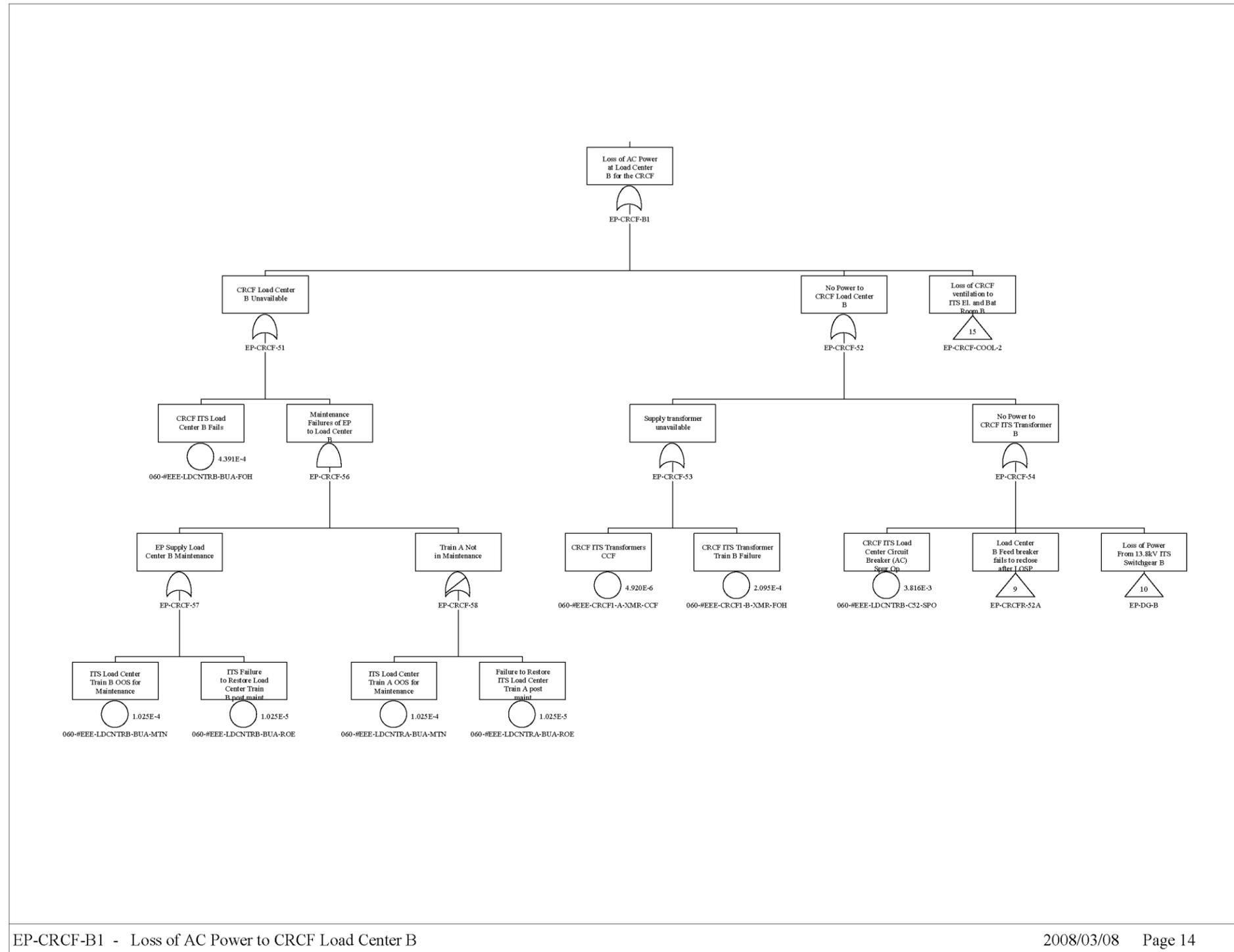
Source: Original

Figure B3.4-15. Loss of Power to CRCF ITS  
Load Center Train A Sheet 11



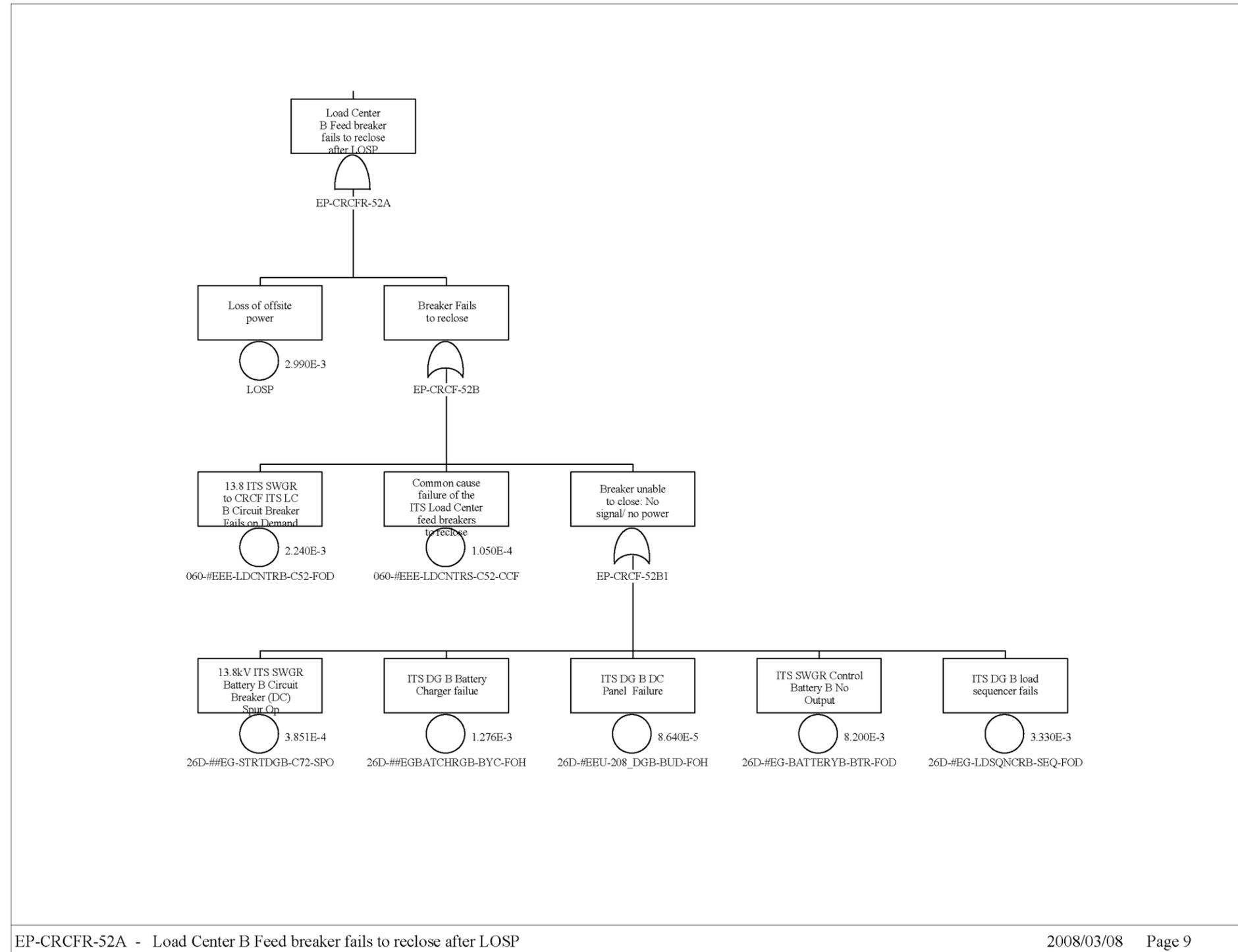
Source: Original

Figure B3.4-16. Loss of Power to CRCF ITS Load Center Train A Sheet 12



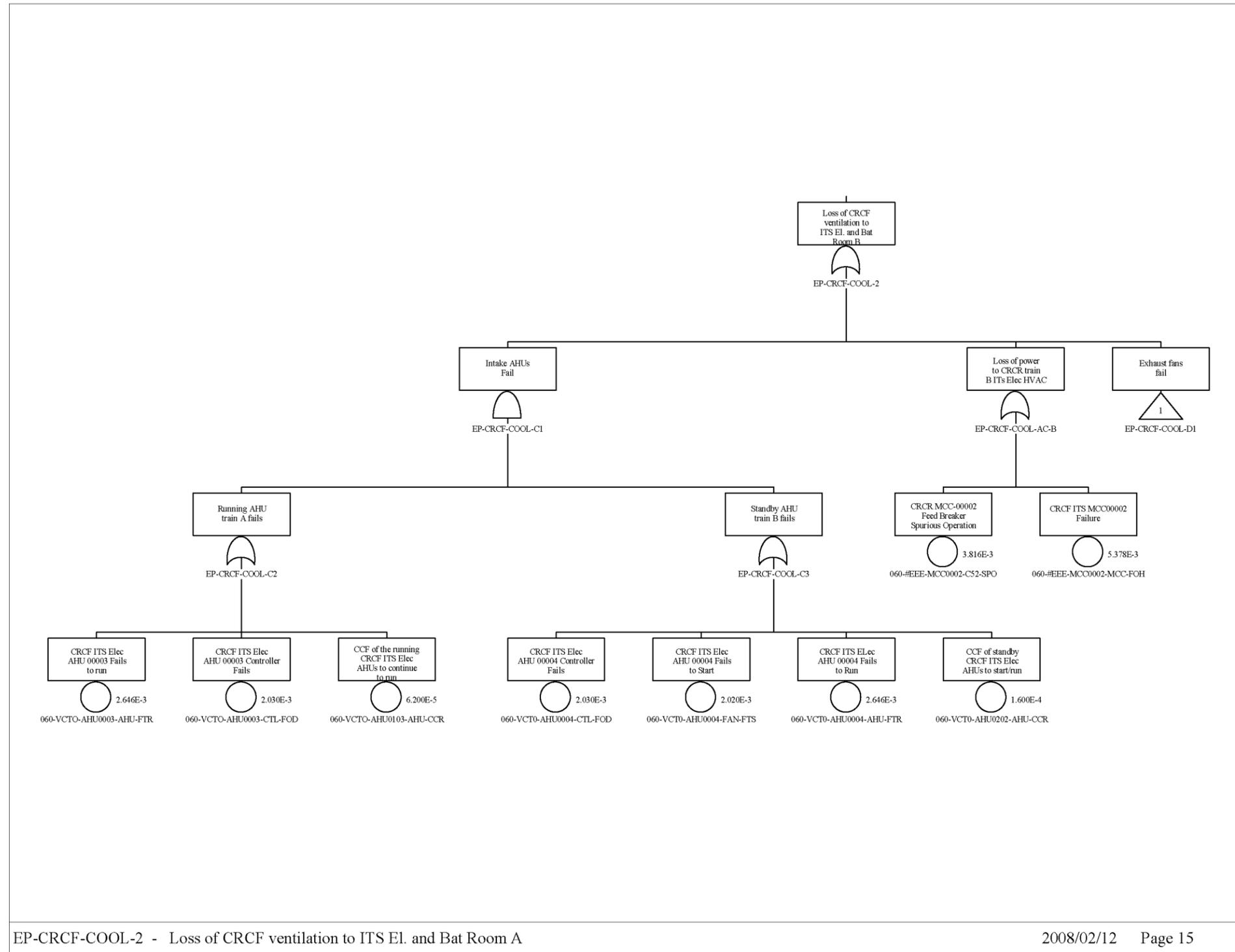
Source: Original

Figure B3.4-17. Loss of Power to CRCF ITS  
Load Center Train B Sheet 1



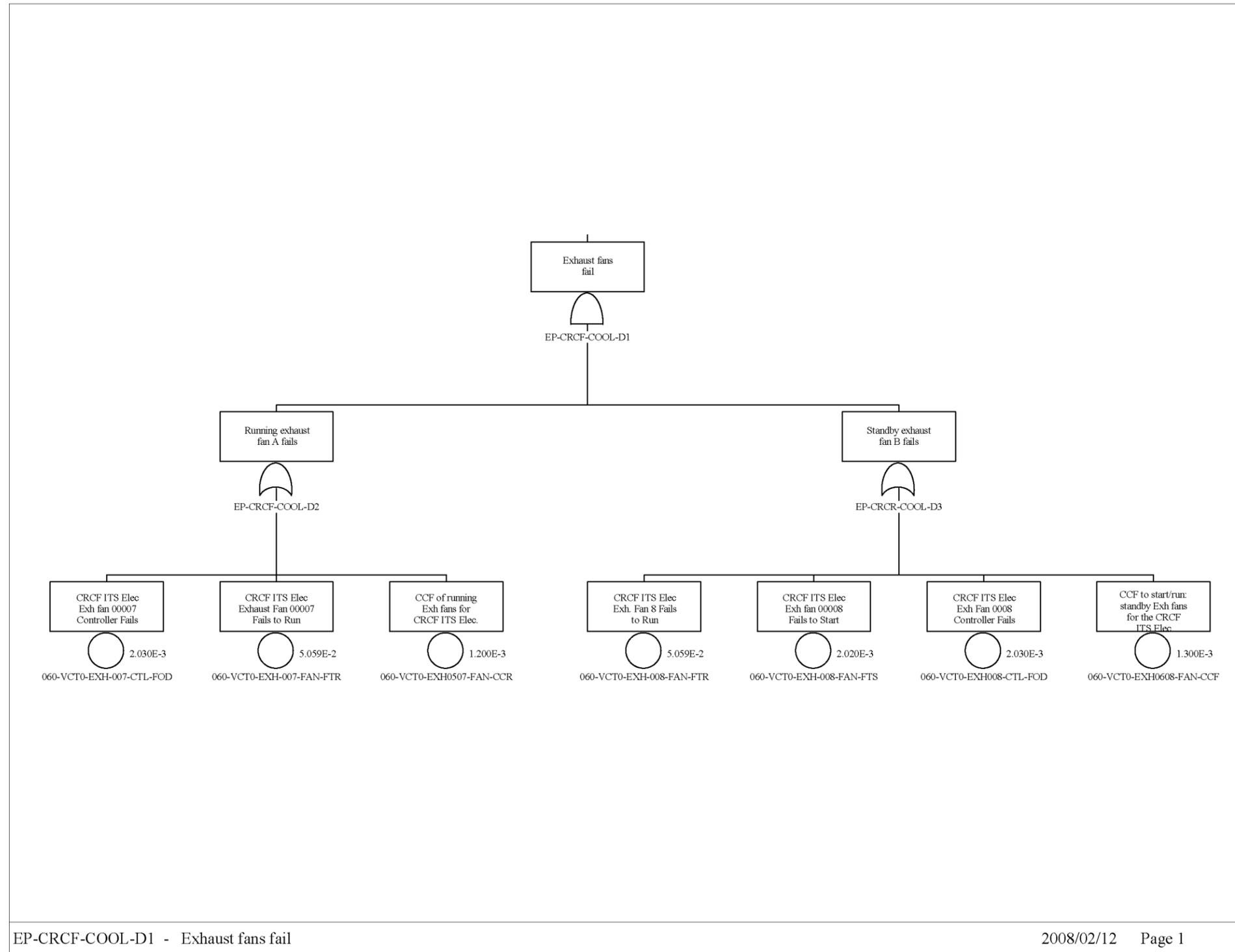
Source: Original

Figure B3.4-18. Loss of Power to CRCF ITS  
Load Center Train B Sheet 2



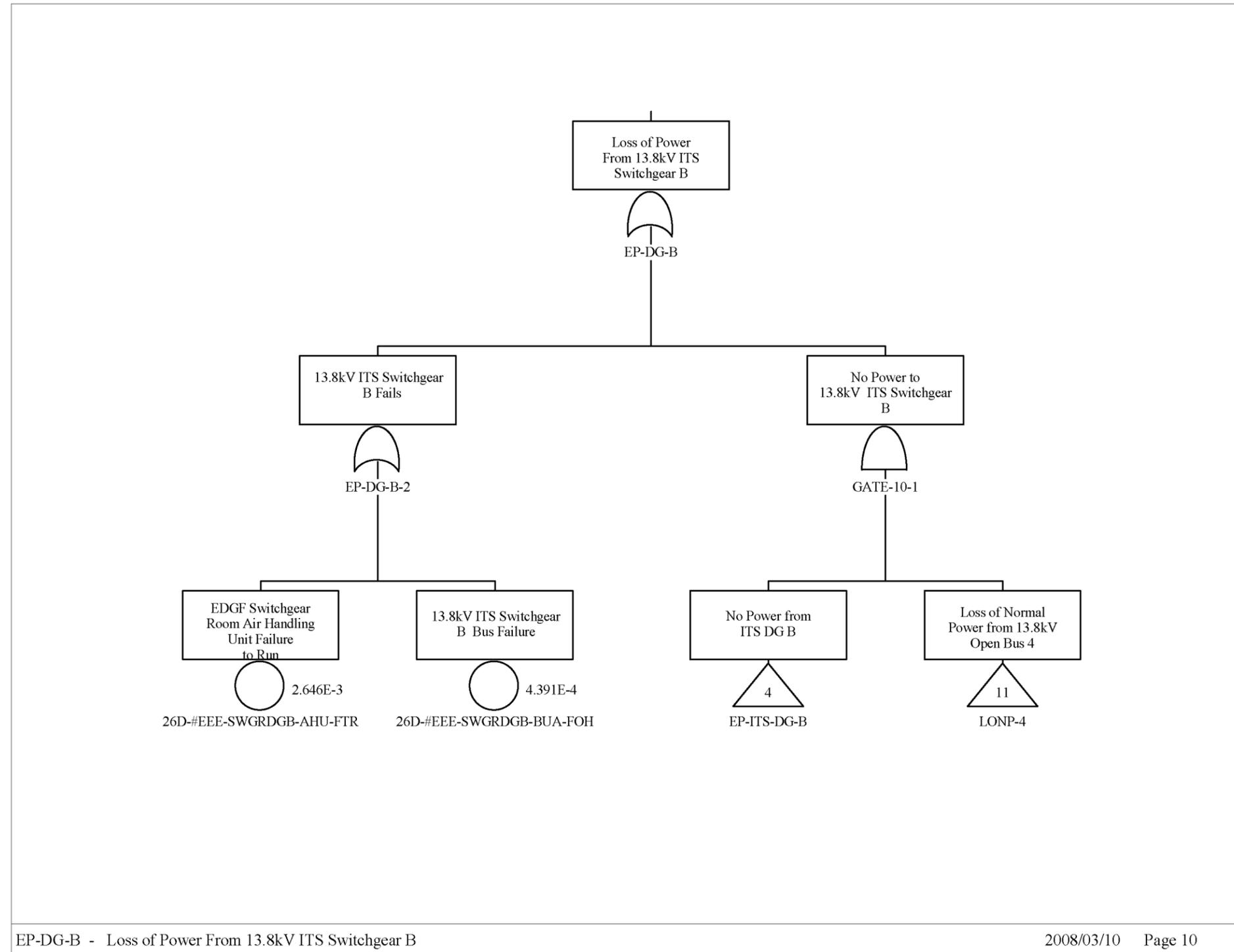
Source: Original

Figure B3.4-19. Loss of Power to CRCF ITS Load Center Train B Sheet 3



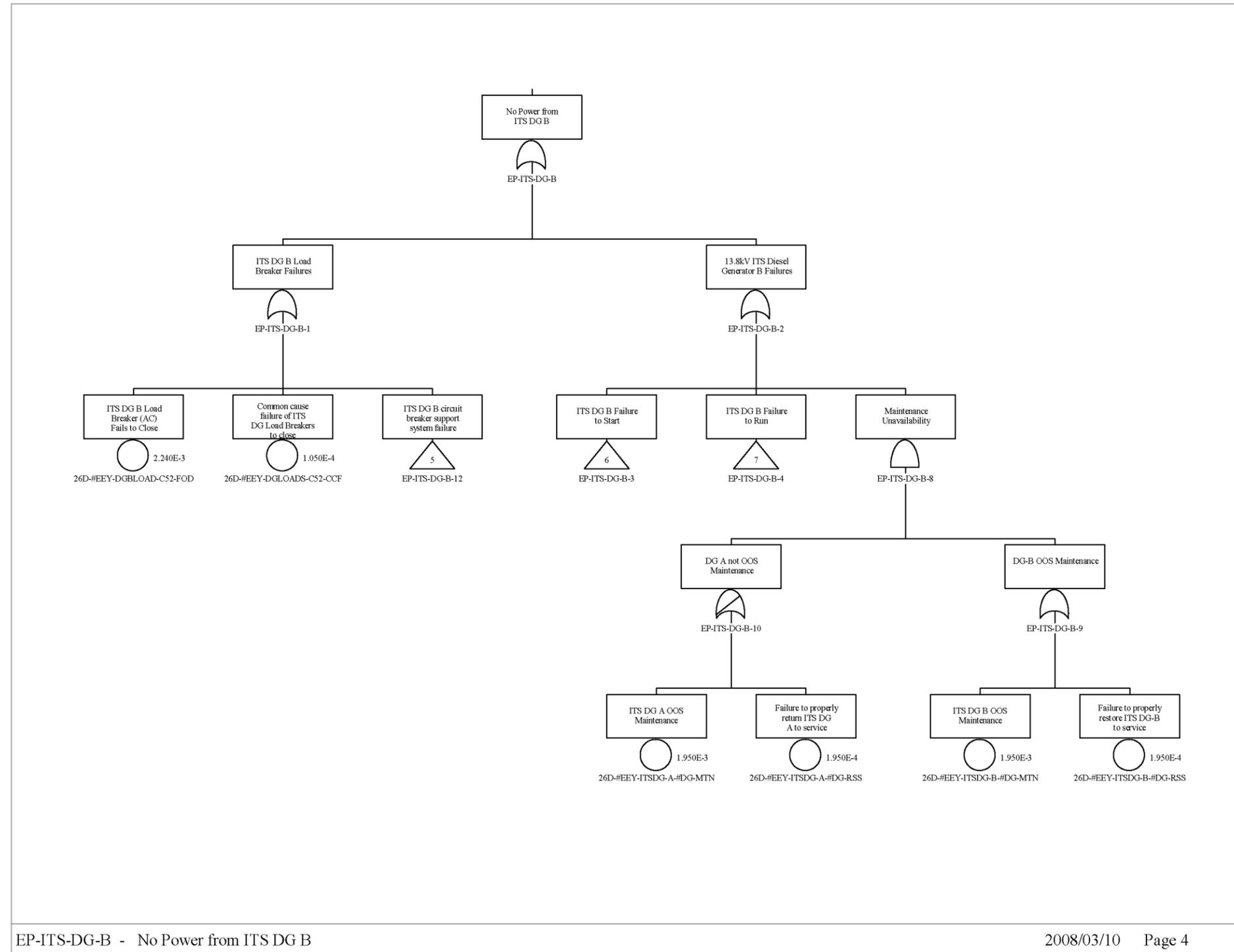
Source: Original

Figure B3.4-20. Loss of Power to CRCF ITS  
Load Center Train B Sheet 4



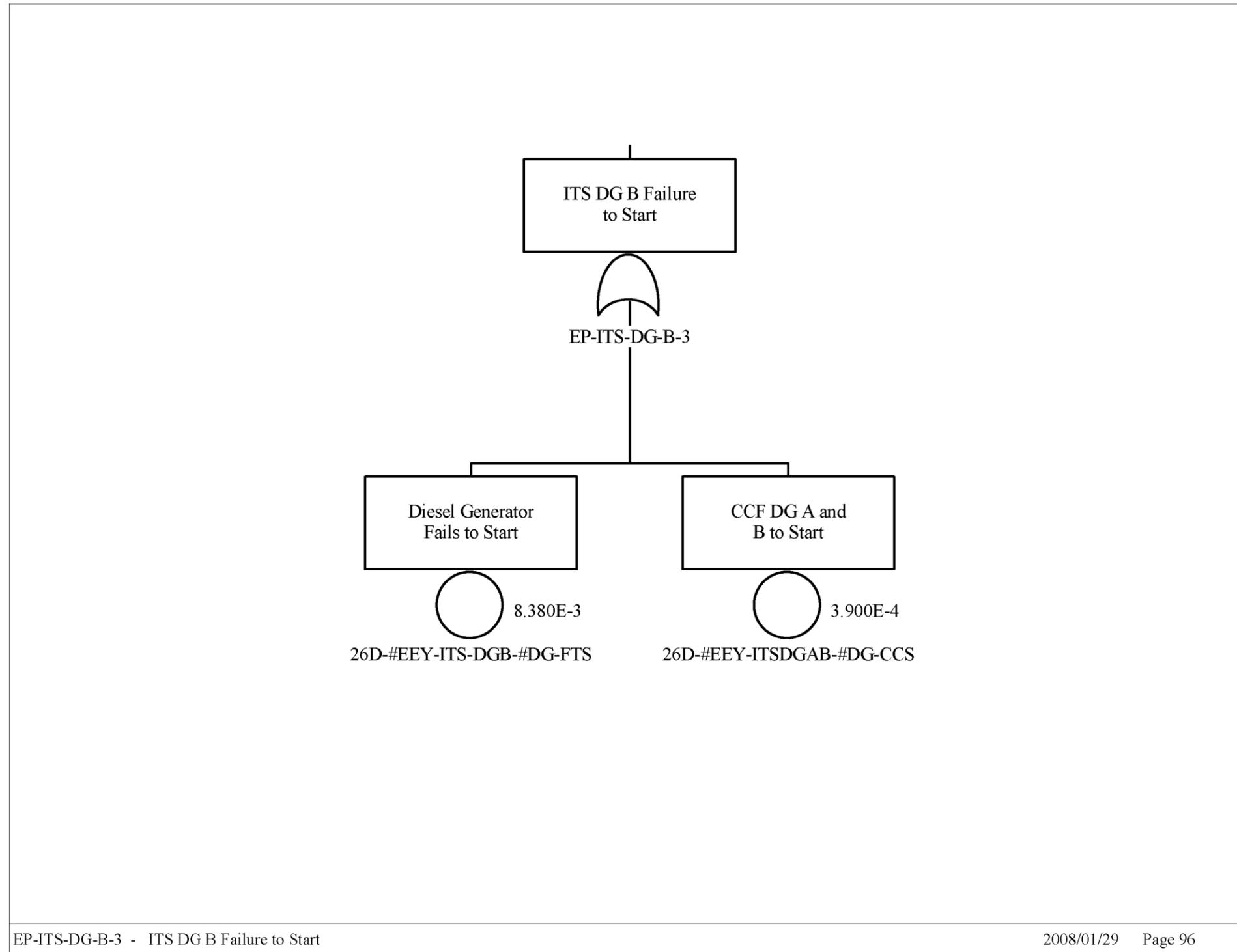
Source: Original

Figure B3.4-21. Loss of AC Power to CRCF ITS Load Center Train B Sheet 5



Source: Original

Figure B3.4-22. Loss of AC Power to CRCF ITS Load Center Train B Sheet 6

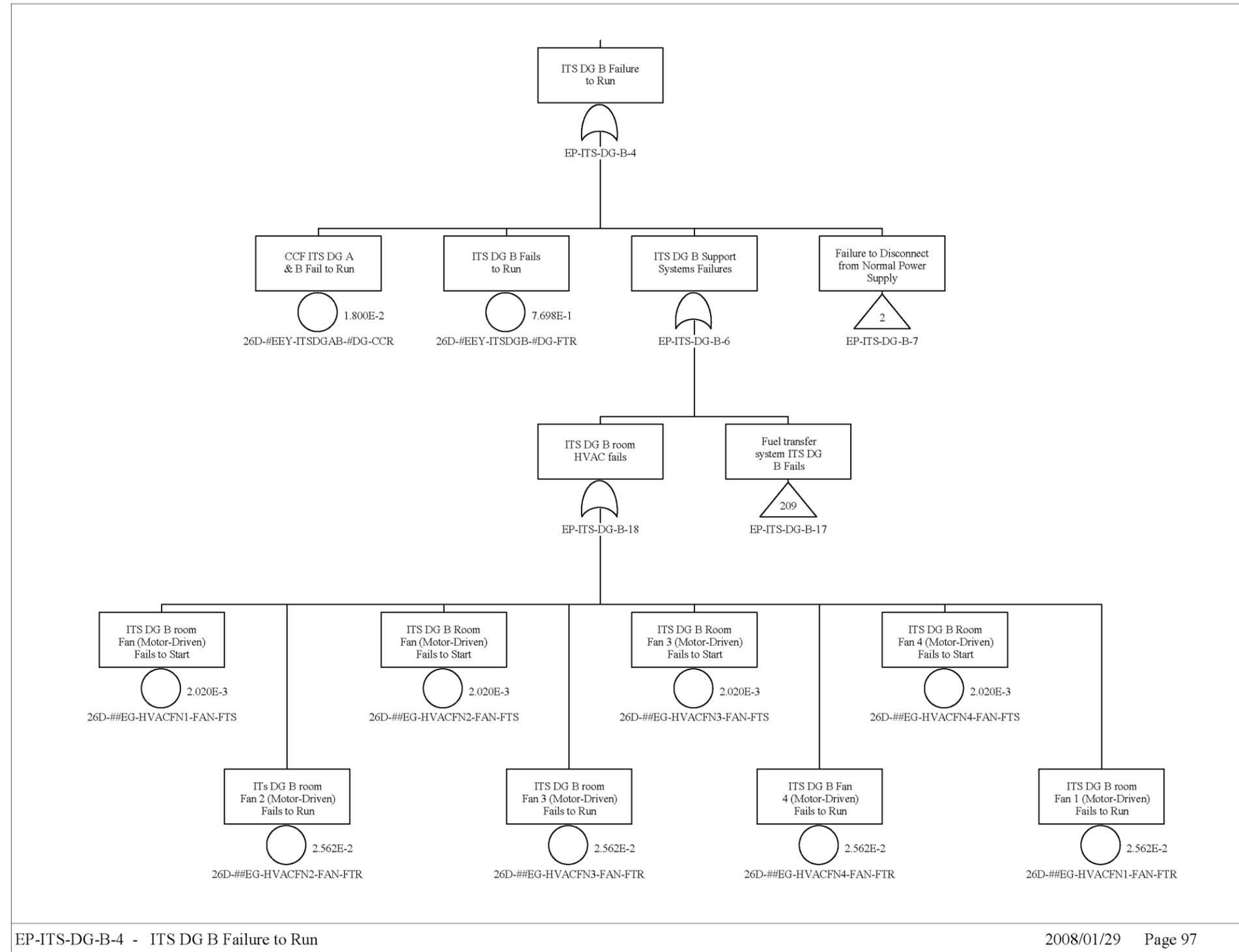


EP-ITS-DG-B-3 - ITS DG B Failure to Start

2008/01/29 Page 96

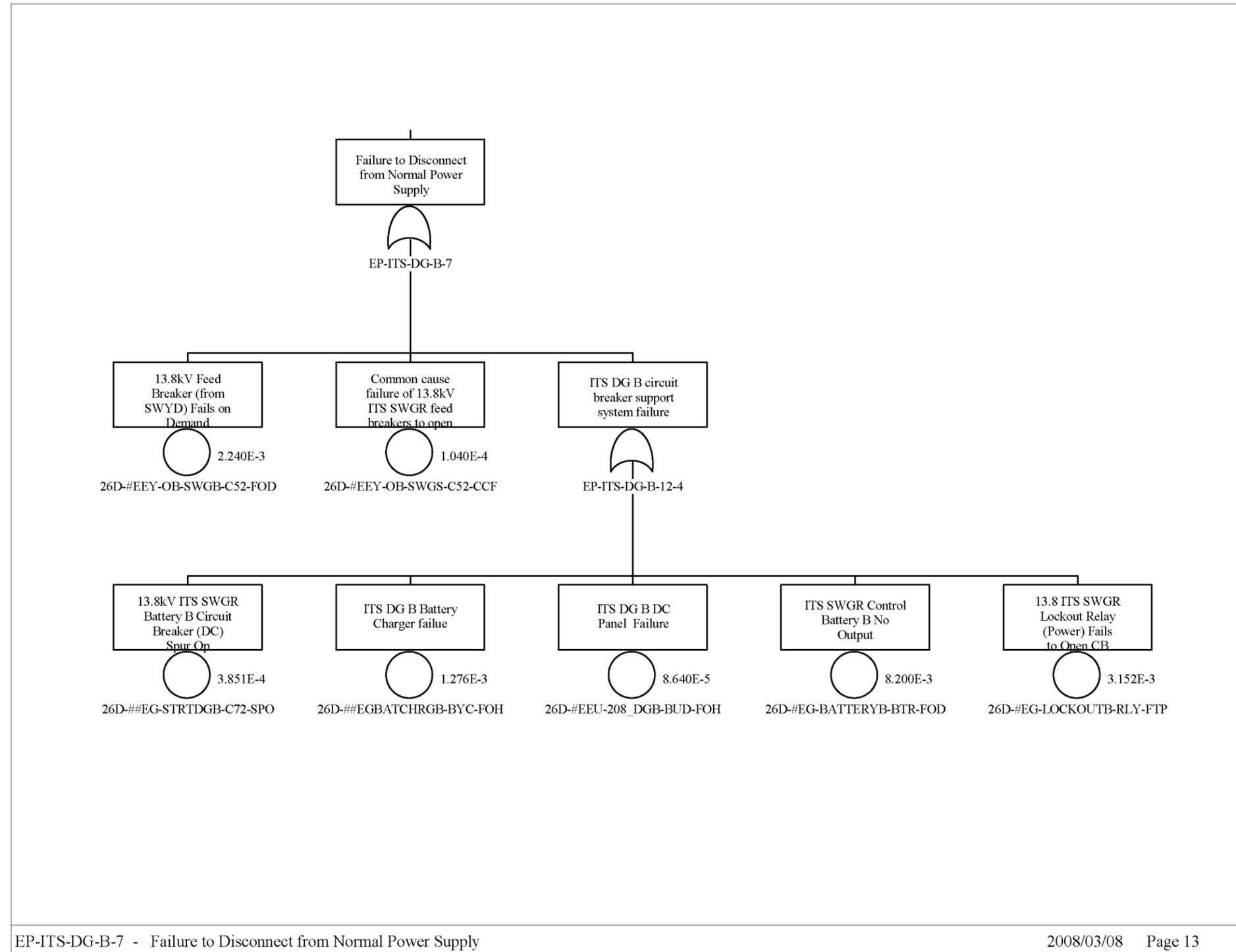
Source: Original

Figure B3.4-23. Loss of AC Power to CRCF ITS  
Load Center Train B Sheet 7



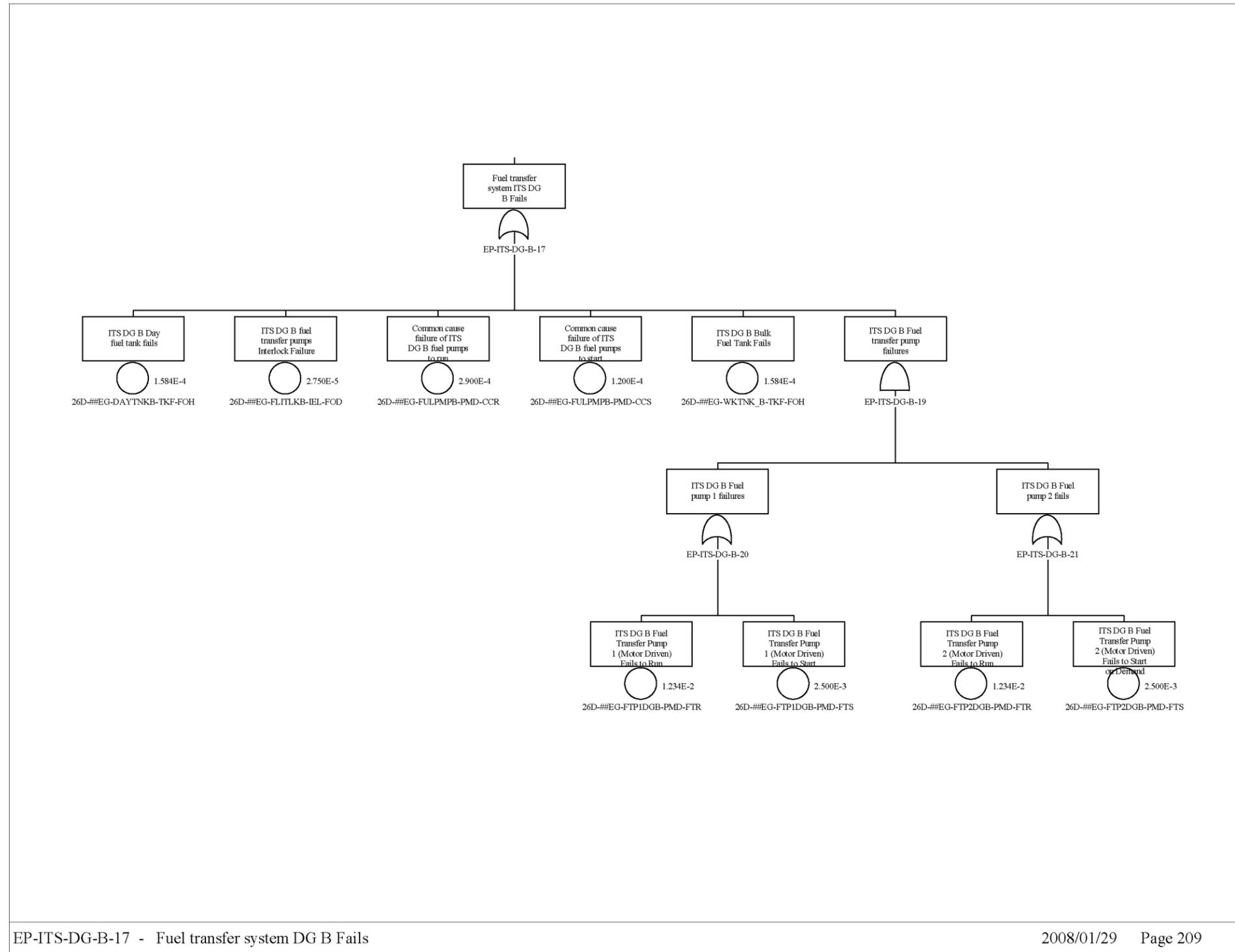
Source: Original

Figure B3.4-24. Loss of AC Power to CRCF ITS Load Center Train B Sheet 8



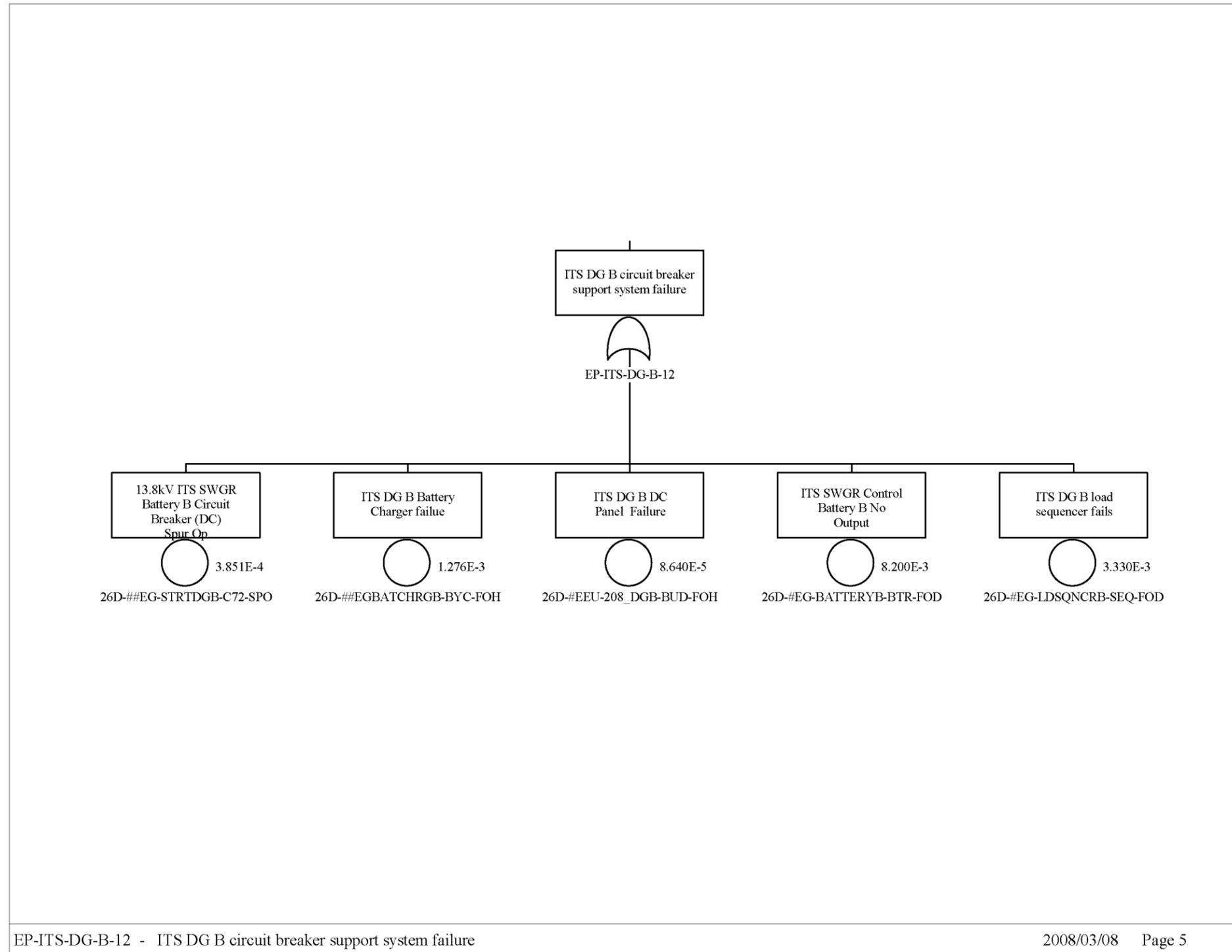
Source: Original

Figure B3.4-25. Loss of AC Power to CRCF ITS Load Center Train B Sheet 9



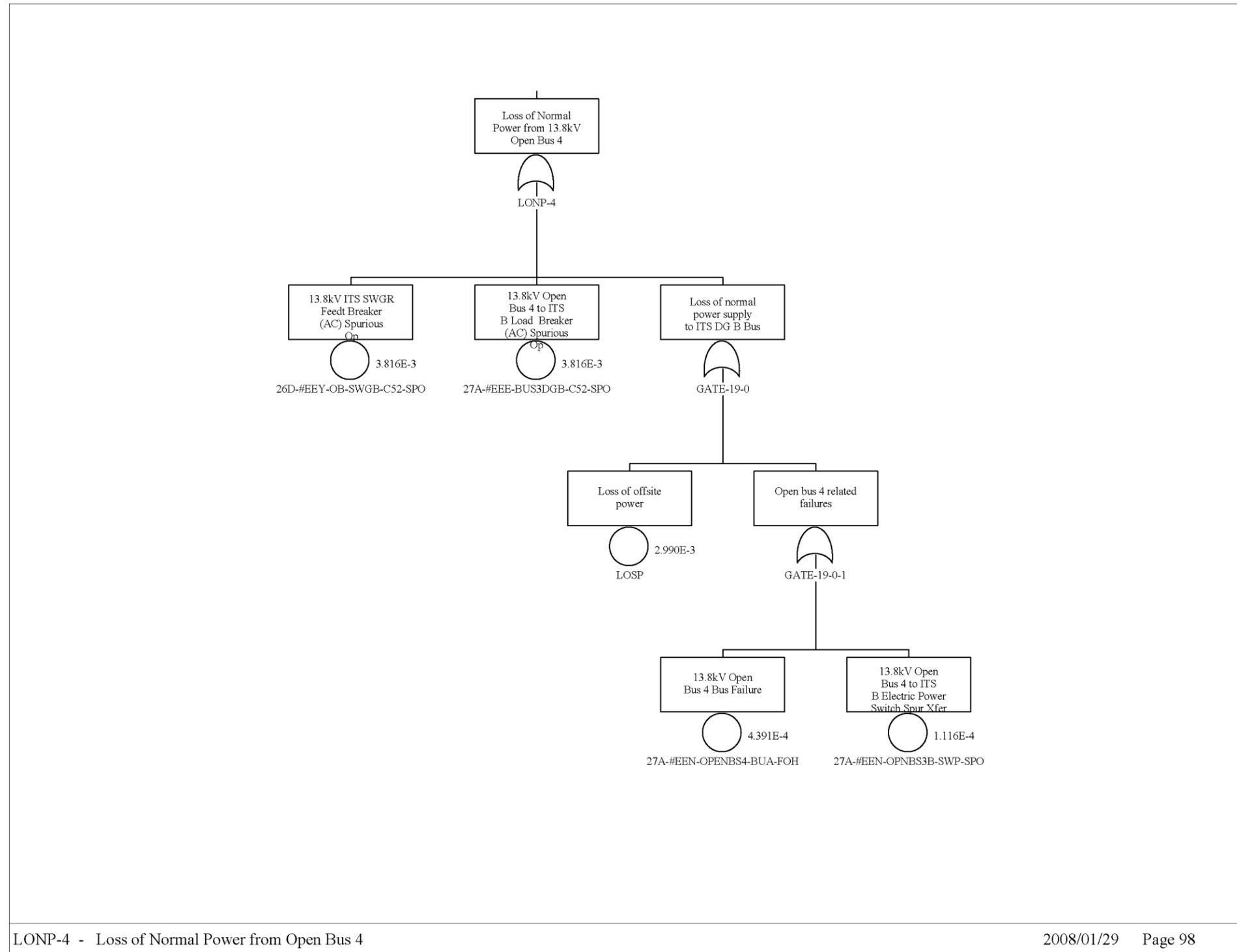
Source: Original

Figure B3.4-26. Loss of AC Power to CRCF ITS Load Center Train B Sheet 10



Source: Original

Figure B3.4-27. Loss of AC Power to CRCF ITS Load Center Train B Sheet 11



Source: Original

Figure B3.4-28. Loss of AC Power to CRCF ITS Load Center Train B Sheet 12

## **B4 DRIP SHIELD EMPLACEMENT GANTRY—FAULT TREE ANALYSIS**

### **B4.1 REFERENCES**

#### **Design Inputs**

The PCSA is a safety analysis 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), paragraph 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.

- B4.1.1 \*BSC (Bechtel SAIC Company) 2007. *Concept of Operations for the Drip Shield Gantry*. 800-30R-HEE0-00200-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070810.0010.
- B4.1.2 BSC 2007. *Drip Shield and Waste Package Emplacement Pallet Design Report*. 000-00C-SSE0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070810.0008.
- B4.1.3 \*BSC 2007. *Emplacement and Retrieval, Drip Shield Emplacement Gantry, Mechanical Equipment Envelope*. 800-MJ0-HE00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0031.
- B4.1.4 BSC 2007. *Interlocking Drip Shield Configuration*. 000-M00-SSE0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070409.0001.
- B4.1.5 BSC 2007. *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3*. 800-MH0-HEE0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0034.
- B4.1.6 \*BSC 2008. *Drip Shield Gantry Mechanical Equipment Envelope Calculation*. 800-MQC-HEE0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080125.0005.

### **B4.2 DRIP SHIELD OVERVIEW**

Just prior to closure of the subsurface facility, drip shields are placed over the waste packages within the emplacement drifts. The purpose of the drip shield is to prevent any water seepage onto the waste packages after repository closure and to protect the waste package from the direct impact of a rockfall.

As shown in Figure B4.2-1, a drip shield has an inverted U shape, and is composed of titanium alloys (UNS R56404 and UNS R52400) with a protective base edge of Alloy 22. A drip shield

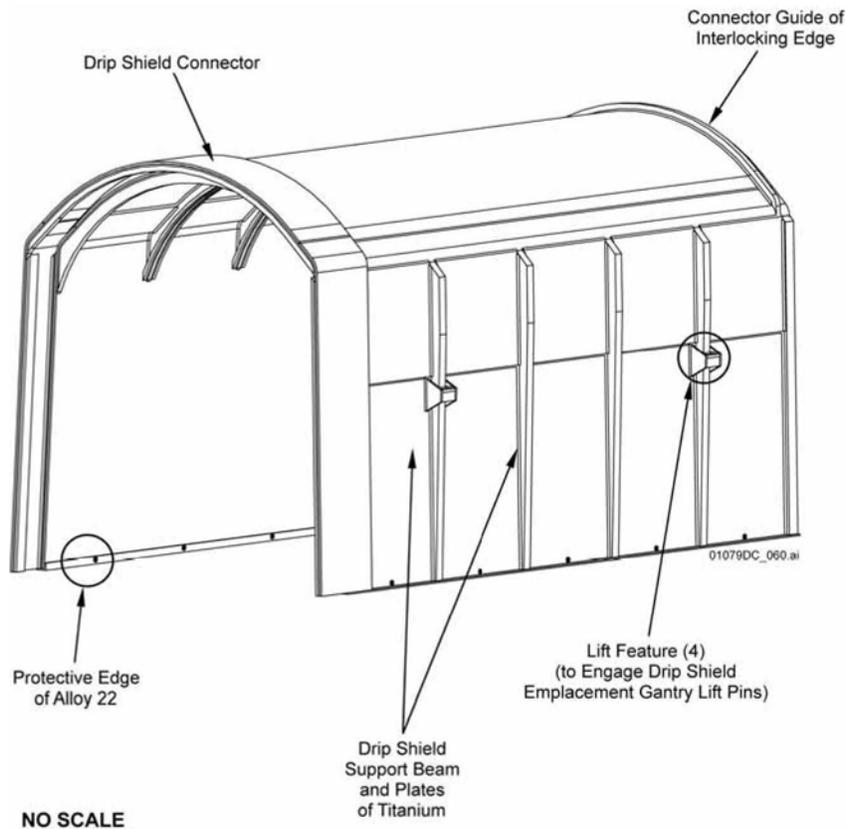
segment is approximately 2.9 m (9.5 ft) high and 5.8 m (19 ft) long and weighs approximately 5 metric tons (5.5 short tons). Each drip shield segment is designed to interlock with a previously emplaced drip shield segment, and when properly interlocked, the drip shield does not contact the emplacement pallet, the waste package, the rock wall or the runway beams of the invert.

## B4.2.1 System Description

### B4.2.1.1 Drip Shield Emplacement Gantry

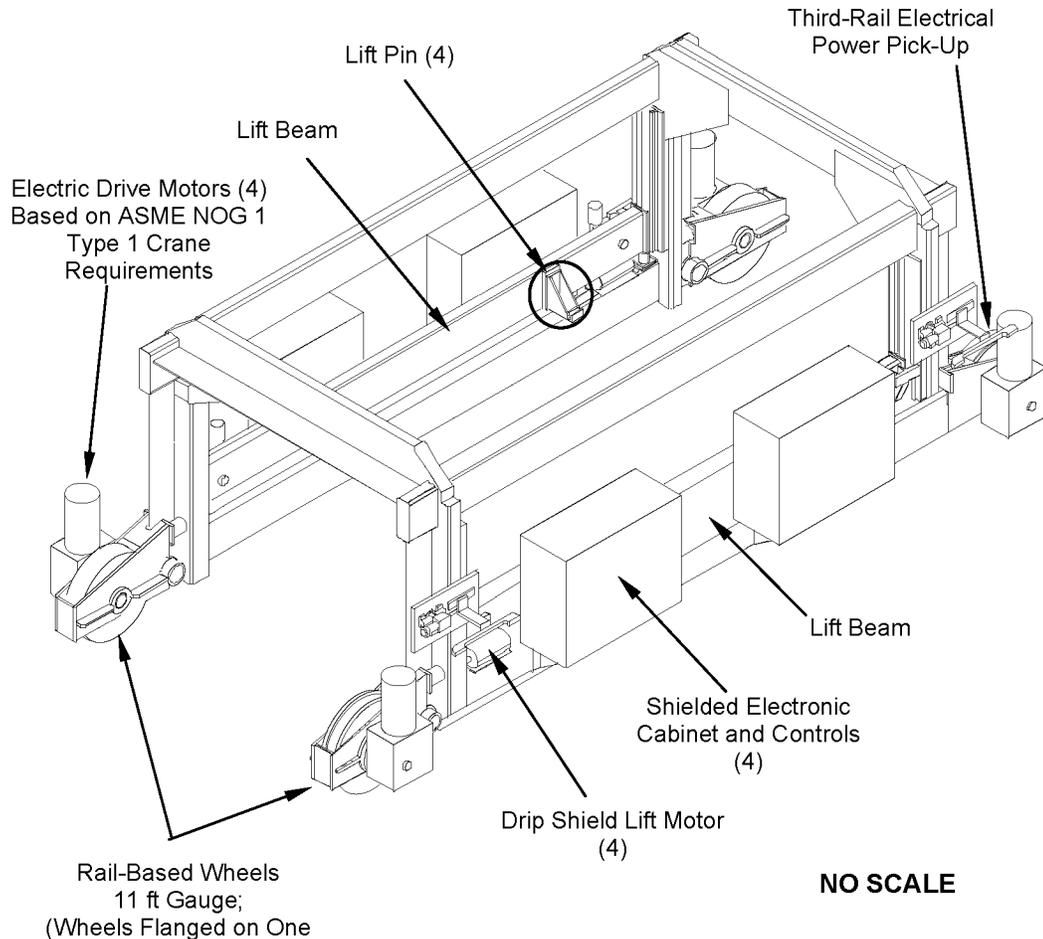
The drip shield emplacement gantry (DSG) is a remotely-operated vehicle that transports drip shields from the Heavy Equipment Maintenance Facility into emplacement drifts. The DSG is illustrated in Figure B4.2-2. Similar to the TEV, the DSG is a rail-based vehicle which is powered by a third rail, and contains PLCs for remote control of the device. In most cases, operation of the DSG is under PLC control with only general oversight from a central control, but some in some cases, operations under total manual control are performed as needed.

The frame of the DSG is a steel structure designed to support its own weight and the weight of the drip shield. The DSG raises the lift beams up to engage the lifting pin assemblies on the drip shield and raises the shield into a carry position.



Source: Modified from (Ref. B4.1.2) and (Ref. B4.1.4.)

Figure B4.2-1. Illustration of a Drip Shield



Source: Modified from (Ref. B4.1.3)

Figure B4.2-2. Illustration of the Drip Shield Emplacement Gantry (DSG)

The DSG has four wheels (two on each side), each driven directly by an electric motor. To limit derailment, the wheels on one side of the vehicle are double-flanged. Disc brakes are integral to the motors on each wheel. The wheels travel on 171 lb crane rail with a gauge of 3.35 m (11 ft), the same track as the TEV. The DSG carries an auxiliary (battery) backup power system to provide a limited supply of power in the event that third rail power is lost. Motors and gearboxes are sealed against environmental effects.

The PLCs and other electronic controls of the DSG are housed in separate equipment compartments (boxes) positioned at the sides of DSG (Figure B4.2-2). Each compartment is insulated and contains equipment to maintain the operating environment for the control instrumentation, together with a fire suppression system.

The unloaded DSG weighs approximately 86 metric tons (95 short tons) and has nominal height, width, and length of 3.5 × 4.9 × 9.4 m (11.6 × 16 × 31 ft) respectively.

Specific components of the TEV that are considered in fault trees are described in the following sections. The discussions are based on *Concept of Operations for the Drip Shield Gantry* (Ref. B4.1.1) and *Drip Shield Gantry Mechanical Equipment Envelope Calculation* (Ref. B4.1.6).

**Drip Shield Lift System**—The DSG lifts and lowers the drip shield using two moving lift beams, one on each side of the gantry. The drip shield has two lifting points or features on each side of the shield (Figure B4.2-1). Each lift beam on the DSG has two corresponding lift features (lift pins) as shown in Figure B4.2-2. Four screw jacks power the lift beam and are used to lift the drip shield; each jack has a nominal capacity of 5 short tons (4.5 metric tons). To drive the screw jack, a 3 hp (2.2 kW) motor or equivalent, is used.

**DSG Linear Drive Gear Motors**—Each of the DSG's four wheels are driven by a 12.5 hp (9.3 kW) linear drive gear motor featuring integral disc brakes.

### **B4.2.1.2 Operations**

#### **B4.2.1.3 Drip Shield Emplacement**

The DSG transports a drip shield from the Heavy Equipment Maintenance Facility to a designated emplacement drift turnout using the same rail system as the TEV. After the DSG stops at the turnout, its positional sensors and devices enable it to calibrate and to establish a positional datum point. Once calibration is complete, the emplacement access door is opened and the DSG with drip shield proceeds through the door, and the door closes after the DSG has passed through.

The DSG proceeds down the turnout drift and enters the emplacement drift at an operational transit speed of approximately 2.7 km/hr (1.7 mph or 150 ft/min) to a predetermined position, where the gantry stops, and re-confirms its location. The DSG moves forward at a slow speed, nominally 4.6 m/min (15 ft/min), to a predetermined position relative to the previously emplaced drip shield. Similar to the TEV, additional onboard positional sensors and devices are activated (e.g., lights, cameras, and ultrasonic sensors), and measurements are made to re-confirm to the position of the DSG and the drip shield it is carrying, in relation to a previously emplaced drip shield.

The DSG moves forward at a crawl speed, nominally 0.46 m/min (1.5 ft/min), until the required final position is achieved. Onboard cameras and sensors report the final position to central control; some correction movement may be required to achieve the desired position. Once the final position is achieved, the gantry lowers the lift beams, lowering the drip shield. The drip shield engages the previously emplaced drip shield interlock (if present), and it rests upon the steel frame of the emplacement drift invert.

The emplacement gantry lowers its lifting features to its travel height and moves at a crawl speed away from the newly emplaced drip shield to a predetermined distance and stops. Upon confirmation of emplacement status, the gantry slowly accelerates to the full operational speed towards the emplacement access door. Once the gantry reaches the emplacement access door, the gantry again stops. The emplacement access door is opened and the gantry passes through the doorway.

Block diagrams of the DSG drip shield operations are provided in *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3* (Ref. B4.1.5).

### B4.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B4.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B4.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Third rail electrical power	Provides power for vehicle motion and controls	—	—	—	—
Programmable logic controllers	Provide local control of TEV mechanical systems	Failure due to high temperature or radiation	—	—	—
Linear-drive gear motors for wheels	Provides locomotive force for vehicle	—	—	—	—
Rail system (including switches)	Constrains and supports vehicle movement	—	Controls vehicle path	—	Seismic loading can fail rail system
Lift pin	Guide drip shield on DSG	Failure due to corrosion	Mates with lift features on drip shield	—	Seismic loading can cause failure
Lift beam	Provide lift for drip shield emplacement operations	Failure due to corrosion	Keeps lift pins in correct location	—	Seismic loading can cause failure
Drip shield lift motor / actuator	Moves lift beams up and down	Failure due to corrosion	—	—	—
Central control and communication system	Controls operation	—	—	Incorrect instruction	—
Manual controls	Controls operation	—	—	Incorrect instruction	—
DSG frame	Constrains and supports lift beams and supports drip shield load	Failure due to corrosion or poor maintenance	Keeps lift beams in correct location	—	Seismic loading can cause failure

NOTE: DSG = drip shield gantry; TEV = transport and emplacement vehicle.

Source: Original

## **B4.4 DSG RELATED FAILURE SCENARIOS**

One scenario and fault tree associated with the DSG is the drop of drip shield onto a waste package.

The fault tree is described in the following subsection.

### **B4.4.1 Drop of Drip Shield onto a Waste Package**

#### **B4.4.1.1 Description**

The scenario describes the drop of a drip shield onto a waste package (or packages) by the DSG, as the DSG is transporting the drip shield into position within an emplacement drift. Just prior to closure, drip shields are transported and moved into emplacement drifts to provide for the long-term protection of the waste packages. The DSG moves a single drip shield in a raised position over a row of waste packages and then lowers the drip shield to interlock with previously-emplaced drip shield to form a continuous barrier. Given the four-position lift system holding the drip shield, at least two of the four lift positions must fail for the drip shield to fall and impact a waste package. As the DSG is moving when such a drop could occur, the drip shield digs into the invert and rotate the drip shield and may derail the DSG.

#### **B4.4.1.2 Success Criteria**

Success criteria for the DSG during the drip shield emplacement process require that the DSG subsystems operate without failure or spurious operations. During the emplacement operations, The DSG lift system should maintain the drip shield above the waste package as the gantry moves along the emplacement drift at an operational speed of 2.7 km/hr (1.7 mph).

#### **B4.4.1.3 Design Features and Input**

The following requirement is identified with respect to this scenario:

- Normal periodic maintenance and inspection are performed on the DSG, especially the lift system and lift pins to allow for the safe operation of the DSG without dropping the drip shield during normal operation.

#### **B4.4.1.4 Fault Tree Model**

The fault tree model for the sequence is labeled as DRIPSHIELD-DROPPED. As shown in Figure B4.4-3, the fault tree describes the drop of the drip shield by the DSG onto a waste package in an emplacement drift. The top event is drop of the drip shield where at least two of the four lift pins or lift beam systems (rigs) have failed. This top event is realized by the occurrence of two of the four basic events through an OR gate; each basic event is the failure of one of the individual lift pins or lift beam systems.

### B4.4.1.5 Basic Event Data

Table B4.3-1 contains a list of basic events used in the fault tree, DRIPSHIELD-DROPPED for impact on a waste package in an emplacement.

Table B4.4-1 Drip Shield Dropped on Waste package

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Probability/Lambda	Miss. Time <sup>a</sup>
800-HEE0-DSLIFTC-LRG-CCF	Common cause failure of 2 of 4 lifting rig or hooks	1	3.730E-09	3.730E-09	0.000E+00
800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook Fails - DSG	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook Fails - DSG	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook Fails - DSG	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook Fails - DSG	3	7.450E-07	7.450E-07	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.

Calc. = calculation; Miss. = mission; Prob. = probability.

Source: Original

#### B4.4.1.5.1 Human Failure Events

No basic event is identified as associated with human error for this model.

#### B4.4.1.5.2 Common-Cause Failures

One CCF failure is identified for this model, the CCF of at least two of four lifting rigs or hooks (800-HEE0-DSLIFTC-LRG-CCF).

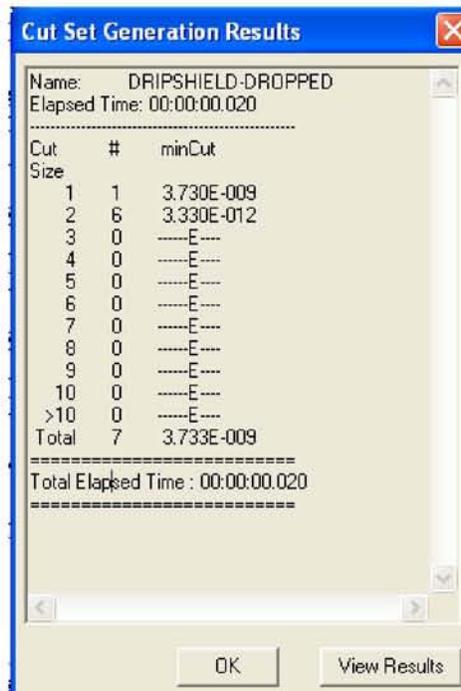
#### B4.4.1.6 Uncertainty and Cut set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree associated with the drop of the drip shield by the DSG, DRIPSHIELD-DROPPED are presented in Figures B4.4-1 and B4.4-2.



Source: Original

Figure B4.4-1. Uncertainty Results for the DRIPSHIELD-DROPPED Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the DRIPSHIELD-DROPPED Fault Tree

**B4.4.1.7 Cut Sets**

Table B4.4-2 contains the cut sets for the DRIPSHIELD-DROPPED fault tree.

Table B4.4-2. DRIPSHIELD-DROPPED Cut Sets

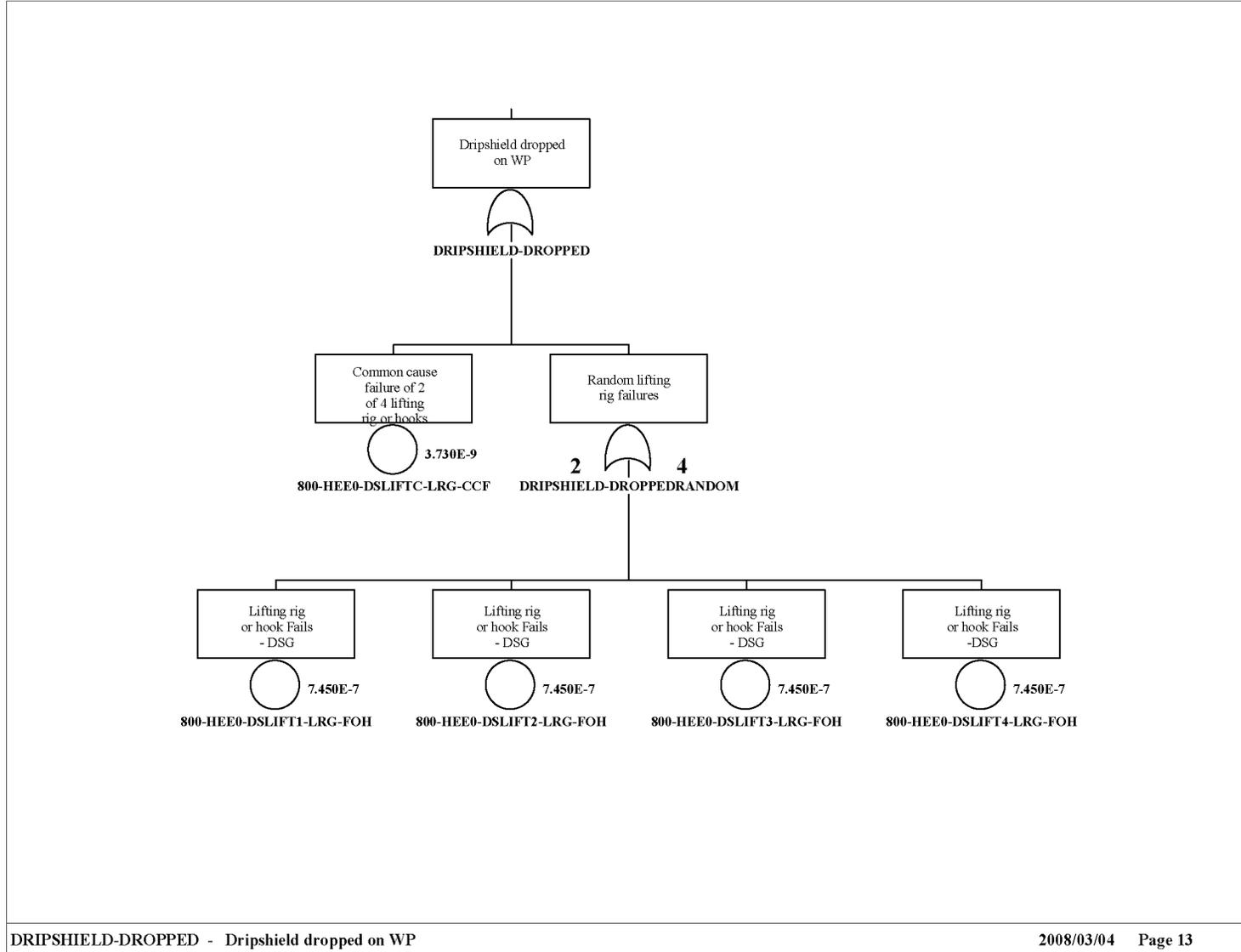
% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.91	99.91	3.730E-09	800-HEE0-DSLIFTC-LRG-CCF	Common cause failure of 2 of 4 lifting rig or hooks	3.730E-09
99.92	0.01	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
99.93	0.01	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
99.94	0.01	5.550E-13	800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
99.95	0.01	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook Fails -DSG	7.450E-07
99.96	0.01	5.550E-13	800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook Fails -DSG	7.450E-07
99.97	0.01	5.550E-13	800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook Fails - DSG	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook Fails -DSG	7.450E-07

NOTE: DSG = drip shield emplacement gantry; Prob. = probability.

Source: Original

**B4.4.1.8 Fault Tree**

Fault trees for the fault tree associated with the DSG identified in Section B.4.3 (DRIPSHIELD-DROPPED) is presented in Figure B4.4-3.



DRIPSHIELD-DROPPED - Dripshield dropped on WP

2008/03/04 Page 13

Figure B4.4-3. DRIPSHIELD-DROPPED - Fault Tree for Drop of Drip Shield onto a Waste Package

## **B5 SHIELD DOOR— FAULT TREE ANALYSIS**

### **B5.1 REFERENCES**

#### **Design Inputs**

The PCSA is a safety analysis 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), paragraph 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

- B5.1.1 BSC 2007. *Nuclear Facilities Equipment Shield Door Process and Instrumentation Diagram*. 000-M60-H000-00101-000 REV 00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0024.
- B5.1.2 BSC 2008. *Canister Receipt and Closure Facility 1 General Arrangement Ground Floor Plan*. 060-P10-CR00-00102-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0013.
- B5.1.3 BSC 2007. *Canister Receipt and Closure Facility 1 General Arrangement Second Floor Plan*. 060-P10-CR00-00103-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0014.

### **B5.2 SHIELD DOOR SYSTEM DESCRIPTION**

#### **B5.2.1 Overview**

Each of the CRCF Waste Package Positioning Rooms (room numbers 1018, 1019) has a shield door providing access to the Waste Package Loadout Room (room number 1015) (Ref. B5.1.2). The shield doors provide shielding during canister unloading and loading. The shield doors are ITS, protecting workers from the hazardous operations that go on inside the loading and unloading rooms.

#### **B5.2.2 Operations Description**

Waste package loading operations in the Waste Package Positioning Rooms are analogous to cask unloading operations.

#### **B5.2.3 Physical Description**

The shield doors consist of pairs of large, heavy doors that are operated by individual motors with over-torque sensors to prevent crushing of an object. Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The obstruction sensor is also alarmed to provide operators indication when an object is between the shield doors. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand

lever that must be enabled by an enable/disable switch. An emergency open switch exists enabling the doors to be opened in case of an emergency situation.

#### B5.2.4 Schematics

Schematics for the shield door are available separately for review (Ref. B5.1.1).

### B5.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with SSCs. The five areas considered are addressed in Table B5.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B5.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Door/gate motors	Over-torque sensors	—	—	Inadvertent operation	—

Source: (Ref. B5.1.3)

### B5.4 SHIELD DOOR FAILURE SCENARIOS

The shield door system has one credible failure scenario for subsurface operations and that is that the shield door closes on a conveyance.

#### B5.4.1 Shield Door Closes on TEV

##### B5.4.1.1 Description

If the shield doors to the loading rooms are closed onto the TEV or waste package as waste packages are transferred from the WP loadout rooms, a release may occur as a result. Measures are in place to ensure this situation does not occur, including the presence of motor over-torque sensors.

##### B5.4.1.2 Success Criteria

The success criteria defined for this scenario are the shield doors not causing a release due to closure on the conveyance. In the event that the shield doors do close on a conveyance, the motor over-torque sensors prevent excessive closure force ensuring no release.

### B5.4.1.3 Design Features and Requirements

Motor over-torque sensors prevent shield doors from causing damage to casks or waste packages in the event of closure on a conveyance. Over torque sensors are the only protective feature modeled in this fault tree. Other fault trees incorporate the modeling of an obstruction sensor that may also prevent collisions with any conveyance being used for transport.

### B5.4.1.4 Fault Tree Model

The top event in this fault tree is “Facility Shield Door – Facility Door Closes on TEV.” This is defined as an inadvertent closure of the shield doors due to either operator action or component failure while the conveyance is in position to be hit by the doors. Faults considered in the evaluation of this top event include: failure of components in the control circuitry of the shield doors and human events that could contribute to the inadvertent shield door closing. The fault tree is shown in Figure B5.4-3.

### B5.4.1.5 Basic Event Data

Eight basic events listed in Table B5.4-1 are used to model this failure scenario, including one human failure event.

Table B5.4-1. Basic Event Data

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time <sup>a</sup>
800-HEE0-FACMO01-MOE-SPO	Shield door Motor #1 Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
800-HEE0-FACMO02-MOE-SPO	Shield door Motor #2 Spurious Operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
800-HEE0-FACTOR1-TL-FOH	Shield Door Motor #1 Over Torque Limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
800-HEE0-FACTOR2-TL-FOH	Shield Door Motor #2 Over Torque Limiter Failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	3	1.460E-06	0.000E+00	3.650E-07	4.000E+000
800-HEE0-WKRFACD-HFI-NOD	Operator closes facility door on TEV	1	2.000E-03	2.000E-03	0.000E+00	0.000E+00
800-SD---SRU001---SRU-FOH	Shield Door Ultrasonic obstruction Sensor Fails	3	9.620E-05	0.000E+00	9.620E-05	1.000E+00
800-SD---TL000-TL---CCF	Over Torque Sensor CCF Failure	1	6.710E-04	6.710E-04	0.000E+00	0.000E+00

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Op = operation; Prob. = probability; TEV = transport and emplacement vehicle

Source: Original

### B5.4.1.5.1 Human Failure Events

One human failure event, 800-HEE0-WKRFACD-HFI-NOD Operator closes facility door on TEV, is modeled in the fault tree as an operator attempting to close the shield doors while a conveyance is between the doors. The screening value used for this HFE has a probability of 2.0E-03.

### B5.4.1.5.2 Common-Cause Failures

One common-cause failure (CCF) is considered in this fault tree, 800-SD---TL000-TL--CCF, the common cause failure of the shield door over torque sensors.

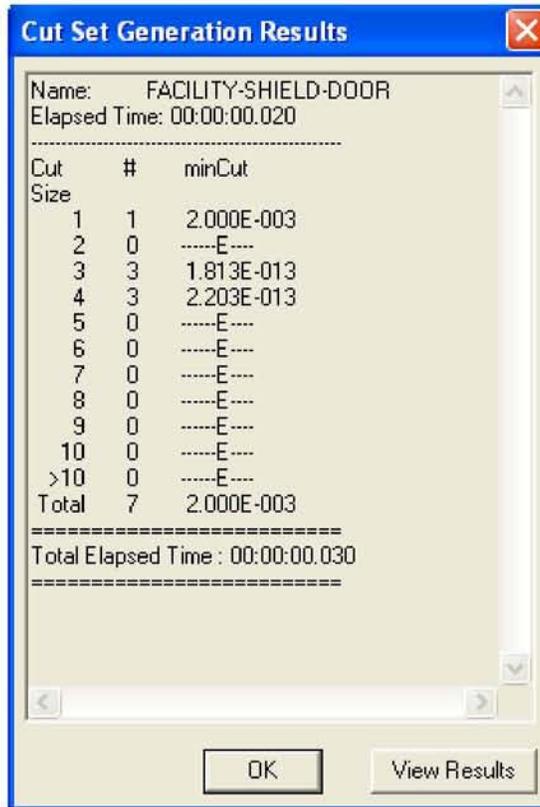
### B5.4.1.6 Uncertainty and Cut Set Generation

Figure B5.4-1 contains the uncertainty results obtaining from running the fault tree “Facility Shield Door – Facility Door Closes on TEV.” Figure B5.4-2 provides the cut set generation results for the “Facility Shield Door – Facility Door Closes on TEV” fault tree.

Uncertainty Results			
Name	FACILITY-SHIELD-DOOR		
Random Seed	1234	Events	8
Sample Size	10000	Cut Sets	7
Point estimate	2.000E-003		
Mean Value	2.029E-003		
5th Percentile Value	2.452E-004		
Median Value	1.258E-003		
95th Percentile Value	6.314E-003		
Minimum Sample Value	2.975E-005		
Maximum Sample Value	5.736E-002		
Standard Deviation	2.590E-003		
Skewness	5.247E+000		
Kurtosis	5.718E+001		
Elapsed Time	00:00:00.630		
<input type="button" value="OK"/>			

Source: Original

Figure B5.4-1. Uncertainty Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree



Source: Original

Figure B5.4-2. Cut Set Generation Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree

### B5.4.1.7 Cut Sets

Table B.4-2 contains the cut sets for the Facility Shield Door – Facility Door Closes on TEV fault tree.

Table B5.4-2. Cut Sets for Facility Shield Door – Facility Door Closes on TEV

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	100.00	2.000E-03	800-HEE0-WKRFACD-HFI-NOD	Operator closes facility door on TEV	2.000E-03
100.00	0.00	1.146E-13	800-HEE0-FACTOR1-TL-FOH	Shield Door Motor #1 Over Torque Limiter Failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield Door Motor #2 Over Torque Limiter Failure	2.856E-02
			800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	1.460E-06

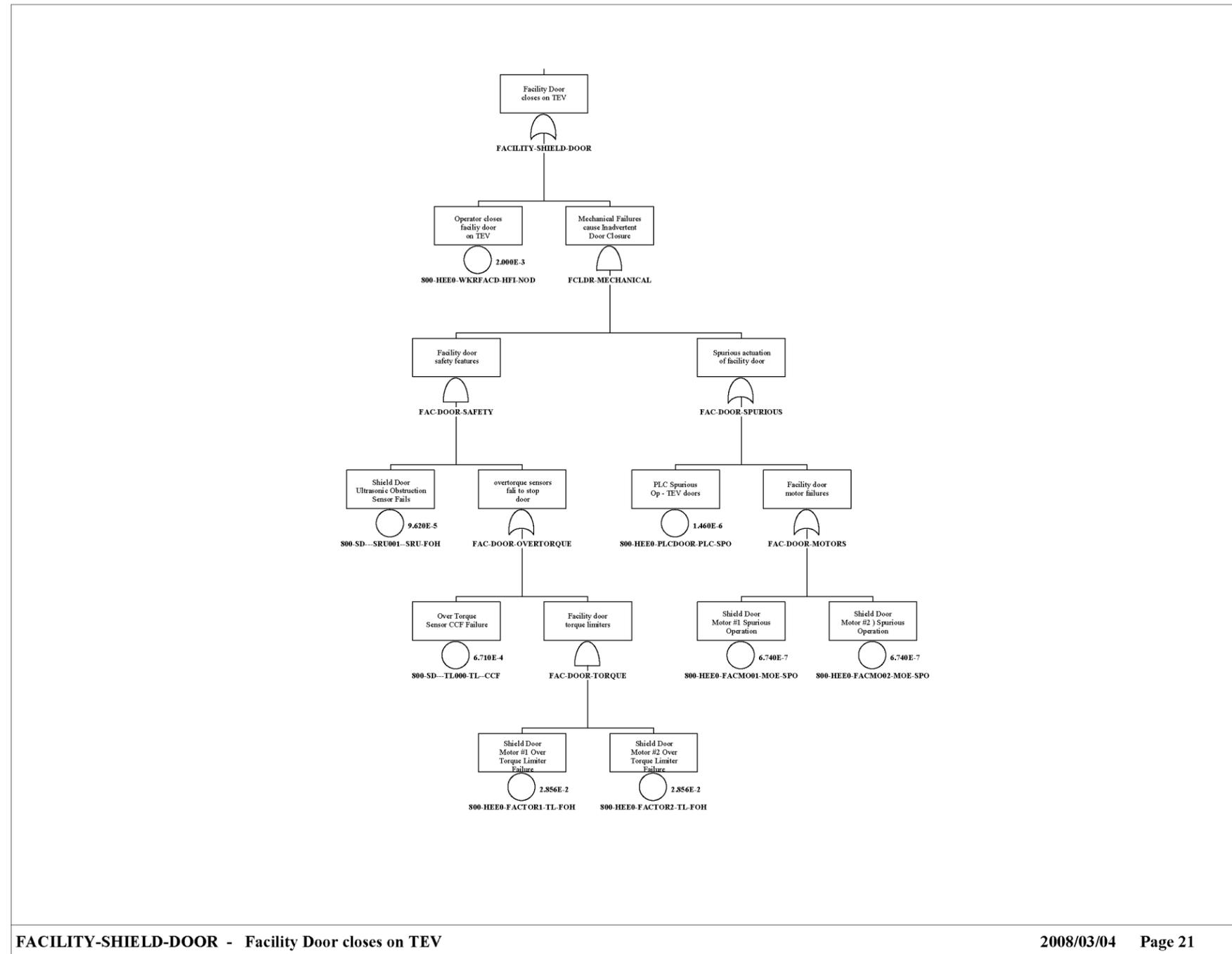
Table B5.4-2. Cut Sets for Facility Shield Door – Facility Door Closes on TEV (Continued)

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
100.00	0.00	9.424E-14	800-HEE0-PLCDOOR-PLC-SPO	PLC Spurious Op - TEV doors	1.460E-06
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
			800-SD---TL000-TL--CCF	Over Torque Sensor CCF Failure	6.710E-04
100.00	0.00	5.290E-14	800-HEE0-FACMO01-MOE-SPO	Shield Door Motor #1 Spurious Operation	6.740E-07
			800-HEE0-FACTOR1-TL-FOH	Shield Door Motor #1 Over Torque Limiter Failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield Door Motor #2 Over Torque Limiter Failure	2.856E-02
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
100.00	0.00	5.290E-14	800-HEE0-FACMO02-MOE-SPO	Shield Door Motor #2 Spurious Operation	6.740E-07
			800-HEE0-FACTOR1-TL-FOH	Shield Door Motor #1 Over Torque Limiter Failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield Door Motor #2 Over Torque Limiter Failure	2.856E-02
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
100.00	0.00	4.350E-14	800-HEE0-FACMO01-MOE-SPO	Shield Door Motor #1 Spurious Operation	6.740E-07
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
			800-SD---TL000-TL--CCF	Over Torque Sensor CCF Failure	6.710E-04
100.00	0.00	4.350E-14	800-HEE0-FACMO02-MOE-SPO	Shield Door Motor #2 Spurious Operation	6.740E-07
			800-SD---SRU001--SRU-FOH	Shield Door Ultrasonic Obstruction Sensor Fails	9.620E-05
			800-SD---TL000-TL--CCF	Over Torque Sensor CCF Failure	6.710E-04

NOTE: Op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

### B5.4.1.8 Fault Trees



Source: Original

Figure B5.4-3. FACILITY-SHIELD-DOOR – Facility Door Closes on TEV Fault Tree Sheet

## **B6 EMPLACEMENT ACCESS DOOR ANALYSIS**

### **B6.1 REFERENCES**

#### **Design Inputs**

The PCSA is a safety analysis 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), paragraph 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

B6.1.1 \*BSC (Bechtel SAIC Company) 2007. *Emplacement Access Door & Turnout Bulkhead*. 800-S0C-SSD0-00600-000 Rev 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070326.0020.

B6.1.2 Not Used.

B6.1.3 \*BSC 2007. *Subsurface Emplacement Access Door and Bulkhead Arrangement for LA (Sheet 2 of 2)*. 800-KV0-VUE0-00402-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070813.0015.

B6.1.4 \*BSC 2007. *Subsurface Emplacement Ventilation System Design Analysis*. 800-KVC-VUE0-00400-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071210.0009.

B6.1.5 \*BSC 2008. *Subsurface Construction and Emplacement Ventilation*. 800-KVC-VU00-00900-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080124.0010.

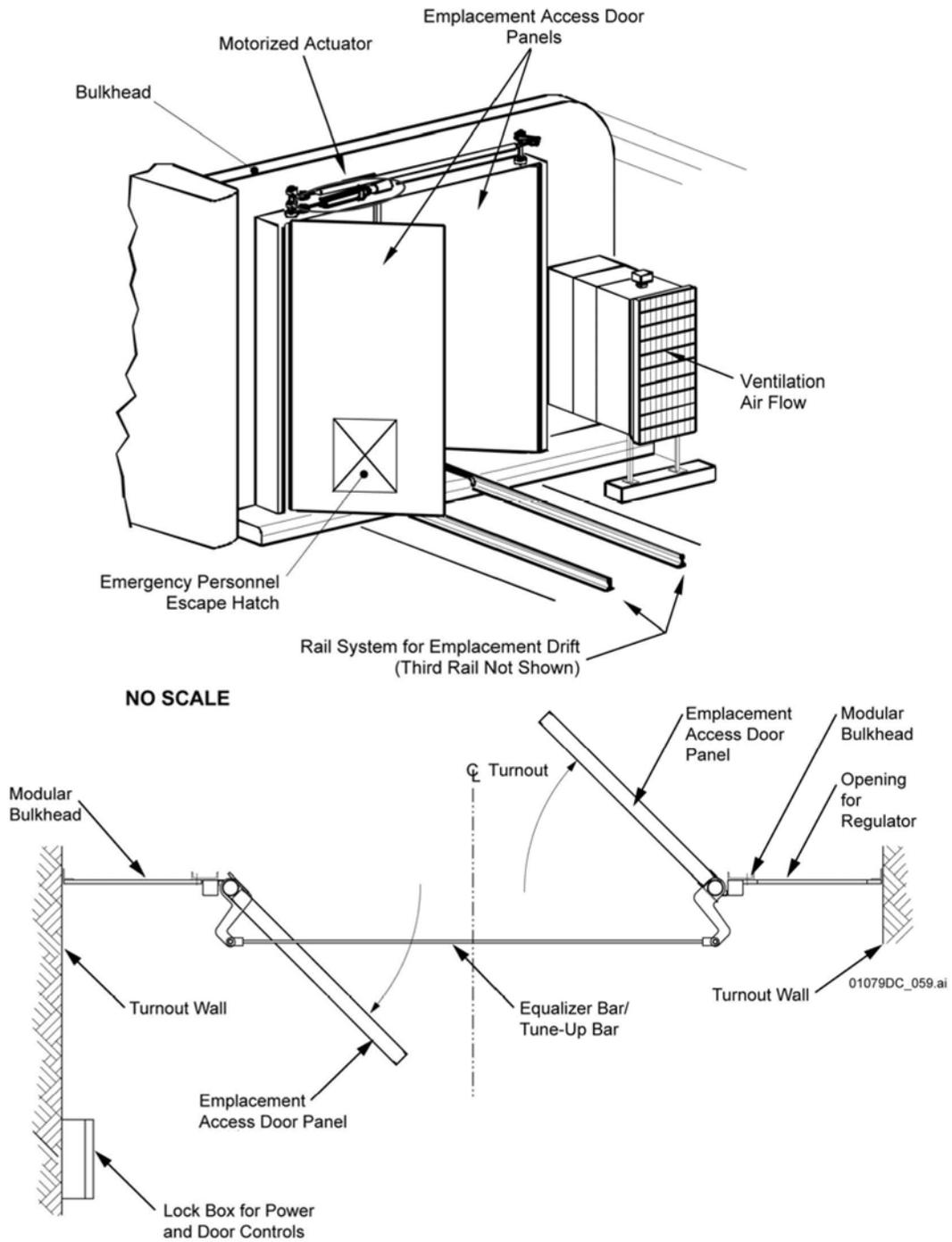
### **B6.2 EMPLACEMENT ACCESS DOOR DESCRIPTION**

The emplacement access door is a counter-opening, two-panel design in which one panel opens inward and the other panel opens outward (Figure B6.2-1). The door is intended to control entry and is not to provide radiation shielding. The overall doorway has a clear opening of approximately 16.5 × 12.4 ft in width/height (Ref. B6.1.4, Figure 7), and the door is approximately 19.3 × 14.1 ft in overall dimension to accommodate door framing. The emplacement access door panels is constructed from 3/16 in. minimum thick steel plates, separated and reinforced by steel spacers. The overall emplacement access door (both door panels) is estimated to weigh approximately 3.0 short tons (Ref. B6.1.1, Section 6.4.5).

For operation, the two door panels are linked together by an equalizer bar/tune-up bar that provides the linkage required for counter-opening the assembly (Figure B6.2-1). The linkage also contains an adjustment mechanism to provide fine-tuning of the door sealing. This design uses a single actuator and linkage bar to open and close both doors, thereby reducing the maintenance cost when compared to dual actuators. The actuator provides the driving force necessary to open the emplacement access door. The capacity of the actuator is not defined.

### **B6.2.1 Operations**

The emplacement access door is typically closed to maintain security and positive control of the emplacement drift. Normal door operation requires central control's input to prevent inadvertent access to the high radiation areas (Ref. B6.1.4, Section 6.9). However, a manual override switch is provided to open the door locally within a locked access box (Ref. B6.1.3). When a TEV is ready to proceed into an emplacement drift, the emplacement access door is remotely opened by the operator in the Central Control Center Facility. The actuator drives the two door panels to swing in opposite directions to open, allowing the TEV to pass through the doorway. Upon visual confirmation that the TEV has passed through the threshold and has completely entered the turnout drift, the operator in the Central Control Center Facility closes the door system. The process is reversed when the TEV is to exit the emplacement drift. It is estimated for emplacement that the emplacement access door for each drift will open and close conservatively about 470 times. The emplacement access door's instrumentation interfaces through the Digital Control and Management Information System to provide real-time status and supervisory control (Ref. B6.1.4, Section 6.9). When the emplacement access door is open, both audible and visual alarms notify workers and central control of the change in position of the doors (Ref. B6.1.4, Section 6.8).



Source: Modified from Ref. B6.1.5, Figure 20 and 21

Figure B6.2-1. Illustration of an Emplacement Access Door

### B6.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with systems, structures, and components. The five areas considered are addressed in Table B6.3-1 with the following dependencies:

1. Functional dependence.
2. Environmental dependence.
3. Spatial dependence.
4. Human dependence.
5. Failures based on external events.

Table B6.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Electrical power	Provides power to door	—	—	—	—
Motorized actuator	Opens and closes the door panels	—	—	—	—
Bulkhead Structure	Constrains and supports door panels	Failure due to corrosion or poor maintenance	Keeps door panels in correct location	—	Seismic loading can cause impact
Central control switch	Controls operation	—	—	Premature activation	—
Manual switch	Controls operation	—	—	Premature activation	—

Source: Original

### B6.4 EMPLACEMENT ACCESS DOOR RELATED FAILURE SCENARIO

One scenario and fault tree is associated with the emplacement access door:

1. Emplacement access door closes on TEV.

The scenario and tree are described in the following subsection.

#### B6.4.1 Description

The scenario describes the closure or failure of the emplacement access door onto the TEV, as the TEV passing through the door. The emplacement access door provides security to restrict the entrance of personnel into a high radiation area, the emplacement drift. However, the door does not provide any shielding protection. The door is actuated remotely to allow the TEV to pass in and out of the emplacement turnout drift as part of waste package emplacement operations.

Door operation is not interlocked with TEV motion and no anti-collision safety features are identified for the door. Cameras on the TEV provide confirmation of door status.

#### **B6.4.1.1 Success Criteria**

The success criterion for the scenario is that the emplacement access door operates without failure or spurious operations and that the operator does not close the door prematurely. During normal operations, the emplacement access door system should not close onto the TEV. During opening and closure operations, the door should not collapse onto the TEV.

#### **B6.4.1.2 Design Requirements and Features**

The following requirements are identified with respect to this scenario:

- The operational status of the door is clearly displayed on visual monitor for the remote operations on the control panel including operations such as opening and closing of the door.
- The TEV shielded enclosure is able to maintain the shielding function in case of closure of the emplacement access door on the TEV.
- Normal periodic maintenance and inspection are performed on the bulkhead and door mounting supports and door mechanism to allow for the safe operation of the door without collapsing the door panels onto the TEV.

#### **B6.4.1.3 Fault Tree Model**

The fault tree model for the sequence is labeled as AC-DRIMP-INIT. (This fault tree has been discussed previously as part of the discussion for the DRIFT-TEV-IMPACT discussion in section B1.) The top event is the initiating event of the doors closing and impacting on the TEV. This top event is realized by either the occurrence of the door closure due to human error or by mechanical failure. Human error is represented by a basic event describing the operator failure by closing the emplacement access door prematurely, prior to the TEV complete passing into the turnout, and the door impacting the TEV. Mechanical failure occurs by the joint occurrence of a spurious signal to close the emplacement access door together with the failure of the door mechanism and safety features; the joint input is represented by an AND gate.

Regarding the failure of the door mechanism and safety features, a single input is identified involving the door actuator motor system. The door drive system is represented by a basic input event representing the failure of the motors driving the door system to stop.

The contributing factor that causes the mechanical door failure is the generation of a spurious signal that activates the door actuator to close. The spurious signal can be generated by either a fault in the programmable logic controller within the remote control and communication system or a failure in the actuator motor. The spurious signal generated by programmable logic controller is represented as a basic event, as is the failure of the actuator motor.

#### B6.4.1.4 Basic Event Data

Table B6.4-1 contains a list of basic events used in the fault tree, AC-DRIMP-INIT, which models the failures associated with the closure of the emplacement drift doors on a TEV.

Table B6.4-1 Basic Event Data for Closure of Drift Doors on TEV

Name	Description	Calc. Type <sup>a</sup>	Calculated Probability	Mean Failure Portability	Lambda	Mission Time <sup>a</sup>
800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	1	2.000E-03	2.000E-03	0.000E+00	0.000E+00
800-HEE0-AXSDR00-PLC-SPO	Programmable Logic Controller Spurious Operation	3	2.081E-09	0.000E+00	3.650E-07	5.700E-03
800-HEE0-AXSM001-MOE-FSO	Motor (Electric) Fails to Shut Off	3	7.695E-11	0.000E+00	1.350E-8	5.700E-03
800-HEE0-AXSM002-MOE-FSO	Motor (Electric) Fails to Shut Off	3	7.695E-11	0.000E+00	1.350E-8	5.700E-03
800-HEE0-ACTADR1-ATP-SPO	Actuator Spurious Op – Emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03
800-HEE0-ACTADR2-ATP-SPO	Actuator Spurious Op – Emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03

NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

Calc. = calculation; Op = operation; TEV = transport and emplacement vehicle.

Source: Original

##### B6.4.1.4.1 Human Failure Events

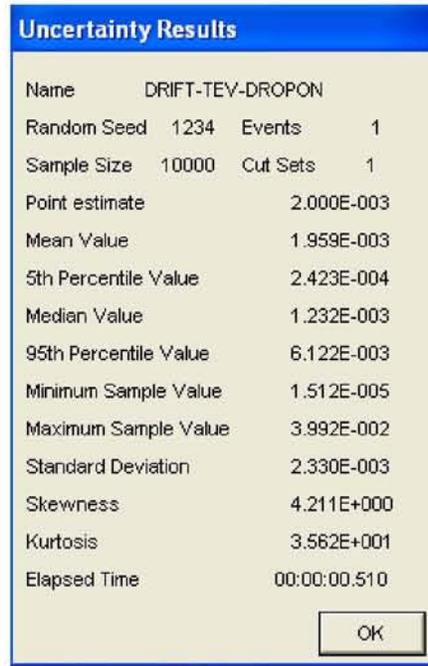
One basic event is identified as associated with human error involving the premature closure of the emplacement access door. The basic event, the operator closes the emplacement drift door on the TEV, is identified as 800-HEE0-AXSDR00-HFI-NOD.

##### B6.4.1.4.2 Common-Cause Failures

There are no CCFs identified for this model.

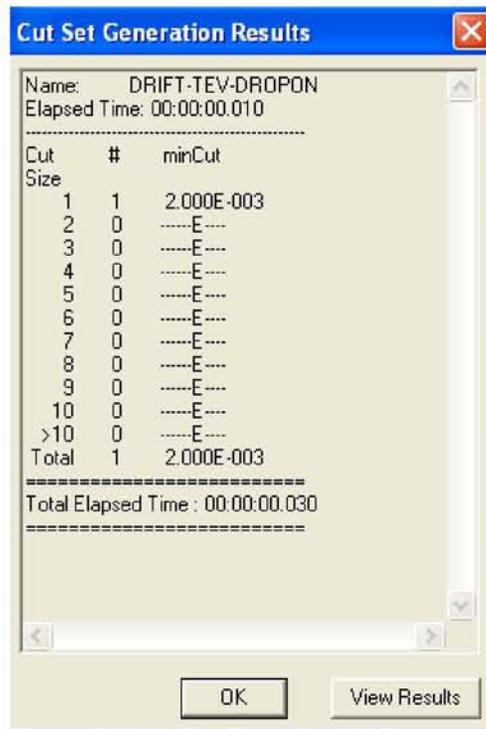
##### B6.4.1.5 Uncertainty and Cut Set Generation Results

Uncertainty and cut set quantification results from SAPHIRE for the fault tree associated with the emplacement access door, AC-DRIMP-INIT are presented in Figures B6.4-1 and B6.4-2.



Source: Original

Figure B6.4-1. Uncertainty Results for AC-DRIMP-INIT



Source: Original

Figure B6.4-2. Cut Set Generation Results for AC-DRIMP-INIT

**B6.4.1.6 Cut Sets**

Table B6.4-2 contains the cut sets for fault tree AC-DRIMP-INIT.

Table B6.4-2. AC-DRIMP-INIT Cut Sets

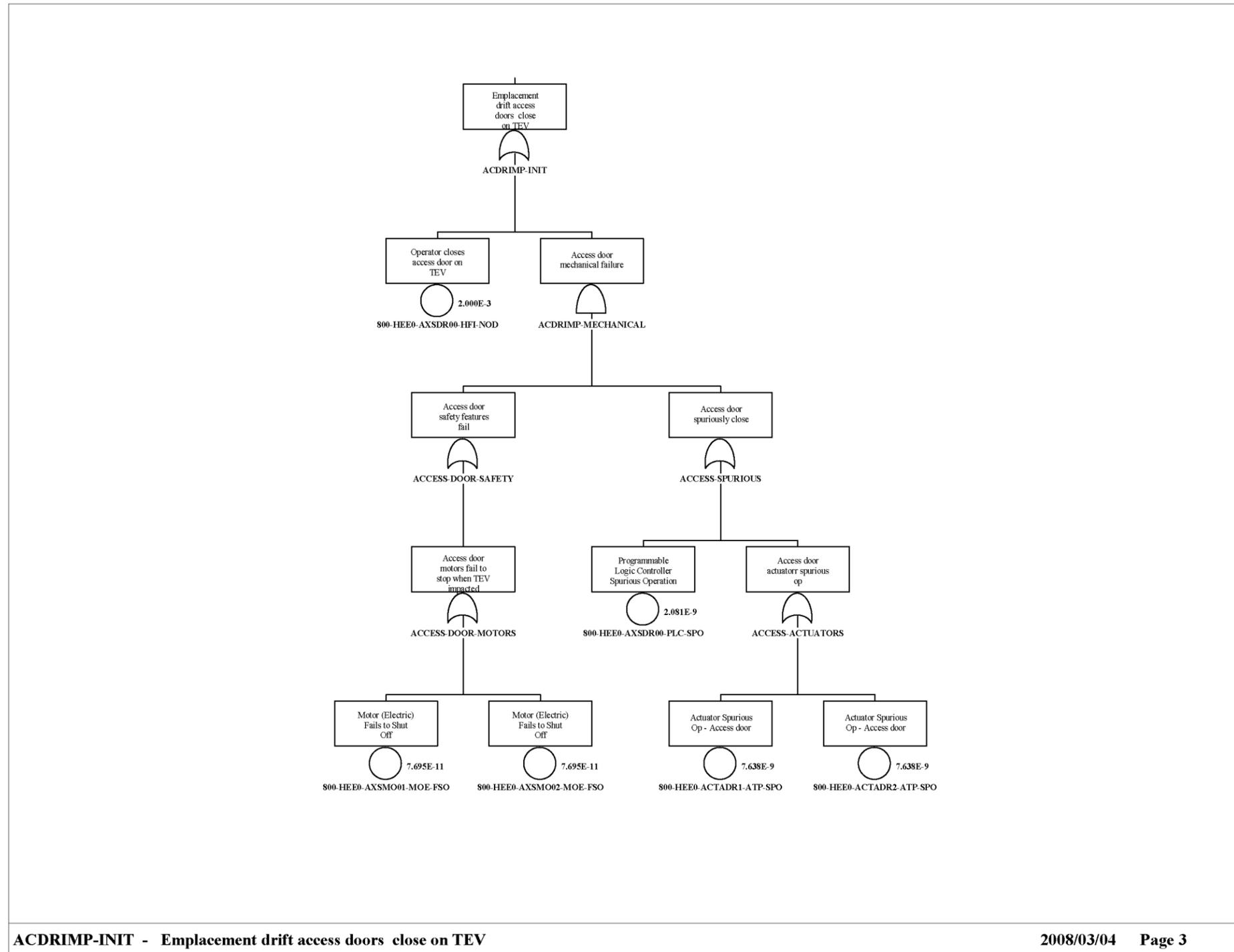
% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	100.00	2.000E-03	800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	2.000E-03
100.00	0.00	5.877E-19	800-HEE0-ACTADR1-ATP-SPO	Actuator Spurious Op - Emplacement access door	7.638E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR2-ATP-SPO	Actuator Spurious Op - Emplacement access door	7.638E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR1-ATP-SPO	Actuator Spurious Op - Emplacement access door	7.638E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR2-ATP-SPO	Actuator Spurious Op - Emplacement access door	7.638E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11
100.00	0.00	1.601E-19	800-HEE0-AXSDR00-PLC-SPO	Programmable Logic Controller Spurious Operation	2.080E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11
100.00	0.00	1.601E-19	800-HEE0-AXSDR00-PLC-SPO	Programmable Logic Controller Spurious Operation	2.080E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (Electric) Fails to Shut Off	7.695E-11

NOTE: Op = operation; TEV = transport and emplacement vehicle.

Source: Original

**B6.4.1.7 Fault Tree**

The fault tree associated with the emplacement access doors (AC-DRIMP-INIT) is presented in Figure B6.4-3.



Source: Original

Figure B6.4-3. DRIFT-TEV-DROPON - Fault Tree for Emplacement Access Door Closes on TEV

## B7 ADDITIONAL FAULT TREES

Seventeen additional fault trees were developed to address events that could impact either a TEV with a waste package or the waste package alone during subsurface operations. These fault trees are identified in Table B7-1. Sixteen of these trees are top level or top level linking trees; the results of quantifying the trees were input directly into the Excel spreadsheet used to quantify subsurface event sequences as initiating events. The seventeenth tree, DSGANT-INIT, is input into the top level fault tree DRIFT-WP-IMPACT.

Table B7-1. Top Level and Linking Fault Trees

Fault Tree	Description	Events considered	Top Level Fault Tree	System Fault Trees Used as Input
FACILITY-DROPON	Object dropped on Waste Package as it leaves facility	Drops from Crane operation	Top level tree	None
TRANSIT-DERAIL	TEV derailed during surface transit to emplacement	Derailment of TEV during surface transit	Top level tree	None
TRANSIT-DROPON	Impact to TEV during transit from falling object	Rockfalls	Top level tree	None
DRIFT-TEV-IMPACT	Impact to TEV during subsurface travel and emplacement	Emplacement door impacts, derailment, and TEV overrun of rails	Top level linking tree	ACDRIMP-INIT (B6), Drift-derail (B4.1), TEV-end-rail (B4.1)
DRIFT-WP-DROPON	Drop of heavy load on WP during subsurface operation	Rockfall and drop of drip shield onto WP	Top level tree	DRIPSHIELD-DROPPED (B4)
DRIFT-WP-IMPACT	WP impacted in the drift	Linking tree to TEV-IMPACTS-WP and DSGANT-INIT	Top level tree	TEV-IMPACTS-WP (B1.4.10), DSGANT-INIT
DSGANT-INIT	Gantry derails and strikes WP	Drip shield gantry derailment	Input to DRIFT-WP-IMPACT	None
SSO-CRCF-SD-IMPACT-HVAC	WP impact facility door In the CRCF where HVAC is available	Impacts with facility door and HVAC failures	Top level linking tree	FACILITY-SHIELD-DOOR (B5), HVAC (B2)
SSO-HVYLOAD-DROPON-HVAC	Heavy load dropped on WP in CRCF where HVAC is available	Crane drops of objects onto WP and HVAC failures	Top level linking tree	FACILITY-DROPON, HVAC (B2)
SSO-TEV-COLL-HVAC	TEV collision in CRCF where HVAC is available	TEV collisions with facility structures with HVAC failures	Top level linking tree	FACILITY-COLLISION (B1.2), HVAC (B2)

Table B7-1. Top Level and Linking Fault Trees (Continued)

<b>Fault Tree</b>	<b>Description</b>	<b>Events considered</b>	<b>Top Level Fault Tree</b>	<b>System Fault Trees Used as Input</b>
SSO-WP-DROP-HVAC	WP dropped in CRCF where HVAC is available	TEV drops WP with HVAC failures	Top level linking tree	FACILITY-DROP (B1.7), HVAC (B2)
SSO-WP-TEV-SD-HVAC	TEV shield door impacts WP in CRCF where HVAC is available	TEV doors close on WP with HVAC failures	Top level linking tree	FACILITY-TEV-DOOR (B1.1), HVAC (B2)
SHIELD-PROXIMITY	Direct exposure due to extended proximity to TEV during transit	Human errors	Top level tree	None
SHIELD-ENTRY	Direct exposure due to emplacement drift entry by workers	Human errors	Top level tree	None
FIRE-DRIFT	Fire impacts WP in Drift	Drift Fires	Top level tree	None
FIRE-SUBSURFACE	Fire impacts WP on subsurface rail	Subsurface fires during transit	Top level tree	None
FIRE-SURFACE	Fire impacts WP on surface rail	Surface fires during transit	Top level tree	None

NOTE: TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

The basic events used in each of these fault trees are provided in Table B7-2.

Table B7-2. Basic Events for Additional Fault Trees

Name	Description	Calc. Type <sup>a</sup>	Calc. Prob.	Fail. Prob. <sup>a</sup>
800-FAC-WPCRNDP-CRW-DRP	WP (Non-SFP) Crane Drop	1	1.050E-04	1.000E-04
800-HEE0-DEAILS-TEV-DER	TEV- Derails per mile	1	1.180E-05	1.18E-05
800-HEE0-DEAILS-DSG-DER	Drip shield gantry derails	1	1.180E-05	1.180E-05
800-TRANSIT-ROCKFALL <sup>b</sup>	Rockfall Probability	1	0.000E+00	0.000E+00
800-TRANSIT-TIME	Transit time from entrance to emplacement drift in years	V	2.200E-04	2.200E-04
DSG-MILES	Miles drip shield gantry travels	V	1.000E-01	1.000E-01
ROCKFALL-ON-WP*	Rockfall on WP in drift	1	0.000E+00	0.000E+00
TEV-DEMAIL-MILES-SURF	Miles travelled by TEV on surface	V	2.000E+00	2.000E+00
800-HEE0-WKRPROX-HRI-NOD	Operator fails to avoid TEV	1	0.000E+00	0.000E+00
800HEE0-WKRDRFT-HRI-NOD	Worker enters drift from access main	1	0.000E+00	0.000E+00
FIRE-IN-DRIFT	Fire frequency divided by three	1	3.030E-07	3.030E-07
FIRE-IN-SUBSURFACE	Fire frequency divided by three	1	3.030E-07	3.030E-07
FIRE-ON-SURFACE	Fire frequency divided by three	1	3.030E-07	3.030E-07

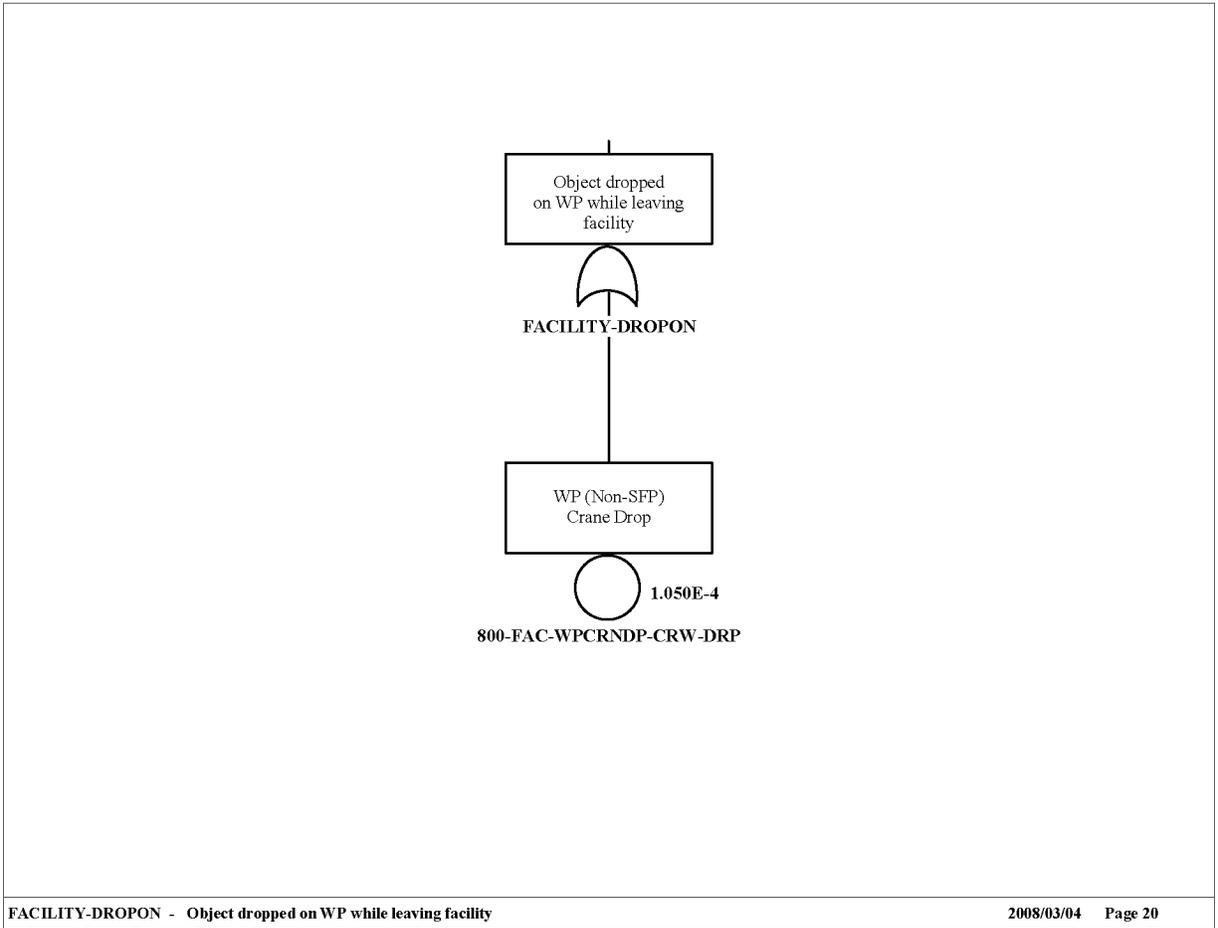
NOTE: <sup>a</sup> For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

<sup>b</sup> Rockfall incorporated into seismic analysis.

Calc. = calculation; Fail. = failure; Prob. = probability; SFP = single failure proof; TEV = transport and emplacement vehicle; WP = waste package.

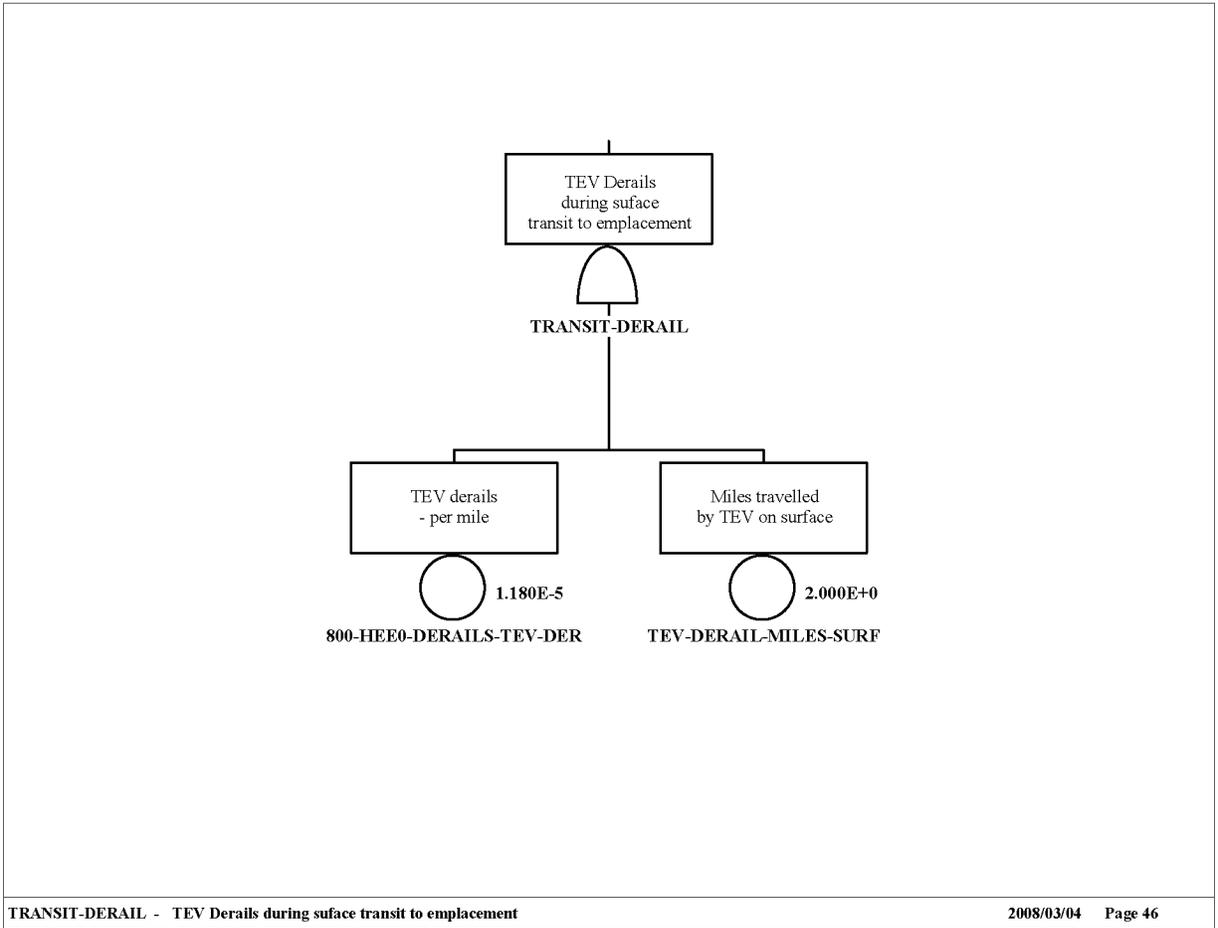
Source: Original

The seventeen fault trees are presented in Figures B7-1 through B7-17.



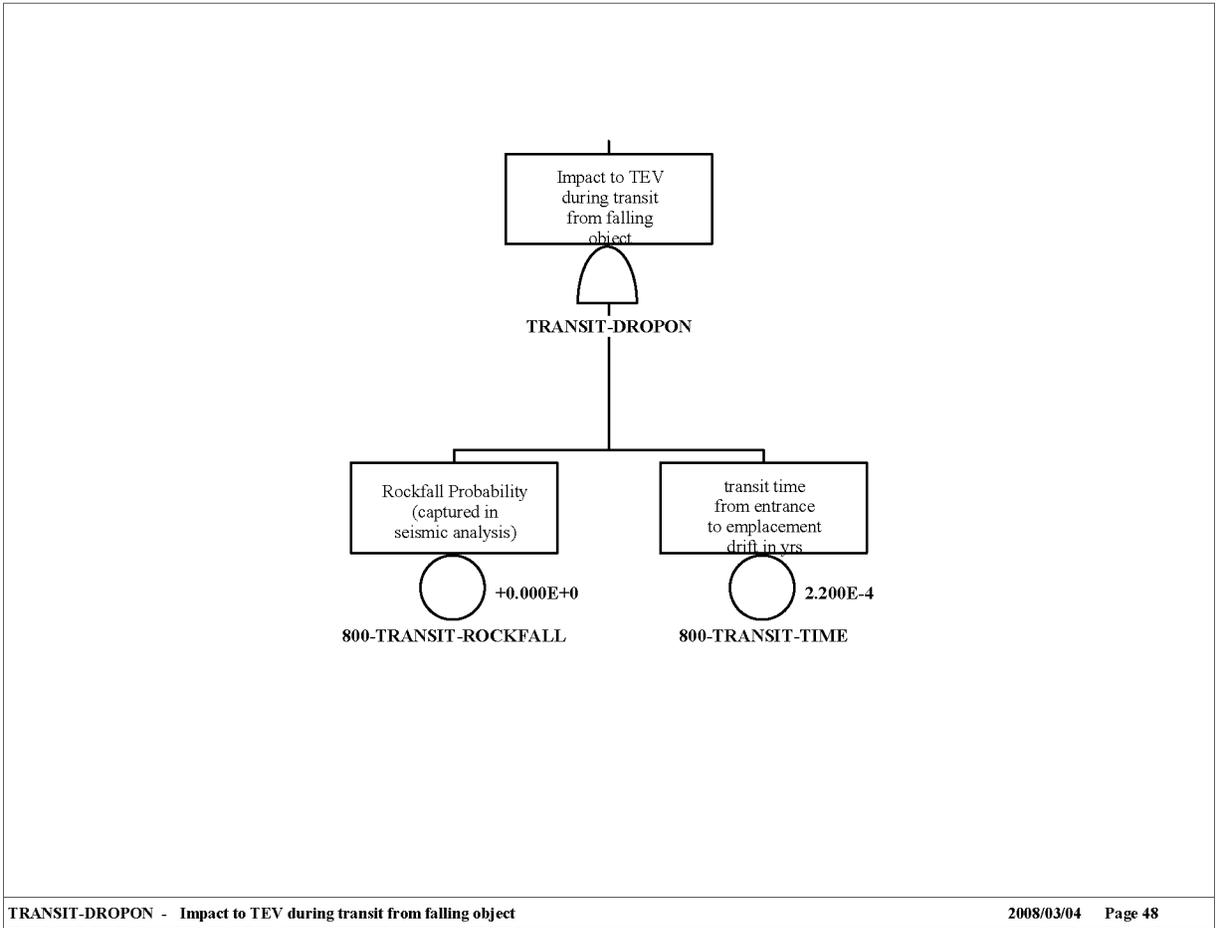
Source: Original

Figure B7-1. Facility-Drop on Fault Tree



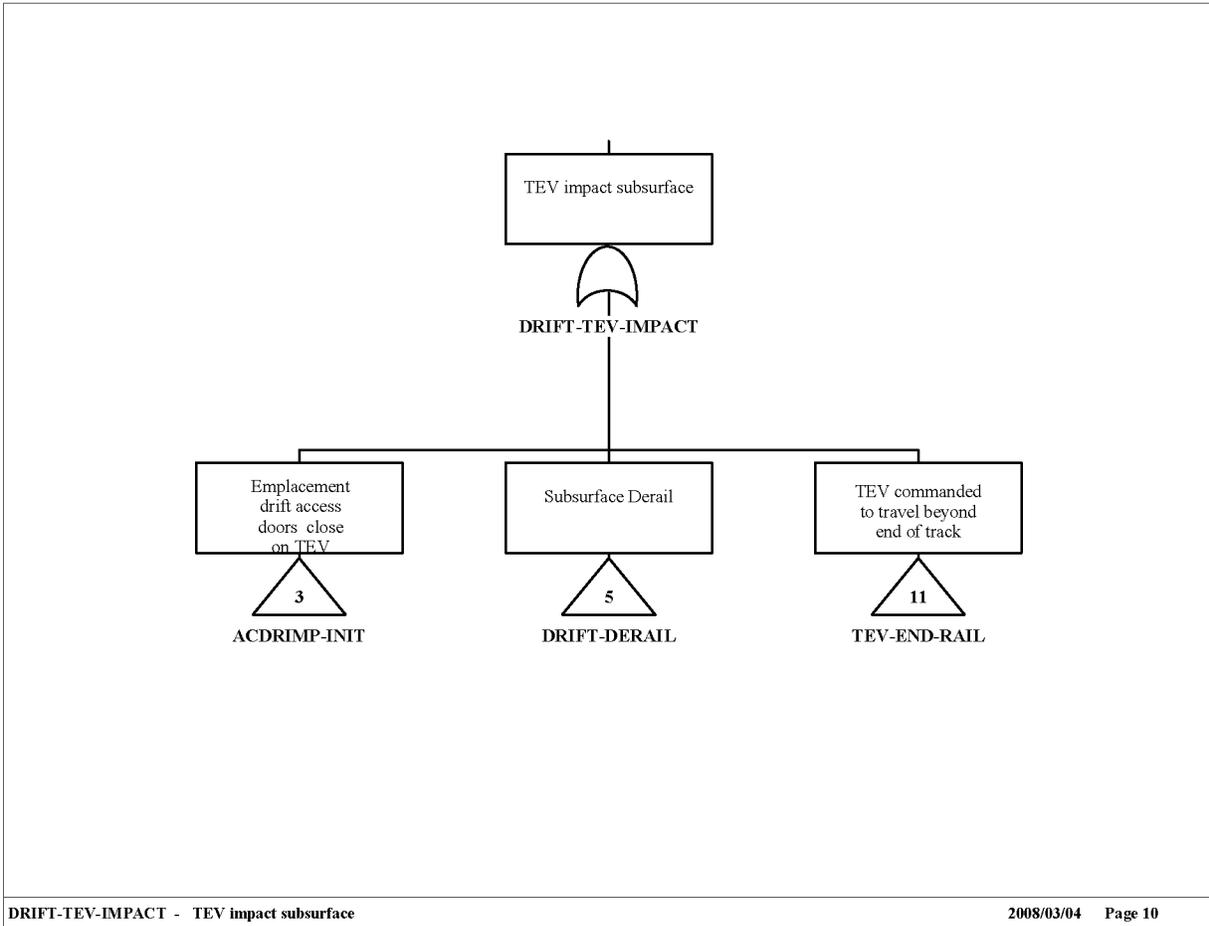
Source: Original

Figure B7-2. Transit-Derail Fault Tree



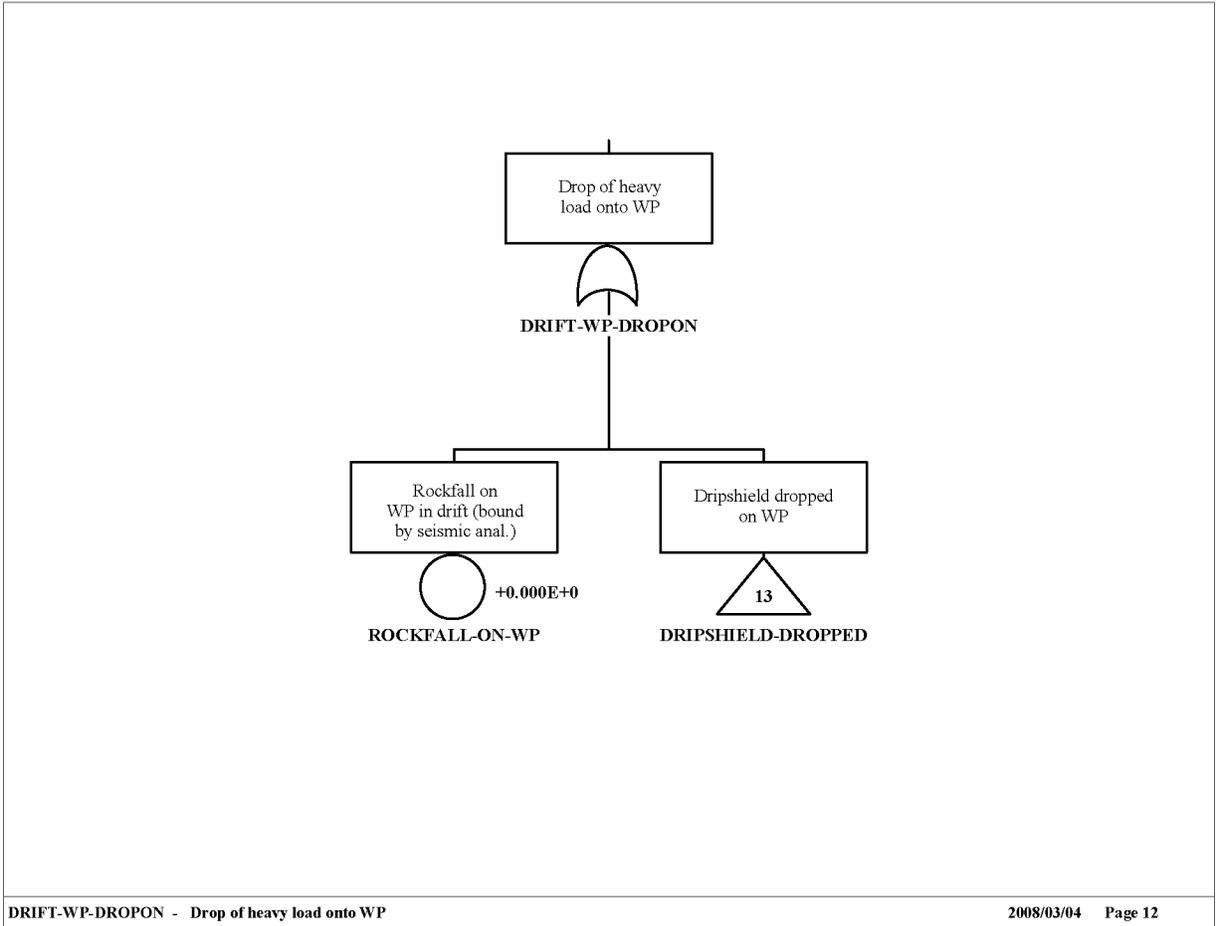
Source: Original

Figure B7-3. Transit-Drop on Fault Tree



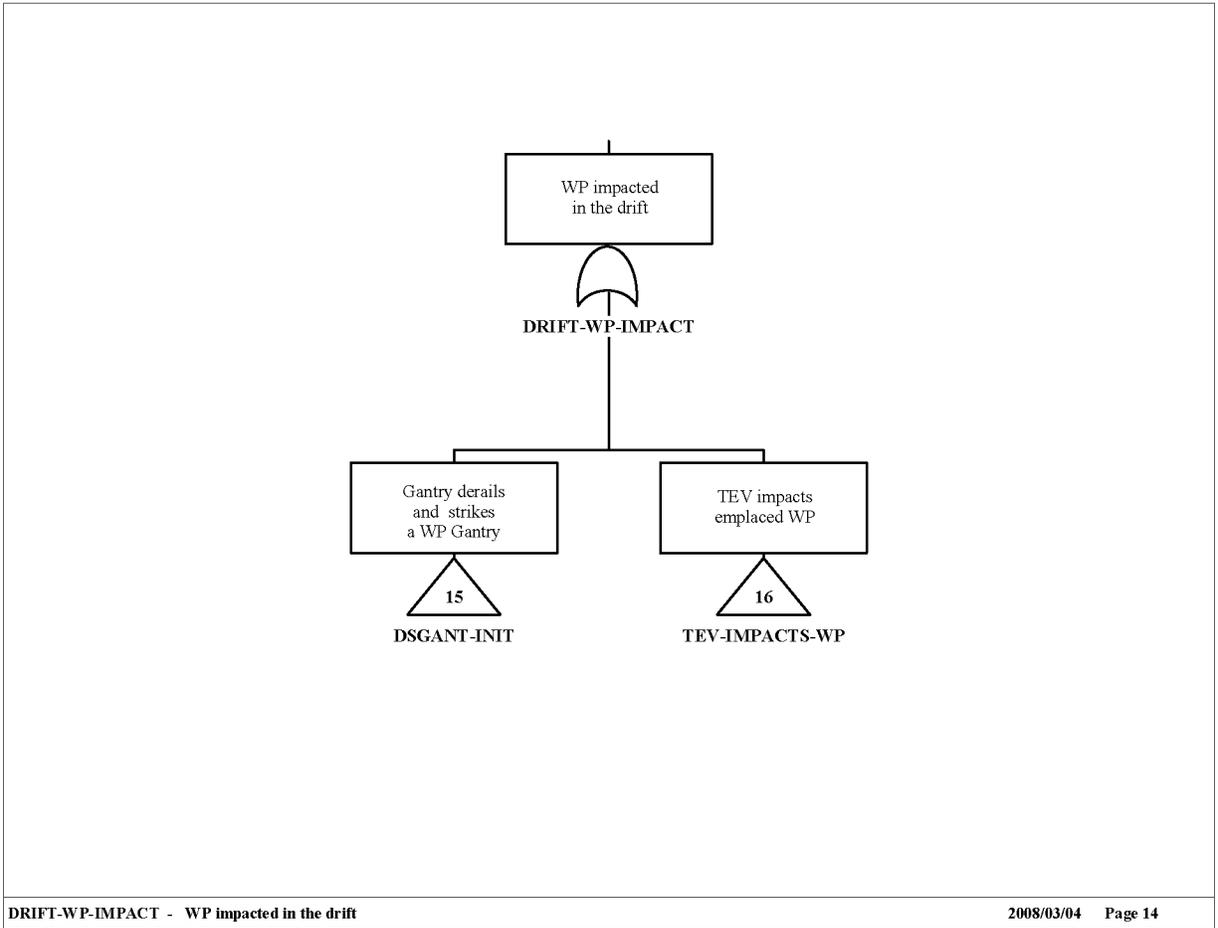
Source: Original

Figure B7-4 DRIFT-TEV-IMPACT Fault Tree



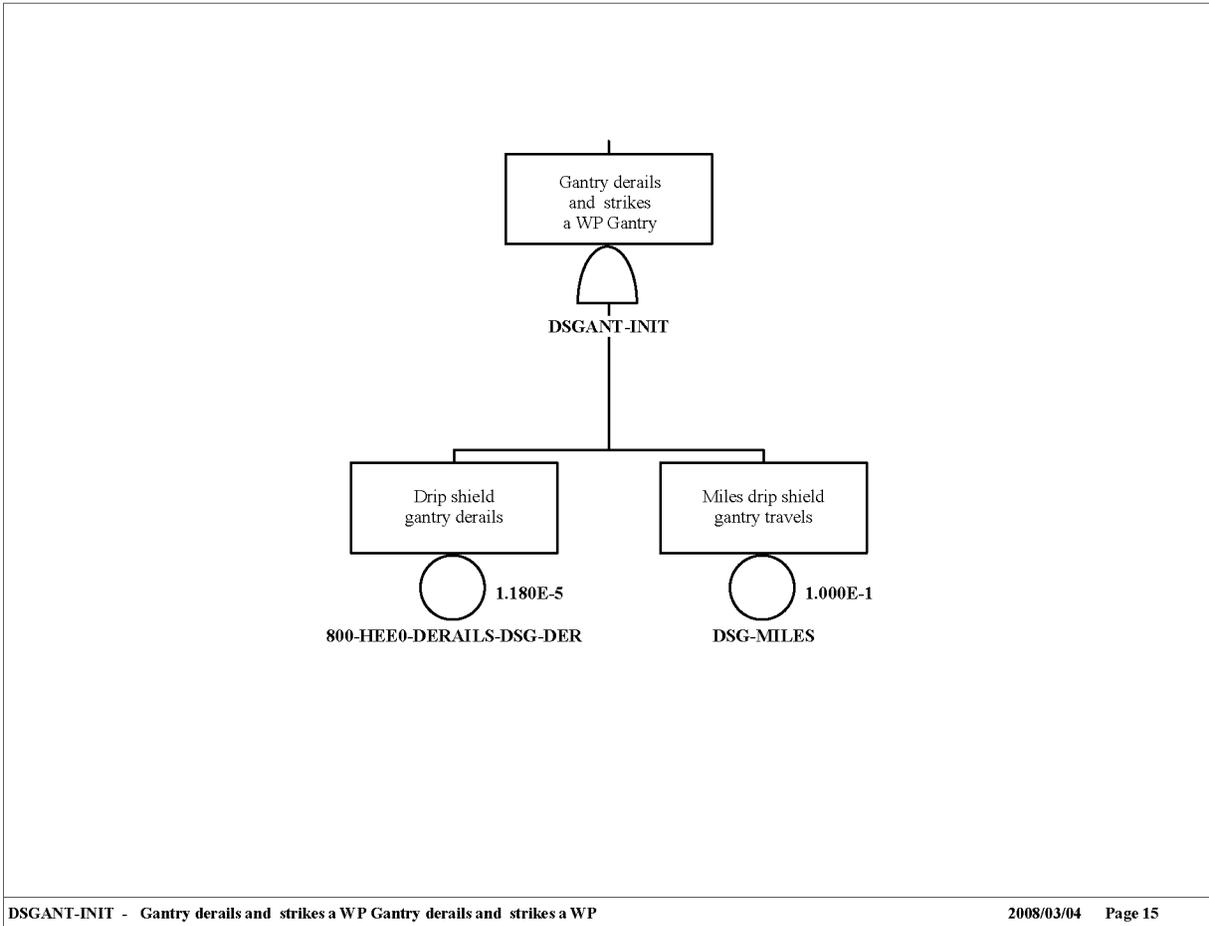
Source: Original

Figure B7-5. Drift-WP-Drop on Fault Tree



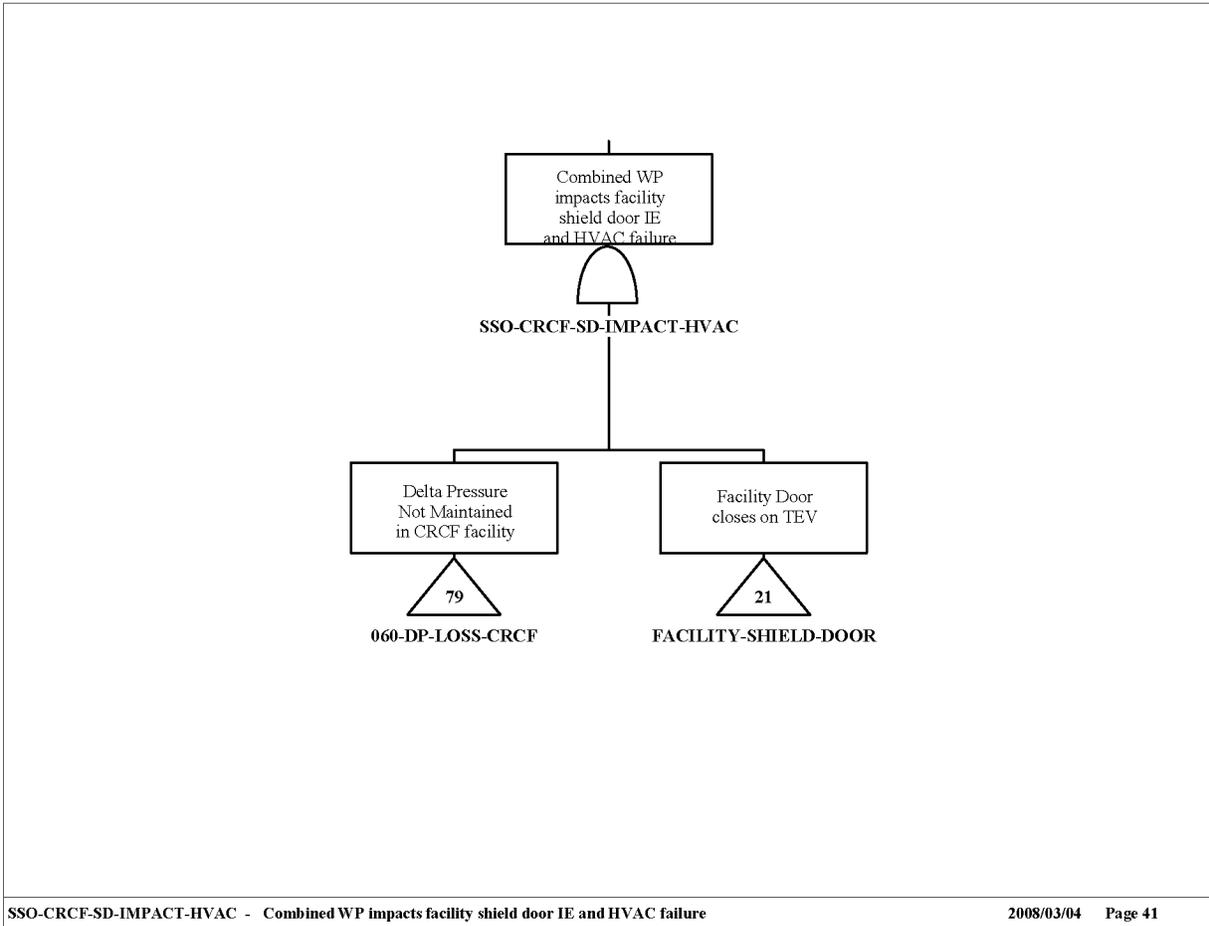
Source: Original

Figure B7-6. Drift-WP-Impact Fault Tree



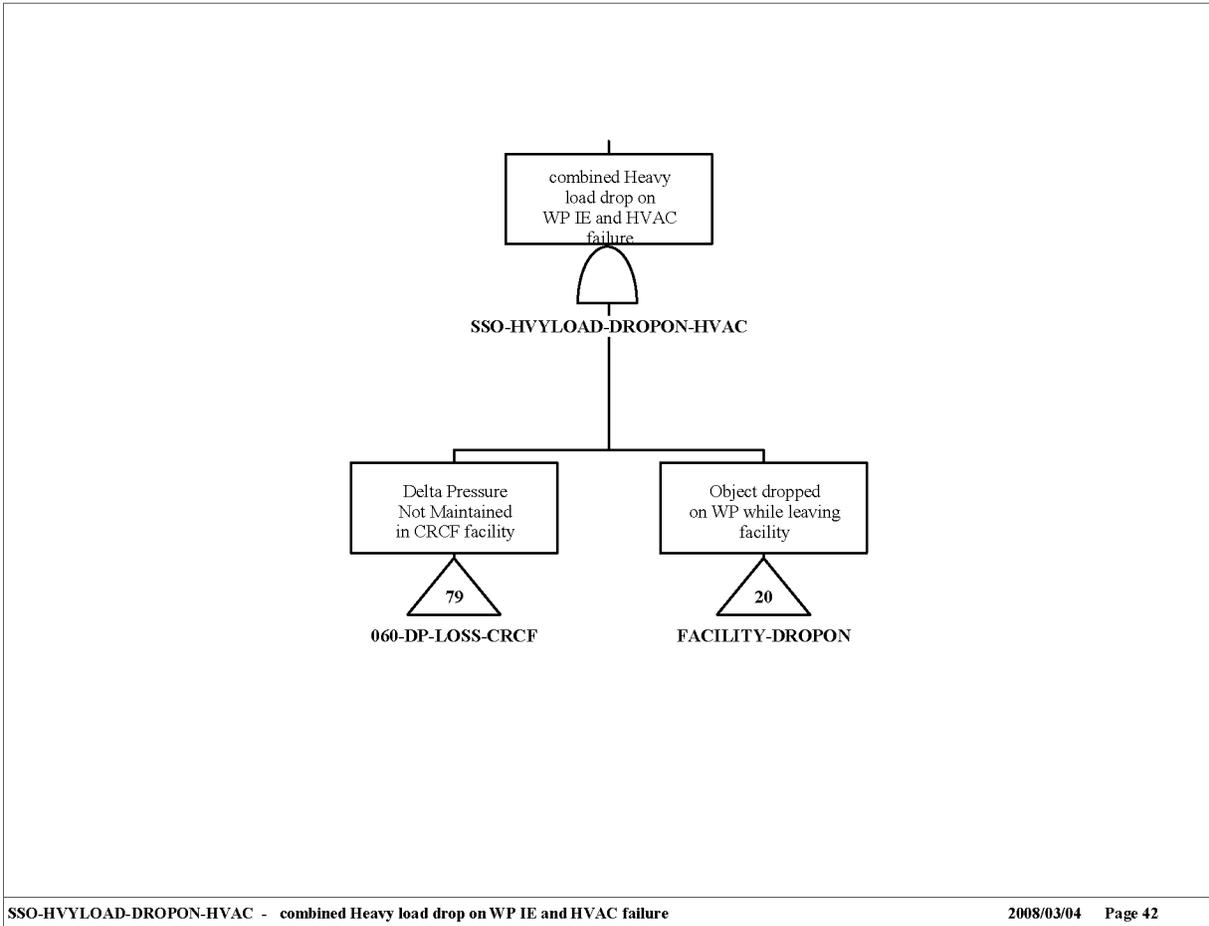
Source: Original

Figure B7-7. DSGANT-INIT Fault Tree



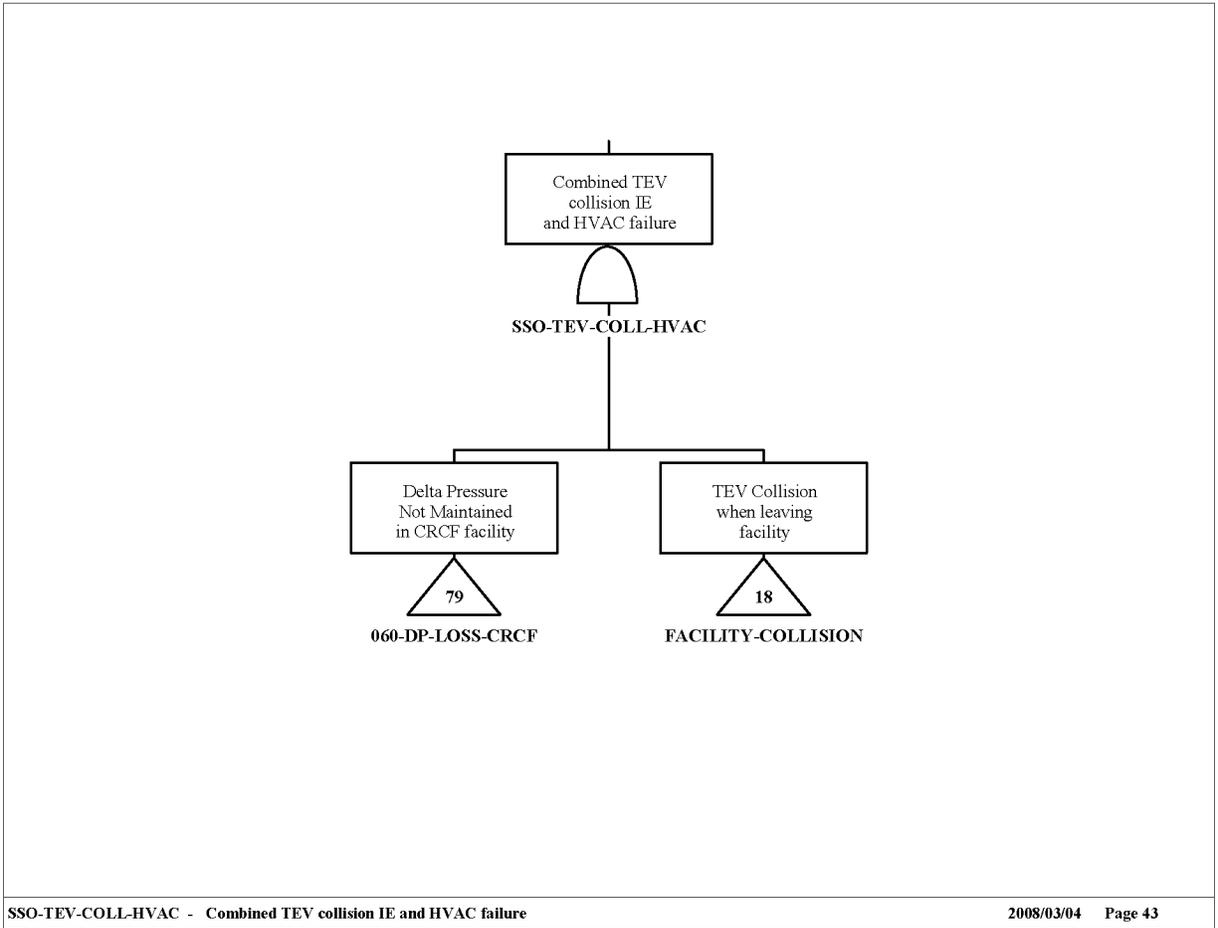
Source: Original

Figure B7-8. SSO-CRCF-SD-IMPACT-HVAC Fault Tree



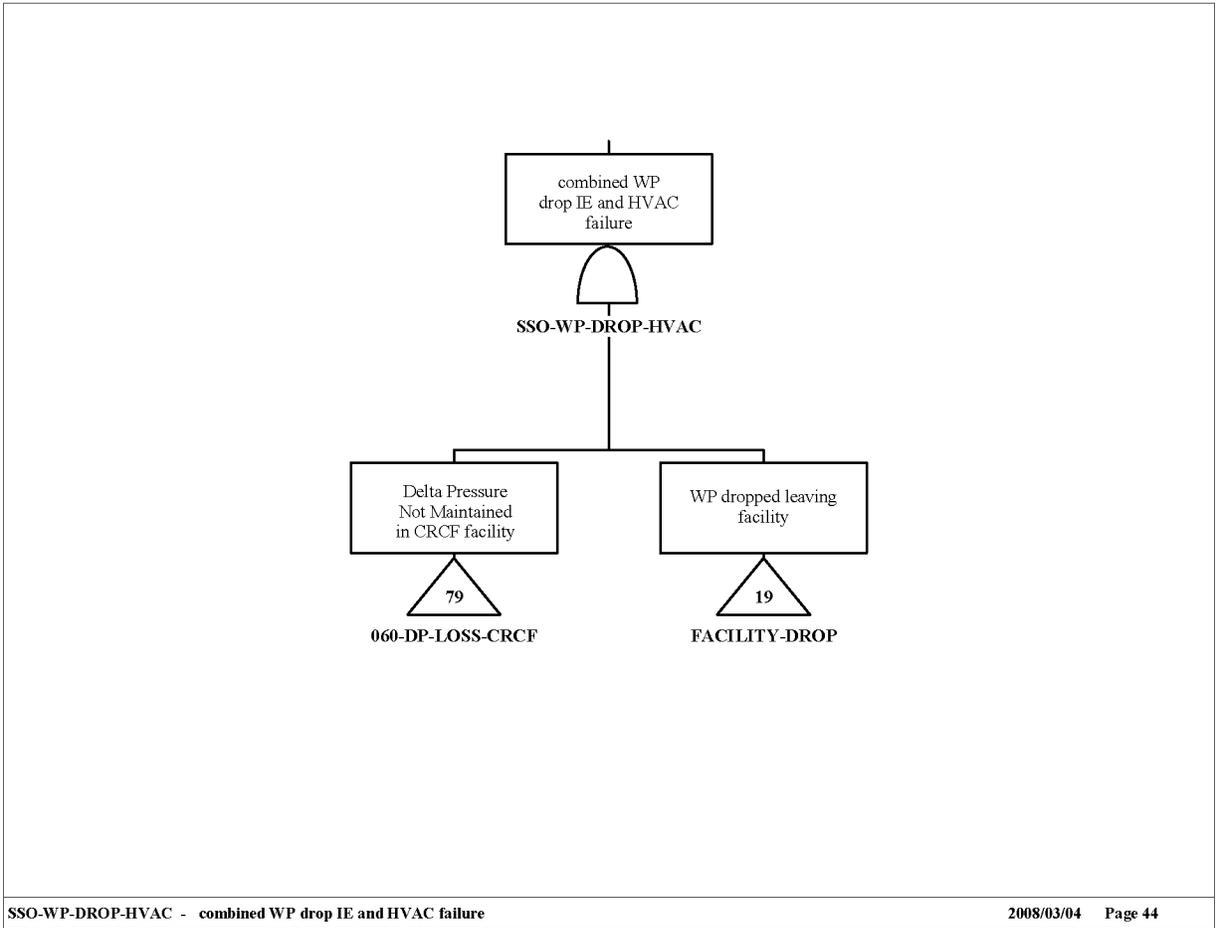
Source: Original

Figure B7-9. SSO-HVYLOAD-DROPON-HVAC Fault Tree



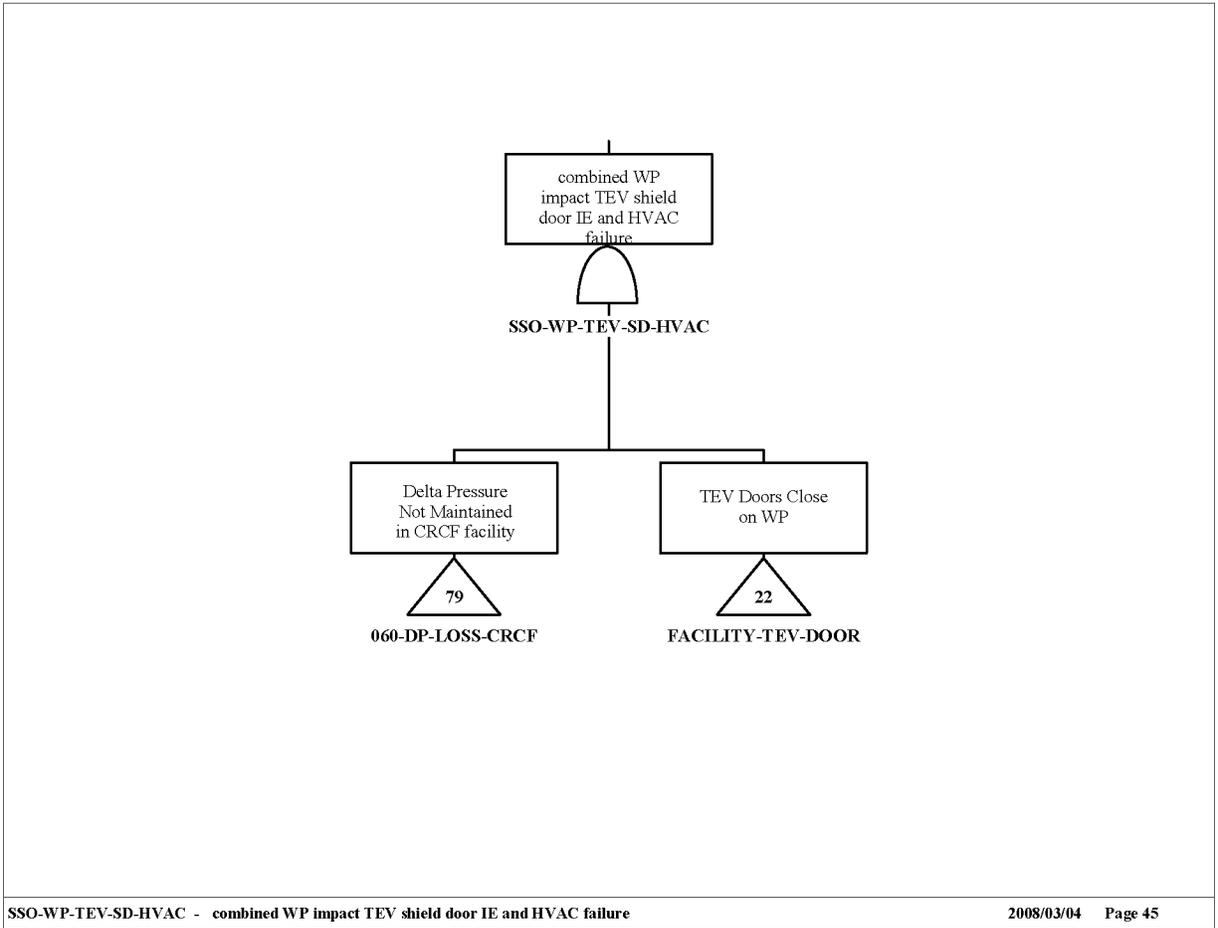
Source: Original

Figure B7-10. SSO-TEV-COLL-HVAC Fault Tree



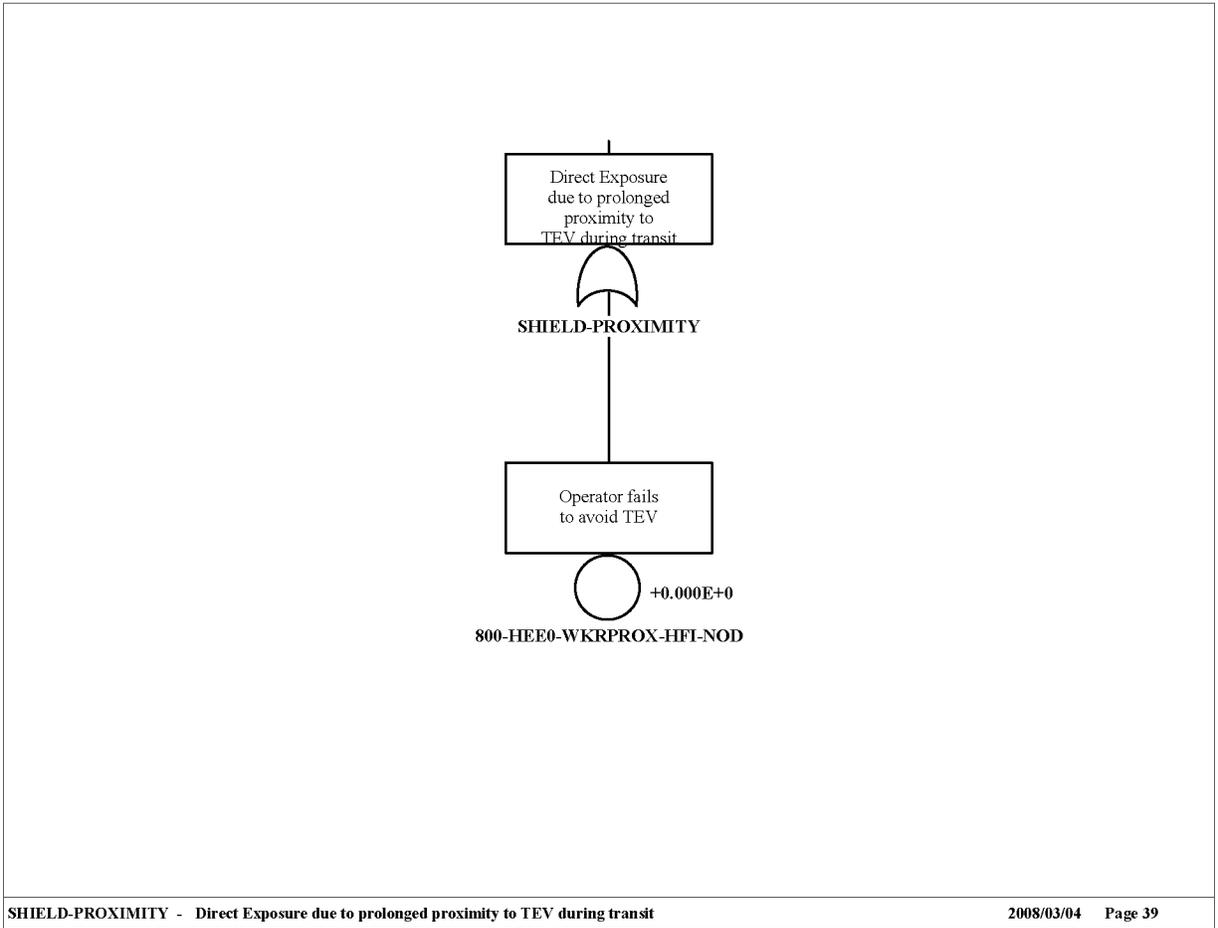
Source: Original

Figure B7-11. SSO-WP-DROP-HVAC Fault Tree



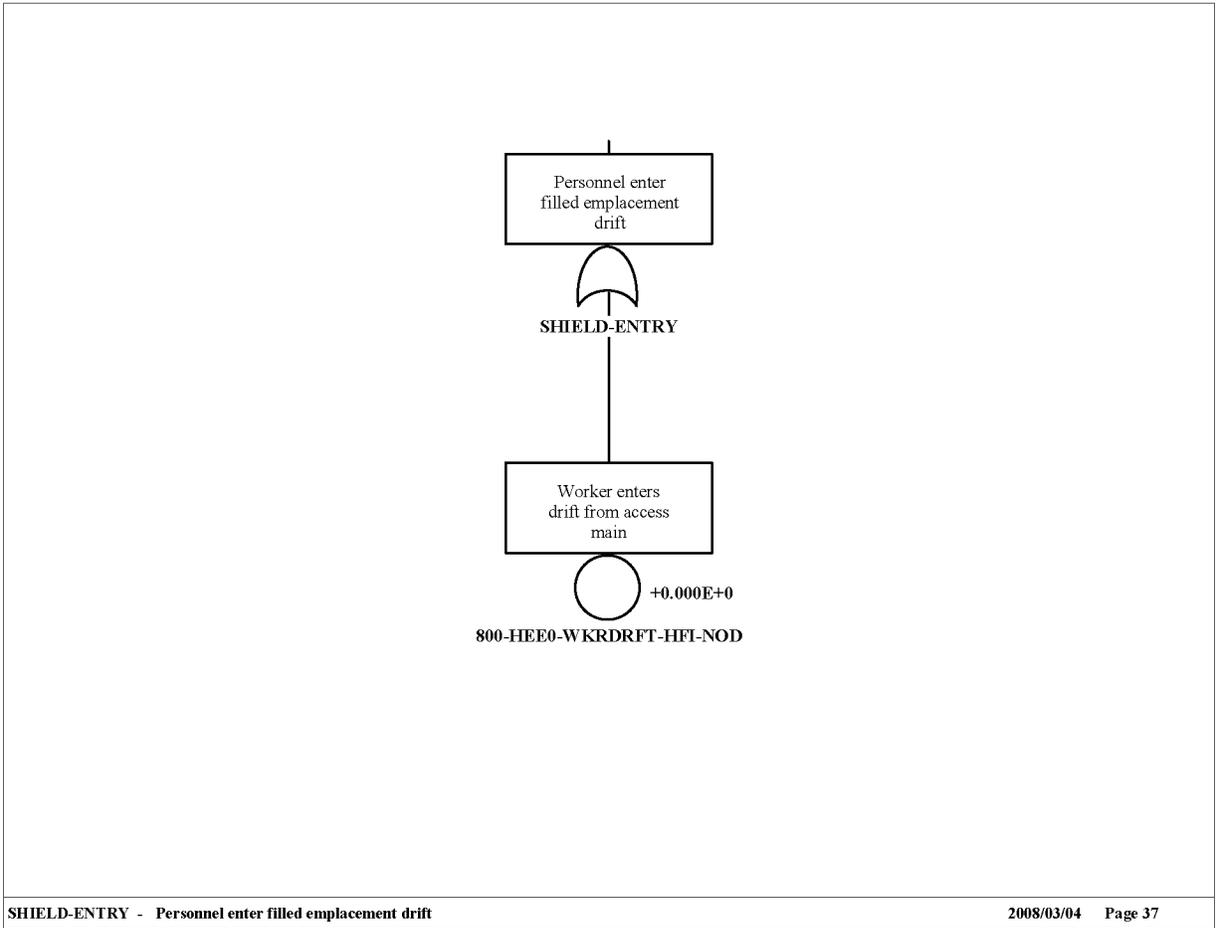
Source: Original

Figure B7-12. SSO-WP-TEV-SD-HVAC Fault Tree



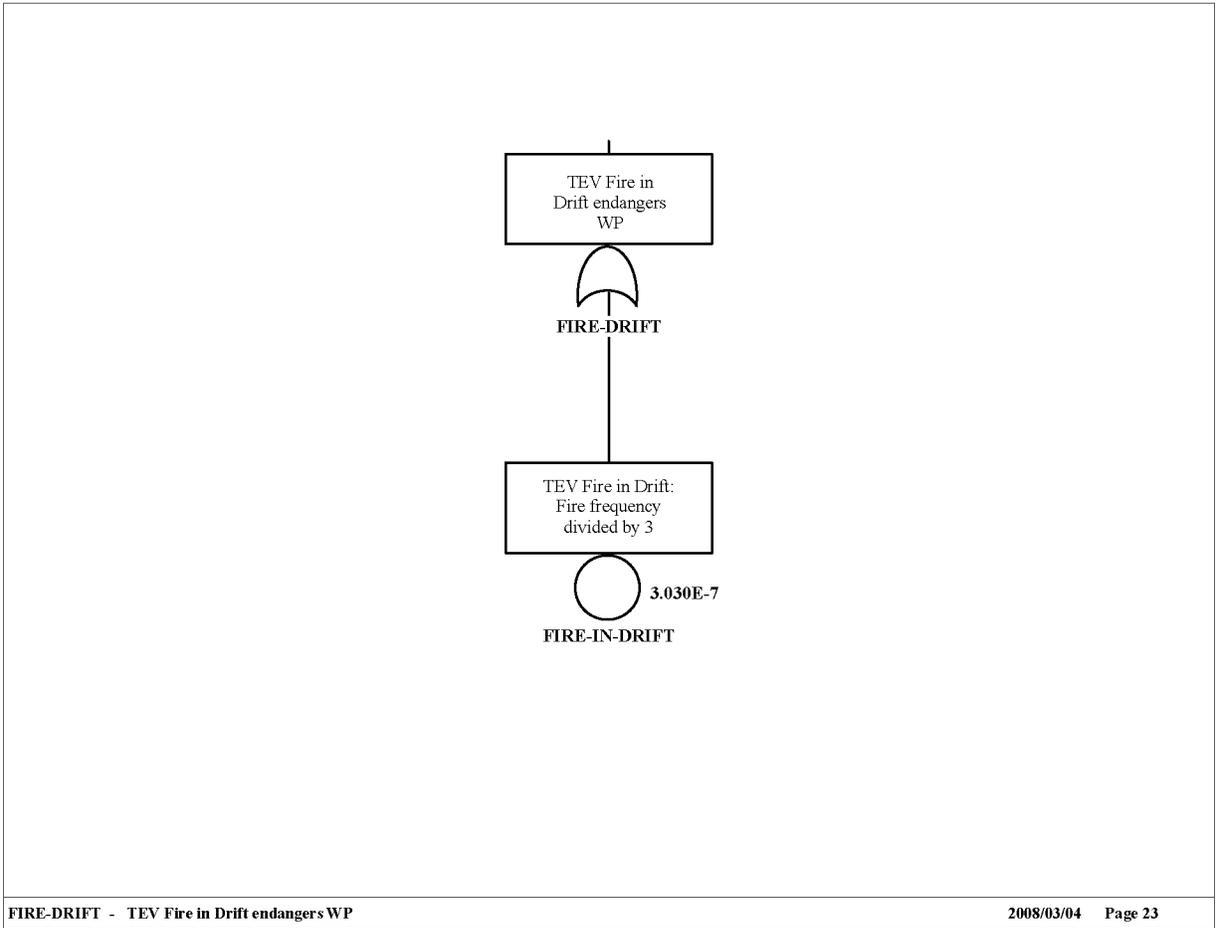
Source: Original

Figure B7-13. SHIELD-PROXIMITY Fault Tree



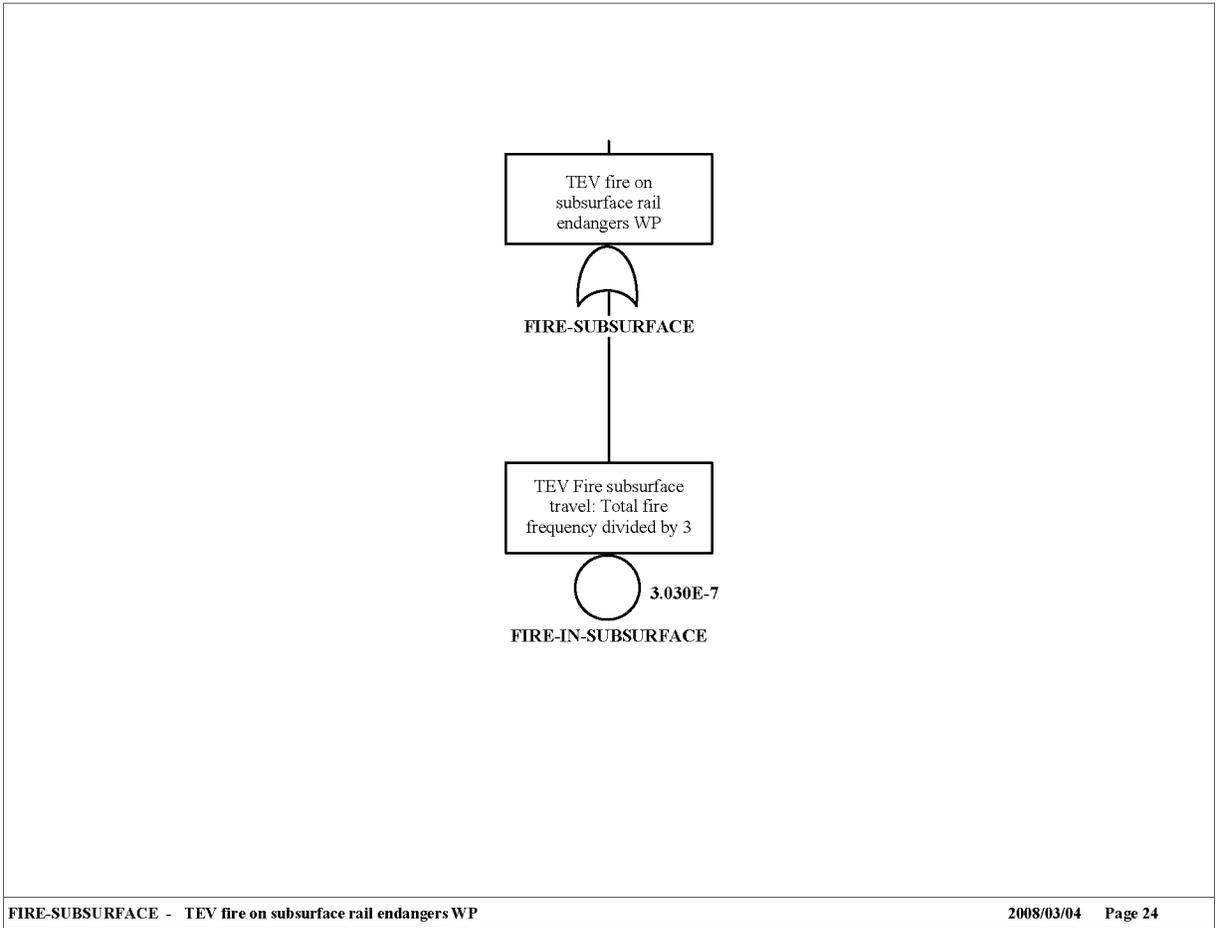
Source: Original

Figure B7-14. SHIELD-ENTRY Fault Tree



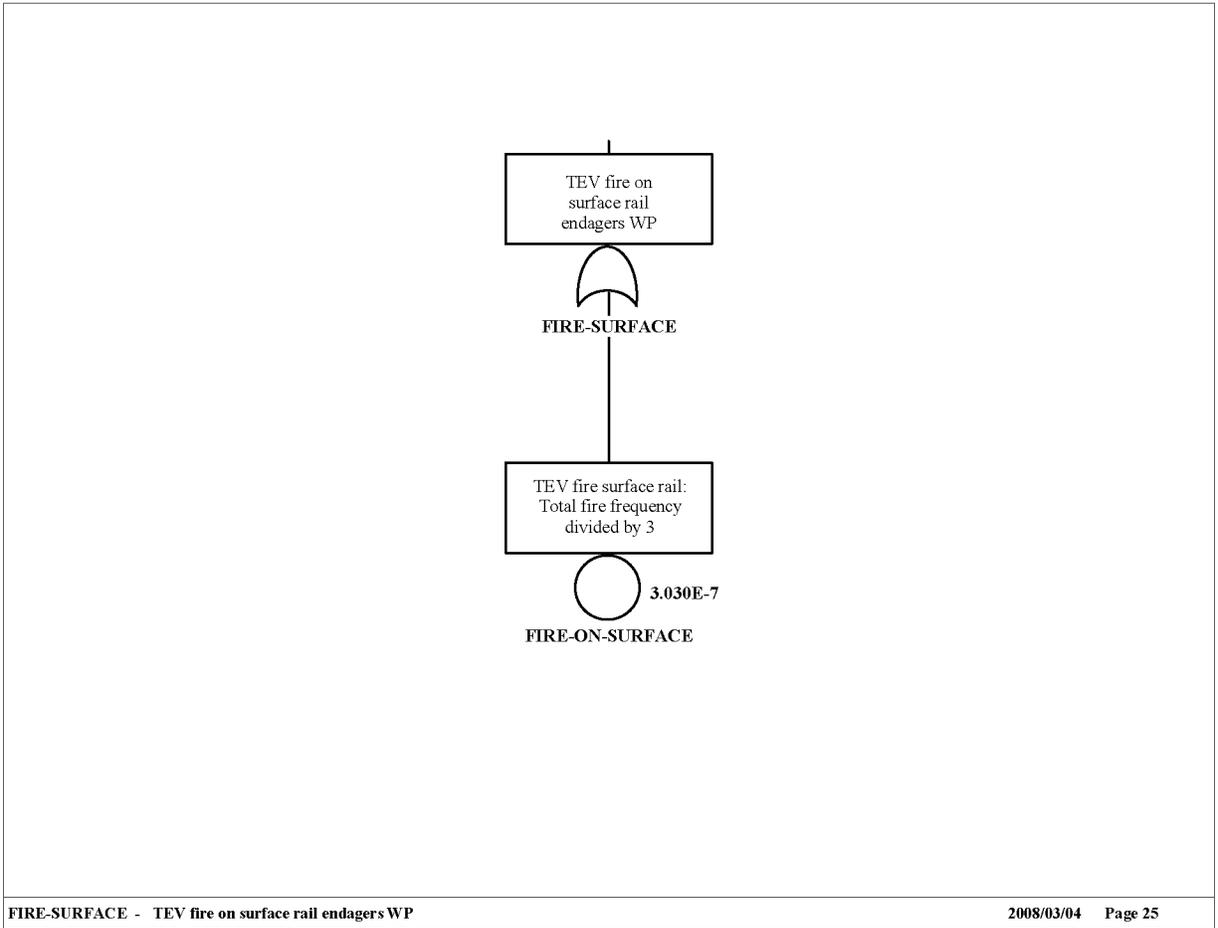
Source: Original

Figure B7-15. FIRE-DRIFT Fault Tree



Source: Original

Figure B7-16. FIRE-SUBSURFACE Fault Tree



Source: Original

Figure B7-17. FIRE-SURFACE Fault Tree

**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)

<b>TYP-FM</b>	<b>Component Name &amp; Failure Mode</b>
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:

$$a := 1..4 \quad fe(a, x) := dlnorm\left(x, \ln(A_{a,1}), \frac{\ln(A_{a,2})}{1.645}\right) \quad (\text{Eq. C-3})$$

$$LA(a, v, \tau) := \int_{10^{-8}}^{10^{-2}} fe(a, x) \cdot dlnorm(x, v, \tau) dx \quad (\text{Eq. C-4})$$

(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:

$$b := 1..8 \quad fd(b, x) := dpois(B_{b,1}, B_{b,2} \cdot x) \quad (\text{Eq. C-5})$$

$$LB(b, v, \tau) := \int_{10^{-8}}^{10^{-2}} fd(b, x) \cdot dlnorm(x, v, \tau) dx \quad (\text{Eq. C-6})$$

(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  $v$  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  $v$  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:

$$L(v, \tau) := \sum_{a=1}^4 \ln(LA(a, v, \tau)) + \sum_{b=1}^8 \ln(LB(b, v, \tau)) \quad (\text{Eq. C-7})$$

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:

<i>Given</i>	$\nu > -20$	$\nu < -1$
	$\tau > 0.01$	$\tau < 5$

The maximum likelihood estimators for  $\nu$  and  $\tau$  are:

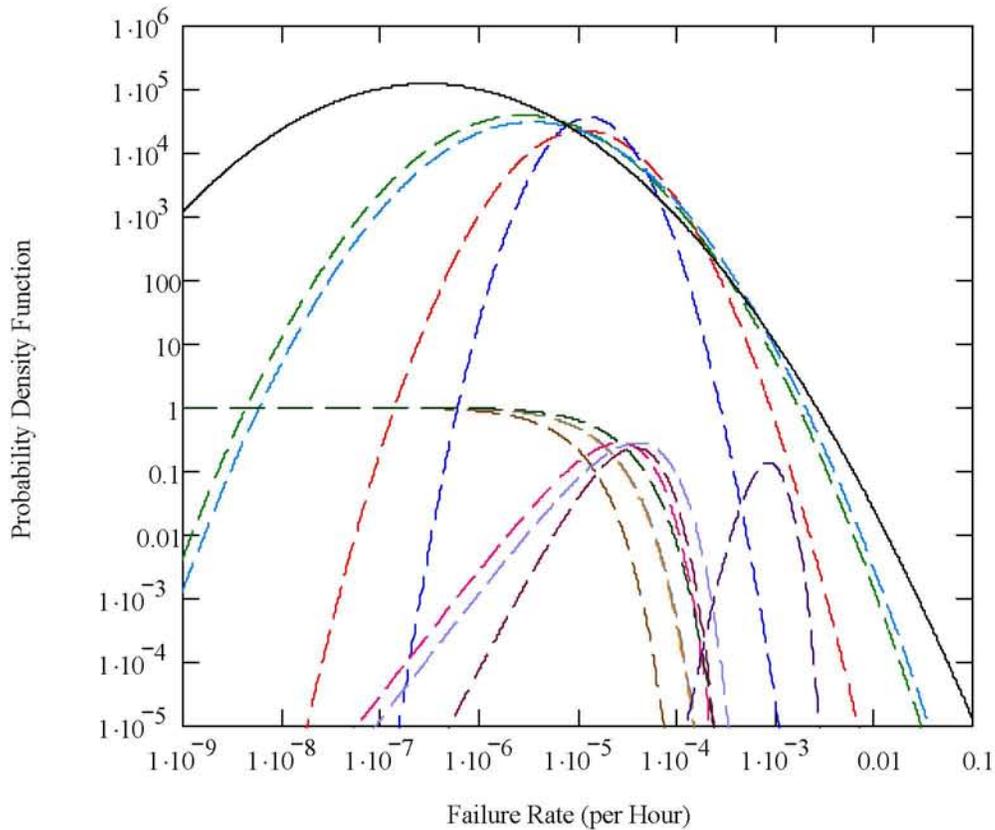
$$\begin{aligned} L := \text{Maximize}(L, \nu, \tau) \quad \nu := L1 & \quad \nu = -11.478 \\ \tau := L2 & \quad \tau = 1.874 \end{aligned}$$

Therefore, the mean and error factors of the population-variability distribution for the failure rate are (based on the formula in NUREG/CR-6823 (Ref. C5.4, Section A.7.3)):

$$\begin{aligned} m := \exp\left(\nu + \frac{\tau}{2}\right) & \quad m = 6.00 \times 10^{-5} \quad \text{per hour} \\ EF := \exp(1.645 \cdot \tau) & \quad EF = 21.8 \end{aligned}$$

Notable percentiles of the population-variability distribution are as follows (expressed as hourly failure rates) and shown in Figure C2.1-1:

1 <sup>st</sup> percentile:	$qnorm(0.01, \nu, \tau) = 1.32 \times 10^{-7}$
5 <sup>th</sup> percentile:	$qnorm(0.05, \nu, \tau) = 4.75 \times 10^{-7}$
10 <sup>th</sup> percentile:	$qnorm(0.10, \nu, \tau) = 9.38 \times 10^{-7}$
50 <sup>th</sup> percentile:	$qnorm(0.50, \nu, \tau) = 1.04 \times 10^{-5}$
90 <sup>th</sup> percentile:	$qnorm(0.90, \nu, \tau) = 1.14 \times 10^{-4}$
95 <sup>th</sup> percentile:	$qnorm(0.95, \nu, \tau) = 2.26 \times 10^{-4}$
99 <sup>th</sup> percentile:	$qnorm(0.99, \nu, \tau) = 8.10 \times 10^{-4}$



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 US Nuclear Regulatory Commission from experience data collected at nuclear power plants. The data analysis reported in NUREG/CR-5485 (Ref. C5.31) consisted of:

1. Identifying the number of redundant components in each subsystem being reported (e.g., two, three, or four (this is termed the CCF group size, CCCG of size  $m$ )).

2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, i.e.,  $k = 1$  for one component at a time,  $k = 2$  for two components at a time,  $k = 3$  for three components at a time, up to  $m$  for failure of all components in a given CCF group.
3. Estimating the alpha factor for a given component type based on its definition as the fraction of total failure events that involve  $k$  component failures due to common cause, for a system of  $m$  redundant components, using the alpha factor equation from NUREG/CR-5485 (Ref, C5.31, Table 5-10), as shown in Figure C3-1.

$$\alpha_k^m = \frac{n_k}{\sum_{j=1}^m n_j} \quad k = 1, \dots, m$$

Source: NUREG/CR-5485, p. 70 (Ref. C5.31)

Figure C3-1. Alpha Factor

4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produced industry-wide prior distributions for the alpha factors for each CCF size, based on all CCF events in their database. Events were mapped to a given CCF size, the maximum likelihood estimator obtained and fit to a constrained noninformative prior distribution. The parameter  $A_T$  of a Dirichlet distribution was then calculated for each alpha and the results combined using the geometric mean. The results are the industry-wide mean alpha factors and uncertainty bounds reported in of NUREG/CR-5485 (Ref. C5.31, Table 5-11) shown in Table C3-1:

Table C3-1. Alpha Factor Table

Table 5-11. Generic prior distributions for various system sizes.

CCCG Size m	$\alpha$ -Factor	Distributions Parameters		Percentiles			Mean
		a	b	P <sub>05</sub>	P <sub>50</sub>	P <sub>95</sub>	
2	$\alpha_1$	9.5300	0.470	8.20E-01	9.78E-01	1.00E-00	0.95300
	$\alpha_2$	0.4700	9.530	1.42E-04	2.16E-02	1.81E-01	0.04700
3	$\alpha_1$	15.2000	0.800	8.42E-01	9.67E-01	9.99E-01	0.95000
	$\alpha_2$	0.3872	15.613	2.10E-05	8.79E-03	1.01E-01	0.02420
	$\alpha_3$	0.4128	15.587	3.45E-05	1.01E-02	1.05E-01	0.02580
4	$\alpha_1$	24.7000	1.300	8.67E-01	9.61E-01	9.95E-01	0.95000
	$\alpha_2$	0.5538	25.446	1.44E-04	1.08E-02	7.81E-02	0.02130
	$\alpha_3$	0.2626	25.737	2.98E-07	1.99E-03	4.82E-02	0.01010
	$\alpha_4$	0.4836	25.516	6.29E-05	8.42E-03	7.17E-02	0.01860
5	$\alpha_1$	38.042	1.958	8.86E-01	9.58E-01	9.91E-01	0.95106
	$\alpha_2$	0.7280	39.272	3.72E-04	1.10E-02	6.05E-02	0.01820
	$\alpha_3$	0.4120	39.588	1.32E-05	3.93E-03	4.22E-02	0.01030
	$\alpha_4$	0.2336	39.766	4.57E-08	8.97E-04	2.89E-02	0.00584
	$\alpha_5$	0.5840	39.416	1.24E-04	7.66E-03	5.27E-02	0.01460
6	$\alpha_1$	50.4724	2.528	8.97E-01	9.58E-01	9.89E-01	0.95231
	$\alpha_2$	0.7791	52.221	3.76E-04	9.20E-03	4.78E-02	0.01470
	$\alpha_3$	0.5406	52.459	6.04E-05	5.02E-03	3.79E-02	0.01020
	$\alpha_4$	0.3127	52.687	9.28E-07	1.56E-03	2.66E-02	0.00590
	$\alpha_5$	0.2433	52.757	5.77E-08	7.67E-04	2.24E-02	0.00459
	$\alpha_6$	0.6519	52.348	1.66E-04	6.93E-03	4.27E-02	0.01230
7	$\alpha_1$	74.5360	3.464	9.12E-01	9.59E-01	9.86E-01	0.95559
	$\alpha_2$	0.9906	77.009	6.44E-04	8.84E-03	3.79E-02	0.01270
	$\alpha_3$	0.6817	77.318	1.39E-04	5.05E-03	2.99E-02	0.00874
	$\alpha_4$	0.4891	77.511	2.21E-05	2.82E-03	2.42E-02	0.00627
	$\alpha_5$	0.2941	77.706	3.39E-07	8.97E-04	1.74E-02	0.00377
	$\alpha_6$	0.2051	77.795	3.84E-09	2.94E-04	1.35E-02	0.00263
	$\alpha_7$	0.8034	77.197	2.89E-04	6.52E-03	3.32E-02	0.01030
8	$\alpha_1$	97.6507	4.349	9.20E-01	9.60E-01	9.84E-01	0.95736
	$\alpha_2$	1.1118	100.888	7.25E-04	7.91E-03	3.13E-02	0.01090
	$\alpha_3$	0.7915	101.209	2.07E-04	4.87E-03	2.52E-02	0.00776
	$\alpha_4$	0.6253	101.375	6.92E-05	3.34E-03	2.17E-02	0.00613
	$\alpha_5$	0.4417	101.558	8.51E-06	1.76E-03	1.74E-02	0.00433
	$\alpha_6$	0.2581	101.742	6.09E-08	4.74E-04	1.21E-02	0.00253
	$\alpha_7$	0.1969	101.803	1.59E-09	1.93E-04	1.00E-02	0.00193
	$\alpha_8$	0.9241	101.076	3.82E-04	6.12E-03	2.78E-02	0.00906

Source: NUREG/CR-5485 (Ref. C5.31)

These values were used in the YMP PCSA by multiplying the mean failure rate for the TYP-FM data by the appropriate alpha factor for k-of-n components for failure-on-demand events (e.g., pump failure to start) and by using the alpha factor divided by two for failure-to-operate events (e.g., pump fails to run) as per the guidance in NUREG/CR-5485 (Ref. C5.31). For example, for a 2-out-of-2 failure on demand event, the mean alpha factor of 0.047 shown in the far right column of Table C3-1 associated with  $\alpha_2$  was multiplied by the mean failure probability for the appropriate component type and failure mode (from Table C4-1) to yield the common cause failure probability.

This approach was considered to provide conservative CCF data for all the component types for which common causes were modeled. This was considered particularly important since the

YMP has never operated and therefore the applicability of conventional nuclear plant alpha factors could not be justified.

The conservatism of this approach can be demonstrated by comparing the alpha factors used for the PCSA diesel generator CCF events to those posted on the U.S. Nuclear Regulatory Commission website for use in Probabilistic Risk Assessment studies of commercial nuclear power plants in the U.S.

The alpha factor used for the PCSA for 2 of 2 diesel generators failing to start was the 0.047 value cited earlier, while the mean alpha factor for a CCG=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)

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)

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)

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)

Subsurface Operations Reliability and Event Sequence Categorization Analysis

000-PSA-MGR0-00500-000-00A

C-43

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>
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand	L	2.10E+00	7.33E-04		2 sources N/D	NUREG/CR-6928 (Ref. C5.16), OREDA-92 (Ref. C5.42)
SRT-FOH	Temperature Sensor/Transmitter Fails	L	1.41E+01		7.05E-07	4 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43)
SRT-SPO	Temperature Sensor Spurious Operation	L	2.80E+01		2.23E-06	1 source; mean + EF	OREDA-2002 (Ref. C5.43)
SRU-FOH	Ultrasonic Sensor Fails	G	5.00E-01		9.62E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
SRV-FOH	Vibration Sensor (Accelerometer) Fails	L	1.07E+01		9.40E-05	4 sources N/D	NPRD-95 (Ref. C5.40)
SRX-FOD	Optical Position Sensor Fails on Demand	B	3.18E+03	1.10E-03		1 source; N/D	SAIC Umatilla (Ref. C5.41)
SRX-FOH	Optical Position Sensor Fails	L	5.00E+00		4.70E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
STU-FOH	Structure (truck or railcar) Failure	G	1.50E+00		4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
SV-FOD	Solenoid Valve Fails on Demand	L	1.17E+01	6.28E-04		4 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
SV-FOH	Solenoid Valve Fails	L	1.70E+01		4.87E-05	1 source; mean + EF	CCPS (Ref. C5.1)
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)

Subsurface Operations Reliability and Event Sequence Categorization Analysis

000-PSA-MGRO-00500-000-00A

C-44

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>
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)

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/b196002.html>
- C5.10 \*Derdiger, J.A.;Bhatt, K.M.;Siegfriedt, W.E. 1981. *Component Failure and Repair Data for Coal-Fired Power Units*. EPRI AP-2071. Palo Alto, CA: Electric Power Research Institute. TIC: 260070.
- C5.11 \*Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications*. AIAA Education Series. Washington, D.C.: American Institute of Aeronautics & Astronautics. TIC: 259878.
- C5.12 \*DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment*. MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.
- C5.13 \*Drago, J.P.; Borkowski, R.J.; Fragola, J.R.; and Johnson, J.W. 1982. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report — The Pump Component*. NUREG/CR-2886. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0222.
- 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, NY: ASME Press (American Society of Mechanical Engineers). ISBN: 0-7918-0233-7. TIC: 259912.
- C5.33 Not Used.
- C5.34 NRC (U.S. Nuclear Regulatory Commission) 1979. *Single-Failure-Proof Cranes for Nuclear Power Plants*. NUREG-0554. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 232978.
- C5.35 NRC 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.
- C5.36 NRC 2005. *CCF Parameter Estimation 2005*. Washington, D.C.: Nuclear Regulatory Commission (NRC). ACC: MOL.20080213.0022.
- C5.37 \*NSWC (Naval Surface Warfare Center) 1998. *Handbook of Reliability Prediction Procedures for Mechanical Equipment*. NSWC-98/LE1. West Bethesda, Maryland: Naval Surface Warfare Center, Carderock Division. TIC: 245703.
- C5.38 \*Peltz, E.; Robbins, M.; Boren, P.; Wolff, M. 2002. "Using the EDA to Gain Insight into Failure Rates." *Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer*. Santa Monica, CA: RAND. TIC: 259917. ISBN: 0-8330-3115-5.
- C5.39 \*Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data*. NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.
- C5.40 \*Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995*. NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.
- C5.41 \*SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment*. Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.
- C5.42 \*SINTEF Industrial Management 1992. *OREDA, Offshore Reliability Data Handbook*. 2nd Edition. Trondheim, Norway: OREDA. ISBN: 825150188.1

- C5.43 \*SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook*. 4th Edition. Trondheim, Norway: OREDA. TIC: 257402. 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-67
D3 SHIELDING DEGRADATION DUE TO IMPACTS .....	D-71
D3.1 DAMAGE THRESHOLDS FOR LOS .....	D-72
D3.2 SEVERITY OF DAMAGE VERSUS IMPACT VELOCITY .....	D-73
D3.3 ESTIMATE OF THRESHOLD SPEEDS FOR LOSS OF SHIELDING DUE TO IMPACTS .....	D-77
D3.4 PROBABILITY OF LOSS OF SHIELDING .....	D-79
D4 REFERENCES .....	D-85
D4.1 DESIGN INPUTS .....	D-85
D4.2 DESIGN CONSTRAINTS .....	D-91

**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-54
D2.1-3.	Yield, Ultimate, and Flow Stress for Type 316 Stainless Steel ..... D-55
D2.1-4.	Probability Distribution for the Failure Temperature of Thin-Walled Canisters..... D-58
D2.1-5.	Probability Distribution for the Failure Temperature of Thick-Walled Canisters..... D-59
D2.1-6.	Probability Distribution for Maximum Canister Temperature – Thin-Walled Canister in a Waste Package ..... D-61
D2.1-7.	Distribution of Radiation Energy from Fire..... D-66
D3.2-1.	Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph ..... D-75
D3.2-2.	Truck Steel/Lead/Steel Inner Shell Strain versus Impact Speed ..... D-76
D3.2-3.	Rail Steel/Lead/Steel Strain versus Impact Speed ..... D-77
D3.4-1.	Summary Event Tree Showing Model Logic for Canisters and Aging Overpacks ..... D-80

**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-27
D2.1-1.	Probability Distribution for Fire Duration - Without Automatic Fire Suppression ..... D-33
D2.1-2.	Probability Distribution for Fire Duration - With Automatic Fire Suppression ..... D-34
D2.1-3.	Effective Thermal Properties for 21-PWR Fuel in a TAD ..... D-39
D2.1-4.	Model Inputs – Bare Canister ..... D-46
D2.1-5.	Model Inputs – Canister in a Waste Package ..... D-47
D2.1-6.	Model Inputs – Canister in Transportation Cask ..... D-48
D2.1-7.	Model Inputs – Canister in a Shielded Bell ..... D-49
D2.1-8.	Summary of Canister Failure Probabilities in Fire ..... D-61
D2.1-9.	Model Inputs – Bare Fuel Cask ..... D-64
D2.1-10.	Summary of Fuel Failure Probabilities ..... D-65
D2.1-11.	Probabilities that Radiation Input Exceeds Failure Energy for Cask ..... D-67
D3.2-1.	Maximum Plastic Strain in Inner Shell of Sandwich Wall Casks ..... D-74

**TABLES (Continued)**

	<b>Page</b>
D3.3-1. Drop Height to Reach a Given Impact Speed.....	D-79
D3.3-2. Impact Speeds on Real Target for Equivalent Damage for Unyielding Targets.....	D-79
D3.4-1. Probabilities of Degradation or Loss of Shielding.....	D-84

---

## 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.

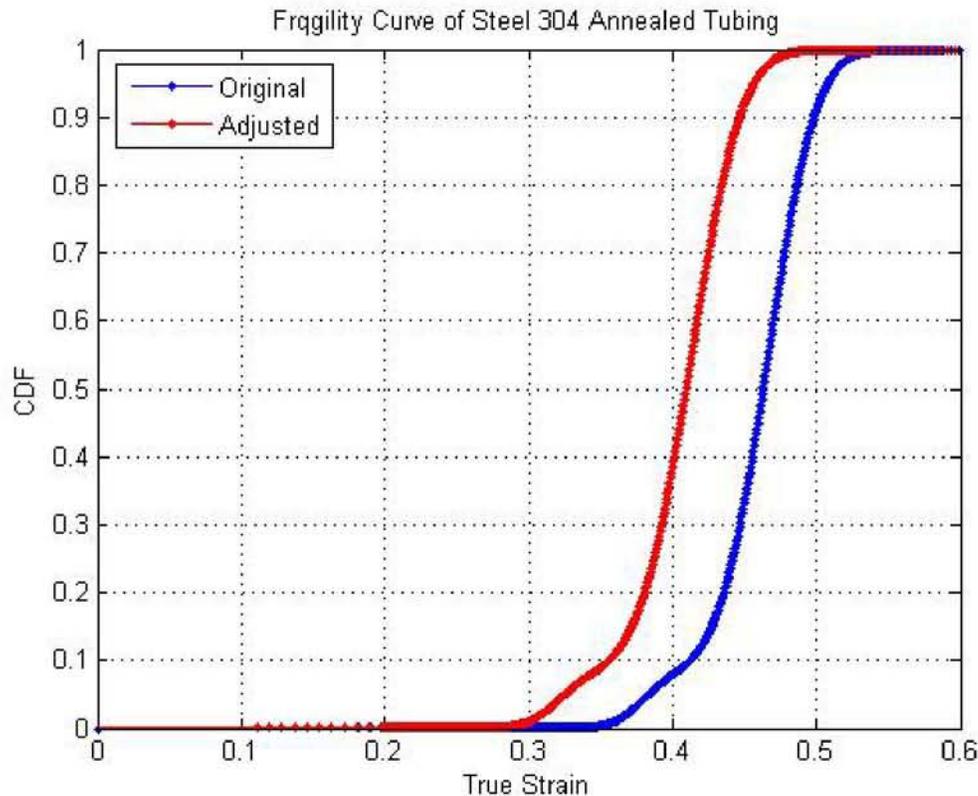
The maximum strain for each scenario was compared with the capacity distribution based on material properties to obtain containment failure probabilities using the methodology described in Section 4.3.2.2. For simplicity and consistency in interpreting results, the impact-surface conditions, including 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

fragility cumulative distribution function (CDF) model was adjusted to different steels used in a typical design and to meet the code specification of the material model used in LS-DYNA. The adjustment consisted of shifting the distribution by -8.3% (Ref. D4.1.27, p. 93). Thus the initial fragility curve was shifted by 8.3% to a lower value of minimum elongation. The fragility curves before and after the shift are shown in Figure D1.1-1 and tabulated in Table D1.1-1. 316L stainless steel might be used for construction of some canisters and casks, but the stress-strain curves would be similar.



Source: Ref. D4.1.27, Figure 6.3.7-3

Figure D1.1-1. Original and Shifted Cumulative Distribution Functions (CDF) for Capacity (or Fragility) Plotted as a Function of True Strain

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1

True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.00	-1.70	0.0000E+00	1.6754E-15	0.36	0.05	1.0506E-02	1.0973E-01
0.01	-1.65	2.0924E-16	1.8688E-15	0.37	0.10	2.3978E-02	1.4282E-01
0.02	-1.60	4.1848E-16	2.0622E-15	0.38	0.15	4.3259E-02	1.9679E-01
0.03	-1.55	6.2772E-16	2.2555E-15	0.39	0.19	6.2863E-02	2.7687E-01

Table D1.1-1. Probability of Failure versus True Strain Tabulated for Figure D1.1-1 (Continued)

True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)	True Strain (TS)	$\frac{TS - TS_{mean}}{TS_{std}}$	Probability of Failure Original	Probability of Failure Adjusted (-8.3% shift)
0.04	-1.50	8.3696E-16	2.4489E-15	0.40	0.24	7.9100E-02	3.8310E-01
0.05	-1.45	1.0462E-15	2.6422E-15	0.41	0.29	9.5539E-02	5.0814E-01
0.06	-1.41	1.2554E-15	2.8356E-15	0.42	0.34	1.2068E-01	6.3823E-01
0.07	-1.36	1.4647E-15	3.0290E-15	0.43	0.39	1.6410E-01	7.5736E-01
0.08	-1.31	1.6739E-15	3.2223E-15	0.44	0.44	2.3393E-01	8.5309E-01
0.09	-1.26	1.8832E-15	3.4157E-15	0.45	0.48	3.3371E-01	9.2036E-01
0.10	-1.21	2.0924E-15	3.6090E-15	0.46	0.53	4.5893E-01	9.6161E-01
0.11	-1.16	2.3016E-15	3.8024E-15	0.47	0.58	5.9615E-01	9.8363E-01
0.12	-1.11	2.5109E-15	2.8601E-14	0.48	0.63	7.2682E-01	9.9385E-01
0.13	-1.07	2.7201E-15	2.3645E-13	0.49	0.68	8.3454E-01	9.9797E-01
0.14	-1.02	2.9294E-15	1.6225E-12	0.50	0.73	9.1117E-01	9.9941E-01
0.15	-0.97	3.1386E-15	9.7686E-12	0.51	0.78	9.5806E-01	9.9985E-01
0.16	-0.92	3.3478E-15	5.2952E-11	0.52	0.82	9.8270E-01	9.9997E-01
0.17	-0.87	3.5571E-15	2.6233E-10	0.53	0.87	9.9379E-01	9.9999E-01
0.18	-0.82	3.7663E-15	1.2513E-09	0.54	0.92	9.9807E-01	1.0000E+00
0.19	-0.78	2.1733E-14	6.9107E-09	0.55	0.97	9.9948E-01	1.0000E+00
0.20	-0.73	2.1209E-13	2.6769E-08	0.56	1.02	9.9988E-01	1.0000E+00
0.21	-0.68	1.7358E-12	1.1600E-07	0.57	1.07	9.9998E-01	1.0000E+00
0.22	-0.63	1.1373E-11	4.8126E-07	0.58	1.11	1.0000E+00	1.0000E+00
0.23	-0.58	6.4625E-11	1.9316E-06	0.59	1.16	1.0000E+00	1.0000E+00
0.24	-0.53	4.1126E-10	7.5246E-06	0.60	1.21	1.0000E+00	1.0000E+00
0.25	-0.48	2.4773E-09	2.8566E-05	0.61	1.26	1.0000E+00	1.0000E+00
0.26	-0.44	1.2132E-08	1.0566E-04	0.62	1.31	1.0000E+00	1.0000E+00
0.27	-0.39	5.2343E-08	3.7635E-04	0.63	1.36	1.0000E+00	1.0000E+00
0.28	-0.34	2.4478E-07	1.2625E-03	0.64	1.41	1.0000E+00	1.0000E+00
0.29	-0.29	1.0945E-06	3.8474E-03	0.65	1.45	1.0000E+00	1.0000E+00
0.30	-0.24	4.7123E-06	1.0185E-02	0.66	1.50	1.0000E+00	1.0000E+00
0.31	-0.19	1.9709E-05	2.2466E-02	0.67	1.55	1.0000E+00	1.0000E+00
0.32	-0.15	7.9860E-05	4.0237E-02	0.68	1.60	1.0000E+00	1.0000E+00
0.33	-0.10	3.1104E-04	5.9110E-02	0.69	1.65	1.0000E+00	1.0000E+00
0.34	-0.05	1.1366E-03	7.5125E-02	0.70	1.70	1.0000E+00	1.0000E+00
<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
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

Table D2.1-2. Probability Distribution for Fire Duration - With Automatic Fire Suppression (Continued)

Fire Duration (min)	Cumulative Probability	Fire Duration Interval (min)	Interval Probability <sup>a</sup>
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:

$$q_{r,fire} = \varepsilon_c A_c F_{c-fire} F_s \sigma (T_{fire}^4 - T_c^4) \quad (\text{Eq. D-7})$$

where

$\varepsilon_c$	=	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:

$$q_{r,f} = \frac{A_c F_{c-f} \sigma (T_c^4 - T_f^4)}{1/\varepsilon_c + 1/\varepsilon_f - 1} \quad (\text{Eq. D-9})$$

where  $F_{c-f}$  is the view factor between the canister and the fuel,  $\varepsilon_f$  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

$\epsilon_{ob}$	=	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:

$$q_{ib} = \frac{A_{ob} F_{oi} \sigma (T_{ob}^4 - T_{ib}^4)}{1/\epsilon_{ib} + 1/\epsilon_{ob} - 1} \quad (\text{Eq. D-14})$$

where

$\epsilon_{ib}$	=	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.

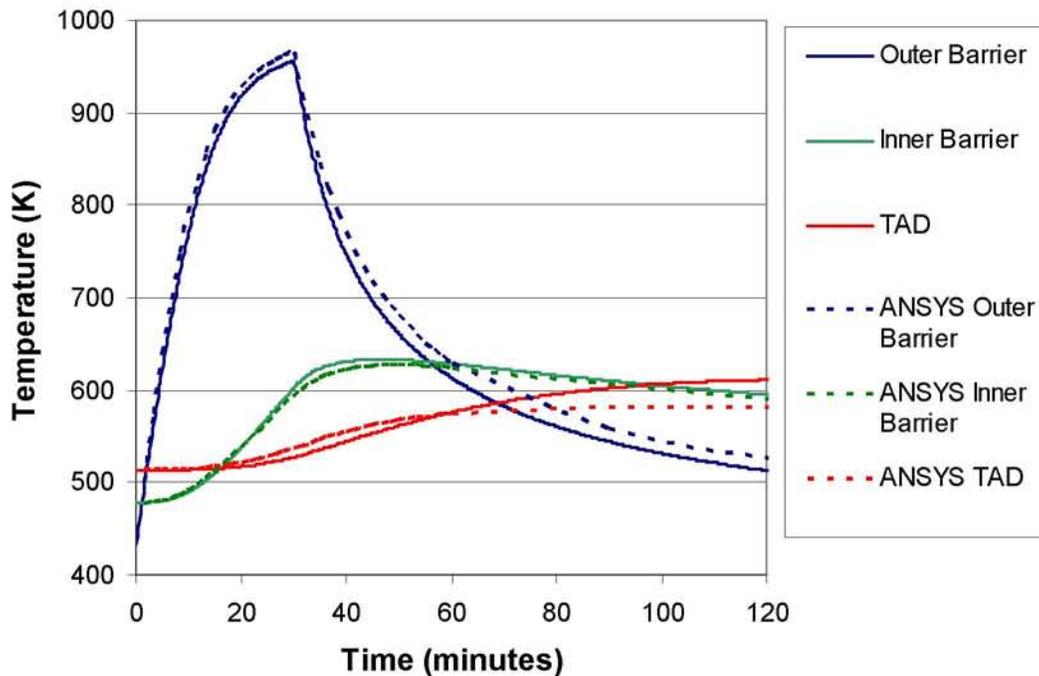
Unlike the bare canister case in which heating of the canister ends when the fire ends, heating of a canister that is inside other containers will increase after the fire ends as heat is transmitted from the heated outer and inner barrier. After the fire has been extinguished, heat will be lost by the 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)
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)
<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)

Table D2.1-5. Model Inputs – Canister in a Waste Package (Continued)

Model Parameter	Value	Basis/Rationale
Initial Temperature (K)	478	From <i>Thermal Responses of TAD and 5-DHLW/DOE SNF Waste Packages to a Hypothetical Fire Accident</i> (Ref. D4.1.25, Figure 1)
<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)
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)

Table D2.1-6. Model Inputs – Canister in Transportation Cask (Continued)

Model Parameter	Value	Basis/Rationale
Emissivity	0.8	Average value for carbon steel in <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)

Table D2.1-7. Model Inputs – Canister in a Shielded Bell (Continued)

Model Parameter	Value	Basis/Rationale
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
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)
- $\sigma$  = the tensile stress exerted on the canister wall, and
- $t_f$  = the canister failure time (the time at which the equality is satisfied).

The function in the denominator of Equation D-16 is

$$t_R = 10^{\frac{P_{LM}-20}{T}} \quad (\text{Eq. D-17})$$

where  $P_{LM}$  is the Larson-Miller parameter (Ref. D4.1.44), which is a material property of the canister material and is a function of the applied stress.

Since the canisters are pressurized to varying degrees with a combination of helium or air used to backfill the canister and gases released when the fuel fails, the pressure inside the canister will increase as the canister gets hotter. The internal pressure exerts a hoop stress in the radial direction that puts the canister wall under tension. It is this stress that controls failure of the canister wall. The hoop stress,  $\sigma$ , 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

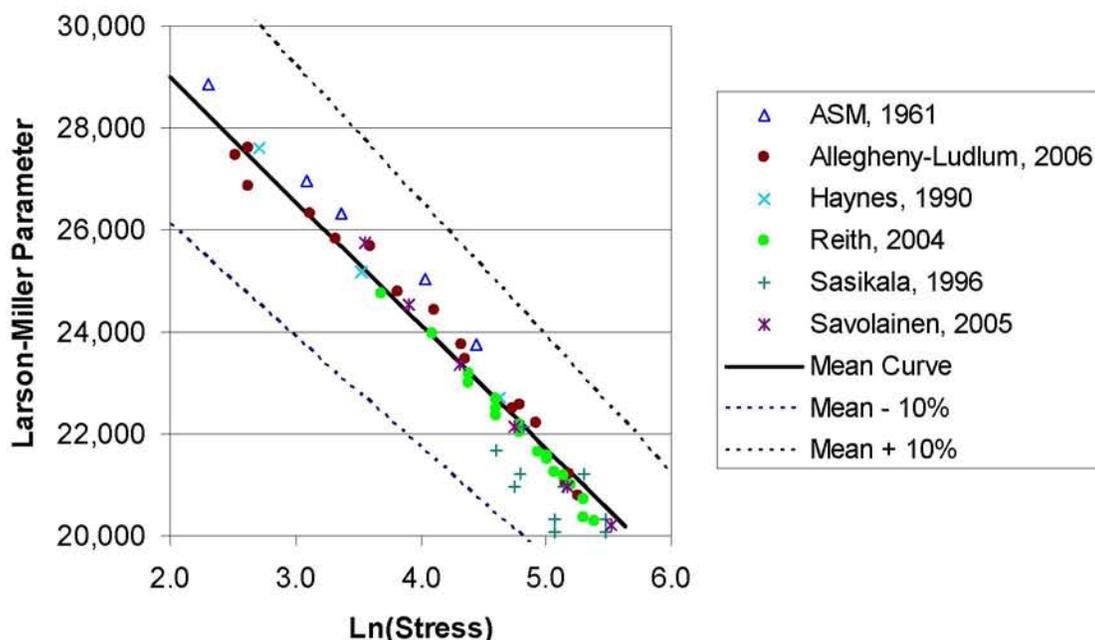
- T = temperature (K)
- t<sub>f</sub> = failure time (hours) determined in testing
- C = a constant that is approximately 20 for most stainless steels

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.



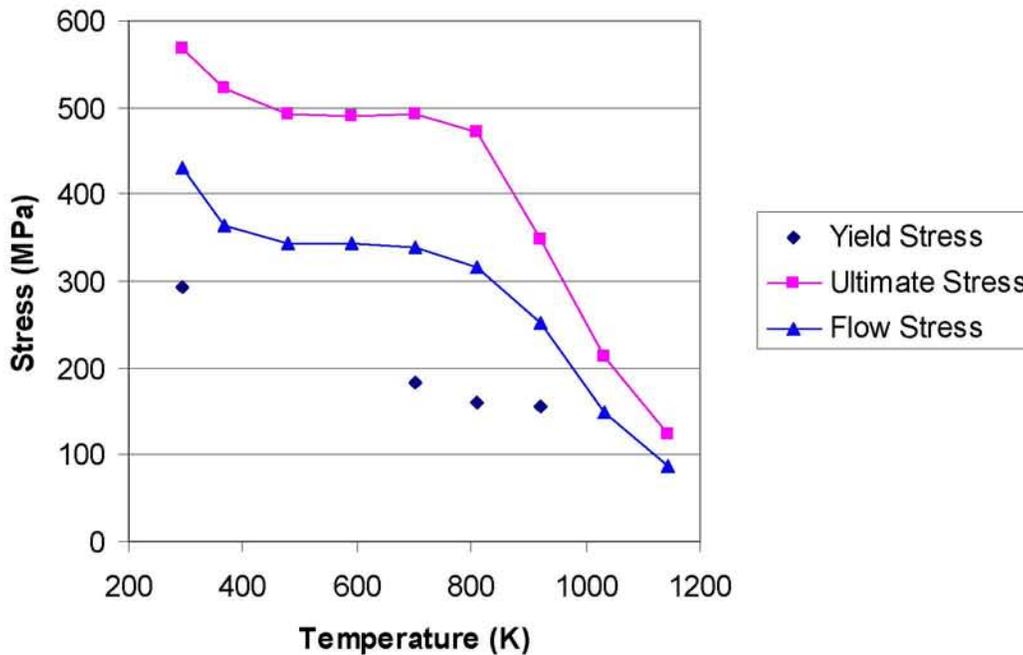
Source: Excel Spreadsheet *Creep rupture - Fast Heatup 1 inch.xls* found in Attachment H.

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.

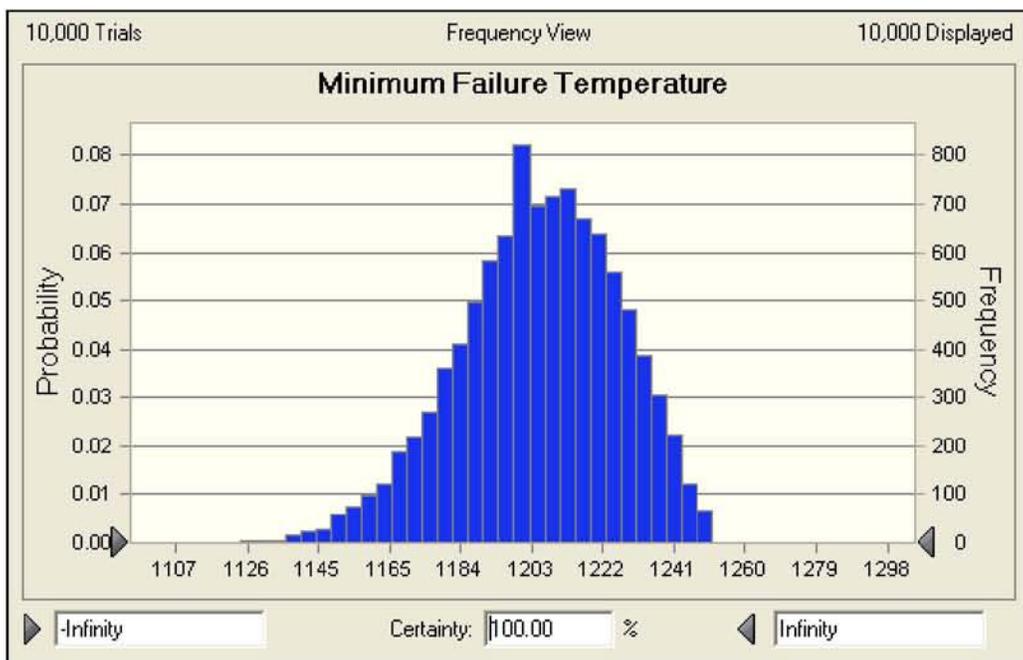
#### **D2.1.5.1 Probabilistic Analysis of Canister Failure Temperature**

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.

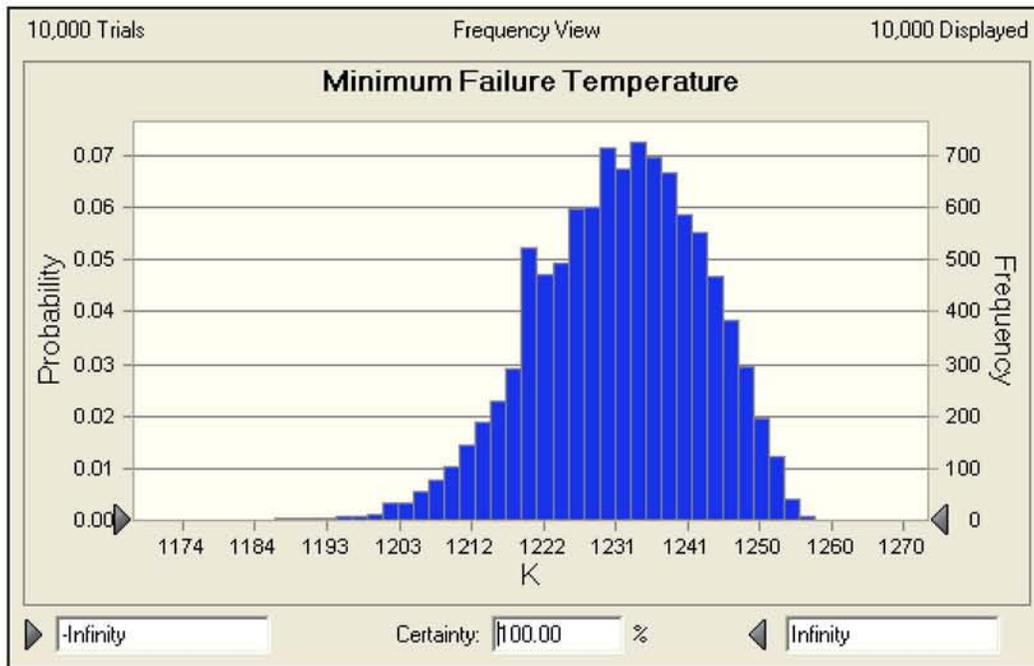
A similar analysis was performed for bare canisters. This calculation used the higher heating rate discussed in Section D2.1.4.5.3.3. The resulting probability distribution was nearly identical to the one shown in Figure D2.1-4. The reason for this is that canister failure was nearly always due to limit 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:

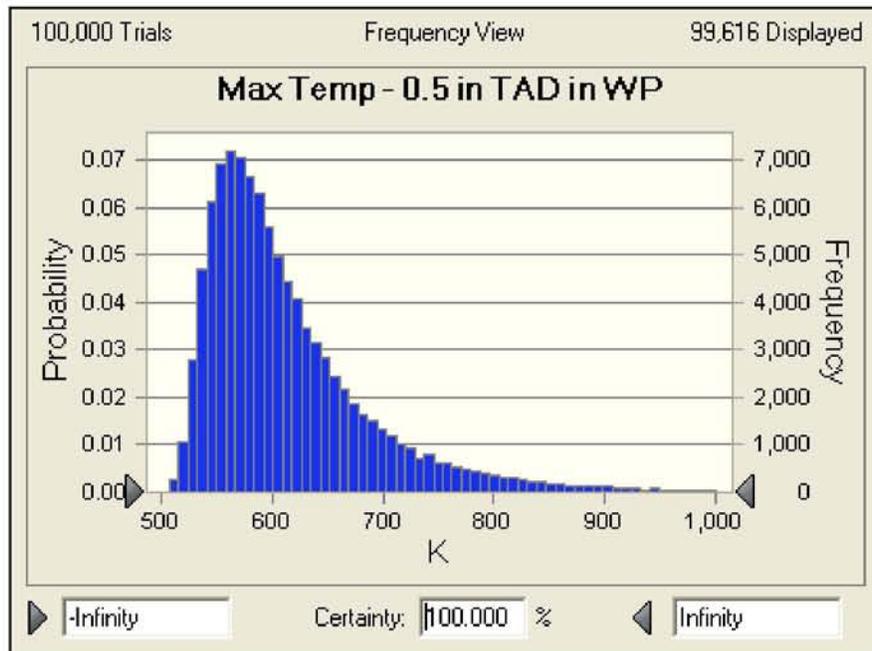
$$\sigma = \sqrt{\frac{\frac{n_{\text{fail}}}{N} \left( \frac{N - n_{\text{fail}}}{N} \right)}{N}} \quad (\text{Eq. D-24})$$

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

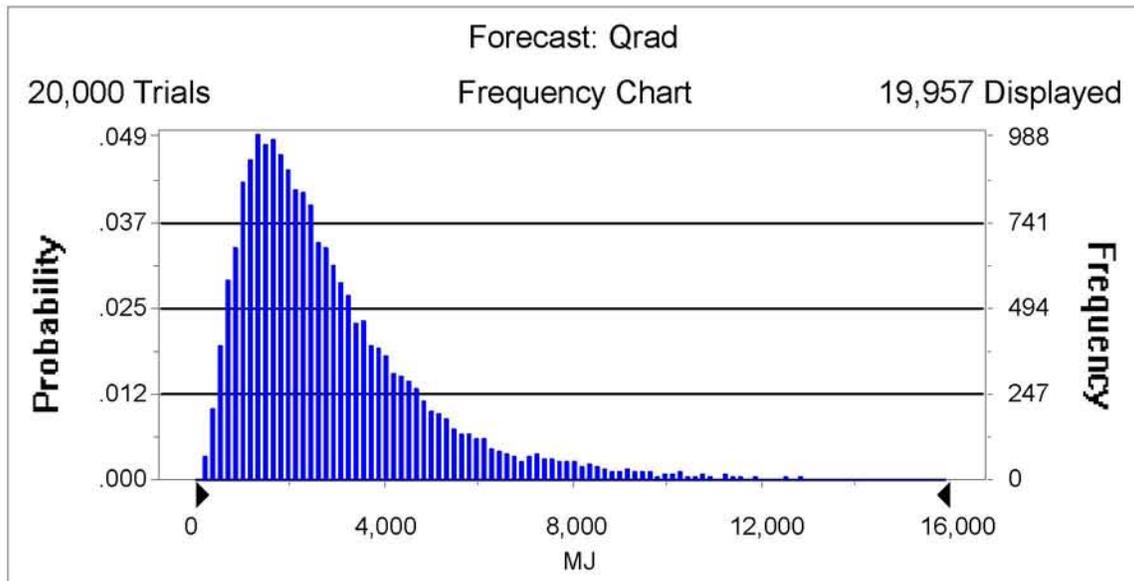
Crystal Ball) for the maximum thermal radiation energy from the fire using the following equation:

$$Q_{\text{rad}} = \sigma A T_{\text{fire}}^4 t_{\text{fire}} \quad (\text{Eq. D-25})$$

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  $1,000^{\circ}\text{C}$  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  $350^{\circ}\text{C}$ , 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.

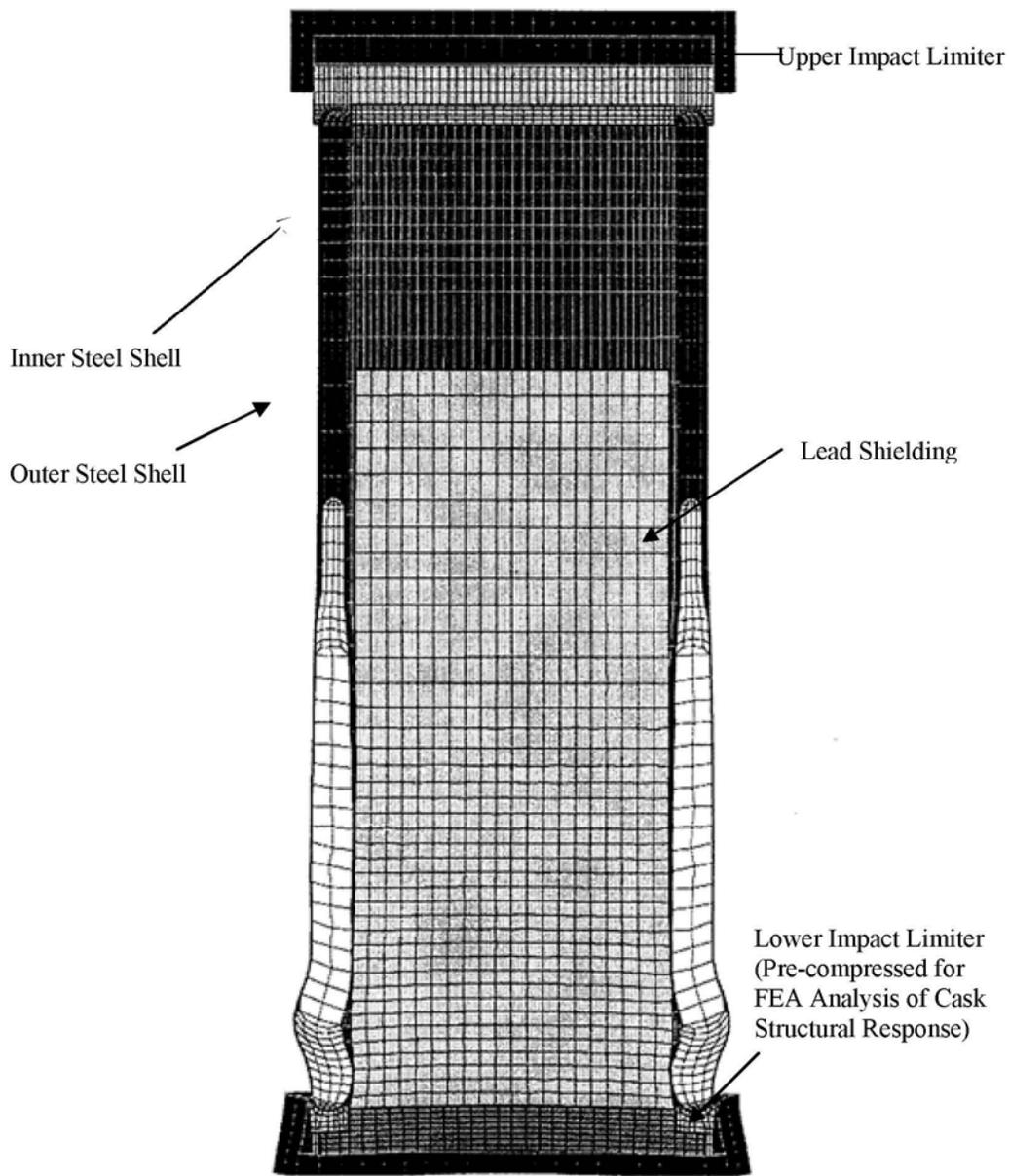
Two horizontal lines were superimposed on Figures D3.2-2 and D3.2-3 to plot the 0.2% and 2.0% strain to represent the respective S2 and S3 thresholds for inner shell strain. The intersections of the strain curves with the respective threshold values indicate the minimum impact speed at which the respective 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

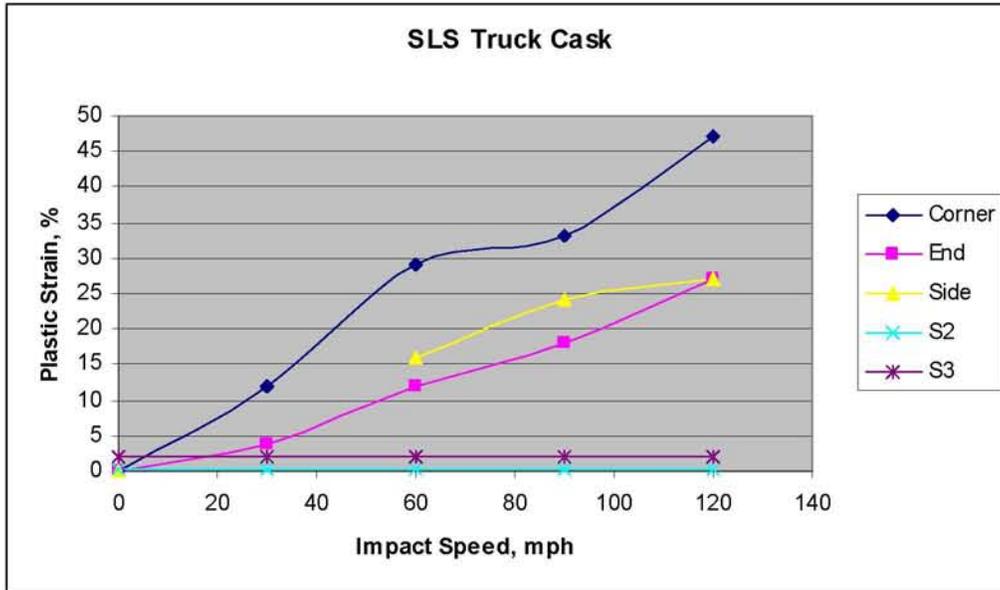
NOTE: SDUS = steel-depleted uranium-steel; SLS = steel-lead-steel.

Source: From Ref. D4.1.65, Table 5.3.



Source: From Ref. D4.1.65, Figure 5.9

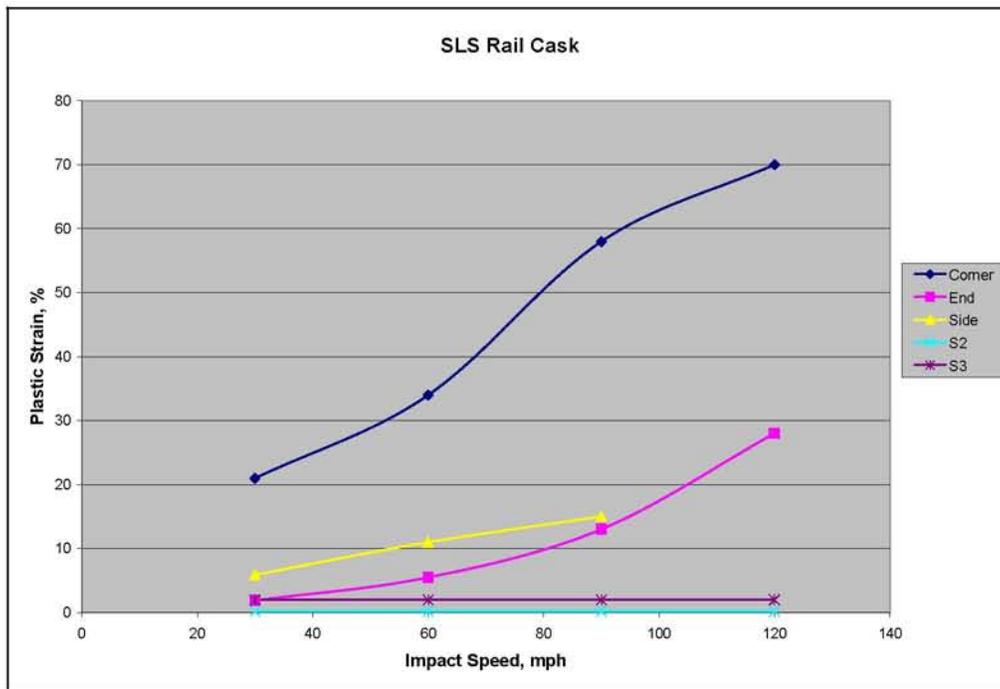
Figure D3.2-1. Illustration of Deformation and Lead Slumping for a SLS Rail Cask Following End-on Impact at 120 mph



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

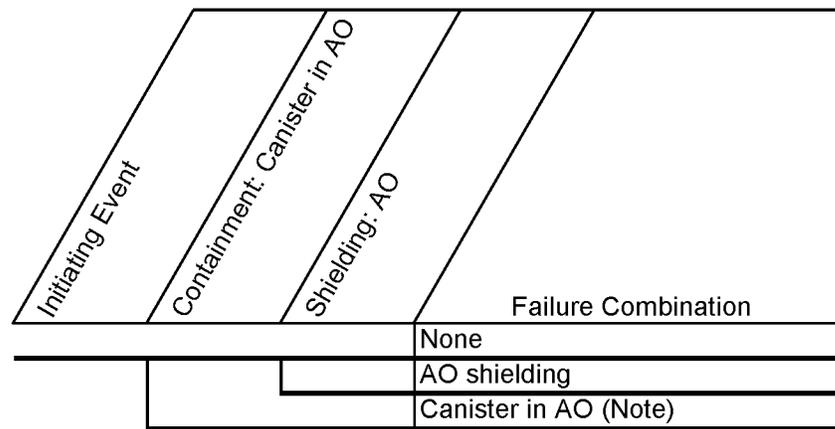
NUREG/CR-6672 (Ref. D4.1.65) do not have any direct relevance to event sequences for waste handling operations. However, the basic approach that breaks down the overall probability of an event sequence involving LOS into conditional probabilities for occurrence of various physical conditions that lead 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.

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-10
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-21
E3.5 DOCUMENTATION OF RESULTS .....	E-22
E4 INFORMATION COLLECTION AND USE OF EXPERT JUDGMENT .....	E-23
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-25
E4.2.2 Role of Subject Matter Expert Judgment .....	E-27
E5 TERMINOLOGY AND OVERVIEW OF HUMAN PERFORMANCE ISSUES .....	E-28
E5.1 TERMINOLOGY .....	E-28

E5.1.1	Classification of HFEs .....	E-28
E5.1.1.1	Temporal Phases of HFEs .....	E-29
E5.1.1.2	Error Modes .....	E-30
E5.1.1.3	Human Failure Type .....	E-30
E5.1.1.4	Informational Processing Failures .....	E-31
E5.1.2	Personnel Involved in Subsurface Operations .....	E-31
E5.2	OVERVIEW OF HUMAN PERFORMANCE ISSUES .....	E-32
E6	ANALYSIS .....	E-33
E6.0	BACKGROUND .....	E-33
E6.0.1	Reader's Guide to the HRA Analysis .....	E-33
E6.1	DESCRIPTION OF SUBSURFACE OPERATIONS BASE CASE SCENARIOS .....	E-34
E6.1.1	Initial Conditions .....	E-35
E6.1.2	Radiologic Inspection of Waste Package .....	E-36
E6.1.3	TEV in Transit from Surface Facility to Emplacement Drift Door .....	E-37
E6.1.4	Waste Package Emplacement (or Retrieval) .....	E-38
E6.1.4.1	Waste Package Emplacement .....	E-38
E6.1.4.2	Waste Package Retrieval .....	E-38
E6.1.5	Drip Shield Emplacement .....	E-39
E6.2	ANALYSIS OF SUBSURFACE HUMAN FAILURE EVENTS .....	E-40
E6.2.1	HFES Common to Multiple Operations .....	E-40
E6.2.2	HFE Descriptions and Preliminary Analysis .....	E-43
E6.3	DETAILED ANALYSIS .....	E-46
E7	HUMAN RELIABILITY ANALYSIS DATABASE .....	E-46
E8	REFERENCES .....	E-47
E8.1	DESIGN INPUTS .....	E-47
E8.2	DESIGN CONSTRAINTS .....	E-49
APPENDIX E.I	RECOMMENDED INCORPORATION OF HUMAN FAILURE EVENTS IN THE YMP PCSA .....	E-50
APPENDIX E.II	GENERAL STRUCTURE OF POST-INITIATOR HUMAN ACTIONS .....	E-51
APPENDIX E.III	PRELIMINARY (SCREENING) QUANTIFICATION PROCESS FOR HUMAN FAILURE EVENTS .....	E-52
APPENDIX E.IV	SELECTION OF METHODS FOR DETAILED QUANTIFICATION .....	E-57
APPENDIX E.V	HUMAN FAILURE EVENTS NAMING CONVENTION .....	E-61

## FIGURES

	<b>Page</b>
E6.0-1. Major Subsurface Operations Steps.....	E-34
E.I-1. Incorporation of Human Reliability Analysis within the PCSA.....	E-50
E.II-1. Post-initiator Operator Action Event Tree.....	E-51
E.V-1. Basic Event Naming Convention.....	E-61

**TABLES**

	<b>Page</b>
E3.3-1. Formulae for Addressing HFE Dependencies .....	E-20
E3.4-1. Lognormal Error Factor Values .....	E-22
E6.0-1. Correlation of Subsurface Operations to ESDs and HAZOP Evaluation Nodes .....	E-34
E6.2-1. Summary of Preliminary Values for the Generic HFEs .....	E-43
E6.2-2. HFE Group #1 Descriptions and Preliminary Analysis .....	E-44
E7-1. HFE Data Summary .....	E-46
E.III-1. Examples of Information Useful to HFE Quantification .....	E-52
E.III-2. Types of HFEs .....	E-55
E.IV-1. Comparison between NPP and YMP Operations .....	E-57
E.V-1. Human Failure Event Type Codes and Failure Mode Codes .....	E-62

## ACRONYMS AND ABBREVIATIONS

### Acronyms

ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Event Analysis
CBDT	Cause-Based Decision Tree
CRCF	Canister Receipt and Closure Facility
CREAM	Cognitive Reliability and Error Analysis Method
EFC	error forcing context
EOC	error of commission
EOO	error of omission
EPRI	Electric Power Research Institute
ESD	event sequence diagram
FLIM	Failure Likelihood Index Methodology
HAZOP	hazard and operability
HCR	Human Cognitive Reliability
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HFE	human failure event
HRA	human reliability analysis
HVAC	heating, ventilation, and air-conditioning
IHF	Initial Handling Facility
ISFSI	independent spent fuel storage installation
MAUD	Multi-Attribute Utility Decomposition
MERMOS	Methode d’Evaluation de la Relisation des Missions Operateur pour la Surete
MLD	master logic diagram
NARA	Nuclear Action Reliability Assessment
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
PCSA	preclosure safety analysis
PIC	person in charge
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSF	performance-shaping factor
SHARP	Systematic Human Action Reliability Procedure

**ACRONYMS AND ABBREVIATIONS (Continued)**

SLIM	Success Likelihood Index Method
SNF	spent nuclear fuel
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SSCs	structures, systems, and components
TEV	transport and emplacement vehicle
THERP	Technique for Human Error Rate Prediction
TRC	Time-Reliability Correlation
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. E8.1.14):

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 Subsurface 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 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 interviewed subject matter experts to identify potential vulnerabilities and HFE scenarios.

The result of this identification process was a list of HFES and a description of each HFE scenario, including system and equipment conditions and any resident or triggered human factor concerns (e.g., performance-shaping factors (PSFs)). This combination of conditions and human factor concerns then became the error forcing context (EFC) for a specific HFE. Additions and refinements to these initial EFCs were made during the preliminary and detailed analyses.

A preliminary, or screening-type, analysis was then performed to preserve HRA resources so that detailed analyses can be focused on only the most risk-significant HFES. The preliminary analysis included verification of the validity of HFES included in the initial PCSA model, assignment of a conservative screening value (mean value) to each HFE, and verification of preliminary values. The actual quantification of preliminary values was a six-step process that is described in detail in Appendix E.III of this analysis. Once the preliminary values were assigned, the PCSA model was quantified (initial quantification), and HFES were identified for detailed analysis if: (1) the HFE was a risk-driver for a dominant sequence, and (2) using the preliminary values, that event sequence was above Category 1 or 2 according to the 10 CFR Part 63 (Ref. E8.2.1) performance objectives. The remaining HFES retained their preliminary values. While most of the activities associated with preliminary analysis were 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. 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 Subsurface Operations and provides a map that links this analysis back to the MLD, the ESD, and the HAZOP evaluation.

## **E2 SCOPE AND BOUNDARY CONDITIONS**

### **E2.1 SCOPE**

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

1. HFEs are only considered if they contribute to a scenario that has the potential to result in a release of radioactivity, a criticality event, or a radiation exposure to workers.
2. Pursuant to the above, the following types of HFEs are excluded:
  - A. HFEs resulting in standard industrial injuries (e.g., falls)
  - B. HFEs resulting in the release of hazardous nonradioactive materials, regardless of amount
  - C. HFEs resulting solely in delays to or losses of process availability, capacity, or efficiency.
3. The identification of HFEs is restricted to those areas of the facility that handle waste forms and only during the times that waste forms are being handled (e.g., HFEs are not identified for the surface transportation of an unloaded transport and emplacement vehicle (TEV) when there is no loaded TEV on the surface tracks).
4. The exception to #3 is that system-level HFEs are considered for support systems when those HFEs could result in a loss of a safety function related to the occurrence or consequences associated with the events specified in #1.
5. Recovery post-initiator actions (as defined in Section E5.1.1.1) are not credited in the analysis; therefore, HFEs associated with them are not considered.
6. In accordance with Section 4.3.10.1 (boundary conditions of the PCSA), initiating events associated with conditions introduced in structures, systems, and components (SSCs) before they reach the site are not, by definition of 10 CFR 63.2 (Ref. E8.2.1), within the scope of the PCSA nor, by extension, within the scope of the HRA.

### **E2.2 BOUNDARY CONDITIONS**

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

- Only HFEs made in the performance of assigned tasks are considered. Malevolent behavior (i.e., deliberate acts of sabotage and the like) are not considered in this task.
- 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.
- YMP 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 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 on site, similar judgments must be made regarding optimal weather and rail 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) (ASME RA-S-2002 *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. E8.1.2) and incorporates the guidance provided by the U.S. Nuclear Regulatory Commission (NRC) in *Preclosure Safety Analysis – Human Reliability Analysis* (Ref. E8.1.15).

### **E3.2 GENERAL APPROACH**

The HRA consists of several steps, that follow the intent of ASME RA-S-2002 (Ref. E8.1.2) and the process guidance provided in *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624 (Ref. E8.1.14). 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. E8.1.14). 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.

---

<sup>1</sup>ATHEANA (Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA). NUREG-1624 (Ref. E8.1.14), 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.”

Human errors were identified based upon the three temporal parts generally analyzed by probabilistic risk assessment (PRA) and are categorized as follows:

- Pre-initiator HFEs
- Human-induced initiator HFEs
- Post-initiator HFEs<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 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 *Subsurface Event Sequence Development Analysis* (Ref. E8.1.6), 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

---

<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.

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 Subsurface 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:

---

<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.

- Investigation of potential vulnerabilities in operator expectations for the scenario
- Understanding of the base case scenario time line and any inherent difficulties associated with the required response
- Identification of operator action tendencies and informal rules
- Evaluation of formal rules and operating procedures expected to be used in the scenario.

The knowledge and information base is taken in the context of the specific HFE being evaluated. It includes not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status). Section E4 provides a description of the information types that comprise this knowledge base.

### **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. E8.1.14), 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 Subsurface Operations event sequence and categorization analysis. Therefore, only a general summary of the methodology associated with detailed quantification is presented in this section.

Detailed HRA quantification is performed for those HFEs that appear in dominant cut sets for event sequences that do not comply with the 10 CFR 63.111 performance objectives (Ref. E8.2.1) after initial fault tree or event sequence quantification. The goal of the detailed analysis is to determine whether or not the preliminary HFE quantification is too conservative such that event sequences can be brought into compliance by a more realistic HRA. However, the detailed analysis may result in a requirement for additional design features or specification of a procedural control (Step 9, Section E3.2.9) that reduces the likelihood of a given HFE in order to achieve compliance with 10 CFR 63.111 (Ref. E8.2.1). The qualitative analysis in steps 3, 5, and 6 sets the stage for the detailed quantification by providing the accident progression(s) for a given HFE and its context. Specifically, the qualitative analysis provides a list of unsafe actions,

along with their context, characteristics, and classification (i.e., EOO or EOC). For each unsafe action, the following steps are performed:

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

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. E8.1.12)<sup>4</sup>
2. HEART/NARA—“HEART – A Proposed Method for Assessing and Reducing Human Error” (Ref. E8.1.19) and *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (Ref. E8.1.7)
3. THERP (with some modifications)—*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Ref. E8.1.18).

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. E8.1.14).

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. E8.1.14) 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.

---

<sup>4</sup>Extended CREAM (Ref. E8.1.12) creates a link between CREAM and HEART (Ref. E8.1.19), and enhances the ability of CREAM to quantify skill-based HFEs.

Appendix E.I of this analysis provides the recommended approach for incorporation of human errors in the YMP PCSA, and Appendix E.V of this analysis provides the recommended naming conventions for HFEs incorporated in the fault tree models.

HFEs are incorporated, in the form of basic events, into the fault trees that support the initiating event and pivotal events of event trees. The HEP that is entered in a basic event is modeled as a lognormal distribution, whose mean value is the nominal value of the HEP, to which an error factor is assigned (Section E3.4) to reflect the uncertainty in the probability estimate. In many cases, the equipment failures and the associated HFEs are calculated as part of an integrated HRA. The resulting probability of both equipment and human failures is then placed in the fault tree as a single basic event.

### **E3.2.9 Step 9: Evaluation of HRA/PCSA Results and Iteration with Design**

This last step in HRA is performed each time the PCSA is quantified. The primary results are the HFEs in dominant cut sets and the associated qualitative inputs to such HFEs. Potential “fixes” to the design or operational environment can be supported by these results.

Because the YMP design and operations were still evolving during the course of this analysis, they could be changed in response to this analysis. This iteration is particularly necessary when an event sequence is noncompliant with the performance objectives of 10 CFR 63.111 (Ref. E8.2.1) because the probability of a given HFE dominates the probability of the event sequence. In those cases, a design feature or procedural safety control could be added to reduce the probability or to completely eliminate the HFE. In such cases, the modification is analyzed for potential new HFEs, and the applicable HFEs are requantified, along with the event sequences.

## **E3.3 DEPENDENCY**

Dependency between human actions is defined to exist when the outcome of a particular human action is related to the outcome of a prior human action or actions. According to THERP (Ref. E8.1.18), 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. E8.1.14)) account for certain types of dependencies within their formulation by combining dependent events as part of the normal process of addressing the accident scenario as a whole. These methods do not require additional treatment.

All event sequences that contain multiple HFEs are examined for possible dependencies. If practical, HFEs that are completely dependent may be redefined and modeled as a single event.

For the preliminary analysis, HFEs are modeled at a high level where several subtasks are combined into a single task so that explicit consideration of dependencies between subtasks is eliminated. For a detailed assessment, where the various actions that constitute an HFE are explicitly quantified, dependencies are explicitly addressed using the formulae in Table E3.3-1 from THERP (Ref. E8.1.18), 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. E8.1.19)/NARA (Ref. E8.1.7) or CREAM (Ref. E8.1.12) has its own dependency model, and NARA (Ref. E8.1.7) specifically endorses the use of the THERP (Ref. E8.1.18) 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. E8.1.18), 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. E8.1.7)
- HEART (Ref. E8.1.19)
- Chapter 9 of CREAM (Ref. E8.1.12)
- Chapter 20 of THERP (Ref. E8.1.18).

Although ATHEANA (Ref. E8.1.14) 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
$\geq 0.05$	3
$>0.0005\text{--}<0.05$	5
$\leq 0.0005$	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, common performance condition) 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 Subsurface 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. Following are sources of information from ISFSI that are applied to support the YMP PCSA:

- Interviews with plant operators, operations personnel, and/or other ISFSI knowledgeable personnel
- Pertinent ISFSI procedures (e.g., operating procedures, test and maintenance procedures)
- Plant walk-downs (e.g., at locations where operations similar to those at repository may be performed) and operations reviews

- Studies, including PRAs and HRAs, conducted at these facilities that would substitute for the previously mentioned sources.

This information was acquired from two sources. First, information was obtained by the HRA team from outside sources specifically for use on the YMP, such as from NPPs, industry organizations, and governmental sources. Some of this information may have been obtained directly by the HRA team or may have been provided to the HRA team by members of the Licensing and Nuclear Safety, Engineering, or Operations departments who had obtained the information as a part of their regular duties on the YMP (Section E4.2.2). Second, information was obtained by the HRA team directly from internal sources, including members of the aforementioned departments who had past experience and information on ISFSIs from prior employment and projects before joining the YMP (Section E4.2.1).

Initially, information is gathered to support the identification of pre-initiator, human-induced initiator, and non-recovery post-initiator HFEs. This information is needed to:

- Identify test and maintenance activities performed for equipment included in the PCSA model
- Determine the frequency of test and maintenance activities
- Identify the procedures used to perform test and maintenance activities
- Determine what equipment is impacted by test and maintenance activities.

For human-induced initiator and post-initiator HFEs, such information is needed to:

- Identify important operator tasks
- Identify the specific actions required for each operator task
- Identify the procedures (e.g., normal operating and emergency operating procedures) and procedure steps associated with each operator task
- Identify the cues (e.g., procedure steps, alarms) for operator tasks
- Assess the procedures that support operator tasks as PSFs
- Assess the training that supports operator tasks as PSFs.

#### **E4.1.2 Industry Data Reviewed by the HRA Team**

Due to the unique nature of the activities and equipment associated with Subsurface Operations, no industry data was available for review. Rather, the HRA team had to rely upon extensive discussion with subject matter experts to gain insights into failure modes and important contexts for Subsurface Operations (Section E4.2.2).

## **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 are provided in the *Subsurface Event Sequence Development Analysis* (Ref. E8.1.6).

### **E4.2.1 Role of HRA Team Judgment**

The preliminary analysis primarily performed by the HRA team in a consensus-based process follows:

- 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 HRA 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 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 Subsurface 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 Novovoronezh Russian nuclear reactor HRAs for the U.S. Department of Energy. 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.

Following 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)
- Radiation protection (e.g., cask shielding/shield rings; locks, interlocks, and procedural controls for entering high radiation areas and drifts)
- General facility (including aging pad and emplacement drifts) layout and time line of operations
- Interlocks (general)
- TEV design and operations

- Drip shield gantry design and operations
- Emplacement drift and portal gate security equipment (e.g., cameras), procedures and staffing
- Safety features of rail crossings with site roadways
- Emplacement procedures, calculations, and accountability
- 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

---

<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 NASA manned-mission risk assessments. Given the type of human actions and HFEs that are important at the YMP, use of this approach for the YMP PCSA HRA is not recommended.

2. Error modes:
  - A. EOOs
  - B. EOCs
3. Human failure types:
  - A. Slips/lapses
  - B. Mistakes
4. Informational processing failures:
  - A. Monitoring and detection
  - B. Situation awareness
  - C. Response planning
  - D. Response implementation.

The following sections define these classification methods.

#### **E5.1.1.1 Temporal Phases of HFEs**

There are three temporal phases of HFEs:

- Pre-initiator HFE—An HFE that represents actions taken before the initiating event that causes systems or equipment to be unavailable. Examples of such HFEs are miscalibration of equipment or failure to restore equipment to an operable state after testing or maintenance activities.
- Human-Induced Initiator—An HFE that represents actions that cause or lead to an initiating event.
- Post-initiator HFE<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.

---

<sup>6</sup> The HRA did not take credit for post-initiator human actions and no post-initiator HFEs were identified.

- 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.

#### **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.

---

<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.

#### E5.1.1.4 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. E8.1.14) 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 Subsurface Operations

A list of personnel involved in Subsurface Operations with a brief description of their duties follows:

**Crew member**—A generic term for personnel (not including TEV operators, radiation protection workers, or supervisors) involved in the facility operations.

**Engineer**—The certified crew member who performs engineering calculations and the verification of programming emplacement locations into the TEV programmable logic controller (PLC).

**Gantry operator**—The person who is designated to operate the drip shield gantry. This person is in charge of ensuring that the gantry is in the appropriate configuration for drip shield emplacement. This person is located in the Central Control Center and controls the gantry remotely.

**Person in charge (PIC)**—The certified crew member who is in charge of coordinating and overseeing the operation. This is the person who is notified when a waste form is ready for transit and who coordinates, according to this information, the appropriate personnel, procedures, and equipment to be used to process this cask type. This person is in charge of communicating this information to all the crew members involved in the emplacement of the waste package and ensuring that the relevant equipment is properly staged and in proper operational condition.

**Quality control**—The certified crew member in charge of quality control. This person is involved in supervising critical operations and tracking the appropriate documentation (i.e., tracking the waste package emplacement position).

**Radiation protection worker**—The certified health physics technician, whose job is to monitor radiation during cask-related activities. This person is responsible for stopping operations if high radiation levels are detected.

**Security guard**—The person responsible for monitoring the activities to ensure that security barriers are maintained and procedures are followed. This person ensures that crew members (or others) do not enter the drifts unless scheduled. Has authorization to halt operations if security is being compromised.

**Supervisor**—The person who is in charge of the given operation and who supervises and checks off critical operations in a given step. For steps requiring independent verification, this analysis uses the term “supervisor” as the person who provides the independent check. This analysis does not rely upon the fact that this check is performed by the actual supervisor, only that an independent check is done by someone with the appropriate training and qualifications (i.e., the supervisor).

**TEV operator**—The person who is designated to operate the TEV. This person is in charge of ensuring that, prior to leaving the facility, the TEV is in the appropriate configuration for movement of a waste package to the drifts. This person is located in the Central Control Center and controls the TEV remotely.

## **E5.2 OVERVIEW OF HUMAN PERFORMANCE ISSUES**

This section discusses the general human performance issues that characterize the human interaction with the Subsurface Operations.

**Communication Difficulties**—There are significant challenges in communication between the local and remote team members performing Subsurface Operations. TEV operators located in the Central Control Room must converse with other crew members local to the drifts (e.g., the security guard) using some sort of communication device (e.g., walkie talkies). Garbled communication (due to system interference or background noise) is clearly possible, and in some cases it may not even be possible to clearly determine who is speaking. A belief that a particular

individual is speaking, even if they are not, can bias the listeners into hearing what they expect to hear.

**Visual Challenges**—For most of the remote operations, successful completion of the operation requires a certain amount of visual acuity both for the performance of the operation and the confirmation of the status. Safety concerns require that visual observation be performed using cameras that provide images to screens in the control room. In addition, views may be obstructed, such as by some structure or equipment.

**Unchallenging Activities**—The activities involved in Subsurface Operations are, in general, heavily automated and therefore the human–machine interface is quite simple in nature. In addition, the speed of the movements is quite slow, so each action takes a long time to complete. Basically, this is mostly boring work, with a significant amount of downtime between actions for some individuals. There is ample opportunity for diversion and distraction, and an air of informality and complacency can easily exist within and amongst the crew members. From a psychological perspective, there is insufficient dynamic activity to generate an optimum stress level for performance.

## **E6 ANALYSIS**

### **E6.0 BACKGROUND**

#### **E6.0.1 Reader’s Guide to the HRA Analysis**

Section E3.2 describes nine steps that comprise the HRA process. This section describes the implementation of Steps 2 through 8.

This section documents the qualitative and quantitative analysis of HFEs associated with Subsurface Operations. Subsurface Operations are significantly less complicated than a set of facility operations; therefore, the entire set of Subsurface Operations was analyzed as one group of operations. Figure E6.0-1 provides an overview of Subsurface Operations. Each high-level operational activity is described in Section E6.1; 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 HAZOP evaluation nodes. 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.



NOTE: CRCF = Canister Receipt and Closure Facility; IHF = Initial Handling Facility; TEV = Transport and Emplacement Vehicle; WP = waste package.

Source: Original

Figure E6.0-1. Major Subsurface Operations Steps

Table E6.0-1. Correlation of Subsurface Operations to ESDs and HAZOP Evaluation Nodes

Activity	HAZOP Evaluation Node	ESD
<b>Transit from Surface Facility to Emplacement Drift Door (Section E6.1.3)</b>		
Loaded TEV exits facility (Section E6.1.3)	1	1
Loaded TEV transit from facility to North Portal (Section E6.1.3)	2	2
Loaded TEV transit from North Portal to emplacement drift door (Section E6.1.3)	3	3
<b>Waste Package Emplacement (or Retrieval) (Section E6.1.4)</b>		
Waste package emplacement (Section E6.1.4.1)	4	3
Waste packager (Section E6.1.4.2)	4	3
<b>Drip Shield Emplacement (Section E6.1.5)</b>		
Drip shield emplacement (Section E6.1.5)	5	3

NOTE: ESD = event sequence diagram; HAZOP = hazard and operability; TEV = transport and emplacement vehicle.

Source: Original

ESD 4 (Event Sequence Associated with Loss or Lack of Shielding) and ESD 5 (Event Sequence Associated with Localized Internal Fire) are applicable to all Subsurface Operations.

## E6.1 DESCRIPTION OF SUBSURFACE OPERATIONS BASE CASE SCENARIOS

Subsurface operations include movement of the loaded TEV to the emplacement drift; emplacement of the waste package; and, once all the waste packages are emplaced, emplacement of the drip shield. While not anticipated to be part of the normal Subsurface Operations, the subsurface operators have the capability to retrieve an emplaced waste package, as well.

### E6.1.1 Initial Conditions

The following conditions and design considerations provide the background for the base case scenario:

- A TEV is sitting in the appropriate facility, loaded with waste packages and with the facility doors shut. The TEV shield doors are closed, and it is ready to leave the facility to go to the subsurface drifts.
- The facility doors are closed.
- The TEV operators are located in the Central Control Center and watch TEV operations via camera (there are cameras on the front and back of the TEV). The only PLC override control these operators have is to signal the TEV to stop. There are lights on the front and back of the TEV and in the access mains (but not necessarily in the emplacement drifts).
- In the Central Control Center there is a display board that has a map of the facility and drifts. This display board has lights to represent movement of the TEV, and the drifts have lights to represent emplaced waste packages. There are also indicators of switch position in the control room.
- There are TEV crossing indicators/lights where the TEV rail intersects site roads.
- For accountability purposes, the drift inventory is verified (by counting the number of waste packages in each drift) every month until the drift is closed. This is done by sending the drip shield gantry with a camera into the drifts to allow the operators to count the number of emplaced waste packages. The gantry can travel the length of the tunnel.
- Safety features of the TEV include an override to stop the shield doors from opening if the operator notices that the TEV is too close to a waste package.
- No construction is permitted in the proximity of the TEV path on the surface; the closest construction to the TEV path is roughly 30 m away.
- The TEV speed is limited to less than 2 mph, and the TEV has visual and auditory alarms when loaded and traveling on the surface. Before the TEV leaves a facility, the operators signal all (intersection) crossings to close (including the crossing gate, lights, and the auditory signal).
- There are operational controls that prohibit another TEV from traveling on the surface while a loaded TEV is traveling on the surface. There is a similar restriction for TEV traffic in the drifts.

- The TEV rails are on a concrete pad; the edge of this pad marks the “exclusion zone.” To exceed the 100-mrem dosage, a person must be located approximately 1 ft from the TEV for approximately 1 hour.
- There is an electromechanical interlock that physically prevents the TEV shield doors from opening during transit. This interlock is engaged or disengaged at the facility door and the drift door.
- There are front and rear anticollision interlocks. These interlocks, however, are routed through the PLC.
- There are operational controls restricting TEV operation during inclement weather (e.g., thunderstorms); however, water or ice on the tracks does not pose a problem for the TEV.
- There are at least two personnel entrances into the drifts: the North Portal and a (or several) sealed bulkhead(s) on the construction side. Both entrances are monitored by security and clearly marked. Personnel expected to enter the drifts are controlled and their positions monitored. The emplacement drift access door has an emergency escape door (roughly 12 by 16 in.) that only allows traffic to exit the drift. The access door itself has a lock box that must either be physically unlocked, or central control can remotely activate the access door. The North Portal is the main access point to the drifts.
- The TEV operates off an electrically powered third rail.

The following personnel are involved in these operations:

- Crew member
- Engineer
- Gantry operator
- PIC
- Quality control
- Radiation protection worker
- Security guard
- Supervisor
- TEV operator.

Section E5.1.2 provides a more detailed description of the duties performed by each of these personnel.

### **E6.1.2 Radiologic Inspection of Waste Package**

**Prejob Plan**—Before the TEV is dispatched to the Canister Receipt and Closure Facility (CRCF)/ Initial Handling Facility (IHF), the PIC is notified of the type of waste package that needs to leave the facility. According to this information, the PIC determines the appropriate procedures to be used in emplacement. The PIC also communicates this information to all the

crew members involved in the emplacement of this waste package. This prejob plan includes engineering calculations to determine in which drift to emplace the waste package, based on the thermal output of the fuel inside the waste package; these calculations are verified by quality control. This plan also includes programming this emplacement location into the TEV PLC; this program is verified by an engineer, quality control personnel, and the supervisor. All crew members are properly trained in their task and abide by the procedures of the facility.

**Radiologic Inspection of the Waste Package**—The waste package cannot be inspected directly; it is inspected visually via camera during TEV loading (in the CRCF or IHF), and a radiological survey is performed on the loaded TEV as a proxy to direct inspection of the waste package. Once the TEV is loaded and ready for export, a radiation protection worker enters the Waste Package Loadout Room of the facility and visually inspects and conducts radiological surveys of the exterior of the TEV.

### **E6.1.3 TEV in Transit from Surface Facility to Emplacement Drift Door**

**Leaving Surface Facility**—Once the TEV is loaded and closed, a crew member opens the facility doors, and the TEV operator signals the TEV to initiate travel to the North Portal.

Prior to the initiation of this step, the TEV track must be cleared of all objects and debris. The operator ensures that all the switches have been properly thrown and that the proper crossing lights and blockades (e.g., at the rail crossings with site roads) have been activated when the TEV moves across the facility.

Once the TEV has left the facility, the facility crew member closes the facility door.

**TEV to North Portal**—The TEV automatically travels from the facility to the North Portal. There are periodic check points (most probably at the switch points) when the operator has to give a confirmation signal for the TEV to continue. There are 5 to 10 switches along the path from a given facility to the North Portal. There is no requirement for a camera view of the switches; however, the switch position is indicated on a switchboard in the control room. Once the TEV has reached the outer gate of the North Portal, it automatically stops.

**TEV Travels into Subsurface**—When the TEV has reached the North Portal, the security guard opens the outer gate, and the TEV operator signals the TEV to proceed. The TEV travels into the gated area and stops after clearing the first gate but before reaching the second gate. The security guard closes the outer gate and verifies that there are no personnel in the drift. Once it is clear, the guard opens the second gate, and the TEV operator signals the TEV to travel to the proper drift.

**TEV to Turnout and Emplacement Drift**—Once the TEV reaches the proper emplacement drift, it automatically stops. As the TEV approaches the drift door, it runs over and trips a switch on the track that signals the drift door to open and that disengages the interlock that prevents inadvertent opening of the TEV shield door. Once the door is open, the operator signals the TEV to start, and the TEV enters partway into the drift and stop. The drift door automatically closes once the TEV has cleared the doorway.

## **E6.1.4 Waste Package Emplacement (or Retrieval)**

### **E6.1.4.1 Waste Package Emplacement**

**TEV Shield Doors Opened**—Once the loaded TEV is stopped midway into the drift (a set distance away from the closest waste package), the TEV shield doors automatically open. No human action is necessary for this step.

**Back Shield Lifted**—After the shield doors are opened, the back shield automatically lifts. No human action is necessary for this step.

**Bottom Shield Extended**—When the back shield is lifted, the bottom shield automatically extends. No human action is necessary for this step.

**TEV Continues to Final Waste Package Position**—Once the bottom shield is extended, the TEV automatically moves the waste package into its emplacement position, roughly 4 in. away from the last waste package in the drift. No human action is necessary for this step.

**Lowering Shielding and Emplacing Waste Package**—The waste package is automatically lowered and emplaced when the TEV is in position. No human action is necessary for this step.

**Confirming Proper Waste Package Location**—The TEV operator uses the camera to confirm proper emplacement of the waste package within the drift. The operator also consults the control board to confirm that the waste package is in the proper drift. Quality control signs off this step.

**Backing TEV away from Waste Package**—Once the waste package is set in position, the TEV automatically backs away from the waste package until the TEV doors have completely cleared the waste package. No human action is necessary for this step.

**Lifting Shielded Compartment**—The TEV stops and then automatically lifts the shielded compartment. No human action is necessary for this step.

**Retracting Bottom Shield**—Once the TEV has cleared the emplaced waste package, it automatically retracts the bottom shield. No human action is necessary for this step.

**Lowering Back Shield and Closing TEV Doors**—With the bottom shield retracted, the back shield automatically lowers, and the TEV doors close in preparation for TEV movement. No human action is necessary for this step.

### **E6.1.4.2 Waste Package Retrieval**

**Moving Empty TEV into Drift**—The TEV operator moves an empty TEV into the drift where the waste package to be retrieved is located.

**TEV Shield Doors Opened**—Once the loaded TEV is stopped midway into the drift (a set distance away from the closest waste package), the TEV shield doors automatically open. No human action is necessary for this step.

**Back Shield Lifted**—After the shield doors are opened, the back shield automatically lifts. No human action is necessary for this step.

**Bottom Shield Extended**—When the back shield is lifted, the bottom shield automatically extends. No human action is necessary for this step.

**Lowering Shielded Compartment**—The shielded compartment is automatically lowered when the TEV is in position. No human action is necessary for this step.

**Driving Forward**—The TEV automatically moves forward to the waste package to be picked up. No human action is necessary for this step.

**Locating Waste Package**—The TEV automatically moves over the waste package to be picked up. No human action is necessary for this step.

**Lifting Shielded Compartment and Waste Package**—The TEV automatically lifts the waste package into the TEV by lifting the shielded compartment.

**Retracting Bottom Shield**—Once the TEV has cleared the emplaced waste package, it automatically retracts the bottom shield. No human action is necessary for this step.

**Lowering Back Shield and Closing TEV Doors**—With the bottom shield retracted, the back shield automatically lowers, and the TEV doors close in preparation for TEV movement. No human action is necessary for this step.

**Leaving Old Drift**—The TEV operator signals the TEV to leave the drift once the TEV has been loaded with the retrieved waste package. The TEV then travels to the drift door and stops. The drift door automatically opens, and the operator signals the TEV to travel out of the emplacement drift to the new drift. The drift door automatically closes, and the TEV shield door interlock reengages once the TEV has cleared the doorway.

**Entering New Drift**—Once the TEV reaches the proper drift, it automatically stops. As the TEV approaches the door, it runs over and trips a switch on the track that signals the drift door to open and that disengages the interlock that prevents inadvertent opening of the TEV shield door. After the drift door has opened, the operator signals the TEV to start, and the TEV enters partway into the drift and stop. The drift door automatically closes once the TEV has cleared the doorway.

**Emplace Waste Package in New Drift**—Further information is provided in Section E6.1.4.1.

### **B6.1.5 Drip Shield Emplacement**

**Drip Shield Gantry to North Portal**—Prior to the initiation of this step, the track must be cleared of all objects and debris. The proper crossing lights and blockades (e.g., at the rail crossings with site roads) activate as the gantry moves across the facility.

The gantry automatically travels from the facility to the North Portal without human interaction. Once the gantry has reached the outer gate of the North Portal, it automatically stops.

**Drip Shield Gantry Continues to Subsurface**—Once the gantry is at the North Portal, the security guard opens the outer gate, and the gantry operator signals the gantry to go. The gantry travels into the gated area and stops after clearing the first gate but before reaching the second gate. The security guard closes the outer gate and verifies that there are no personnel in the drift. Once the area is verified as clear, the guard opens the second gate, and the gantry operator signals the gantry to travel to the proper drift.

**Drip Shield Gantry to Turnout and Selected Drift**—At the point where the gantry reaches the proper drift, it automatically stops. As the gantry approaches the door, it runs over a switch on the track that signals the drift door to open. Once the door is open, the operator signals the gantry to start, and the gantry enters the drift. The drift door automatically closes once the gantry has cleared the doorway.

**Continuing to Final Drip Shield Position**—The gantry automatically continues until it is in position, and then it stops.

**Lowering Drip Shield**—The gantry is automatically lowered into place and released.

**Confirming Proper Drip Shield Location and Interlock**—The gantry operator uses the camera to confirm proper placement of the drip shield within the drift. Quality control signs off this step. The drip shield is lowered onto the part of the previous segment of drip shield and mechanically locks into place.

**TEV to Drift Entrance and Turnout**—Once the gantry has set the drip shield down in the proper location, the gantry operator signals the gantry to leave the drift. The gantry moves to the drift door and stops. The drift door automatically opens, and the operator signals the gantry to travel out of the emplacement drift to the new drift. The drift door automatically closes once the gantry has cleared the doorway. The gantry then exits the subsurface.

## **E6.2 ANALYSIS OF SUBSURFACE 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 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 chosen by the HRA team to assign preliminary HEPs when interlocks were present was simplified. Since the interlock would prevent the operator from completing an unsafe action (even if the operator tried to) it was conservatively analyzed as if the operator would always take the unsafe action (i.e., the HEP for the HFE containing the unsafe action was conservatively set to 1.0 as a first approximation of the HEP). Unless otherwise specified, this was done for all cases where the

human cannot easily defeat the interlock that protects against the associated unsafe action and 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 PLCs were not credited in this analysis since they won't be declared important to safety.

**HVAC System**— For Subsurface Operations that occur in the CRCF Loadout Room, the CRCF heating, ventilation, and air-conditioning (HVAC) system is an integral part of the system modeled. (NOTE: This is not applicable to waste packages exported from the IHF as the IHF has no HVAC system important to safety. Also, the Subsurface drifts may have a ventilation system, but this system is also not important to safety.) The following pre-initiating HFEs were identified and assigned preliminary values:

060-VCTO-DR00001-HFI-NOD: Operators Open Two or More Vestibule Doors in CRCF

**Preliminary Value:**  $1E-02$

**Justification:** Used general guidance for pre-initiator HFE preliminary values in Table E.III-2 for failure to properly restore an operating system to service when the degraded state is not easily detectable.

060-VCTO-HFIA000-HFI-NOM: Human Error: Exhaust Fan Switch Wrong Position

**Preliminary Value:** 1E-01

**Justification:** Used general guidance for pre-initiator HFE preliminary values in Table E.III-2 for failure to properly restore a standby system to service.

060-VCTO-HEPALK-HFI-NOD: Operator Fails to Notice HEPA Filter Leak in Train A

**Preliminary Value:** 1.0

**Justification:** To be conservative, credit was not given for the operator noticing HEPA filter leaks.

**Electrical System**— For Subsurface Operations that occur in the CRCF Loadout Room, the CRCF Electrical system is an integral part of the system modeled because it affects the CRCF HAVC system reliability. (NOTE: This is not applicable to waste packages exported from the IHF as the IHF has no HVAC system important to safety. Also, the Subsurface drifts may have a ventilation system and other electrical systems, but these systems are also not important to safety.) The following pre- and post-initiating HFEs were identified and assigned preliminary values:

060-#EEE-LDCNTRA-BUA-ROE and 060-#EEE-LDCNTRB-BUA-ROE: Operator Fails to Restore ITS Load Center Post Maintenance

26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS: Operator Fails to Restore Diesel Generator to Service

**Preliminary Values and Justification:** For electrical systems, the HFE assigned to operator failure to restore a system (i.e., motor control center or diesel generator) to service was assigned a conservative value of 0.1. The overall failure probability for load centers (060-#EEE-LDCNTRA-BUA-ROE and 060-#EEE-LDCNTRB-BUA-ROE) is 1.03E-05 and for diesel generators (26D-#EEY-ITSDG-A-#DG-RSS and 26D-#EEY-ITSDG-B-#DG-RSS) is 1.95E-04. These failure probabilities reflect the probability that the motor control center or diesel generator requires service, and they are further discussed in Attachment B. Table E6.2-1 summarizes the preliminary values for the cross-operation generic HFEs.

Table E6.2-1. Summary of Preliminary Values for the Generic HFEs

HFE ID	HFE Brief Description	Preliminary Value
060-VCTO-DR00001-HFI-NOD	Operators Open Two or More Vestibule Doors in CRCF	1E-02
060-VCTO-HFIA000-HFI-NOM	Human Error: Exhaust Fan Switch Wrong Position	1E-01
060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1.0
060-#EEE-LDCNTRA-BUA-ROE 060-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore ITS Load Center Post Maintenance	1.03E-05
26D-#EEY-ITSDG-A-#DG-RSS 26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator to Service	1.95E-04

NOTE: CRCF = Canister Receipt and Closure Facility; HEPA = high-efficiency particulate air filter; HFE = human failure event; ID = identification; ITS = important to safety.

Source: Original

### E6.2.2 HFE Descriptions and Preliminary Analysis

This section defines and screens the HFEs that are identified for the base case scenario, that can affect the probability of initiating events occurring, and that could lead to undesired consequences. Descriptions and preliminary analysis for the HFEs of concern during Subsurface Operations are summarized in Table E6.2-2. 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 E6.2-2. HFE Group #1 Descriptions and Preliminary Analysis

HFE ID	HFE Brief Description	ESD	Preliminary Value	Justification
TEV derailment	<i>Operator Causes TEV to Derail as it Travels between the Facility and the Drifts</i>	2, 3	N/A <sup>a</sup>	Throughout Subsurface Operations the TEV travels on rail to and from various locations. A human-induced derailment HFE was not explicitly quantified because the probability of derailment due to human failure is incorporated in the historical data used to provide a general failure probability for derailment. Documentation for this failure can be found in Attachment C.
800-HEE0-WKRDRFT-HFI-NOD	<i>Worker Enters Drift from Access Main:</i> If a worker enters an active drift, purposefully or accidentally, then that worker would get a direct exposure.	4	N/A	If a worker enters an active drift for a prolonged period of time, purposefully or accidentally, then the worker would get a direct exposure. This failure event was omitted from analysis by the subsurface analysts and is not part of this HRA. Section 6.0 of the main report provides a screening justification.
800-HEE0-WKRPROX-HFI-NOD	<i>Worker Stands too Close to TEV for an Extended Period of Time:</i> If a worker stands too close to a loaded TEV for a prolonged period of time (~1 hour), purposefully or accidentally, then that worker would get a direct exposure.	4	N/A	If a worker stands too close to a loaded TEV for a prolonged period of time, purposefully or accidentally, then the worker gets a direct exposure. This failure event was omitted from analysis by the subsurface analysts and is not part of this HRA. Section 6.0 of the main report provides screening justification.
800-HEE0-WKRFACD-HFI-NOD	<i>Operator Causes Collision of TEV with Facility Doors:</i> While exiting the CRCF or IHF, the operator can signal the TEV to move before the facility doors are completely open, or the facility doors can be closed on the TEV before the TEV has cleared the doorway.	1	2.0E-03	The facility doors are normally in the safe load path of the TEV and, during export, the doors can be partially open such that the operator thinks there is enough clearance to pass through but collides instead. Alternatively, the operator can inadvertently close the door on the TEV. There are no hardwired interlocks that would prevent this failure; the anticollision interlock on the TEV is not sufficient because the door is considered to be mostly open. The TEV is a large vehicle with operators watching the operations via camera, and it would go against operator training to begin moving the TEV before the doors are completely open or for the operator to begin closing the door before the TEV is completely through. This failure was considered highly unlikely (0.001, which also corresponds to the default probability for a simple action performed daily) and was adjusted to account for the fact that TEV operations are viewed via camera (×2).
800-HEE0-SIDEIMP-HFI-NOW	<i>Operator Causes Collision of TEV with SSC:</i> While the TEV is in transit between the facility and the emplacement drift, it can collide with an SSC on the tracks or with a site vehicle.	2	3.0E-04	In this step, the TEV is impacted by a site vehicle, most likely at an intersection or crossing. Aboveground, during TEV travel, all intersections have special crossing barricades and/or signals (like railroad crossing signals); in the drifts, all traffic is operationally restricted from being in the same area as a loaded TEV. The TEV also has an operator watching the TEV via camera, and the TEV moves very slowly, roughly 2 mph. Because of the special operational restrictions, the training that the operations personnel have regarding the TEV, and the slow speed of the TEV, this failure mode was determined to be roughly an order of magnitude lower than a collision of a vehicle while exiting the facility (800-HEE0-WKRFACD-HFI-NOD).
800-HEE0-TEVDOOR-HFI-NOD	<i>Human Error Causes TEV Doors to Open during Transit:</i> If the TEV operator prematurely signals the TEV shield doors to open, and the doors indeed open, then any personnel present would be exposed.	4	1.0E-03	The TEV is controlled remotely by highly trained operators. The TEV shield doors are only opened in the facility and in the drifts, where they do so semiautomatically. There are interlocks to prevent inadvertent TEV door opening during transit. In order to commit this unsafe action, the operator would have to be quite careless as it is expected that the control, which would allow the operator to open the TEV doors, is quite distinct from the other TEV controls. Therefore, this action was considered highly unlikely and assigned the default preliminary value of 0.001.
800-HEE0-AXSDR00-HFI-NOD	<i>Operator Causes Collision of TEV with Access Doors:</i> While entering the North Portal or a drift, the operator can signal the TEV to move before the portal gate or drift door is completely open, or the gate/door can be closed on the TEV before the TEV has cleared the doorway.	2, 3	2.0E-03	The TEV automatically stops in front of the North Portal/drift doors, and the operator, watching via camera, has to give a "go" signal to the TEV for it to continue its operations. If the operator prematurely signals the TEV to enter through the North Portal or drift door before the door/gate is open, doing so would result in a collision of the TEV. The chance that the operator would fail to look closely at the gate/door before giving the "go" signal is highly unlikely (0.001) but was adjusted (×2) to account for the fact that this is a camera operation and might, therefore, involve some visibility issues. This failure is similar to 800-HEE0-WKRFACD-HFI-NOD, and it is consistent for these two failures to have the same preliminary values.
800-HEE0-IMPACTF-HFI-NOD	<i>Human Error Causes TEV to Impact WP in the Drift:</i> While emplacing the WP in a drift, the TEV is under manual control. The TEV operator could collide into an emplaced WP. The TEV operator can also impact an emplaced WP with the TEV shield doors if the TEV is too close to the WP when the operator signals the shield doors to be opened.	3	1.0E-03	Once inside the drift, the operators manually control the TEV for waste package emplacement. There are two ways the operator can damage a waste package in the drift during this step: collide the TEV directly into a waste package or open the shield doors into the waste package. The TEV can only move very slowly (2 mph or less), and there are guide marks to aid in positioning the TEV. TEV operations, however, are done via camera and, in the drift, the only available lighting comes from the TEV itself. It is expected that the operator would be quite attentive during this step, as it requires active control. This error was assessed to be highly unlikely and thus assigned the default value of 0.001.
HFE-RUNAWAY-RESPONSE	<i>Operator Fails to Stop TEV Using Manual Override during a Runaway Event:</i> If speed control for the TEV malfunctions and the TEV begins to overspeed, the TEV operator must use the manual override to stop the TEV before a high-speed collision occurs.	1, 2, 3	N/A	No credit is given for recovery actions; therefore, this HFE is not modeled.

Table E6. 1-1. HFE Group #1 Descriptions and Preliminary Analysis (Continued)

OP-FAILS-ENDOFRAIL	<i>Operator Error Causes TEV to Run over End of Rail:</i> TEV movement across the surface and into the drifts is highly automated. If the operator misprograms the TEV such that it overtravels a segment of path, the TEV can collide into an SSC or overrun the rails.	2, 3	1.0E-03	If the operator improperly programs the TEV route, then the TEV can overtravel the rail and collide into the end stop. This failure is separate from a collision with a waste package during emplacement because emplacement is performed manually. For the portions of travel for which this failure is relevant, there are a consistent set of coordinates that do not change except to chose which surface facility the waste package originates from. This is similar to the pre-initiator "calibration error," which has a default preliminary value of 0.01. This value was adjusted by an order of magnitude ( $\times 0.1$ ) to account for the fact that the programming process, including an independent check, is designed to be more rigorous than the average calibration process during routine maintenance. Also, the TEV operator is closely watching the TEV during the operation and would have the opportunity to stop the TEV if it does not seem to be properly programmed.
Drip shield emplacement	<i>Operator Error Causes Impact to WP during Drip Shield Emplacement:</i> During drip shield emplacement, the operator moves a heavy drip shield into the drift and installs it over the WPs. If an operator improperly performs this operation, the operator can potentially impact a WP with the drip shield or the drip shield gantry.	3	N/A	The drip shield gantry runs on rails that cause its travel to be wider and higher than the emplacement path of the waste packages, and the analysts could not find any plausible scenarios by which humans could impact a waste package during drip shield emplacement; therefore, this failure mode was omitted from analysis.

NOTE: <sup>a</sup>Historical data was used to produce the probability; this historical data is not included as part of the HRA but is addressed in Attachment C on active component failure data.  
CRCF = Canister Receipt and Closure Facility; ESD = event sequence diagram; HFE = human failure event; HRA = human reliability analysis; ID = identification;  
IHF = Initial Handling Facility; N/A = not applicable; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WP = waste package.

Source: Original

### 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 HUMAN RELIABILITY ANALYSIS DATABASE

Table E7-1 presents a summary of all of the human failures identified in this analysis. It also 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
060-#EEE-LDCNTRA-BUA-ROE	Operator Fails to Restore Load Center A Post Maintenance	1	1.03E-05	10	Preliminary
060-#EEE-LDCNTRB-BUA-ROE	Operator Fails to Restore Load Center B Post Maintenance	1	1.03E-05	10	Preliminary
060-VCTO-DR00001-HFI-NOD	Operators Open Two or More Vestibule Doors in CRCF	1	1E-02	3	Preliminary
060-VCTO-HFIA000-HFI-NOM	Human Error: Exhaust Fan Switch in Wrong Position	1	1E-01	3	Preliminary
060-VCTO-HEPALK-HFI-NOD	Operator Fails to Notice HEPA Filter Leak in Train A	1	1.0	N/A	Preliminary
26D-#EEY-ITSDG-A-#DG-RSS	Operator Fails to Restore Diesel Generator A to Service	1	1.95E-04	10	Preliminary
26D-#EEY-ITSDG-B-#DG-RSS	Operator Fails to Restore Diesel Generator B to Service	1	1.95E-04	10	Preliminary
800-HEE0-WKRDRFT-HFI-NOD	Worker Enters Drift from Access Main	4	N/A <sup>b</sup>	N/A	Omitted from Analysis
800-HEE0-WKRPROX-HFI-NOD	Worker Stands too Close to TEV for an Extended Period of Time	4	N/A <sup>b</sup>	N/A	Omitted from Analysis
800-HEE0-WKRFACT-HFI-NOD	Operator Causes Collision of TEV with Facility Doors	1	2.0E-03	5	Preliminary
800-HEE0-SIDEIMP-HFI-NOW	Operator Causes Collision of TEV with SSC	2	3.0E-04	10	Preliminary
800-HEE0-TEVDOOR-HFI-NOD	Human Error Causes TEV Doors to Open during Transit	4	1.0E-03	5	Preliminary
800-HEE0-AXSDR00-HFI-NOD	Operator Causes Collision of TEV with Access Doors	2, 3	2.0E-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
800-HEE0-IMPACT-HFI-NOD	Human Error Causes TEV to Impact WP in the Drift	3	1.0E-03	5	Preliminary
Drip shield emplacement	Operator Error Causes Impact to WP during Drip Shield Emplacement	3	N/A <sup>b</sup>	N/A	Omitted from Analysis
HFE-RUNAWAY-RESPONSE	Operator Fails to Stop TEV Using Manual Override during a Runaway Event	1, 2, 3	N/A <sup>b</sup>	N/A	Omitted from Analysis
OP-FAILS-ENDOFRAIL	Operator Error Causes TEV to Run over End of Rail	2, 3	1.0E-03	5	Preliminary
TEV derailment	Operator Causes TEV to Derail as It Travels between the Facility and the Drifts	2, 3	N/A <sup>a</sup>	N/A	Historical Data

NOTE: <sup>a</sup>HRA value replaced by use of historic data (Attachment C provides further information on active component failure data).

<sup>b</sup>These HFEs were initially identified, but omitted from analysis for various reasons, including a design change precluding the human failure, or the failure would require a series of unsafe actions in combination with mechanical failures, such that the event is no longer credible. See Section E6.2 for a case-by-case justification for these omissions.

CRCF = Canister Receipt and Closure Facility; ESD = event sequence diagram; HEPA = high-efficiency particulate air filter; HFE = human failure event; N/A = not applicable; SSC = structure, system, or component; TEV = transport and emplacement vehicle; WP = waste package.

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 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.

- E8.1.3\* BSC (Bechtel SAIC Company) 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.
- E8.1.4\* 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.
- E8.1.5\* BSC 2007. *Repository System Codes*. 000-30X-MGR0-01200-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071101.0022.
- E8.1.6 BSC (Bechtel SAIC Company) 2008. *Subsurface Operations Event Sequence Development Analysis*. 000-PSA-MGR0-00400-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080214.0004.
- E8.1.7\* 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.
- E8.1.8\* 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.
- E8.1.9\* 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.
- E8.1.10\* 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.
- E8.1.11\* 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.
- E8.1.12\* Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM*. 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.
- E8.1.13 NRC (U.S. Nuclear Regulatory Commission) 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. )
- E8.1.14 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.

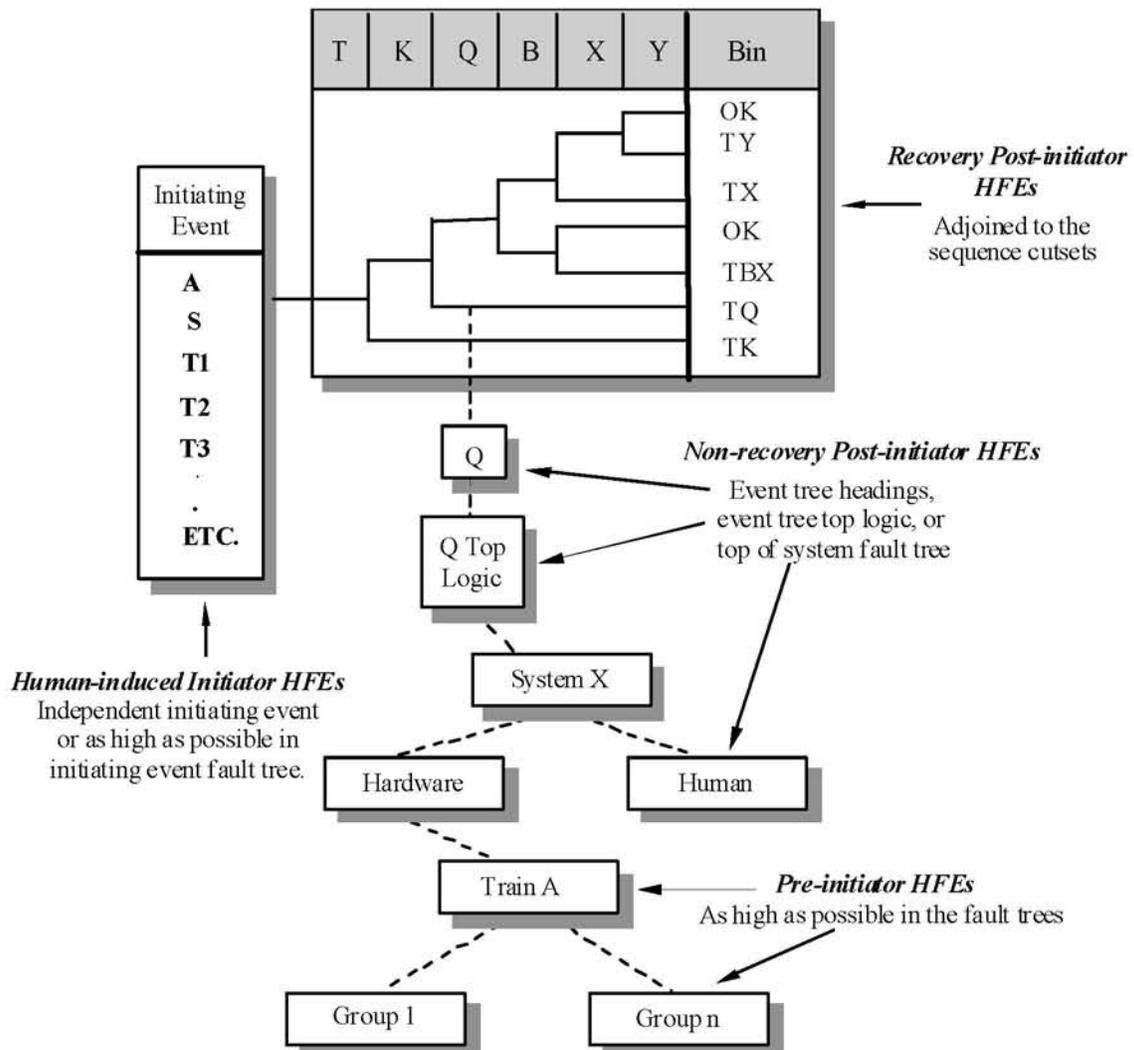
- E8.1.15 NRC 2007. *Preclosure Safety Analysis - Human Reliability Analysis*. HLWRS-ISG-04. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071211.0230.
- E8.1.16\* Rasmussen, J. 1983. "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance 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.
- E8.1.17\* 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.
- E8.1.18\* 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.
- E8.1.19\* 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.
- E8.1.20\* 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) 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.

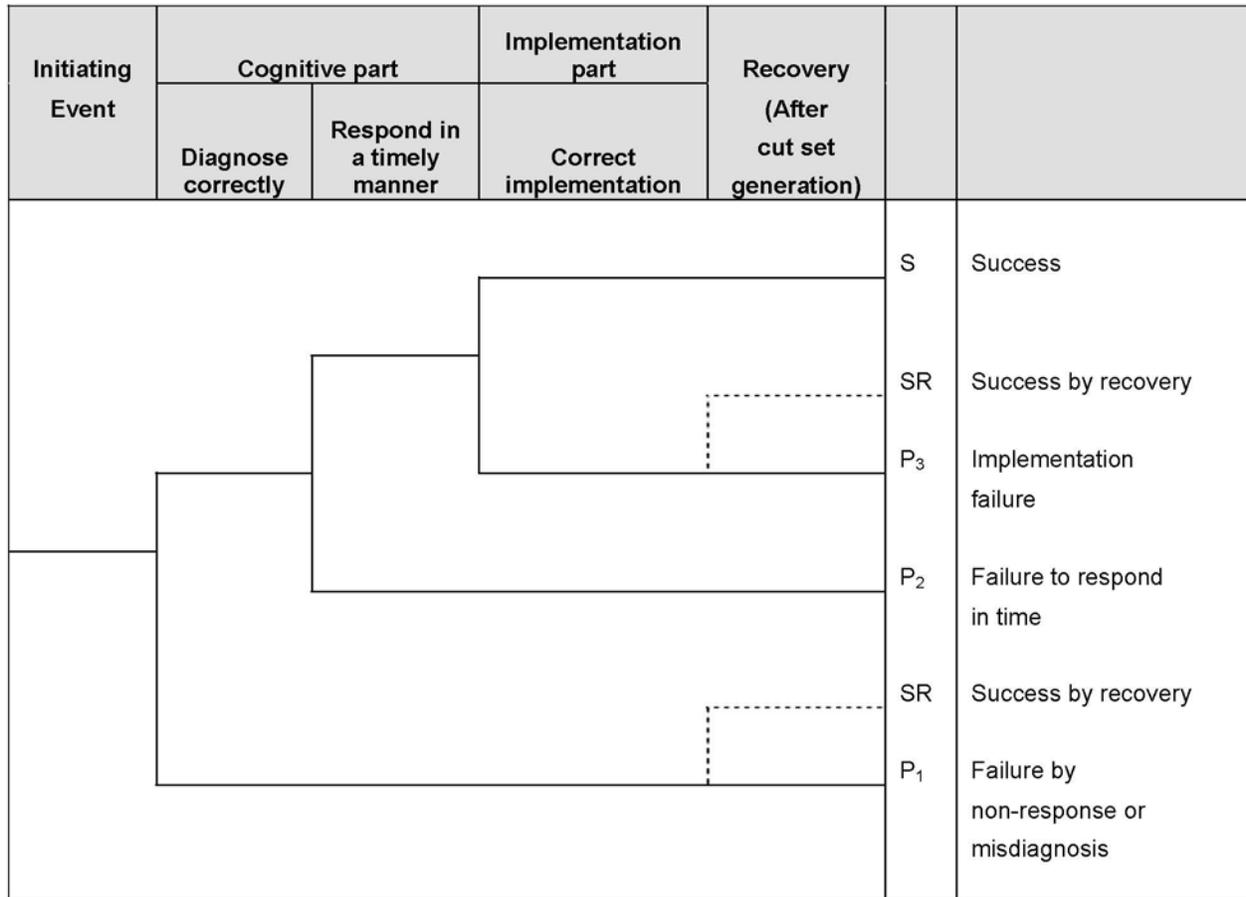


NOTE: HFE = human failure event.

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. E8.1.14) that serves as inputs to the quantification process. The HFE/context descriptions in Table E.III-1 touch briefly on the information that is relevant to the screening-level quantification of the HFE. Since the baseline scenario generally touches on much of this information, the point of including the HFE/context descriptions is to summarize the information that pertains to the specific HFE to minimize the need for the analysts to refer back to the baseline scenario, except to obtain additional detail.

Table E.III-1. Examples of Information Useful to HFE Quantification

Information Type	Examples
Facility, conditions, and behavior for possible deviations of the scenarios	Reasonably possible unusual plant behavior and failures of systems; equipment, and indications, especially those that may be unexpected or difficult to detect by operators. Includes presence of interlocks that would have to fail to promote the deviation.
Operating crew characteristics (i.e., crew characterization)	Crew structure, communication style, emphasis on crew discussion of the “big picture.”
Features of procedures	Structure, how implemented by operating crews, opportunities for “big picture” assessment and monitoring of critical safety functions, emphasis on relevant issue, priorities, any potential mismatches with deviation scenarios.
Relevant informal rules	Experience, training, practice, ways of doing things—especially those that may conflict with informal rules or otherwise lead operators to take inappropriate actions.
Timing	Plant behavior and requirements for operator intervention versus expected timing of operator response in performing procedure steps, etc.

Table E.III-1. Examples of Information Useful to HFE Quantification (Continued)

Information Type	Examples
Relevant vulnerabilities	Any potential mismatches between the scenarios and expected operator performance with respect to timing, formal and informal rules, biases from operator experience, and training, etc.
Error mechanisms	Any that may be particularly relevant by plant context or implied by vulnerabilities; applicable mechanisms depend upon whether HFE is a slip or mistake. Examples include: failures of attention, possible tunnel vision, conflicts in priorities, biases, missing or misleading indications, complex situations, lack of technical knowledge, timing mismatches and delays, workload, and human-machine interface concerns.
Performance-shaping factors	Those deemed associated with, or triggered by, the relevant plant conditions and error mechanisms.

NOTE: HFE = human failure event.

Source: Original

In Step 1, interpreting and prioritizing all information with respect to relevance, credibility, and significance is especially important if:

- Some information is applicable only to certain scenarios, HFEs, or contexts
- There are conflicts among information sources
- Information is ambiguous, confusing, or incomplete
- Information must be extrapolated, interpolated, etc.

Completion of the “lead-in” initial conditions is primarily performed by a single individual, using the results of the YMP HAZOP evaluation process and reviews of other relevant information sources. Discussions are also held with the Operations Department to augment that information, and the resulting write-ups are reviewed by the PCSA facility leads and the HRA team. The initial conditions are refined as part of an open discussion among the experts (in this case, the HRA team for the study) involved in the expert opinion elicitation process. The goal of this discussion is not to achieve a consensus but, rather, to advance the understanding of all the experts through the sharing of distributed knowledge and expertise. In each case, the scenario (or group of similar scenarios) and the HFE in question are described and the vulnerabilities and strong points associated with taking the right action are discussed openly among the HRA team.

**Step 2—Identify the Key or Driving Factors of the Scenario Context.**

The purpose of Step 2 is to identify the key or driving factors on operator behavior/performance for each HFE and associated context. Each expert participating in the elicitation process individually identifies these factors based on the expert’s own judgment. Usually, these factors are not formally documented until Step 4.

Typically, there are multiple factors deemed most important to assessing the probability for the HFE in question. This is due to the focus of the ATHEANA search process on combinations of factors that are more likely to result in an integrated context (Ref. E8.1.14). 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 nonoptimal 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 these values

<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.

<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.

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:

- 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. E8.1.11; Ref. E8.1.8; Ref. E8.1.16; Ref. E8.1.13). As discussed in Section E3.2 the following four were chosen:

- ATHEANA expert judgment (Ref. E8.1.14)
- CREAM (Ref. E8.1.12)
- HEART (Ref. E8.1.19)/NARA (Ref. E8.1.7)
- THERP (Ref. E8.1.18).

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. E8.1.2) to the extent that those requirements, which were written for application to NPP PRA, apply to the types of operations conducted at the YMP. Certainly, all of the high level HRA quantification requirements were considered to be applicable. Further, all of the supporting requirements to these high level requirements were considered applicable, at least in regards to their intent. In some cases, the specifics of the supporting requirements are only applicable to NPP HRA and some judgment is needed on how to apply them. This was particularly true of those supporting requirements that judged certain specific quantification methods acceptable. This appendix lays out the specific case for the methods selected for use at the YMP (or, more to the point, the exclusion of certain methods that would normally be considered acceptable under the standard, but are deemed inappropriate for use for the YMP PCSA).

**Differences between NPP and the YMP Relevant to HRA Quantification**—There are a number of contrasts between the operations at the YMP and the operations at an NPP that affect the selection of approaches to performing detailed HRA quantification (Table E.IV-1).

Table E.IV-1. Comparison between NPP and YMP Operations

NPP	YMP
Central control of operations maintained in control room.	Decentralized (local), hands on control for most operations.
Most important human actions are in response to accidents.	Most important human actions are initiating events.
Postaccident response is important and occurs in minutes to hours. Short time response important to model in HRA.	Postaccident response evolves more slowly (hours to days). Short time response not important to model.

Table E.IV-1. Comparison between NPP and YMP Operations (Continued)

NPP	YMP
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. E8.1.18).
- 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 semiautomated (e.g., crane operation, trolley operation, canister transfer machine 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. E8.1.8), examples of time-response methods include: HCR (Ref. E8.1.8) and TRCs (Ref. E8.1.10).
  - 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. E8.1.19; Ref. E8.1.20)/NARA (Ref. E8.1.7), CREAM (Ref. E8.1.12), and ATHEANA expert judgment (Ref. E8.1.14).
  - 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. E8.1.19)/NARA (Ref. E8.1.7) and CREAM (Ref. E8.1.12) 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. E8.1.19)/NARA (Ref. E8.1.7) approach and others that would best fit the CREAM (Ref. E8.1.12) 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. E8.1.7) specifically endorses the THERP (Ref. E8.1.18) approach and so this is used. However, other gaps exist. For these cases, the ATHEANA (Ref. E8.1.14) 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. E8.1.2) 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.

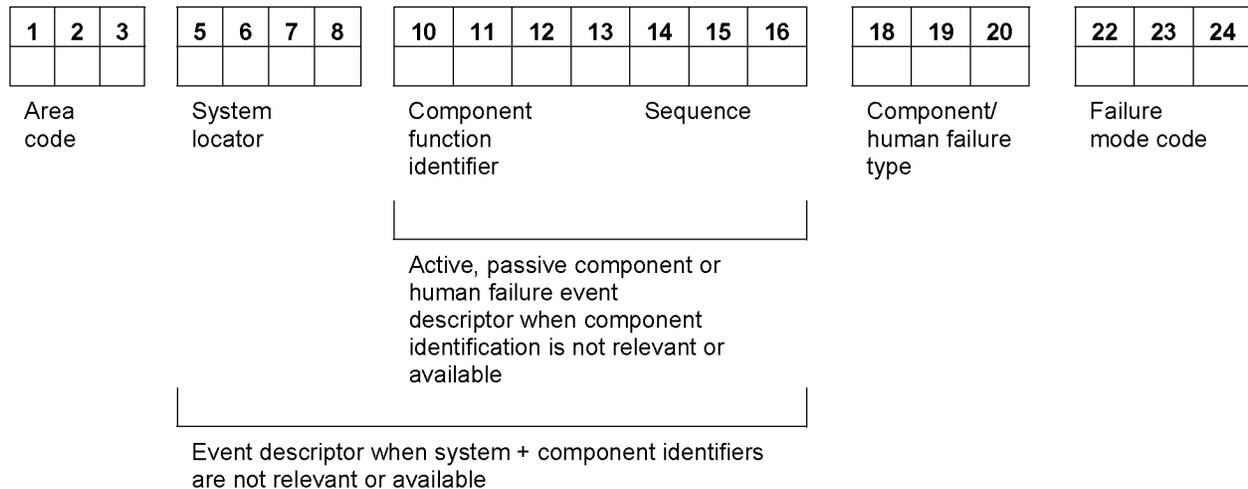
4. Simplified methods:

- 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. E8.1.17), SPAR-H (Ref. E8.1.9).
- 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 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. E8.1.4). 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 Wet Handling Facility is 050, the Receipt Facility is 200, the Initial Handling Facility is 51A, and Subsurface is 800. Intra-Site Operations could fall under one of several repository area codes and therefore the most appropriate code to use was the repository general area code. However, this code was insufficient for the purposes of this analysis, and a designator of ISO was substituted instead. For the majority of cases, the area coding of HFEs in Attachment E reflects the location of the operations being evaluated, such as ISO for Intra-Site Operations. However, for certain HFEs, the coding corresponds to the location of the systems impacted by the human failure, such as HVAC, which is specific to the CRCF and therefore retains the 060 coding, and AC power, which retains the 26x and 27x coding. For these specific instances, such coding provides better traceability of the HFE back to the affected equipment.

The system locator code identifies operational systems and processes. System locator codes (four characters) are listed in Table 1 of *Repository System Codes* (Ref. E8.1.5). 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. E8.1.3). These are generally three or four characters long. Some Bechtel SAIC Company, LLC, component function identifiers for typical components are shown in Table E.V-1, but in cases where there is not an equivalent match, the most appropriate PCSA type code should be used (also given in Table E.V-1).

The sequence code is a numeric sequence and train assignment (suffix), if appropriate, that uniquely identifies components within the same area, system, and component function.

If an HFE is related to the failure of an individual component with an existing component function identifier and sequence code, the naming scheme should utilize these codes in the event name. If an HFE is such that these codes do not apply, the basic event name can be a free form field for describing the nature of the event, such as HCSKSCF for operator topples cask during scaffold movement or HFCANLIDAJAR for operator leaves canister lid ajar, utilizing either seven characters when there is a relevant system locator code, or 12 characters when no system codes are applicable.

The human failure type and failure mode codes are three characters each, consistent with the coding provided in Table E.V-1.

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

Table E.V-1. Human Failure Event Type Codes and Failure Mode Codes (Continued)

	Operation is performed only very infrequently (once per month or less)	COM
Operation is extremely complex AND conducted under environmental or ergonomic stress	Operation is performed on a daily basis.	CSD
	Operation is performed on a very regular basis (on the order of once per week)	CSW
	Operation is performed only very infrequently (once per month or less)	CSM
<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>
F1 INTRODUCTION .....	F-4
F2 REFERENCES .....	F-4
F3 BOUNDARY CONDITIONS .....	F-5
F3.1 INTRODUCTION .....	F-5
F4 ANALYSIS METHOD.....	F-7
F4.1 INTRODUCTION .....	F-7
F4.2 IDENTIFICATION OF OUTSIDE FIRE INITIATING EVENTS.....	F-7
F4.3 QUANTIFICATION OF FIRE IGNITION FREQUENCY .....	F-8
F5 ANALYSIS.....	F-12
F5.1 INTRODUCTION .....	F-12
F5.2 INITIATING EVENT FREQUENCIES.....	F-12
F5.3 RESULTS .....	F-14

**TABLES**

	<b>Page</b>
F4.2-1. Outside Fire Area Categories.....	F-8
F4.3-1. Types of Facilities: Cross Reference Between NFPA and NAICS .....	F-10
F4.3-2. Fraction of Fires and Fire Frequency for Outside Areas of a Facility .....	F-11
F5.3-1. Onsite Transport Fire Initiating Event Frequency and Associated Distribution.....	F-14

## ATTACHMENT F SUBSURFACE FIRE ANALYSIS

### F1 INTRODUCTION

This attachment describes the work scope, definitions and terms, method, and results for the fire analysis performed as a part of the Yucca Mountain Project (YMP) preclosure safety analysis (PCSA). Fire analysis is divided into four major areas:

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

#### 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 (\*) fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

- F2.1 \*ASME (American Society of Mechanical Engineers) RA-S-2002. *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, New York: American Society of Mechanical Engineers. TIC: 255508. ISBN: 0-7918-2745-3.
- F2.2 \*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.

- F2.3 \*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.
- F2.4 \*EPRI and NRC (Nuclear Regulatory Commission) 2005. *Detailed Methodology*. Volume 2 of *EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities*. EPRI TR-1011989 and NUREG/CR-6850. Palo Alto, California: Electric Power Research Institute. ACC: MOL.20070323.0062.
- F2.5 \*ANSI/ANS (American National Standards Institute/ American Nuclear Society)-58.23-2007. 2007. *Fire PRA Methodology*. La Grange Park, Illinois: American Nuclear Society. TIC: 259894.
- F2.6 BSC (Bechtel SAIC Company) 2008. *Subsurface Operations Event Sequence Development Analysis*. 000-PSA-MGR0-00400-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080214.0004.
- F2.7 \*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.
- F2.8 \*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
- F2.9 \*Nevada State Fire Marshal 2007. *2006 Annual Fire Statistics Report, National Fire Incident Reporting System (NFIRS)*. Carson City, Nevada: Nevada Department of Public Safety. ACC: MOL.20070718.0052.
- F2.10 \*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.
- F2.11 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.

### **F3 BOUNDARY CONDITIONS**

#### **F3.1 INTRODUCTION**

The general boundary conditions used during the analysis of fire vulnerabilities and fire model development are clearly stated and documented. In general, the general boundary conditions are compatible with those ones usually applied to fire events. The principal boundary conditions for the fire analysis are listed in the following sections.

### **F3.1.1 Plant Operational State**

The initial state of the facility is normal, with each system operating within its limiting condition of operation (LCO) limits.

### **F3.1.2 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 re-ignition once a fire is extinguished, are not considered.

### **F3.1.3 Relationship to Process Buildings**

Subsurface fires 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. The number of main process buildings at YMP is six (IHF, RF, WHF and three CRCFs).

### **F3.1.4 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.

### **F3.1.5 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 will cause 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.

### **F3.1.6 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.

### **F3.1.7 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.

### **F3.1.8 Internal Events PCSA Model**

To implement the systems analysis guidance contained herein, the fire preclosure safety analysis (PCSA) team uses the internal events PCSA model, which is developed concurrently with the fire PCSA. This internal events PCSA is used as the basis for the fire PCSA. The internal events PCSA is in general conformance with the ASME PRA *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications* (Ref. F2.1).

## **F4 ANALYSIS METHOD**

### **F4.1 INTRODUCTION**

The general methodological basis of this analysis is the *Chemical Agent Disposal Facility Fire Hazard Assessment Methodology*, (Ref. F2.2). 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 have similar issues and needs. This is a “data based” approach because it utilizes actual historical experience of 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, *EPR/NRC-RES Fire PRA Methodology for Nuclear Power Facilities* (Ref. F2.3 and F2.4) is also considered in the development of this analysis method. The method complies with the applicable requirements of the ANS fire PRA standard (Ref. F2.5) that are relevant to a non-reactor facility. Many of the definitions, modeling approximations, and requirements of these documents were used to develop this document.

### **F4.2 IDENTIFICATION OF 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 this potential. The initiating events for Subsurface Operations were identified in *Subsurface Operations Event Sequence Development Analysis* (Ref. F2.6). The steps of the fire analysis are provided in the following sections.

#### **F4.2.1 Identify Areas On-Site Where Waste Forms Can Be Present**

The processes for the movement of waste forms on site, while outside of buildings, are evaluated and the areas where the waste forms 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 NFPA Historical Database for Outside Fires**

The National Fire Protection Association (NFPA) historical database (F2.8) identifies the areas outside buildings where fires have occurred. These have been grouped into broader categories for use in this study. These groupings are shown 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.

Source: Original

### F4.2.3 Define Initiating Events

Fire ignition occurrences are identified for each outside area where a waste form 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 (USCB), which conducts an economic census (Ref. F2.7). The second piece of data is tracked by NFPA. This approach uses historical data over a 10-year period (1988 to 1997) 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*<sup>1</sup> (Ref. F2.8). These data are used to develop estimates for the total frequency of fires and the distribution of fires on the grounds of the facility.

The primary source of data on the number of fires is the National Fire Incident Reporting System (NFIRS) (Ref. F2.9), which is jointly administered by the Federal Emergency Management Agency (FEMA) and NFPA. NFIRS provides annual computerized databases of fire incidents. The NFIRS is a voluntary program wherein individual fire departments complete data forms and

<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.

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 the NFIRS results develops NFPA's national fire estimates. To project the NFIRS results, at least an estimate of the NFIRS fires as a fraction of the total is needed. However, the NFIRS data do not provide any information on the total population from which the data are 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 are maintained by the USCB, which conducts an economic census (Ref. F2.7). It performs a count of all businesses in the United States and categorizes them in accordance with the North American Industry Classification System (NAICS). 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. F2.8) and NAICS (Ref. F2.7) clearly leads to the classifications shown in the table.

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

Source: Ref. F2.8 (NFPA/FEMA) and Ref. F2.7 (NAICS)

Two different calculations are performed on two different subpopulations 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. F2.10), there are approximately 287 outside fires involving property of value annually (2870 total fires in the ten year period) in such facilities. (Ref. F2.10) is an e-mail that was sent from the author of (Ref. F2.8) (M. Ahrens) to one of the originators 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. F2.8).

According to NAICS, the total number of facilities of this type is 29,303. Therefore, the frequency of potentially significant fires in these facilities is:

$$F = \frac{287 \text{ fires/yr}}{(29,303 \text{ facilities})} = 9.8 \times 10^{-3} \text{ fires/facility-yr} \quad (\text{Eq. F4.3-1})$$

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, 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, the total number of facilities in the corresponding subcategories is 5,870. Therefore, the frequency of potentially significant fires in these facilities is:

$$F = \frac{62 \text{ fires/yr}}{(5,870 \text{ facilities})} = 1.1 \times 10^{-2} \text{ fires/facility-yr} \quad (\text{Eq. F4.3-2})$$

Thus, the two estimates of the outside fire frequency are virtually the same. Overall, the use of a total mean outside fire frequency of  $1 \times 10^{-2}$  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. F2.8), 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 below.

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-yr
Storage areas – to include all areas where products are held while awaiting process, shipment, or use	125	0.20	$2.0 \times 10^{-3}$
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	$9.2 \times 10^{-4}$
Trash/rubbish areas	84	0.135	$1.4 \times 10^{-3}$
Areas containing equipment – to include all areas outside the building that contain operating process, HVAC, maintenance, or other machinery and equipment	121	0.195	$2.0 \times 10^{-3}$
Open areas – to include fields, roads, and right of ways	84	0.135	$1.4 \times 10^{-3}$
Vehicles	16	0.025	$2.5 \times 10^{-4}$
Other – primarily applies to exterior structural areas of buildings	136	0.22	$2.2 \times 10^{-3}$

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).

Source: Ref. F2.8, 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 YMP constitutes a facility, and that the subsurface 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). Subsurface Operations will not be considered a separate facility, but rather a support area for the process buildings (i.e., it is an integral part of a typical facility in that it takes the “product” from the process). In addition, the other support buildings will also not be considered facilities for the purpose of determining the overall frequency of subsurface fires, for a similar reason. Therefore, the overall frequency of subsurface 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. 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 Subsurface 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 was one initiating event identified for subsurface:

- Fire Threatens a Waste Form During On-Site Transport (TEV)

The selection of these events is documented in *Subsurface Operations Event Sequence Development Analysis* (Ref. F2.6). This section addresses the quantification of these events.

#### **F5.2.1 Fire Threatens a Waste Form in During Transport (TEV)**

This represents fires that ignite on/in the transportation vehicles while moving waste forms around the site. The transportation vehicles include the TEV, site transporter, truck trailer, and SPM. While it could be argued that a vehicle fire can occur at any time, it is more likely that it will occur while the vehicle is in use. For that reason, the fire frequency per year will be 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 form and when not) per year. This will allow initiating event frequencies over the preclosure period to be determined for each vehicle and waste form to be quantified by multiplying by the total number of operations for each vehicle and waste form when the waste form is present.

The outside area that is relevant to this event, from Table F4.3-2, is “vehicles.” That is, the waste form is vulnerable to a vehicle fire during transport. The total frequency per facility-year

of such fires is, from the same table,  $2.5 \times 10^{-4}$  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.

$$\begin{aligned}\text{Site Vehicle Fire Frequency/year} &= 2.5 \times 10^{-4} \text{ fires/facility-year} \times 6 \text{ facilities} \\ &= 1.5 \times 10^{-3} \text{ fires/year}\end{aligned}$$

This is then converted to the total expected number of vehicle fires over the 50-year preclosure period.

$$\begin{aligned}\text{Site Vehicle Fire Frequency (preclosure period)} &= 1.5 \times 10^{-3} \text{ fires/year} \times 50 \text{ years} \\ &= 7.5 \times 10^{-2} \text{ fires}\end{aligned}$$

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. However, as the facility is not yet fully designed there is no estimate available for the number of such vehicle movements that will occur on site. The only thing that is known with any level of confidence is the number of waste form movements (since this is integral to the throughput of the site). Therefore, the potential for fires in other types of vehicles will be ignored, which will add a level of conservatism to the results.

The PCSA throughput analysis (Ref. F2.11) estimates that there are *approximately* 40,000 waste form movements outside of the process buildings during the preclosure period. This includes operations of the site transporter, truck trailer, SPM, and TEV.<sup>2</sup> For each waste form movement, there will be another movement of the vehicle when a waste form 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:

$$\begin{aligned}\text{Fire Threatens a Waste Form during Onsite Transport} &= 7.5 \times 10^{-2} \text{ fires} / 80,000 \text{ operations} \\ &= 9 \times 10^{-7} \text{ fires/operation}^3\end{aligned}$$

### F5.2.2 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.

---

<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 subsurface operations. When assembling the risk model for subsurface, the resultant rate is used as the initiating event frequency and is multiplied only by the number of subsurface 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.

The accuracy of the databases is also unclear. The NFPA data on fires is based on voluntary 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 as regards physical locations, but not clear as regards multiple operations at one location. The approach used in this analysis to consider each of the six process 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 frequency and its associated distribution (Table F5.3-1). The initiating event frequency represents the probability that a fire will threaten the stated waste form during onsite transport over the length of the pre-closure period.

Table F5.3-1. Onsite Transport Fire Initiating Event Frequency and Associated Distribution

Initiating Event	Mean frequency (per 50 years)	Error Factor	Distribution
Fire Threatens a Waste Form During Onsite Transport	$9 \times 10^{-7}$ fires/operation	15	lognormal

Source: Original

**ATTACHMENT G**  
**EVENT SEQUENCE QUANTIFICATION SUMMARY TABLES**

## **ATTACHMENT G**

### **EVENT SEQUENCE QUANTIFICATION SUMMARY TABLE**

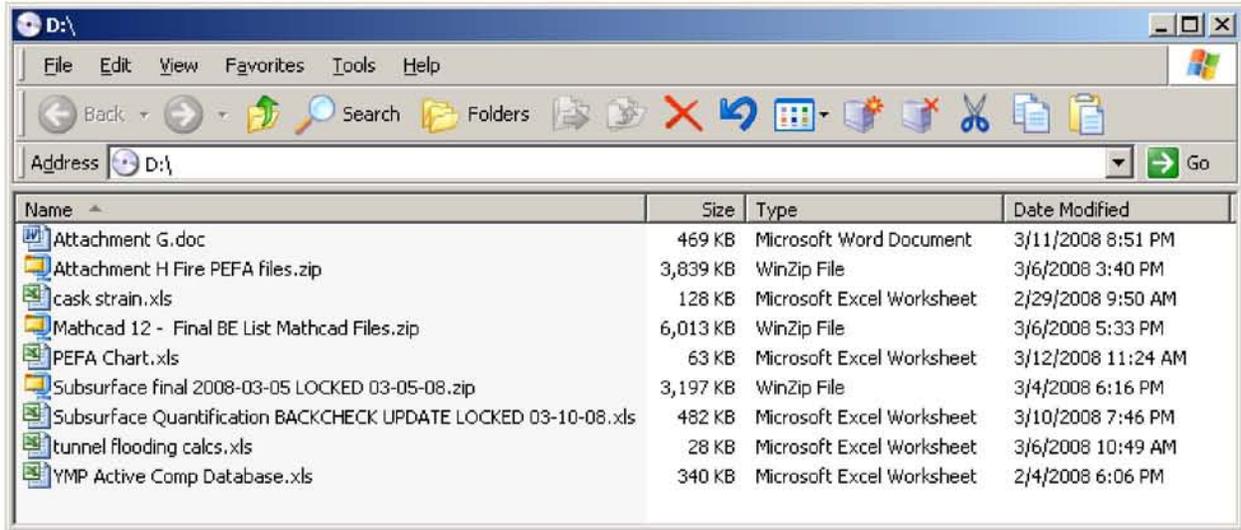
Attachment G contains the event sequence quantification summary table (Table G-1) referenced by Section 6.7. It also contains Table G-2, *Final Event Sequence Summary*; Table G-3, *Beyond Category 2 Final Event Sequence Summary*; and Table G-4, *Important to Criticality Final Event Sequence Summary* that are referenced in Section 6.8. Cells in these tables with 0.00E+00 indicate that the value is <E-12.

The Excel spreadsheet that was used to quantify the Subsurface Operations event sequences that are referenced in Section 6.8 is included in the CD in Attachment H and is titled *Attachment G.xls*.

**ATTACHMENT H**  
**SAPPHIRE MODEL AND SUPPORTING FILES**

## ATTACHMENT H SAPHIRE MODEL AND SUPPORTING FILES

This attachment is the CD containing the SAPHIRE model and supporting files. The electronic files contained on the CD are identified below.



Name	Size	Type	Date Modified
Attachment G.doc	469 KB	Microsoft Word Document	3/11/2008 8:51 PM
Attachment H Fire PEFA Files.zip	3,839 KB	WinZip File	3/6/2008 3:40 PM
cask strain.xls	128 KB	Microsoft Excel Worksheet	2/29/2008 9:50 AM
Mathcad 12 - Final BE List Mathcad Files.zip	6,013 KB	WinZip File	3/6/2008 5:33 PM
PEFA Chart.xls	63 KB	Microsoft Excel Worksheet	3/12/2008 11:24 AM
Subsurface final 2008-03-05 LOCKED 03-05-08.zip	3,197 KB	WinZip File	3/4/2008 6:16 PM
Subsurface Quantification BACKCHECK UPDATE LOCKED 03-10-08.xls	482 KB	Microsoft Excel Worksheet	3/10/2008 7:46 PM
tunnel flooding calcs.xls	28 KB	Microsoft Excel Worksheet	3/6/2008 10:49 AM
YMP Active Comp Database.xls	340 KB	Microsoft Excel Worksheet	2/4/2008 6:06 PM

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 3/12/08	3. Accession Number ATT. TO: ENG.20080312.0034
4. Author Name(s) PHUOC LE	5. Authorization Organization BSC/PCSA
6. Title/Description SUBSURFACE OPERATIONS RELIABILITY AND EVENT SEQUENCE CATEGORIZATION ANALYSIS (ATTACHMENT H)	
7. Document Number(s) 000-PSA-MGR0-00500-000	8. Version Designator 00A
9. Document Type DATA	10. Medium 2 CD'S
11. Access Control Code PUB	
12. Traceability Designator 000-PSA-MGR0-00500-000-00A	
13. Comments 1 ORIGINAL 1 COPY  VALIDATION OF COMPLETE FILE TRANSFER. ALL FILES COPIED. SOFTWARE USED SAPHIRE, MS EXCEL, MSWORD, AND WINZIP.	

14. RPC Electronic Media Verification
<p><b>XREF</b>      MOL.20080312.0015</p> <p>MAR 14 2008      <i>T Church / BSC</i></p> <p><b>MD5 Validation</b></p> <p style="text-align: right;"><b>THIS IS AN ELECTRONIC ATTACHMENT</b></p>

dir.txt

Volume in drive D is 080312\_1506  
Volume Serial Number is 79E0-62F9

Directory of D:\

03/11/2008	08:51 PM	480,256	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
03/06/2008	05:33 PM	6,157,289	Mathcad 12 - Final BE List Mathcad Files.zip
03/12/2008	11:24 AM	64,512	PEFA Chart.xls
03/04/2008	06:16 PM	3,273,033	Subsurface final 2008-03-05 LOCKED
03-05-08.zip			
03/10/2008	07:46 PM	493,056	Subsurface Quantification BACKCHECK UPDATE
LOCKED 03-10-08.xls			
03/06/2008	10:49 AM	28,672	tunnel flooding calcs.xls
02/04/2008	06:06 PM	347,648	YMP Active Comp Database.xls
	9 File(s)	14,905,258	bytes

Total Files Listed:  
9 File(s)  
0 Dir(s)

14,905,258 bytes  
0 bytes free