ENG.20090112.0009

BSC

Design Calculation or Analysis Cover Sheet

Complete only applicable items.

1. QA: ~~QA~~ QA
2. Page 1

3. System	4. Document Identifier
Monitored Geologic Repository – Subsurface Operations	000-PSA-MGR0-00500-000-00B

5. Title
Subsurface Operations Reliability and Event Sequence Categorization Analysis

6. Group
Preclosure Safety Analyses

7. Document Status Designation
☐ Preliminary ☒ Committed ☐ Confirmed ☐ Cancelled ☐ Superseded

8. Notes/Comments
This revision addresses the condition reports (CRs) noted in the table on pp. 2 and 3. The table describes substantive changes and indicates the affected portions of the document for each CR action. In addition, editorial changes (including updating headers and footers) have been made throughout and affect every page. Changes have been made in response to CR numbers 12103, 12025, 11966, 11989, 12002, 12024, 12105, 12177, 12230, 12245, and 12310.

Attachments		Total Number of Pages
Attachment A.	Event Trees	34
Attachment B.	System/Pivotal Event Analysis – Fault Trees	326
Attachment C.	Active Component Reliability Data Analysis	~~56~~ 58
Attachment D.	Passive Equipment Failure Analysis	96
Attachment E.	Human Reliability Analysis	68
Attachment F.	Fire Analysis	20
Attachment G.	Event Sequence Quantification Summary Tables	22
Attachment H.	SAPHIRE Model and Supporting Files	4 + 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/See Page 2	See Page 3	Mike Frank	Mark Wisenburg
00B	The purpose of this revision is to respond to the condition reports noted in Block 8 and in the table on pages 2 and 3. Editorial corrections have also been made. This revision does not update the analysis to design changes that may have occurred since Rev. 00A was approved.	838	H-4	R. J. Garrett [signature] 11/24/08	Laura Plumb [signature] 11/24/08	Sen Sung Tsai for Michael Frank [signature] for M. Frank 11/26/08	Michael Frank [signature] 1/7/09

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.

Substantial changes have been made to the following Sections, Tables, and Figures:

CR-Action	Location of Change	Description of Change
12025-003	Section B2	Resolve inconsistencies between fault trees for the CRCF HVAC system and the repository design.
11966-006	Section 6.3.1.1, Table C1.1-1, Section C1.3, Table C4-1	Removed references to jib cranes from the main body and Attachment C
11989-006	Section 1	Rewrite 'intentional malevolent acts' text
12002-006	Table 6.3-1, Section C1.3, Table C4-1	Incorporated the latest drop rate data for the cask handling crane, 3.16E-5 drops per lift.
12024-007	Sections B3.4.1.4, B3.4.2.4	Added discussion of transmission of electrical energy using conduits, bus ducts, conductor bars, etc.
12103-011	Table 6.3-1, Attachment B, and selected basic events in the SAPHIRE model. Tables B1.4-5, B1.4-6, B1.4-7, B1.4-8, B1.4-9, B1.4-13, B1.4-14 through B1.4-20, B2.4-1, B3.4-1, B3.4-5, B4.4-1, B4.4-2, B5.4-1, B5.4-2, B6.4-1, B6.4-2, B7-2, Figures B1.4-5, B1.4-7, B1.4-8, B1.4-13 through B1.4-18, B1.4-23, B1.4-25, B1.4-27, B1.4-37, B1.4-38, B1.4-40, B1.4-40, B4.4-1, B4.4-2, B5.4-1, B6.4-1, B6.4-2	Resolved inconsistencies found between Table 6.3-1, Attachment B, other tables and figures in Attachment B, and the SAPHIRE model.
12105-014	Tables 6.3-1, 6.3-4, 6.3-7, 6.3-8, 6.3-9, C4-1, and numerous other tables throughout. These tables include Tables 6.0-3, 6.7-1, 6.8-3, 6.9-1, B1.3-1, B1.4-6, B1.4-8, B1.4-12, B1.4-14, B1.4-16, B1.4-18, B1.4-20, B2.4-3, B3.4-4, B3.4-8, B4.4-2, B5.4-2, B6.4-2, D1.1-1, D2.1-4 through D2.1-7, D2.1-9, and D3.4-1.	Eliminated blank cells in tables by hiding inappropriate cell divisions, inserting indicators such as “N/A” or “—“ to indicate that there is no information to display, added a table note to indicate blank cells were intentional, or inserted information into the cell.

Substantial changes have been made to the following Sections, Tables, and Figures: (Continued)

CR-Action	Location of Change	Description of Change
12245-006	Table 6.3-1; Section C3, Tables B1.4-5, B1.4-7, B1.4-13, B1.4-15, B1.4-17, B2.4-1, B3.4-1, B3.4-7, B4.4-1, B5.4-1 Figures B1.4-5, B1.4-7, B1.4-8, B1.4-13 through B1.4-18, B1.4-23, B1.4-25, B1.4-27, B1.4-37, B1.4-38, B1.4-40, B1.4-42, B3.4-1 through B3.4-9, B3.4-13 through B3.4-15, B3.4-17 through B3.4-22, B3.4-25 through B3.4-28, B4.4-1 through B4.4-3, B5.4-1, B5.4-3	Create more robust common cause failure (CCF) probability distributions; update the CCF results accordingly.
12310-005	Section 6, Tables 6.3-1 and 6.7-1. Attachment B; in particular: Tables B1.4-5 through B1.4-9, B1.4-13 through B1.4-19; Figures B1.4-5, B1.4-7 and B1.4-8, B1.4-13 through B1.4-18, B1.4-23, B1.4-25, B1.4-27, B1.4-37, B1.4-38, B1.4-40, B1.4-42; Section B2.2; Tables B2.2-1 through B2.2-3; Section B2.3; Table B2.3-1 Section B2.4; Tables B2.4-1 through B2.4-3; Figures B2.4-1 through B2.4-23; Section B3.4.14; Tables B3.4-1, B3.4-4, B3.4-5, B3.4-7, B3.4-8; Figures B3.4-1, B3.4-3 through B3.4-5, B3.4-8, B3.4-9, B3.4-13 through B3.4-15, B3.4-17 through B3.4-22, B3.4-25 through B3.4-28; Tables B4.4-1, B4.4-2; Figures B4.4-1 through B4.4-3; Tables B5.4-1, B5.4-2; Figures B5.4-1, B5.4-3; Figures B6.4-1, B6.4-2; Table B7-2 Attachment C: Table C1.1-1; Section C1.3; Section C3 Attachment G: Tables G-1 through G-3	Updated the SAPHIRE model and results to ensure that the latest results are captured in the documentation.
12230-001	Table 6.9-2, Section 6.9-2	Resolve discrepancies between Table 6.9-2 and Table 1 of *Preclosure Procedural Safety Controls*.
12177-005	Sections 2.2.90 and 6.2.2.8.1.	Reference for Inter Office Memorandum that provides estimate of quantities of wet piping in the nuclear facility buildings. These values are used in the internal flooding analyses.

INTENTIONALLY LEFT BLANK

CONTENTS

INTENTIONALLY LEFT BLANK

FIGURES

Page

INTENTIONALLY LEFT BLANK

TABLES

Page

INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

Acronyms

BSC	Bechtel SAIC Company, LLC
CCF	common-cause failure
CCCF	Central Control Center Facility
CRCF	Canister Receipt and Closure Facility
CTM	canister transfer machine
CTT	cask transfer trolley
DOE	U.S. Department of Energy
DPC	dual-purpose canister
EDGF	Emergency Diesel Generator Facility
EFC	error-forcing context
EOC	errors of commission
EOO	errors of omission
ESD	event sequence diagram
FEA	finite element analysis
FEM	finite element modeling
FTA	fault tree analysis
GROA	geologic repository operations area
HAZOP	hazard and operability
HEPA	high-efficiency particulate air
HFE	human failure event
HLW	high-level radioactive waste
HRA	human reliability analysis
HVAC	heating, ventilation, and air conditioning
IET	initiator event tree
IHF	Initial Handling Facility
ITC	important to criticality
ITS	important to safety
LLNL	Lawrence Livermore National Laboratory
LOSP	loss of offsite power
LOS	loss of shielding
LS-DYNA	Livermore Software–Dynamic Finite Element Program
MCC	motor control centers
MCO	multicanister overpack
MLD	master logic diagram

ACRONYMS AND ABBREVIATIONS (Continued)

NAICS	North American Industry Classification System
NARA	Nuclear Action Reliability Assessment
NFPA	National Fire Protection Association
NRC	U.S. Nuclear Regulatory Commission
NUREG	Nuclear Regulation (U.S. Nuclear Regulatory Commission)
PCSA	preclosure safety analysis
PEFA	passive equipment failure analysis
PFD	process flow diagram
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSC	procedural safety controls
PSF	performance-shaping factor
RF	Receipt Facility
SFTM	spent fuel transfer machine
SLS	steel/lead/steel
SNF	spent nuclear fuel
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
WHF	Wet Handling Facility
WPTT	waste package transfer trolley
YMP	Yucca Mountain Project

Abbreviations

AC	alternating current
°C	degrees Celsius
cfm	cubic feet per minute
cm	centimeter
DC	direct current
ft	foot, feet
gpm	gallons per minute
Hg	mercury

ACRONYMS AND ABBREVIATIONS (Continued)

hp	horsepower
hr, hrs	hour, hours
J	joule
K	Kelvin
km	kilometer
kV	kilovolt
lb	pound
m	meter
min	minute, minutes
MPa	megapascal
Mrem	millirem
mph	miles per hour
sec	second
Torr	a unit of pressure equal to 0.001316 atmosphere
V	volt
W	watt
yr, yrs	year, years

INTENTIONALLY LEFT BLANK

1. PURPOSE

This document and its companion document titled *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) constitute a portion of the preclosure safety analysis (PCSA) that is described 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 the waste handling activities and facilities of the geologic repository operations area (GROA) from the beginning of operations to the end of the preclosure period. *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 event sequence categorization per the definition provided by 10 CFR 63.2 (Ref. 2.3.2).

The PCSA uses probabilistic risk assessment (PRA) technology derived from both nuclear power plant and aerospace methods and applications in order to perform analyses to comply with the risk informed aspects of 10 CFR 63.111 and 63.112 (Ref. 2.3.2) and to be responsive to the acceptance criteria articulated in the *Yucca Mountain Review Plan, Final Report*. NUREG-1804 (Ref. 2.2.71). The PCSA, however, limits the use of PRA technology to the 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, onsite, and offsite members of the public, and criticality.

The radiological consequence assessment relies on bounding inputs with deterministic methods to obtain bounding dose estimates. These dose estimates were developed using broad categories of scenarios that might cause a radiological release or direct exposure to workers and onsite and offsite members of the public. 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 have been categorized as Category 1 or Category 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, event 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 categorized as Category 1 or Category 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 operation, 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. These parameters include waste form characteristics, reflection, interaction, neutron absorbers (fixed and soluble), geometry, and moderation. The criticality sensitivity calculations determine the sensitivity of the effective neutron multiplication factor (k_{eff}) to variations in any of these parameters as a function of the other parameters. The PCSA criticality analyses determined the parameters that should be included in this event sequence analysis. 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 considered in the event sequence analysis for similar reasons include the presence of 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 the presence (or absence) of sufficient soluble boron in the pool in the Wet Handling Facility (WHF).

The initiating events considered in the PCSA define what event could potentially 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 (defined as those hazards presented by the operation of the facility and by its associated processes that can potentially lead to a radioactive release or cause a radioactive hazard) occurring during waste handling operations conducted within the GROA and external events (events that involve natural phenomena and external man-made hazards; e.g., seismic, wind energy, aircraft crash, 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 offsite conditions that are excluded from consideration 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; offsite tornado or missile strikes on a transportation cask, and nonconformances introduced during cask or canister manufacturing that result in a reduction of containment strength. Such potential precursors are subject to deterministic regulations that include 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, were considered in a separate safeguards and security analysis performed by others.

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 Category 2 event sequence for purposes of dose calculations
- Identified important to safety (ITS) SSCs
- Required nuclear safety design bases for those ITS SSCs
- Required procedural safety controls (PSCs).

Other PCSA documents that will use the results from *Subsurface Operations Event Sequence Development Analysis* (Ref. 2.2.40) and this analysis as input include:

- *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. 14. *Calculations and Analyses.* Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20081114.0008.

2.1.2 EG-PRO-3DP-G04B-00046, Rev. 13. *Engineering Drawings.* Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG. 20081114.0009.

2.1.3 IT-PRO-0011, REV 10. *Software Management.* Las Vegas, Nevada: Bechtel SAIC Company. ACC: DOC.20080923.0003.

2.1.4 LS-PRO-0201, REV 7. *Preclosure Safety Analysis Process.* Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20081119.0007.

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 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), paragraph 3.2.2.F) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of this document. There are no superseded or cancelled documents associated with the modifications that led to the issuance of this revision. Cancelled or superseded documents associated with the portions of this document for which the snapshot has not yet been updated are designated herein with a dagger (†).

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

The inputs in this Section that are noted with an asterisk (*) indicate that they fall into one of the categories in Section 4.1 that describe the suitability of each input for its 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.* TP 14367E. Ontario, Canada: Transportation Development Centre of Transport Canada. ACC: MOL.20071113.0095.

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

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

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

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

2.2.7 ASME 2004. *2004 ASME Boiler and Pressure Vessel Code.* 2004 Edition. New York, New York: American Society of Mechanical Engineers. TIC: 256479. 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 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).* 000-M0C-MWL0-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071101.0013.

2.2.24 †BSC 2007. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle.* 000-30R-HE00-00200-000 REV 002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0006.

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 Not used.

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, Nevada: 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, 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 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. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 205084.

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

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

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

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

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

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

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

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

2.2.75 Regulatory Guide 1.174, Rev. 1. 2002. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing*

Basis. Washington, D.C.: U. S. Nuclear Regulatory Commission.
ACC: MOL.20080215.0049.

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

2.2.77 SAPHIRE V. 7.26. 2007. VMware/WINDOWS XP. STN: 10325-7.26-01.

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. Two volumes. Washington, D.C.: U.S. Nuclear Regulatory Commission.
ACC: MOL.20001010.0217.

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

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

2.2.86 *U.S. Census Bureau 2000. "Manufacturing United States." *1997 Economic Census: Summary Statistics for the United States.* Washington, D.C.: U.S. Census Bureau.

Accessed March 7, 2008. 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." *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.

2.2.90 *Tooker, D. W. 2007. "Estimated Quantities of Wet Piping in the Nuclear Facility Buildings (CRCF, RF, WHF, and IHF)." Interoffice Memorandum from D. W. Tooker (BSC) to Distribution, November 29, 2007, 1129072284. ACC: CCU.20071130.0012.

2.3 DESIGN CONSTRAINTS

2.3.1 10 CFR 50. 2007. Energy: Domestic Licensing of Production and Utilization Facilities. U.S. Nuclear Regulatory Commission.

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

2.3.3 10 CFR 71. 2007. Energy: Packaging and Transportation of Radioactive Material. U.S. Nuclear Regulatory Commission. ACC: MOL.20070829.0114.

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

2.4 DESIGN OUTPUTS

2.4.1 BSC 2008. *ITS SSC/Non-ITS SSC Interactions Analysis*. 000-PSA-MGR0-02300-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080312.0035.

2.4.2 BSC 2008. *Preclosure Nuclear Safety Design Bases*. 000-30R-MGR0-03500-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080312.0036.

2.4.3 BSC 2008. *Preclosure Procedural Safety Controls.* 000-30R-MGR0-03600-000-001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080313.0002.

2.4.4 BSC 2008. *Seismic Event Sequence Quantification and Categorization*. 000-PSA-MGR0-01100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080311.0032.

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 the reliability of the equipment and SSCs 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 sources of equipment reliability data 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 those represented in the sources of equipment reliability data. In some cases, system-level information from the industry-wide information sources, such as crane load-drop rates, 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 of reliability data takes advantage of many observations (as opposed to fewer), which yields more precise statistical information regarding the uncertainty associated with the resulting reliability estimates.

INTENTIONALLY LEFT BLANK

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 analytical methods 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 YMP that was produced by outside organizations. These inputs are suitable for their intended uses because they provide information that was developed for the YMP 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). 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 that 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 is classified as Level 2 software, as defined in *Software Management* (Ref. 2.1.3). 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 *Globally Registered Controlled Software for Level 2 Usage*. 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 *Globally Registered Controlled Software for Level 2 Usage Report*. Crystal Ball version 7.3.1 (a commercial off-the-shelf, Excel-based risk-analysis tool) is listed on the *Globally Registered Controlled Software for Level 2 Usage 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.

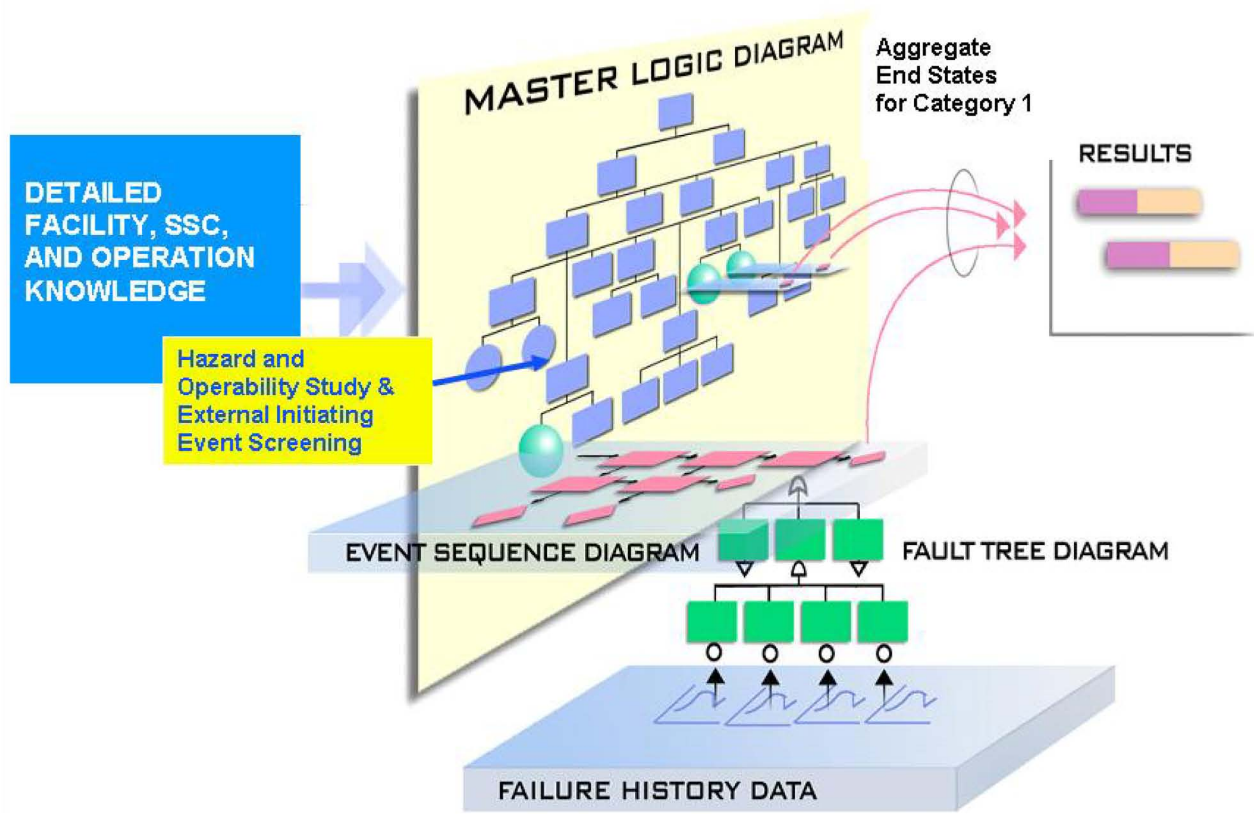
- WinZip 9.0, a file compression utility for Windows, is listed in the current *Globally Registered Controlled Software for Level 2 Usage Report*. WinZip 9.0 is used in this analysis to compress files for presentation on compact disc in Attachment H.

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 subsurface 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 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 effort 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 the SSCs within the facility can fail. An important additional set of information is called *success criteria*.

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 to the environment through a filtered path. The release is filtered when it is confined and filtered through the successful operation of the heating, ventilation, and air conditioning (HVAC) system over its mission time. This end state excludes moderator intrusion.

5. Radionuclide Release, Unfiltered: Indicates a release of radioactive material from its confinement through the pool (of the WHF only) or to the environment through an unfiltered path. 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 Part 63 (Ref. 2.3.2). Radiation doses to individuals from direct exposure and radionuclide release are addressed in a companion consequence analysis by modeling the effects of bounding event sequences related to the various waste forms and the facilities that handle them.

The radiological consequence analysis develops a set of bounding consequences. Each bounding consequence represents a group of like event sequences. The group (or bin) is based on such factors as characteristics of the waste form involved, availability of HEPA filtration, location of occurrence (in water or air), and characteristics of the surrounding material (such as transportation cask or a 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, presence of 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 a detailed discussion of the treatment of criticality in event sequences.

The third question, "How likely is it?" is answered by the estimation of event sequence frequencies. The PCSA uses ***failure history*** records (for example, *Nonelectronic Parts Reliability Data* (Ref. 2.2.45) and NUREG/CR-4639, *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR): Data Manual, Part 4: Summary Aggregations* (Ref. 2.2.55)), structural reliability analysis, thermal stress analysis, and engineering and scientific knowledge about the design as the basis for estimation of probabilities and frequencies. These sources, coupled with the techniques of probability and statistics (e.g., *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.

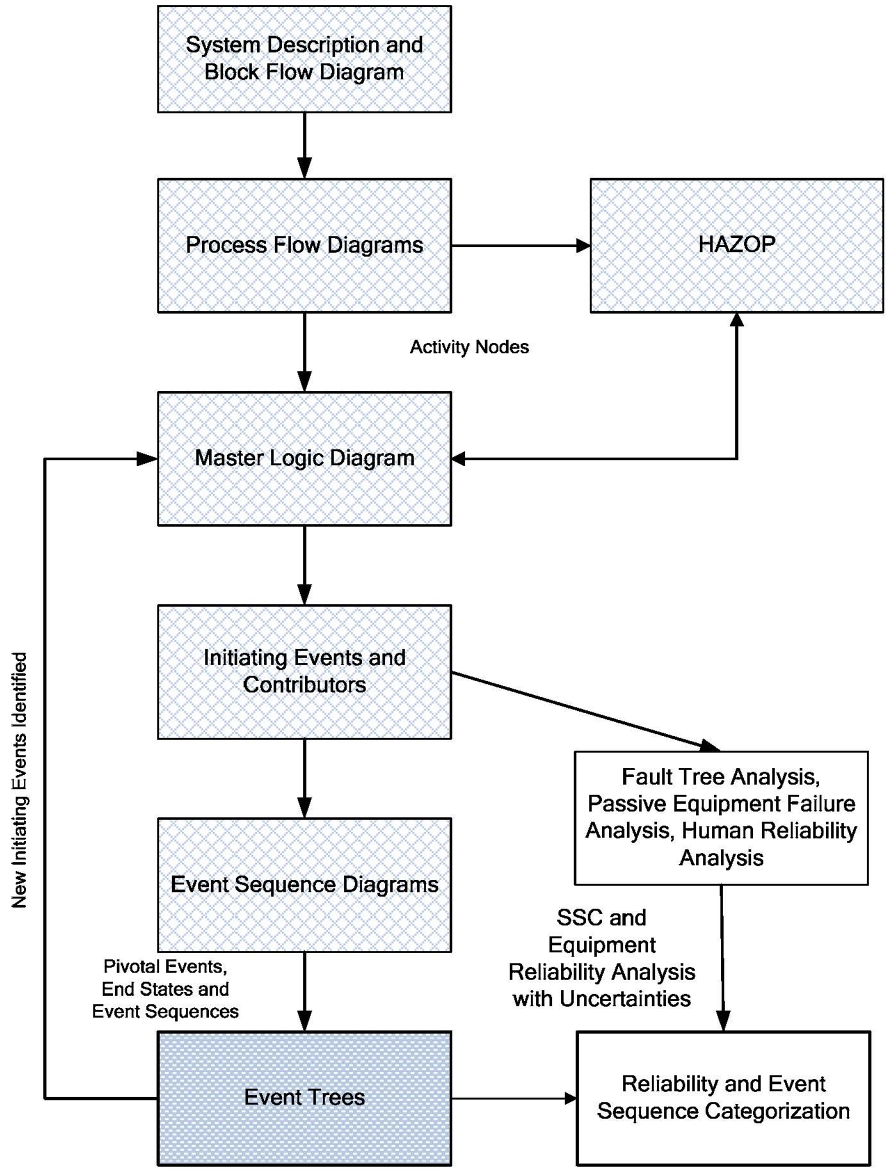
The activities required to accomplish these objectives are illustrated in Figure 4.3-2 and described below.

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). The interface between the event sequence development analysis and the event sequence 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 event sequence categorization analysis. The unshaded boxes represent the analysis performed in this study; the methodology used in this analysis is described in Section 4.

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).



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

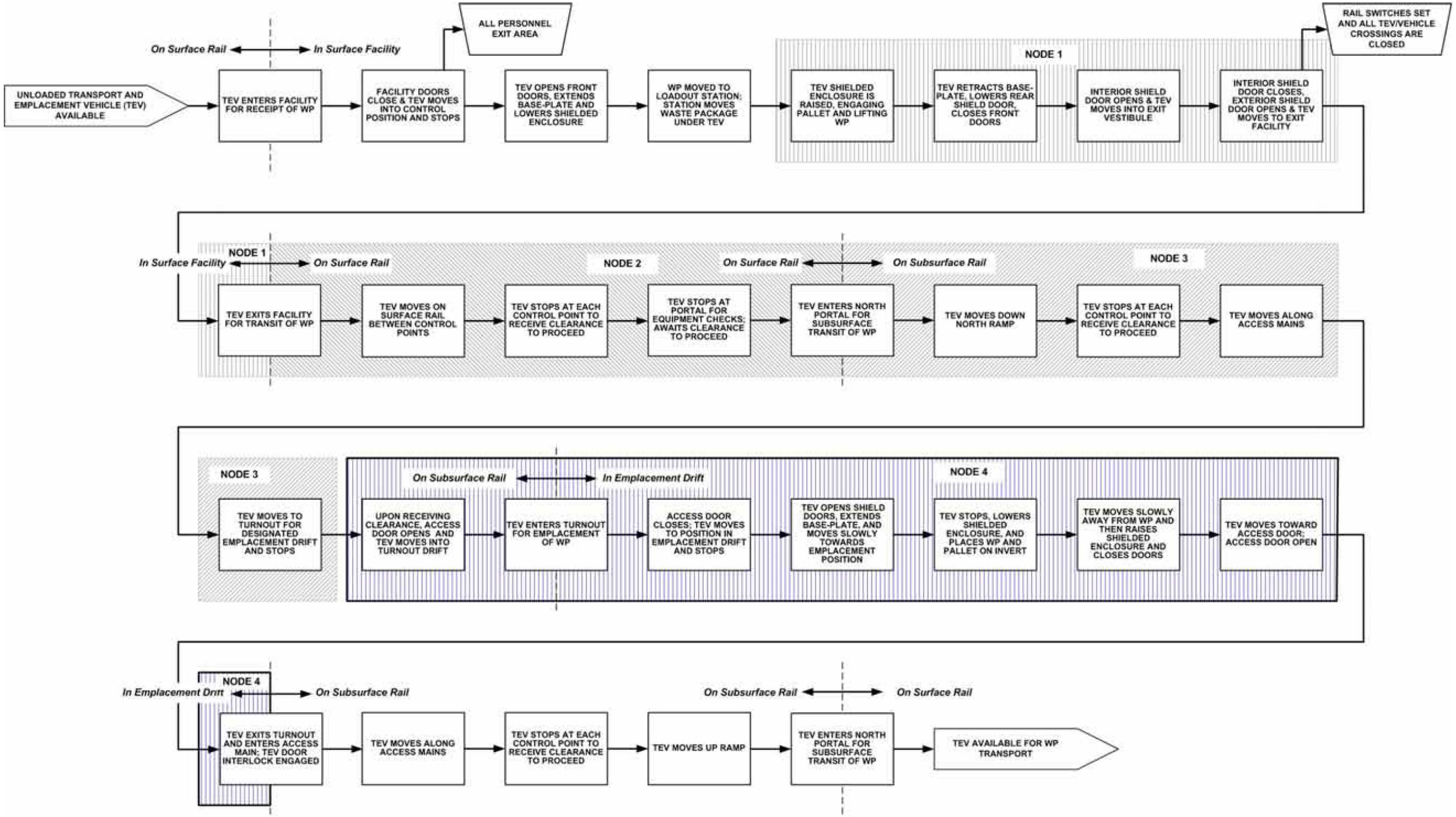
Source: Modified from Ref. 2.2.40, Figure 2

Figure 4.3-2. Preclosure Safety Assessment Process

The 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. Examples include 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).

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., presence of HVAC/high-efficiency particulate air (HEPA) filtration) become pivotal events in the ESD.

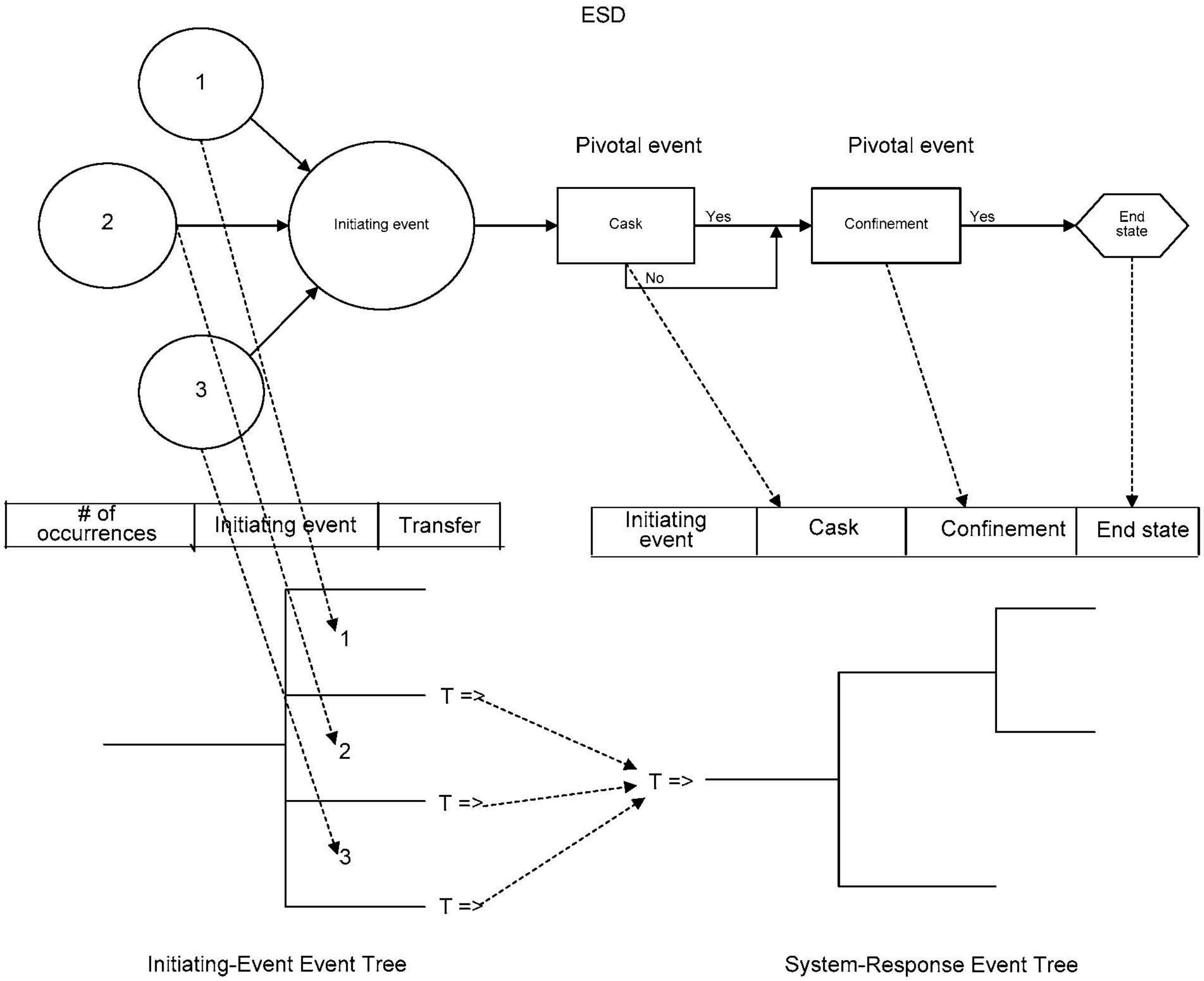


NOTE: CTT = cask transfer trolley; CTM = canister transfer machine; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Excerpt from Ref. 2.2.40

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

INTENTIONALLY LEFT BLANK



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 small circles (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 small circle, but all of the initiating events included in the small circle 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 small circles may be aggregated further into large circles as depicted in Figure 4.3-4. The large circle 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 small circle. All initiating events represented by the large circle 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 small circle.

4.3.1 Event Tree Analysis and Categorization

The relationship of the YMP ESDs to their equivalent event trees is also illustrated in Figure 4.3-4. 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 nor 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 small circle, one horizontal line per small circle. This configuration is called the initiator event tree (IET). The second event tree contains the pivotal events and end states. This configuration 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 IETs and SRETs is quantified for each waste container type (e.g., dual-purpose canisters (DPCs), transportation, aging, and transport, aging, and disposal (TAD) canisters, and 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 large circle 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 large circle. If an event sequence has only one small circle, 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 an example to illustrate how the quantification is performed 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). Although this example includes an event sequence applicable to intra-site operations, the methodology is also applicable to subsurface operations.

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 probability 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 that 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 (again, for intra-site operations) is provided in Figure 4.3-5).

TADs	Event Tree / Sequence No.													
	ISO-ESD02-TAD	No. of AOs	No. of moves (each)	IE mean	IE median	IE std dev	TRANSCASK	CANISTER	SHIELDING	MODERATOR	Calc'd Mean	Calc'd Median	Calc'd StdDev	End State
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. circ1	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 A(	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. circ2	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	Initial Categ.
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**	*Cat2*
RR-UNFILT	**ISO02-TAD-SEQ3-RRU**	**8.2E-07**	**3.3E-07**	**1.6E-07**	*BC2*
RR-UNFILT	**ISO02-TAD-SEQ4-RUC**	**0.0E+00**	**0.0E+00**	**0.0E+00**	*BC2*

Source: Original

Note: The blank cells in this table are intentional and have been verified.

Figure 4.3-5. Example Excel Spreadsheet

The example 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. The drop is followed by the breach of the canister without potential for moderator entry into the canister.

The event sequence (that leads to an unfiltered radionuclide release that is not important to criticality) 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:

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

where

X and Y are independent variates

μ_X is the mean value for one distribution

μ_Y is the mean value for a second distribution

The standard deviation, σ, is calculated as the square root of the sum of the squares, based on the following property for combining variance, σ^2, of two distributions in Equation 2.

$$\sigma^2_{X+Y} = \sigma^2_X + \sigma^2_Y \qquad \text{(Eq. 2)}$$

where

X and Y are independent variates

σ^2_X is the variance for one distribution

σ^2_Y is the variance for the second distribution

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

$$\sqrt{\sigma^2_{X+Y}} = \sqrt{\sigma^2_X + \sigma^2_Y} \qquad \text{(Eq. 3)}$$

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:

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

where

μ is the mean for the lognormal distribution (i.e., μ_{X+Y} for the summed distributions)

σ^2 is the variance for the lognormal distribution (i.e., σ^2_{X+Y} 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	Initial Categ.
OK	ISO02-TAD-SEQ1-OK	8.1E+01	3.3E+01	1.6E+01	
DE-SHIELD-LOSS	ISO02-TAD-SEQ2-DEL	8.1E-04	3.3E-04	1.6E-04	Cat2
RR-UNFILTERED	ISO02-TAD-SEQ3-RRU	8.2E-07	3.3E-07	1.6E-07	BC2
RR-UNFILTERED-ITC	ISO02-TAD-SEQ4-RUC	0.0E+00	0.0E+00	0.0E+00	BC2

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 the term "expected number of occurrences" when discussing event sequence quantification. This process 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) 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. However, the components that comprise the piece of equipment usually will have common uses such that 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 (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 concept.

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.