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 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 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 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 is 3.2E-02; the initiating frequency of a loss of offsite power lasting more than 24 hours would be:

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

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 have a frequency that is categorized as beyond Category 2. Therefore, a worker dose assessment is not needed to comply with 10 CFR 63.111 (Ref. 2.3.2). No further work is required for this initiating event. This drift access control program is included 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 includes 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 10 CFR 63.111(Ref. 2.3.2). No further work is done on this initiating event. This proximity control program is included in Table 6.9-2.
No applicable event trees	Loss of ventilation to the drift	According to *Waste Package Misplacement Probability* (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, *Waste Package Misplacement Probability* (Ref. 2.2.41) concludes that the probability of misplaced waste packages causing temperature elevation is categorized as 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 presented 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 runway 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 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 as (1.42E-9/trip * 12,268 trips) = 1.7E-5 during the preclosure period. The event sequence frequency is categorized as Beyond Category 2, and thus is screened from further analysis.

NOTE: Initiator event trees (including branch numbers) 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

Per 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 floodwater, whether caused by random failures or earthquakes, emerge from two sources. Floodwater can be produced from an inadvertent actuation of the fire-suppression system. Floodwater can also be produced as a result of a 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 a 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 as a result of exposure to water. Canisters are surrounded by transportation casks and waste packages. Transportation casks are elevated at least five feet above the floor at all times by a railcar, truck, or a cask transfer trolley (CTT). Waste packages are similarly elevated on the WPTT. The waste package is elevated approximately 1 foot above the floor inside the TEV. 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 high-level radioactive waste (HLW) and SNF are contained in canisters within a sealed waste package at all times during subsurface operations and these containers do not fail from short-term exposure to floodwater. In this context, short-term is a period that is at least 30 days but is less than the period 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 are 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 is taken out in the muck and the rest collects 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 in., 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 in. 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 $h - d \times \sin(1.35°)$ (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 θ (in radians) = $2 \cos^{-1} \{[r - (h - d \sin(1.35°)] / r\}$. 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)	θ/2 (radians)	Segment Area (ft^2)	Segment Volume (ft^3)
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^3, 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 passive equipment failure analysis (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 RF accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.

2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program for placement in waste packages destined for emplacement in the repository emplacement drifts. 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 IHF accepts canisters from the Naval Nuclear Propulsion Program and some canisters containing high-level radioactive waste (HLW) 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 6.1-1 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 6.1-1. 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 FTA for initiating and pivotal events, including an example fault tree. Many of the initiating events involve faults in complex machinery for which no historical data exists at the system level. However, historical data for the derailment of railed vehicles is available. 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 ("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 waste package loadout activities involving the TEV and movement of the loaded TEV 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 the results are used as input to 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 waste package loadout and emplacement operations conducted over the preclosure period. The following sections provide 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 either the CRCF or the IHF and then travels directly into the emplacement drift to emplace the waste package. The TEV is powered by a third rail electrical power system 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, the TEV operates under PLC control with only general oversight from the Central Control Center Facility (CCCF); however, manual control is performed as needed. The TEV instrumentation 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 major subsystems of the TEV include the following:

- **TEV Control Compartment** – The TEV electronic controls are housed in an exterior compartment at the rear 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 an 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; however, it prevents direct radiation streaming and restricts an

external, shielded dose rate not to exceed 100 mrem/hr at 30 cm (11.81 in). The non-metallic neutron shielding material 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 (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 base plate is mechanically interlocked with the TEV front shield doors to prevent extension of the base plate if the shield doors are closed. The base plate cannot 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 electro-mechanical 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 for easy and precise movement of the heavy doors. These doors 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. The TEV incorporates an electro-mechanical interlock to prevent the inadvertent opening of the shield doors during transit. This interlock prevents the actuation of the doors unless the TEV is in the Waste Package Loadout Room or in an emplacement drift.

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

6.2.2.1.2 Operations

The three phases of TEV operations are loadout, transit, and emplacement. These operational phases are addressed in the PCSA. Other TEV operations (such as operations involving an empty TEV) 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 the loaded TEV out of the facility. The TEV is controlled by an on-board PLC system and monitored from the CCCF. Waste packages are loaded into the TEV in either the IHF or one of the CRCFs. The loadout configuration and operations are the same for all facilities.

A TEV enters a facility and moves forward to position the vehicle directly over the loadout station prior to the movement of a filled, sealed waste package into the loadout area via a WPTT. The facility exterior shield doors are closed and the TEV is positioned such that its lifting

features can engage the waste package pallet after the pallet and waste package are correctly positioned following extraction from the WPTT.

After receiving confirmation on positioning from the CCCF, the TEV 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 sealed, filled 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 the CCCF. 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 the CCCF for all transit operations and the CCCF operator has override control to stop the TEV in case of an emergency.

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

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 to establish a positional datum point. The emplacement access door panels are opened for the period required to admit the TEV into the drift. An electro-mechanical switch de-activates the interlock to enable the opening of the TEV shield doors. The TEV passes into a curved tunnel segment (with a positive grade of approximately 1.75%) and then passes into the emplacement drift. This drift has a nominal grade of 0 %. The TEV movement ceases and the location of the TEV is confirmed. 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 move the TEV forward at a crawl speed (approximately 4.6 m/min (15 ft/min.)). The TEV travel ceases at a position close to a previously emplaced waste package (as applicable).

Additional on-board positional sensors and devices (e.g., lights, cameras, and ultrasonic sensors) are then activated and measurements are made to re-confirm to the position of the TEV and the waste package. The TEV moves forward at a slow positioning speed (approximately 0.46 m/min (1.5 ft/min.)) until the required final position is achieved. The shield enclosure is lowered to position the waste package and pallet on the emplacement drift invert. The TEV is backed away from the emplaced waste package and pallet at the positioning speed to a predetermined distance. Here 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 the CCCF (in most cases)
- Manual control when required via override from the CCCF
- 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 the CCCF
- 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 1.5 ft/min.

6.2.2.1.4 System/Pivotal Event Success Criteria

Success criteria for the TEV include the following:

- Prevent impact to a waste package due to spurious movement of TEV or impact to the waste package by the TEV front shield doors
- Prevent collisions involving the TEV within the facility
- Prevent collisions involving the TEV during transit or when entering an emplacement drift by preventing spurious operation of the TEV and the drift access doors
- Prevent the spurious opening of the TEV front shield doors
- Prevent the dropping of a waste package due to TEV spurious operations or TEV structural failure
- Prevent the dropping or dragging of a waste package in an emplacement drift due to TEV spurious operations or TEV structural failure
- TEV structure sustains impacts without damage to the waste package
- TEV shielding sustains 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 the 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 emplacement operations 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 during transit between facility doors
- 1 hr for spurious operation of TEV motors while a waste package is being positioned in the emplacement drift
- 8 hr for transit from the surface facility to the emplacement drift; used for potential exposure times for a stopped TEV.

6.2.2.1.6 Fault Tree Results

The application of the TEV fault trees to ESDs for subsurface operations is documented in Attachment B, Section B1; included is 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 operations:

1. TEV door impacts a waste package
2. TEV collision within facility
3. TEV collides with object during emplacement
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	3.5E-3
Impact to TEV during transit	2.9E-4	6.4E-4
TEV stops for extended time	6.9E-4	6.1E-5
Inadvertent TEV door opening during transit	1.2E-7	1.2E-6
Waste package drop in facility	1.3E-6	2.6E-6
Waste package dropped during transit	1.1E-7	9.9E-8
Waste package drop or dragging in an emplacement drift	1.3E-6	2.5E-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 system 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 % efficiency), two high efficiency filters for particulate removal in air (99.97 % efficiency), and a mister/demister for maintaining proper humidity levels.

3. One exhaust fan with a rated capacity of 40,500 cfm and an exhaust fan motor rated at 200 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 event 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 4.5E-02
- The standard deviation is 1.0E-01.

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 138 kV 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 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 480 V 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 13.8 kV ITS switchgears to the CRCF passes through a 13.8 kV to 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 onsite 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 Facility (EDGF). Each is sized to provide sufficient 13.8 kV power to support all ITS loads in six facilities (i.e., three CRCFs, the WHF, RF, and the EDGF).

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 13.8 kV 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 LOSP, both ITS diesel generators will 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 13.8 kV switchgear in each division automatically opens. Both ITS diesel generators start automatically and are connected to the 13.8 kV 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 ITS diesel generators continue to supply AC power until normal power is restored.

Environmental systems are provided to maintain the temperature in the various EDGF 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 13.8 kV ITS switchgear. The 13.8 kV 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 13.8 kV 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 3.1E-02
- The standard deviation is 7.7E-02.

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

6.2.2.4 Drip Shield Emplacement Gantry Analysis

Drip shields will be placed over the waste packages within the emplacement drifts prior to closure of the Subsurface Facility. The drip shields are designed 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 interlocks with a previously emplaced drip shield segment. 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 text summarizes the design, operations, success criteria, and results of the fault tree quantification.

6.2.2.4.1 Physical Description

The drip shield emplacement gantry is a remotely-operated vehicle that transports drip shields from the Heavy Equipment Maintenance Facility into emplacement drifts. Similar to the TEV, the drip shield emplacement gantry is a rail-based vehicle which is powered by a third rail electrical power system. The gantry contains PLCs for localized control of the device. Operation of the gantry is under PLC control in most cases, with only general oversight from the CCCF. However, operations under remote manual control are performed as needed.

6.2.2.4.2 Operations

The drip shield emplacement gantry 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 gantry travels into the emplacement drift to a predetermined position, ceases travel, and re-confirms its location. The gantry 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, thereby lowering the drip shield. The drip shield engages the previously emplaced drip shield interlock (if present) and is lowered to rest upon the steel frame of the emplacement drift invert. The emplacement gantry then lowers its lifting features to their 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 the CCCF (in most cases)
- Manual control when required via override from the CCCF
- Automatic operational sequences to emplace the drip shield
- Automatic stop at each rail segment to await a permissive signal from the CCCF to proceed
- Fail-safe on loss of power: the gantry stops, retains its load, and enters a locked mode until operator action is taken
- Sensors and logic to confirm the position of the gantry 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 1.5 ft/min.).

6.2.2.4.4 Success Criteria

One scenario and fault tree is associated with the drip shield emplacement gantry: drop of a drip shield onto a waste package.

Success criteria for the drip shield emplacement gantry during the drip shield emplacement process require that the gantry subsystems operate without failure or spurious operations. The gantry lift system maintains 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) during the emplacement operations.

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 a drop of the drip shield in which 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 2.8E-8
- The standard deviation is 2.5E-8.

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

6.2.2.5 Shield Door System Analysis

The shield door system FTA is detailed in Attachment B, Section B5. The following text summarizes 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 to workers during canister unloading and loading operations.

The shield doors consist of a pair of large heavy doors that close together. The shield doors utilize motor over-torque sensors to prevent the shield doors from causing damage to casks or waste packages in the event of closure of the doors 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 scenario associated with subsurface operations: shield doors close on a conveyance (i.e., the TEV).

6.2.2.5.3 Control System

The shield door system is a manually operated system.

6.2.2.5.4 Success Criteria

The shield door system has one credible failure scenario associated with subsurface operations: shield doors close on a conveyance (i.e., the 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 event 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 are:

- The mean system probability of failure value is 2.0E-03
- The standard deviation is 2.5E-03.

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

6.2.2.6 Emplacement Drift Access Door Analysis

The emplacement drift access door FTA is detailed in Attachment B, Section B6. The following text summarizes the design, operations, success criteria, and results of the fault tree quantification.

6.2.2.6.1 Physical Description

The emplacement drift 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 designed to provide radiation shielding.

6.2.2.6.2 Operation

The emplacement drift access door is typically closed to maintain security and maintain positive control of the emplacement drift. Normal door operation requires CCCF input to prevent inadvertent access to the high radiation areas. However, a manual override switch is provided within a locked access box to locally open the door. The emplacement access door is remotely opened by the operator in the CCCF when a TEV is ready to proceed into an emplacement drift. The operator in the CCCF then closes the door upon visual confirmation that the TEV has passed through the threshold and has completely entered the turnout drift. The process is reversed when the TEV is to exit the emplacement drift.

6.2.2.6.3 Control System

This door system is either remotely controlled by operators in the CCCF or locally through use of the manual override switch in the locked access box.

6.2.2.6.4 Success Criteria

One scenario and fault tree is associated with the emplacement drift access door: the emplacement access door closes on the TEV.

The success criterion for this scenario stipulates that the emplacement access door operates without failure or spurious operation and that the operator does not close the door prematurely. The emplacement access door system is not to close onto the TEV during the waste package emplacement normal operations. 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 during 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 involving 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 due to mechanical failure. The system value and standard deviation are:

- 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 carrying a loaded, sealed waste package or an unenclosed waste package 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

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 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)

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
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
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: CRCF = Canister Receipt and Closure Facility; TEV = transport and emplacement vehicle; HVAC = heating, ventilation, and air conditioning; WP = waste package.

Source: Original

6.2.2.8 Potential Moderator Sources

6.2.2.8.1 Internal Floods

The addition of moderator into a canister is a pivotal event associated with 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.

A canister is surrounded by at least one other barrier to water intrusion during most of its handling at the repository. These barriers include 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 fire protection 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, lasting from the

occurrence of the canister breach to the time that definitive action can be taken to prevent the introduction of water into the canister, is considered to be reasonable. This duration is the same as the period that is used to assess the dose for a radiological release. The spurious actuation frequency over a 30-day mission time following a canister 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 the 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^2 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 (room 1015) is 7,470 ft^2 (Ref. 2.2.23, Table 10). At a spacing of 130 ft^2/sprinkler, 58 sprinklers are estimated to be present. The failure of any sprinkler in the room is then estimated to be 58 × 1.6E-6/yr × 1/8,760 hrs/yr, or 1.1E-8/hr.

The frequency of a spurious opening of a pre-action valve is estimated using the solenoid valve spurious open data found in Section 6.3 of 8.1E-07/hr. This value is reasonable because a solenoid valve must open to relieve the air pressure from the diaphragm that keeps the valve closed.

The value of the first cut set is (1.6E-6/yr × 1/8,760 hr/yr × 720 hr) × (8.1E-7/hr × 720 hr) = 8E-11/sprinkler head. The second cut set is more significant: 0.025 (human error screening value) × (1.6E-6/yr × 1/8,760 hr/yr × 720 hr) = 3E-9/sprinkler head.

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

Table 6.2-3 Probability of Spurious Sprinkler Actuation

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

NOTE: [a] CRCF area based on room numbers 1005E, 1016-1026, 2004,2007, 2007A, and 2007B
IHF area based on room numbers 1001-1003, 1006-1008, 1011,1012, 1026 and 2004
RF area based on room numbers 1013, 1015, 1016, 1017, 1017A, and 2007
WHF area based on room numbers 1007-1010, 1016, 2004, 2006, and 2008.
CRCF = Canister Receipt and Closure Facility, 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 the waste handling areas of the CRCF and WHF are less than 100 feet per facility ("Estimated Quantities of Wet Piping in the Nuclear Facility Buildings (CRCF, RF, WHF, and IHF)" (Ref. 2.2.90)). The probability of a pipe crack in a 30-day period was estimated using the pipe leak data from NUREG/CR-6928, *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants* (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 $hr^{-1}ft^{-1}$

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

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

CRCF = 2.8E-10 $hr^{-1}ft^{-1}$ × 100 ft × 720 hr = 2.0E-05

IHF < 2.8E-10 $hr^{-1}ft^{-1}$ × 6800 ft × 720 hr = 1.4E-03

WHF = 2.8E-10 $hr^{-1}ft^{-1}$ × 75 ft × 720 hr = 1.5E-05

RF = 2.8E-10 $hr^{-1}ft^{-1}$ × 0 ft × 720 hr = 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.

This analysis is applicable to the event sequences that do not involve fires as an initiating event. Fire suppression would actuate in the locations sufficiently heated by a fire during fire initiating event sequences. The fire initiating event analysis is described in Section 6.5; the conditional probability of canister failure due to a fire is described in Section 6.3. This fire-induced canister failure 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 occurring 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 analyzed as occurring at floor level; the transportation casks may be located as much as 20 ft above the floor. Casks are relatively thick-walled when compared to canisters; in addition, casks 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 the analysis in Attachment D. This canister failure 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 failure 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 cask failure occurs because of bolt stretching, the cask lid remains on top of the cask, thereby preventing fire suppression water from entering. Casks are raised above the floor. They lay horizontally on railcars, are lifted from the railcars by cranes, and reside horizontally inside a CTT at least five feet above the floor surface. If the bottom portion of the canister breaches, there is no physical mechanism for water to enter the cask, enter the canister and optimally mix with the fuel rods such that a criticality occurs.

This situation is also applicable to canisters sealed within a welded waste package. The waste package either resides vertically inside a WPTT, resides on the waste package transfer carriage prior to introduction to the TEV, or is located inside a TEV. In the WPTT, the waste package is more than three feet above the floor (Ref. 2.2.18). Prior to, and following insertion into the TEV, the waste package on its pallet sits approximately one foot above the floor (Ref. 2.2.20). 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 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.

The orientation of a canister inside of an open transportation cask or an open waste package is always vertical; the cask and waste package are always elevated above the floor when the top lids are removed. 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 enter the open vessel. The building configuration, however, precludes this occurrence. The cask lids are removed while in the upload cell, below the canister transfer machine (CTM). The cask and waste package ports are located above the casks and waste package. There is no

fire suppression piping spanning the cask and waste package ports; the ports must be kept clear in order to perform lift and load operations. Once the waste package enters the Waste Package Positioning Room and welding area, the lid has already been positioned on the waste package. No fire suppression piping is located above an open waste package due to the presence of the welding machine.

Upon failure of the canister inside the cask, the sealed cask will not be susceptible to pressurization failures (as described previously). Instead, water can only enter a sealed cask (or sealed waste package) if the cask body melts and breaches. Fires within the waste handling facilities capable of melting stainless steel or Alloy 22, however, have an occurrence frequency 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 from a cask into the CTM shield bell, moved, and lowered into a waste package, it is not inside an outer cask. However, fires cannot 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 sequence yields a mean probability value of 3E-03. The large error factor is assigned because of the potential for human error to defeat some of the measures normally taken to ensure 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). The assignment of these analysis values is consistent with the methodology on the use of judgment provided in Section 4.3.10.

6.2.2.8.2 Lubricating Fluid

Another potential source of moderator is crane lubricating fluid. A limited quantity of crane lubrication oil (<150 gallons) is housed in a welded gear box that is equipped with a leak pan capable of capturing the entire gearbox fluid inventory. An estimate of the leakage rate of oil 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-year preclosure period by the conditional probability of oil pan failure. A loss of lubrication would fail the crane gearbox; this failure would 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 (720 hr). 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/hr × 50 yr × 8760 hr/yr × 0.34E-06/hr × 720 hr = 9.4E-05 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 obtained from previous safety/risk analyses and reliability studies performed nationally or internationally; these sources can also 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, 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 the 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 % of the TYP-FMs are quantified with one data source, 8 % with two data sources, 8 % with three data sources, and 31 % with four or more data sources.

6.3.1.2 Application of Bayes' Theorem to PCSA Database

The application of 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.

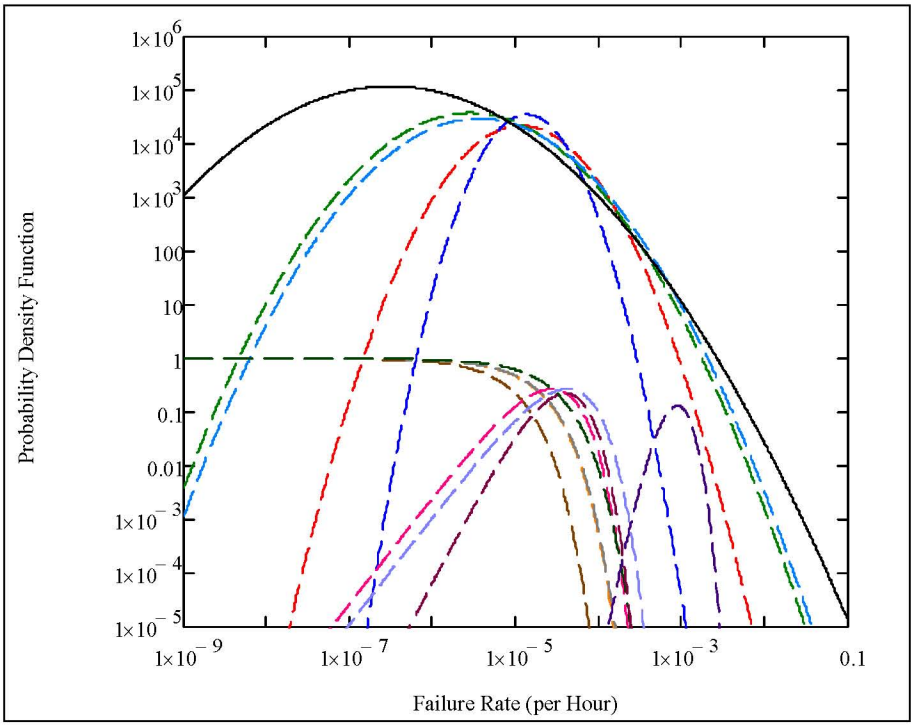
2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trials if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure 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, v and τ, respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating v and τ involves calculating the likelihood function associated with the reliability information in each data source. For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate x, and characterized by its median value and associated error factor. For a data source providing exposure data (given in the form of a number n of recorded failures over an exposure time t), the likelihood function is a Poisson distribution, expressing the probability that n failures are observed when the expected number of failures is x times t.

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



Source: Attachment C, Figure C2.1-1

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

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

Example implementations of the methods used for these cases are provided in Attachment C, 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 HRA. Otherwise, potential dependencies known as CCFs are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method.

Therefore, another subtask of the active component reliability data analysis is to estimate common-cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor Method (Ref. 2.2.53), the Multiple Greek Letter method (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 two-out-of-two failure on demand event, the mean alpha factor of 0.047 (shown in the far right column of Table C3-1 associated with α_2) was used in conjunction with the mean failure probability for the appropriate component type and failure mode (from Table C4-1) as inputs to a compound event to yield the CCF probability.

Similarly, for the two-out-of-two operational failure, the mean alpha factor identified above is divided by two (0.0235) and is used in conjunction with the mean failure probability for the appropriate component type and operational failure mode. In addition, the parameter b associated with the beta distribution function for the alpha factor (Table C3-1) is modified to reflect the change in the alpha factor mean value while preserving the coefficient of variation from the distribution described by the parameters presented in Table C3-1. To preserve the

coefficient of variation, the variance associated with the distribution is reduced by a factor of four (the square of the reduction of the mean). (See Attachment C, Section C3 for the derivation of the value for the parameter b.) The parameter b for the operational α_2 is 21.03.

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	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
060-#EEE-CRCF1-A-XMR-CCF	CRCF ITS transformer train A CCF	C	4.92E-06	2.91E-07	3.38E+01
060-#EEE-CRCF1-A-XMR-FOH	CRCF ITS train A transformer failure	3	2.10E-04	2.91E-07	720
060-#EEE-CRCF1-B-XMR-FOH	CRCF ITS transformer train B failure	3	2.10E-04	2.91E-07	720
060-#EEE-LDCNTRA-BUA-FOH	CRCF load center A fails	3	4.39E-04	6.10E-07	720
060-#EEE-LDCNTRA-C52-FOD	Load center A feed breaker (AC) fails to reclose	1	2.24E-03	—	—
060-#EEE-LDCNTRA-C52-SPO	Load center A feed circuit breaker (AC) spurious operation	3	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	1	2.24E-03	—	—
060-#EEE-LDCNTRB-C52-SPO	CRCF ITS load center circuit breaker (AC) spur op	3	3.82E-03	5.31E-06	720
060-#EEE-LDCNTRS-C52-CCF	CCF of the ITS load center feed breakers to reclose	C	1.05E-04	—	—
060-#EEE-MCC0001-C52-SPO	CRCF ITS MCC 0001 feed breaker spurious operation	3	3.82E-03	5.31E-06	720
060-#EEE-MCC0001-MCC-FOH	CRCF ITS MCC 00001 fails	3	5.38E-03	7.49E-06	720
060-#EEE-MCC0002-C52-SPO	CRCR MCC-00002 feed breaker spurious operation	3	3.82E-03	5.31E-06	720
060-#EEE-MCC0002-MCC-FOH	CRCF ITS MCC00002 failure	3	5.38E-03	7.49E-06	720
060-VCT0-EXH-005-FAN-FTR	CRCF ITS elec exhaust fan 00005 fails to run	3	5.06E-02	7.21E-05	720
060-VCT0-EXH-006-FAN-FTR	CRCF ITS elec exh. fan fails to run	3	5.06E-02	7.21E-05	720
060-VCT0-AHU0001-AHU-FTR	CRCF ITS elec AHU 00001 fails to run	3	2.73E-03	3.80E-06	720

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
060-VCT0-AHU0001-CTL-FOD	CRCF ITS elec AHU 00001 controller fails	1	2.03E-03	—	—
060-VCT0-AHU0002-AHU-FTR	CRCF ITS elec AHU 00002 fails to run	3	2.73E-03	3.80E-06	720
060-VCT0-AHU0002-CTL-FOD	CRCF ITS elec AHU 00002 controller fails	1	2.03E-03	—	—
060-VCT0-AHU0002-FAN-FTS	CRCF ITS elec AHU 00002 fails to start	1	2.02E-03	—	—
060-VCT0-AHU0103-AHU-CCR	CCF of the running CRCF ITS elec AHUs to continue to run	C	6.42E-05	—	—
060-VCT0-AHU0202-AHU-CCR	CCF of standby CRCF ITS elec AHUs to run	C	6.42E-05	—	—
060-VCT0-AHU0202-AHU-CCS	CCF of standby CRCF ITS elec AHUs to start	C	9.49E-05	—	—
060-VCT0-EXH-005-CTL-FOD	CRCF ITS elec exh fan 00005 controller fails	1	2.03E-03	—	—
060-VCT0-EXH-006-FAN-FTS	CRCF ITS elec exh fan 00006 fails to start	1	2.02E-03	—	—
060-VCT0-EXH006-CTL-FOD	CRCF ITS elec exh fan 0006 controller fails	1	2.03E-03	—	—
060-VCT0-EXH0507-FAN-CCR	CCF of running exh fans for CRCF ITS elec.	C	1.19E-03	—	—
060-VCT0-EXH0608-FAN-CCF	CCF to run: standby exh fans for the CRCF ITS elec	C	1.19E-03	—	—
060-VCT0-EXH0608-FAN-CCS	CCF to start: standby exh fans for the CRCF ITS elec	C	9.49E-05	—	—
060-VCT0-AHU0004-AHU-FTR	CRCF ITS elec AHU 00004 fails to run	3	2.73E-03	3.80E-06	720
060-VCT0-AHU0004-CTL-FOD	CRCF ITS elec AHU 00004 controller fails	1	2.03E-03	—	—
060-VCT0-AHU0004-FAN-FTS	CRCF ITS elec AHU 00004 fails to start	1	2.02E-03	—	—
060-VCT0-EXH-007-CTL-FOD	CRCF ITS elec exh fan 00007 controller fails	1	2.03E-03	—	—
060-VCT0-EXH-007-FAN-FTR	CRCF ITS elec exhaust fan 00007 fails to run	3	5.06E-02	7.21E-05	720
060-VCT0-EXH-008-FAN-FTR	CRCF ITS elec exh. fan 8 fails to run	3	5.06E-02	7.21E-05	720
060-VCT0-EXH-008-FAN-FTS	CRCF ITS elec exh fan 00008 fails to start	1	2.02E-03	—	—
060-VCT0-EXH008-CTL-FOD	CRCF ITS elec exh fan 0008 controller fails	1	2.03E-03	—	—
060-VCTO-AHU0013-	AHU 013 fan fails to run	3	5.06E-02	7.21E-05	720

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
FAN-FTR					
060-VCTO-AHU0014-FAN-FTR	AHU 014 fan fails to run	3	2.56E-02	7.21E-05	360
060-VCTO-AHU0003-CTL-FOD	CRCF ITS elec AHU 00003 controller fails	1	2.03E-03	—	—
060-VCTO-BDMP00A-UDM-FOH	Damper (backdraft) failure	3	1.61E-02	2.26E-05	720
060-VCTO-BDMP00B-DMP-FRO	Train B fan discharge backdraft damper fails closed	3	8.10E-03	2.26E-05	360
060-VCTO-BDMP00B-DMP-FTO	Train B backdraft damper fails to open when fan starts	1	8.71E-04	—	—
060-VCTO-DCT0A-DTC-RUP	Train A duct ruptures	3	2.68E-03	3.72E-06	720
060-VCTO-DCT0B-DTC-RUP	Train B duct ruptures	3	1.34E-03	3.72E-06	360
060-VCTO-DMP000A-DMP-FRO	Train A fan discharge manual isolaton damper fails closed	3	6.03E-05	8.38E-08	720
060-VCTO-DMP000B-DMP-FRO	Train B fan discharge manual isolaton damper fails closed	3	3.02E-05	8.38E-08	360
060-VCTO-DMPF00A-DMP-FRO	Train A fan inlet manual isolation damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-DMPF00B-DMP-FRO	Train B fan inlet manual isolation damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-DR0001-HFI-NOD	Operator opens 1 inner door and 1 outer door	1	1.00E-02	—	—
060-VCTO-FAN00A-FAN-FTR	Exhaust fan in train A fails	3	5.06E-02	7.21E-05	720
060-VCTO-FAN00A-PRM-FOH	Train A exhaust fan fails due to ASD malfunction	3	3.87E-04	5.38E-07	720
060-VCTO-FAN00B-FAN-FTR	Train B exhaust fan fails to run	3	2.56E-02	7.21E-05	360
060-VCTO-FAN00B-FAN-FTS	Train B exhaust fan fails to start	1	2.02E-03	—	—
060-VCTO-FAN00B-PRM-FOH	Train B exhaust fan fails due to ASD malfunction	3	1.94E-04	5.38E-07	360
060-VCTO-FANBASD-CTL-FOD	Train B ASD start logic signal fails	1	2.03E-03	—	—
060-VCTO-HEPA-CCF	CCF of 2 of 3 filter plenums	C	9.53E-05	—	—
060-VCTO-HEPAB-	Common-cause failure of	C	4.77E-05	—	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
CCF	HEPA filters (2 of 3)				
060-VCTO-HEPALK-HFI-NOD	Operator fails to shift trains when alarm occurs	1	1.00E+00	—	—
060-VCTO-HFIA000-HFI-NOM	HVAC train B control switch in wrong position	1	1.00E-01	—	—
060-VCTO-IEL0001-IEL-FOD	CRCF door interlock failure	1	2.75E-05	—	—
060-VCTO-IEL0002-IEL-FOD	Interlock failure on demand	1	2.75E-05	—	—
060-VCTO-PLEN09-DMS-FOH	Train A plenum 09 moisture seperator/demister plugs	3	6.55E-03	9.12E-06	720
060-VCTO-PLEN09-HEP-LEK	Train A plenum 9 HEPA filters leak	3	2.16E-03	3.00E-06	720
060-VCTO-PLEN09-HEP-PLG	Train A plenum 9 HEPA filters plug	3	3.07E-03	4.27E-06	720
060-VCTO-PLEN09I-DMP-FRO	Train A filter plenum 09 inlet damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-PLEN09O-DMP-FRO	Train A filter plenum 09 outlet damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-PLEN10-DMS-FOH	Train A plenum 10 moisture seperator/demister plugs	3	6.55E-03	9.12E-06	720
060-VCTO-PLEN10-HEP-LEK	Train A plenum 10 HEPA filters leak	3	2.16E-03	3.00E-06	720
060-VCTO-PLEN10-HEP-PLG	Train A plenum 10 HEPA filters plug	3	3.07E-03	4.27E-06	720
060-VCTO-PLEN10I-DMP-FRO	Train A filter plenum 10 inlet damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-PLEN10O-DMP-FRO	Train A filter plenum 10 outlet damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-PLEN11-DMS-FOH	Train A plenum 11 moisture seperator/demister plugs	3	6.55E-03	9.12E-06	720
060-VCTO-PLEN11-HEP-LEK	Train A plenum 11 HEPA filters leak	3	2.16E-03	3.00E-06	720
060-VCTO-PLEN11-HEP-PLG	Train A plenum 11 HEPA filters plug	3	3.07E-03	4.27E-06	720
060-VCTO-PLEN11I-DMP-FRO	Train A filter plenum 11 inlet damper fails to remain open	3	6.03E-05	8.38E-08	720

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
060-VCTO-PLEN11O-DMP-FRO	Train A filter plenum 11 outlet damper fails to remain open	3	6.03E-05	8.38E-08	720
060-VCTO-PLEN12-DMS-FOH	Train B plenum 12 moisture seperator/demister plugs	3	3.28E-03	9.12E-06	360
060-VCTO-PLEN12-HEP-LEK	Train B plenum 12 HEPA filters leak	3	1.08E-03	3.00E-06	360
060-VCTO-PLEN12-HEP-PLG	Train B plenum 12 HEPA filters plug	3	1.54E-03	4.27E-06	360
060-VCTO-PLEN12I-DMP-FRO	Train B filter plenum 12 inlet damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-PLEN12O-DMP-FRO	Train B filter plenum 12 outlet damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-PLEN13-DMS-FOH	Train B plenum 13 moisture seperator/demister plugs	3	9.12E-06	9.12E-06	—
060-VCTO-PLEN13-HEP-LEK	Train B plenum 13 HEPA filters leak	3	3.00E-06	3.00E-06	—
060-VCTO-PLEN13-HEP-PLG	Train B plenum 13 HEPA filters plug	3	1.54E-03	4.27E-06	360
060-VCTO-PLEN13I-DMP-FRO	Train B filter plenum 13 inlet damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-PLEN13O-DMP-FRO	Train B filter plenum 13 outlet damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-PLEN14-DMS-FOH	Train B plenum 14 moisture seperator/demister plugs	3	3.28E-03	9.12E-06	360
060-VCTO-PLEN14-HEP-LEK	Train B plenum 14 HEPA filters leak	3	3.00E-06	3.00E-06	—
060-VCTO-PLEN14-HEP-PLG	Train B plenum 14 HEPA filters plug	3	1.54E-03	4.27E-06	360
060-VCTO-PLEN14I-DMP-FRO	Train B filter plenum 14 inlet damper fails to remain open	3	3.017E-05	8.38E-08	360
060-VCTO-PLEN14O-DMP-FRO	Train B filter plenum 14 inlet damper fails to remain open	3	3.02E-05	8.38E-08	360
060-VCTO-RSH005-SRR-FOH	High rad door interlock permissive fails	3	8.80E-02	1.28E-04	720
060-VCTO-RSH114-SRR-FOH	Exhaust high rad alarm fails	3	2.00E-05	2.00E-05	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
060-VCTO-TDMP00A-DTM-FOD	Train A tornado damper fails closed when tornado conditions don't exist	3	1.61E-02	2.26E-05	720
060-VCTO-TDMP00B-DTM-FOH	Train B tornado damper fails closed when tornado conditions don't exist	3	8.10E-03	2.26E-05	360
060-VCTO-TRAINB-MAINT	Train B unavailable due to maintenance	1	4.57E-03	—	—
060-VCTO-TRATRIP-CTL-FOD	Logic controller fails on demand	1	2.03E-03	—	—
26D-##EG-DAYTNKA-TKF-FOH	ITS DG A day tank (00002A) fails	3	1.58E-04	4.40E-07	360
26D-##EG-DAYTNKB-TKF-FOH	ITS DG B day fuel tank fails	3	1.58E-04	4.40E-07	360
26D-##EG-FLITLKA-IEL-FOD	ITS DG A fuel transfer pumps Interlock Failure	1	2.75E-05	—	—
26D-##EG-FLITLKB-IEL-FOD	ITS DG B fuel transfer pumps Interlock Failure	1	2.75E-05	—	—
26D-##EG-FTP1DGA-PMD-FTR	ITS DG A fuel transfer pump fails to run	3	1.23E-02	3.45E-05	360
26D-##EG-FTP1DGA-PMD-FTS	ITS DG A fuel pump 1A fails to start	1	2.50E-03	—	—
26D-##EG-FTP1DGB-PMD-FTR	ITS DG B fuel transfer pump 1 (motor driven) fails to run	3	1.23E-02	3.45E-05	360
26D-##EG-FTP1DGB-PMD-FTS	ITS DG B fuel transfer pump 1 (motor driven) fails to start	1	2.50E-03	—	—
26D-##EG-FTP2DGA-PMD-FTR	ITS DG A fuel transfer pump 2A fails to run	3	1.23E-02	3.45E-05	360
26D-##EG-FTP2DGA-PMD-FTS	ITS DG A fuel transfer pump 2A fails to start	1	2.50E-03	—	—
26D-##EG-FTP2DGB-PMD-FTR	ITS DG B fuel transfer pump 2 (motor driven) fails to run	3	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	1	2.50E-03	—	—
26D-##EG-FULPMPA-PMD-CCR	CCF of ITS DG A fuel pumps to run	C	2.90E-04	—	—
26D-##EG-FULPMPA-PMD-CCS	CCF of ITS DG A fuel pumps to start	C	1.18E-04	—	—
26D-##EG-FULPMPB-PMD-CCR	CCF of ITS DG B fuel pumps to run	C	2.90E-04	—	—
26D-##EG-FULPMPB-PMD-CCS	CCF of ITS DG B fuel pumps to start	C	1.18E-04	—	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
26D-##EG-HVACFN1-FAN-FTR	ITS DG B room fan 1 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-##EG-HVACFN1-FAN-FTS	ITS DG B room fan (motor-driven) fails to start	1	2.02E-03	—	—
26D-##EG-HVACFN2-FAN-FTR	ITS DG B room fan 2 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-##EG-HVACFN2-FAN-FTS	ITS DG B room fan (motor-driven) fails to start	1	2.02E-03	—	—
26D-##EG-HVACFN3-FAN-FTR	ITS DG B room fan 3 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-##EG-HVACFN3-FAN-FTS	ITS DG B room fan 3 (motor-driven) fails to start	1	2.02E-03	—	—
26D-##EG-HVACFN4-FAN-FTR	ITS DG B fan 4 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-##EG-HVACFN4-FAN-FTS	ITS DG B room fan 4 (motor-driven) fails to start	1	2.02E-03	—	—
26D-##EG-STRTDGA-C72-SPO	ITS switchgear A battery circuit breaker (DC) spur op	3	3.85E-04	1.07E-06	360
26D-##EG-STRTDGB-C72-SPO	13.8kV ITS SWGR battery B circuit breaker (DC) spur op	3	3.85E-04	1.07E-06	360
26D-##EG-WKTNK_A-TKF-FOH	ITS DG A bulk fuel tank (00001A) fails	3	1.58E-04	4.40E-07	360
26D-##EG-WKTNK_B-TKF-FOH	ITS DG B bulk fuel tank fails	3	1.58E-04	4.40E-07	360
26D-##EGBATCHRGA-BYC-FOH	ITS switchgear A battery: battery charger failure	3	1.28E-03	7.60E-06	168
26D-##EGBATCHRGB-BYC-FOH	ITS DG B battery charger failure	3	1.28E-03	7.60E-06	168
26D-#EEE-SWGRDGA-BUA-FOH	13.8 kV ITS switchgear A failure	3	4.39E-04	6.10E-07	720
26D-#EEE-SWGRDGB-AHU-FTR	EDGF switchgear room air handling unit failure to run	3	2.73E-03	3.80E-06	720
26D-#EEE-SWGRDGB-BUA-FOH	13.8 kV ITS switchgear B bus failure	3	4.39E-04	6.10E-07	720
26D-#EEESWGRDGA-AHU-FTR	13.8 kV ITS switchgear room air handling unit fails	3	2.73E-03	3.80E-06	720
26D-#EEG-HVACFA1-FAN-FTR	ITS DG A room fan 1 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-#EEG-HVACFA1-FAN-FTS	ITS DG A room fan 1 (motor-driven) fails to start	1	2.02E-03	—	—

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
26D-#EEG-HVACFA2-FAN-FTR	ITS DG A room fan 2 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-#EEG-HVACFA2-FAN-FTS	ITS DG A room fan 2 (motor-driven) fails to start	1	2.02E-03	—	—
26D-#EEG-HVACFA3-FAN-FTR	ITS DG A room fan 3 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-#EEG-HVACFA3-FAN-FTS	ITS DG A room fan 3 (motor-driven) fails to start	1	2.02E-03	—	—
26D-#EEG-HVACFA4-FAN-FTR	ITS DG A room fan 4 (motor-driven) fails to run	3	2.56E-02	7.21E-05	360
26D-#EEG-HVACFA4-FAN-FTS	ITS DG A room fan 4 (motor-driven) fails to start	1	2.02E-03	—	—
26D-#EEU-208_DGA-BUD-FOH	ITS DC panel A DC bus failure	3	8.64E-05	2.40E-07	360
26D-#EEU-208_DGB-BUD-FOH	ITS DG B DC panel failure	3	8.64E-05	2.40E-07	360
26D-#EEY-DGALOAD-C52-FOD	DG A load breaker (AC) fails to close	1	2.24E-03	—	—
26D-#EEY-DGBLOAD-C52-FOD	ITS DG B load breaker (AC) fails to close	1	2.24E-03	—	—
26D-#EEY-DGLOADS-C52-CCF	CCF of ITS DG load breakers to close	C	1.05E-04	—	—
26D-#EEY-ITS-DGB-#DG-FTS	Diesel generator fails to start	1	8.38E-03	—	—
26D-#EEY-ITSDG-A-#DG-FTR	ITS diesel generator A fails to run	3	7.70E-01	4.08E-03	360
26D-#EEY-ITSDG-A-#DG-FTS	Diesel generator fails to start	1	8.38E-03	—	—
26D-#EEY-ITSDGAB-#DG-CCR	CCF ITS DG A & B fail to run	C	1.81E-02	—	—
26D-#EEY-ITSDGAB-#DG-CCS	CCF DG A and B to start	C	3.94E-04	—	—
26D-#EEY-ITSDGB-#DG-FTR	ITS DG B fails to run	3	7.70E-01	4.08E-03	360
26D-#EEY-OB-SWGA-C52-FOD	13.8 kV ITS SWGR feed breaker (AC) fails to open	1	2.24E-03	—	—
26D-#EEY-OB-SWGA-C52-SPO	13.8 kV ITS SWGR A feed breaker spurious operation	3	3.82E-03	5.31E-06	720
26D-#EEY-OB-SWGB-C52-FOD	13.8 kV feed breaker (from SWYD) fails on demand	1	2.24E-03	—	—
26D-#EEY-OB-SWGB-C52-SPO	13.8 kV ITS SWGR feed breaker (AC) spurious op	3	3.82E-03	5.31E-06	720

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
26D-#EEY-OB-SWGS-C52-CCF	Common cause failure of 13.8 kV ITS SWGR feed breakers to open	C	1.05E-04	—	—
26D-#EG-BATTERYB-BTR-FOD	ITS SWGR control battery B no output	1	8.20E-03	—	—
26D-#EG-LCKOUTRL-RLY-FTP	13.8 kV its switchgear feed breaker lock out relay fails to open CB	3	3.15E-03	8.77E-06	360
26D-#EG-LDSQNCRB-SEQ-FOD	ITS DG B load sequencer fails	1	2.67E-03	—	—
26D-#EG-LOCKOUTB-RLY-FTP	13.8 kV ITS swgr lockout relay (power) fails to open CB	3	3.15E-03	8.77E-06	360
26D-#EGLDSQNCRA-SEQ-FOD	DG A load sequencer fails	1	2.67E-03	—	—
26D-EG-BATTERYA-BTR-FOD	ITS switchgear A battery no output given challenge	1	8.20E-03	—	—
27A-#EEE-BUS2DGA-C52-SPO	13.8 kV open bus 2 ITS load breaker spurious operation	3	3.82E-03	5.31E-06	720
27A-#EEE-BUS3DGB-C52-SPO	13.8 kV open bus 4 to ITS B load breaker (AC) spurious op	3	3.82E-03	5.31E-06	720
27A-#EEN-OPENBS2-BUA-FOH	13.8 kV open bus 2 bus failure	3	4.39E-04	6.10E-07	720
27A-#EEN-OPENBS4-BUA-FOH	13.8 kV open bus 4 bus failure	3	4.39E-04	6.10E-07	720
27A-#EEN-OPNBS1A-SWP-SPO	13.8 kv open bus 2 to ITS div A electric power switch spur. xfer	3	1.12E-04	1.55E-07	720
27A-#EEN-OPNBS3B-SWP-SPO	13.8 kV open bus 4 to ITS B electric power switch spur xfer	3	1.12E-04	1.55E-07	720
800-FAC-WPCRNDP-CRW-DRP	WP (Non-SFP) crane drop	1	1.05E-04	—	1
800-HEE0-3RDRAIL-THR-BRK	Third rail breaks	3	1.01E-08	0.000E+00	8
800-HEE0-ACTADR1-ATP-SPO	Actuator spurious op - access door	3	7.64E-09	1.34E-06	5.70E-03
800-HEE0-ACTADR2-ATP-SPO	Actuator spurious op - access door	3	7.64E-09	1.34E-06	5.70E-03
800-HEE0-ACTDR01-ATP-SPO	Actuator spurious op - TEV door	3	5.36E-06	1.34E-06	4
800-HEE0-ACTDR02-ATP-SPO	Actuator spurious op - TEV door	3	5.36E-06	1.34E-06	4
800-HEE0-AXSDR00-	Programmable logic	3	2.08E-09	3.65E-07	5.70E-03

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type[a]	Basic Event Mean Probability[b]	Mean Failure Rate[b]	Mission Time (Hours)
PLC-SPO	controller spurious operation				
800-HEE0-AXSMO01-MOE-FSO	Motor (electric) fails to shut off	3	<1.00E-09	1.35E-08	5.70E-03
800-HEE0-AXSMO02-MOE-FSO	Motor (electric) fails to shut off	3	<1.00E-09	1.35E-08	5.70E-03
800-HEE0-BEDEXTD-ATP-SPO	Actuator spurious op - TEV base plate	3	5.36E-06	1.34E-06	4
800-HEE0-DERAILS-DSG-DER (DER-FOH)	Drip shield gantry derails	1	1.18E-05	—	—
800-HEE0-DERAILS-TEV-DER (DER-FOH)	TEV derails - per mile	1	1.18E-05	—	—
800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook fails - DSG	3	7.45E-07	7.45E-07	1
800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook fails - DSG	3	7.45E-07	7.45E-07	1
800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook fails - DSG	3	7.45E-07	7.45E-07	1
800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook fails - DSG	3	7.45E-07	7.45E-07	1
800-HEE0-DSLIFTC-LRG-CCF	Common cause failure of 2 of 4 lifting rig or hooks	C	2.78E-08 [1]	—	—
800-HEE0-FACMO01-MOE-SPO	Shield door motor #1 spurious operation	3	6.74E-07	6.74E-07	1
800-HEE0-FACMO02-MOE-SPO	Shield door motor #2) spurious operation	3	6.74E-07	6.74E-07	1
800-HEE0-FACTOR1-TL-FOH	Shield door motor #1 over torque limiter failure	3	2.86E-02	8.05E-05	360
800-HEE0-FACTOR2-TL-FOH	Shield door motor #2 over torque limiter failure	3	2.86E-02	8.05E-05	360
800-HEE0-GEARBX1-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX2-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX3-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX4-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX5-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX6-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX7-GRB-STH	Gear box stripped	3	3.14E-07	7.86E-08	4
800-HEE0-GEARBX8-	Gear box stripped	3	3.14E-07	7.86E-08	4