

The failure components described above are analogous to the failure modes of a two train system in standby where at least on train must successfully start and run for a specified mission time to prevent system failure.

The fourth component described above dominates probabilistically and its calculation is described below. The sum of the other three event sequences are more than two orders of magnitude lower.

The likelihood of an extended LOSP has been estimated by using the probability of a LOSP exceeding 24 hours, which is the longest non-recovery period identified in NUREG/CR-6890 (Ref. 2.2.38). The 720 hour period for which a brake holding failure has been modeled should provide ample time to either recover offsite power or for operators to implement an alternative means to safely lower any load. Provision for manual lowering of loads is provided in NOG-1 cranes (Ref. 2.2.7).

The probability of the fourth component described above – the combination of LOSP and load drop (brakes set but fail to hold over a 720-hr mission time) is:

$$\begin{aligned} & \text{LOSP-IE} \times \text{Holding brake fails} \times \text{Emergency brake fails} = \\ & = 3.2\text{E-}02 \times (8.4\text{E-}06 \times 720) \times (4.4\text{E-}06 \times 720) \\ & = 6.1\text{E-}07 \end{aligned}$$

Thus, the LOSP load drop probability over the preclosure period is estimated to be 6E-07. This number of occurrences of the compound initiating event is much less than one chance in 10,000 (1E-4) during the preclosure period. Therefore, event sequences with LOSP and a coincident drop load as the initiating event are Beyond Category 2.

The possibility of inadvertent direct exposure of workers due to a loss of electrical power is considered next. Canisters are always shielded during facility operations by a transportation cask, a canister preparation platform, concrete floors and walls, the CTM shield bell and shield skirt, the WPTT, facility shield doors, and the TEV shield compartment. Loss of electrical power to any of these simply stops operations while maintaining shielding. For example, inadvertent shield bell and shield door motion can not occur in the absence of electrical power. Therefore, direct exposure to workers owing to loss of electrical power is considered to be Beyond Category 2.

It has been shown that loss of electrical power in conjunction with other failures is screened out as an initiating event. Nevertheless, this compound failure mode is included in the initiating and pivotal event fault trees as appropriate. For example, the hoist brake on the CTM requires electrical power to remain unengaged. A loss of power would cut power to the brake, leading to its automatic engagement. If the brake fails in conjunction with a loss of power in this scenario, a drop of the load could occur, initiating an event sequence. This failure scenario is included in the CTM fault tree. For the overhead cranes, the initiating event frequencies are based on industry-wide empirical data for cranes. The ITS HVAC system depends on continued electrical power and it is explicitly modeled in the fault tree for this pivotal event.

6.0.3 Screening of Internal Initiating Events

All facility safety analyses, whether risk-informed or not, take into account the physical conditions, dimensions, materials, human-machine interface, and other attributes such as operating conditions and environments, to assess potential failure modes and event sequences. Such accounting guides the assessment of what can happen, the likelihood, and the potential consequences. In many situations, it is obvious that the probability of a particular exposure scenario is very low. 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 *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28) for quantitative treatment in the present analysis. For completeness, some events that were identified in the event sequence development analysis are extremely unlikely or physically unrealizable and can reasonably be qualitatively screened from further consideration. A qualitative screening argument for certain internal initiating events is developed in the present analysis as documented in Table 6.0-2. The first column of Table 6.0-2 indicates the branch of the initiator event tree (where applicable) that pertains to the screened initiating event. Each branch of an initiator event tree represents an initiating event or an initiating event group that includes other similar initiating events and corresponds to a little bubble on an ESD (Ref. 2.2.28; Attachments F and G). Some of the initiating events that are addressed in Table 6.0-2 were implicitly screened out in the event sequence development analysis and for that reason there is no applicable event tree. The screening argument for internal flooding is presented in Section 6.0.4. The screened 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 #)	Initiating Event Description	Screening Basis
IHF-ESD-01-HLW (#3) (Figure A5-2)	Rollover of a truck trailer carrying a transportation cask in the Cask Preparation Area	For a truck trailer to roll over, its center of mass has to move laterally beyond the wheel base of the trailer. This could occur upon traversing a significantly uneven surface, running over a very large object, or turning sharply at high speed. There are no uneven surfaces in the Cask Preparation Area. It is a flat concrete surface. There are no objects that could be run over that could significantly shift the trailer's center of mass. Turning sharply at high speed is not possible inside the building because the Cask Preparation Area is too narrow and the truck comes to a complete stop outside the closed entrance door prior to the door opening and the truck entering. Therefore, event sequences associated with this failure mode are considered to be physically unrealizable.
IHF-ESD-05-HLW (#2) (Figure A5-10) IHF-ESD-05-NVL (#2) (Figure A5-12)	Structural damage to transportation cask due to impact from the crane hook or rigging while under the cask preparation platform	In this operation, the lid is unbolted and the lid lift fixture is attached. The cask is flush or recessed with respect to the cask preparation platform, and therefore cannot be impacted. Therefore, event sequences associated with these initiating events are considered to be physically unrealizable.
IHF-ESD-07-HLW(#2) (Figure A5-16)	Drop of a heavy object onto an HLW canister	The waste package inner lid and the transportation cask lid are the only pertinent heavy objects (except for another canister) whose drop onto an HLW canister could jeopardize the canister's structural integrity. (Drop of one HLW canister onto another is not screened out.) Divider plates in the codisposal waste package extend higher than the canisters inside. Therefore, a dropped waste package lid would not impact the canisters. Transportation casks containing HLW canisters are designed such that a lid drop would not impact the canisters inside. Thus, a drop of a heavy load does not have an adverse effect on the integrity of HLW canisters and can be screened from further consideration.
IHF-ESD-07-HLW(#6) (Figure A5-16) IHF-ESD-07-NVL(#6) (Figure A5-17)	Side impact from a slide gate	Slide gate impacts during CTM transfer are included in the CTM fault tree as a cause of canister drop, rather than as an independent initiating event. In addition, the motors on the slide gates have insufficient power to significantly damage a canister.
IHF-ESD-09-HLW(#2) (Figure A5-21) IHF-ESD-09-NVL(#2) (Figure A5-23)	Welding of the waste package lid causes canister breach	No plausible scenarios have been identified whereby the gas tungsten arc welding process could cause burn through of the waste package and canister (Ref. 2.2.13). Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.
IHF-ESD-11-HLW(#2) (Figure A5-27) IHF-ESD-11-NVL(#2) (Figure A5-28)	TEV collision with stationary waste package	The TEV is parked in the Waste Package Loadout Room when the waste package enters via the WPTT, and cannot collide with the waste package. The WPTT is on rails so its path is well defined. The TEV is separated from the WPTT by the docking station. Even a TEV and/or WPTT derailment cannot cause a collision between the two vehicles because of the extremely low speed of these vehicles. Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
No applicable event trees	Internal flooding	Internal flooding as an initiating event is screened from further analysis in Section 6.0.4.
No applicable event trees	Canister dropped into the Cask Unloading Room or Waste Package Positioning Room with no waste package present	Dropping a canister through a port without a staged waste package below would require a series of human failures and mechanical failures that makes the initiating event unlikely. The design incorporates an interlock to prevent the opening of the waste package port slide gate when the WPTT and waste package shield ring are not present (Ref. 2.2.30). The combination of (a) failure to stage the waste package, (b) failure of more than one operator to notice that it is not staged, (c) failure of the hardwired interlock, and (d) drop of the canister are required for such an initiating event to occur. Considering the combination of unlikely events that must occur to cause this initiating event, event sequences involving this combination of failures are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part.
No applicable event trees	Tipover of CTT	The CTT is designed to prevent tipover (Ref. 2.2.22, Section 3.2). The size, weight, low center of gravity, and low speed of the CTT ensure that no tipover can occur. During cask preparation activities, the CTT is set on the floor inside the cask preparation platform. As such, tipover is not physically realizable during preparation activities. During transit, the CTT glides slowly on a cushion of air, an inch or less above the floor. If air pressure is lost, the CTT, with its load, settles to the floor. While the CTT is in transit, or after settling to the floor, any applied force from facility operations is incapable of tipping over the CTT. Due the slow travel of the CTT, a loss of air pressure or a collision with other equipment or a facility structure will not result in tipover. Therefore, tipover of the CTT is considered physically unrealizable for internal events. CTT tipover, however, is analyzed in the seismic event sequence and categorization (Ref. 2.4.4).
No applicable event trees	Conveyance carrying a waste form collides with a shield door, causing the door to dislodge from its supports and fall onto the waste form	The shield doors are designed to withstand collision of the conveyance into the door without dislodging from their supports such that the stress of all support mechanisms of the door stay below yield. Therefore, this initiating event is considered physically unrealizable.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
IHF-ESD-08-HLW(#3) (Figure A5-18) IHF-ESD-08-NVL(#3) (Figure A5-20) IHF-ESD-10-HLW(#3) (Figure A5-24) IHF-ESD-10-NVL(#3) (Figure A5-26)	Tilt-down of WPTT at uncontrolled speed	The main feature of the WPTT is the shielded enclosure, which holds the waste package, the waste package pallet, the waste package transfer carriage, and the waste package pedestal (Ref. 2.2.23, Section 2.1.1). The enclosure pivots between vertical and horizontal orientations to position the waste package for loading and unloading. There are two sets of redundant tipping motor-and-gear systems, each of which is designed to withstand the maximum possible torque without failure. If one motor-and-gear system were to fail, the shielded enclosure would still be supported. The center of gravity of the shielded enclosure is positioned such that the vertical position is the most stable position (Ref. 2.2.23, Section 3.3.2). Therefore, even in the unlikely event that both motor-and-gear systems fail catastrophically, the shielded enclosure would not undergo tilt-down at uncontrolled speed.
No applicable event trees	Operator drops cask during cask preparation activities	The cask preparation crane, rather than the cask handling crane, is used in the lid-removal operation for the naval cask. Because the cask is not intentionally lifted in this step, dropping the cask would require a series of extraordinary human failures. The HLW-cask lid is not removed during preparation activities. For naval casks, a cask drop would require a series of human failures as follows. During lid removal, the crew must fail to remove some fraction of the lid bolts, fail to properly use the check list to verify bolt removal, and use the wrong crane (the cask preparation crane would be incapable of lifting the cask). The crane operator and at least two other crewmembers will be standing on the platform in direct view of the cask during lid removal and they all would have to fail to notice that the entire cask is being lifted before the bolts break. Therefore, event sequences associated with this initiating event are judged to contribute insignificantly to the frequency of the grouped event sequences of which they would be a part. For HLW casks, the lid is not removed from the cask at this point. Therefore, no configuration that could result in a crane lifting the cask occurs for such casks. This initiating event, as it relates to HLW casks, is considered to be unrealizable.
IHF-ESD-07-HLW(#8) (Figure A5-16) IHF-ESD-07-NVL(#8) (Figure A5-17)	Canister dropped inside shield bell (with CTM slide gate closed)	Drops within the shield bell are subsumed within the initiating event for drops from the operational lift height, and are not separately addressed. This is conservative because the drop height within the shield bell is less than the operational lift height.
No applicable event trees	Explosion of site prime mover fuel tank	The fuel tank of the site prime mover has safety features that preclude fuel tank explosion. Therefore, this initiating event is considered physically unrealizable.

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
No applicable event trees	Neutronic interaction involving more than two naval canisters.	<p>The <i>Preclosure Criticality Safety Analysis</i>, (Ref. 2.2.32, Section 2.3.2.5) indicates that interaction must be controlled for highly enriched DOE SNF. Similarly, because NNPP SNF is highly enriched and is expected to have similar neutronic characteristics, interaction between naval canisters also needs to be controlled. Interactions involving two naval canisters in close proximity are analyzed in the classified NNPP documents that contain a bounding criticality calculation for interaction involving naval canisters. However, interactions involving more than two canisters have not been evaluated for criticality. The following screening argument demonstrates that placing more than two naval canisters in close proximity in the IHF is not reasonably achievable.</p> <p>Given the mechanical handling-capabilities of the IHF as described in <i>Initial Handling Facility Event Sequence Development Analysis</i> (Ref. 2.2.28, Section 6.1, Attachment A, and Attachment B), reasonably achievable configurations involving two naval casks or canisters can be imagined. However, in each case, as demonstrated below, adding a third cask or canister is not achievable.</p> <p>(1) Normal handling operations for naval casks allow a single cask to be present in the Cask Preparation Area. A conceivable human error could result in receipt of a second naval cask on a railcar while the first cask is still in the CTT in the Cask Preparation Area. Once this has been done, operators could conceivably be unaware that a cask is already present in the CTT and attempt to use the cask handling crane to load the second cask into the CTT. The error would become inescapably obvious when operators attempt to load the second cask into the CTT, which is already occupied by the first cask. At this point, two casks may be side by side in close proximity. The design of the facility does not admit the possibility of bringing in a third cask because the crane is already occupied with the second cask.</p> <p>(2) Two naval canisters may conceivably be brought end to end as follows. Suppose that a canister has been loaded into the CTM. Given a series of human errors, it is conceivable that the presence of the canister in the CTM could be forgotten. Then, another naval cask could be brought in, loaded into the CTT, and then transferred into the Cask Unloading Room underneath the first canister in the CTM. At this point, the slide gates could be opened and the canister in the CTM could be brought into end-to-end contact with the canister in the cask. The facility is not capable of bringing a third canister into close proximity because the CTT is already occupied.</p>

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

Initiator Event Tree (Branch #)	Initiating Event Description	Screening Basis
(Continued)	(Continued)	(3) A similar end-to-end configuration could conceivably be achieved after a canister has been loaded into the waste package in the Waste Package Loading Room. In this case, the presence of the canister in the waste package has been forgotten and a second canister is erroneously loaded into the CTM. Operators attempt to load the second canister into the waste package, which already contains a canister. The facility is not capable of bringing a third canister into close proximity because the CTM and WPTT are already occupied with canisters.
		(4) An end-to-end configuration involving loaded, sealed waste packages is also conceivable. In this case, the operators have placed a waste package into the TEV and forgotten that it is there. Another waste package is brought into the Waste Package Loadout Room on the WPTT. The TEV doors are opened and the WPTT transfer carriage carries the second waste package end to end with the first. The facility is not capable of bringing a third waste package into close proximity because the WPTT and TEV are already occupied with waste packages.

NOTE: Initiator event trees are provided in Attachment A in the figures cited. The branch numbers are shown in each figure under the column labeled "#".

CTM = canister transfer machine; CTT = cask transfer trolley; DPC = dual-purpose canister; HLW = high-level radioactive waste; TEV = transport and emplacement vehicle; WP = waste package; WPTT = waste package transfer trolley.

Source: Original

6.0.4 Screening of Internal Flooding as an Initiating Event

By the definition of an event sequence, a flood inside a facility would be an initiating event if it led to a sequence of events that would either breach waste containers, causing a release, or caused elevated radiological exposure without a release (i.e., direct exposure of personnel). Internal floods, whether caused by random failure or earthquakes, emerge from two sources. The first is inadvertent actuation of the fire-suppression system. The second is failure of water-carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems. Drains, channels and curbs are situated to remove water from these sources. However, the following discussion does not rely on these.

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

Water impingement on electrical equipment (e.g., motor control centers, motors, and switchgear cabinets) would ordinarily trigger circuit protection features that would open the circuit and cause a loss of electrical power (which is covered in Section 6.0.2.2). If a short circuit occurred as a result of water impingement, normal circuit protection features or overheating of the wires would subsequently open the affected circuit. In an extreme situation, an electrical fire might be started. Fires from all causes are covered in Section 6.5.

Now consider the possibility of inadvertent direct exposure of workers due to internal flooding. Direct exposure to workers during a flood would occur if shielding were disabled as a result of the flooding. Canisters are always shielded during facility operations by transportation casks, cask preparation platforms, concrete floors and walls, the CTM shield bell or shield skirt, the WPTT, canister transfer trolley, shield doors, or the shield compartment of the TEV. Loss of electrical power to any of these simply stops operation, if any, without affecting the shielding. Flooding might also cause hot shorts in control boxes. However, hardwired interlocks between the CTM slide gate, shield bell skirt, and shield doors prevents such inadvertent motion. Therefore, internal flooding cannot initiate an event sequence that causes increased levels of radiological exposure to workers.

Moderator intrusion into canisters resulting from event sequences that might breach a waste container is treated quantitatively as described in the pivotal event descriptions of Section 6.2.

6.1 EVENT TREES

The event trees that are quantified in this analysis were developed from ESDs in the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28, Attachments F and G). This section describes the use of SAPHIRE (Section 4.2) to model 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 linked event trees with linked fault trees to calculate the frequency of occurrence of event sequences. The SAPHIRE computer program (Section 4.2) is used for this purpose. The event tree quantification is supported by FTA (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), and PEFA (Section 6.3 and Attachment D). The YMP preclosure handling is performed using four kinds of buildings as summarized below:

1. The Receipt Facility (RF) accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.
2. The CRCF accepts all waste containers except those supplied by the NNPP for placement in waste packages destined for emplacement in the repository emplacement drifts.
3. The Wet Handling Facility (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 SNF canisters from the NNPP and some canisters containing high-level radioactive waste for placement in waste packages destined for emplacement in the repository emplacement drifts.

Preclosure waste handling as modeled in the PCSA also includes TEV and Subsurface Operations. The TEV accepts waste packages from the IHF and CRCF and, by means of rail, transports them and deposits them into designated locations 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. Because each type of waste container in the IHF has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container. As described in the *Initial Handling Facility Event Sequence Development Analysis* (Ref. 2.2.28), event sequences are also developed separately for each major group of waste handling processes by location within the building. 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 mutually exclusive end states:

1. OK
2. Direct Exposure, Degraded Shielding
3. Direct Exposure, Loss of Shielding
4. Radionuclide Release, Filtered (HVAC is represented in the event sequences despite the fact that it is not relied upon for the IHF for prevention or mitigation of event sequences.)
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 IHF)

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.

The SAPHIRE computer program has advanced features that permit the analyst to control the inputs and conditions for quantifying linked event trees and fault trees. One feature is the use of “basic rules” by which the analyst tells the program how and when to link certain variations of fault trees and basic event data that describe a given initiating and pivotal event. This allows path-dependent development of sequence-minimal cut sets and probabilities.

The primary inputs to the program are the following:

- Event tree logic models
- Fault tree logic models for initiating and pivotal events
- Initiating event frequencies derived from waste-form throughputs and numbers of opportunities for initiating an event sequence
- 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 event tree and fault tree logic models are linked to the basic event library.)

Each basic event is characterized by a probability distribution. The SAPHIRE Monte Carlo sampling method is employed to propagate the uncertainties to obtain event sequence mean values and parameters of the underlying probability distribution such as variance. As described in Section 4.3.6, categorization is done on aggregated event sequences whose resultant probability distributions are also obtained by Monte Carlo simulation. 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. 2.2.28, Attachment F). An example is IHF-ESD-06-NVL, which is shown in Figure A5-17 in Attachment A. The feed on the left side of the 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 the challenge is equal to the number of transportation casks containing naval canisters that are handled over the preclosure period. The initiating event is presented next, followed by the pivotal events. By convention, the description of each branching event is stated as a success. The branching under each event heading represents success by an upward branch and failure by a downward branch. If a given pivotal event cannot occur in a given sequence due to a prior pivotal event or is irrelevant to the sequence, it does not appear in the event sequence as illustrated in the corresponding ESD 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” often means that normal operation can continue. The undesired end states represent a release of airborne radioactivity, a direct exposure to radiation, or a potential criticality condition.
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. 2.2.28, 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, IHF-ESD-01-HLW, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, IHF-RESP-TC1, is shown in Figure A5-3. 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 transportation casks containing HLW canisters that are received during the preclosure period. Initiator event trees do not end at end states but transfer to a system response event tree. System response event trees contain only pivotal events. The user specifies the models to be used for the initiating events associated with each initiator event tree and the pivotal events

associated with the corresponding system response event tree by writing “basic rules,” which are attached to the initiator event tree in SAPHIRE. In accordance with the user-specified basic rules, the SAPHIRE program links a specific fault tree model or basic event to a given initiating event or 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 SAPHIRE as many times as there are initiating events in the 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, transportation cask, canister, shielding properties, HEPA filtration availability, and moderator intrusion susceptibility. The pivotal events are summarized 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. Two kinds of fault trees are developed and represented in Attachment B. The first type represents equipment fault trees including HFEs that contribute directly to the specific pivotal or initiating event. The second type links initiating and pivotal events to these equipment fault trees (via transfer gates) and miscellaneous events. This second type is called a linking or connector fault tree. The equipment 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 basic events in the reliability database entered into SAPHIRE. Section 6.2 provides 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 form units (such as casks, canisters, or waste packages) to be handled over the life of the IHF. The throughputs are identified in Table 6.1-1 and are drawn into the descriptions of specific event trees as needed. With the number of waste form units as a multiplier in the event tree and the initiating events specified as a probability per waste form unit, the value passed to the system response is the number of occurrences of the initiating event expected over the life of the facility.

Table 6.1-1. Waste Form Throughputs for the IHF Over the Preclosure Period

Waste Form Unit	IHF Throughput	Comment
Transportation casks containing a naval canister	400	—
Transportation casks containing HLW canisters	600	100 rail-based transportation casks containing 5 HLW canisters and 500 truck-based transportation casks contain 1 HLW canister
Naval canisters	400	—

Table 6.1-1. Waste Form Throughputs for the IHF Over the Preclosure Period (Continued)

Waste Form Unit	IHF Throughput	Comment
HLW canisters	1000	—
Waste packages containing a naval canister	400	—
Waste packages containing HLW canisters	200	5 canisters per waste package

NOTE: IHF = Initial Handling Facility; HLW = high-level radioactive waste;

Source: Ref. 2.2.26, Table 4

6.1.3 Guide to Event Trees

Event trees are located in Attachment A. Table 6.1-2 contains the crosswalk from the ESD (Ref. 2.2.28, Attachment F) to the initiating event tree and response tree figure location in Attachment A.

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

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
IHF-ESD-01	Event Sequences for Activities Associated with Receipt of Naval or HLW TC on RC or TT in Cask Preparation Area and Upending and Transfer of Naval TC to CTT	ESD-01-HLW ESD-01-NVL	Figure A5-2 Figure A5-4	IHF-RESP-TC1 IHF-RESP-TC1	Figure A5-3
IHF-ESD-02	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending and Transfer of HLW Cask to CTT and Removal of Impact Limiters from Naval TC	ESD-02-HLW ESD-02-NVL	Figure A5-5 Figure A5-6	IHF-RESP-TC1 IHF-RESP-TC1	Figure A5-3 Figure A5-3
IHF-ESD-03	Event Sequences for Activities Associated with Cask Preparation Activities Associated with Unbolting and Lid Adapter Installation for the HLW Cask	ESD-03-HLW	Figure A5-7	IHF-RESP-TC1	Figure A5-3

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

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
IHF-ESD-04	Event Sequences for Activities Associated with Removal of the Naval Cask Lid and Installing the Naval Canister Lifting Adapter	ESD-04-NVL	Figure A5-8	IHF-RESP-CAN1	Figure A5-9
IHF-ESD-05	Event Sequences for Activities Associated with Transfer of a Cask on CTT from Cask Preparation Area to Cask Unloading Room	ESD-05-HLW	Figure A5-10	IHF-RESP-CAN2-HLW	Figure A5-11,
		ESD-05-NVL	Figure A5-12	IHF-RESP-CAN2-NVL	Figure A5-13
IHF-ESD-06	Event Sequences for Activities Associated with Collision of CTT with Cask Unloading Room Shield Door	ESD-06-HLW	Figure A5-14	N/A	N/A
		ESD-06-NVL	Figure A5-15	N/A	N/A
IHF-ESD-07	Event Sequences for Activities Associated with the Transfer of a Canister from a TC to a WP with CTM	ESD-07-HLW	Figure A5-16	IHF-RESP-CAN1	Figure A5-9
		ESD-07-NVL	Figure A5-17	IHF-RESP-CAN1	Figure A5-9
IHF-ESD-08	Event Sequences for Activities Associated with WP Transfer from WP Loading Room to Closing Position in WP Positioning Room below WP Closure Room	ESD-08-HLW	Figure A5-18	IHF-RESP-WP1	Figure A5-19
		ESD-08-NVL	Figure A5-20	IHF-RESP-WP1	Figure A5-19
IHF-ESD-09	Event Sequences for Activities Associated with Assembly and Closure of the WP	ESD-09-HLW	Figure A5-21	IHF-RESP-WP2	Figure A5-22
		ESD-09-NVL	Figure A5-23	IHF-RESP-WP2	Figure A5-22
IHF-ESD-10	Event Sequences for Activities Associated with the Transfer of the WP from the WP Positioning Room to the WPTT Docking Station	ESD-10-HLW	Figure A5-24	IHF-RESP-WP3	Figure A5-25
		ESD-10-NVL	Figure A5-26	IHF-RESP-WP3	Figure A5-25

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

ESD#	ESD Title	IE Event Tree Name	IE Event Tree Location	Response Tree Name	Response Tree Location
IHF-ESD-11	Event Sequences for Activities Associated with Exporting a WP	ESD-11-HLW	Figure A5-27	IHF-RESP-WP3	Figure A5-25
		ESD-11-NVL	Figure A5-28	IHF-RESP-WP3	Figure A5-25
IHF-ESD-12	Event Sequences for Activities Associated with Direct Exposure During Various Activities	ESD-12A-HLW	Figure A5-29	N/A	N/A
		ESD-12A-NVL	Figure A5-30	N/A	N/A
		ESD-12B-HLW	Figure A5-31	N/A	N/A
		ESD-12B-NVL	Figure A5-32	N/A	N/A
		ESD-12C-HLW	Figure A5-33	N/A	N/A
		ESD-12C-NVL	Figure A5-34	N/A	N/A
IHF-ESD-13	Event Sequences Associated with Fires Occurring in the IHF	ESD-13-HLW-CAN	Figure A5-35	IHF-RESP-FIRE	Figure A5-36
		ESD-13-HLW-CSK	Figure A5-37	IHF-RESP-FIRE	Figure A5-36
		ESD-13-HLW-WP	Figure A5-38	IHF-RESP-FIRE	Figure A5-36
		ESD-13-NVL	Figure A5-39	IHF-RESP-FIRE	Figure A5-36

NOTE: CAN = canister; CTM = canister transfer machine; CTT = cask transfer trolley; ESD = event sequence diagram; HLW = high-level radioactive waste; IHF = Initial Handling Facility; NVL = naval; RC = railcar; RESP = response; TC = transportation cask; TT = transfer trolley; WP = waste package; WPTT = waste package transfer trolley.

Source: Attachment A, Table A5-1

INTENTIONALLY LEFT BLANK

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, an exception being historical data on load drops from cranes. Therefore, FTA is employed to map elements of equipment design and operational features to various failure modes of components down to a level of assembly, termed “basic events” for which historical data is available. Attachment B presents the fault tree logic and stand-alone quantifications.

Much of the equipment used in the IHF is also used in other surface facilities and Intra-Site Operations. Furthermore, a given system, such as the waste package transfer trolley, may affect the event sequences for several operational nodes of the same facility or several kinds of waste forms, as it does for the IHF. Therefore, the logic of the fault trees described in this section and Attachment B are linked to event trees where appropriate via an intermediate top event name that is unique to the event sequence per the waste form involved and operational node. In this way, the logic structure of the system fault tree may be used over and over but, by virtue of the rules feature of SAPHIRE, the inputs to each fault tree can be tailored to fit the event sequence.

The fault trees are linked to the event trees via the initiating event tree rules file and the application of linking fault trees. The rules file specifies the names of the linking fault trees for initiating event and pivotal event fault trees to be substituted into the event tree top events during quantification. The rules files also specify the use of particular values for basic events and other probabilistic factors that affect the event sequence quantification. The linking fault trees have unique names for the facility and the operational nodes for each event tree. The linking fault trees are very simple, usually having a single top event that is an OR gate that connects to one of the system fault trees. This allows for application of unique top event probabilities to the different initiating events modeled in the initiating event tree.

Attachment B, Sections B1 to B5, presents the system fault trees. The present section describes the bases for the system fault trees and the quantification of their top events.

Attachment B, Section B6, presents the linking fault trees used in the IHF analysis. The linking fault trees are self explanatory. No quantification is performed for the linking trees alone.

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

Each of the top events for the initiating event fault trees represent the conditional probability that the top event will occur when the system is put into service. That is, the results of the FTA answer a question such as “What is the probability for each canister lift that the CTM drops the canister, given a lift?” The expected number of canister drop initiating events during the preclosure period is the product of the number of times a canister is lifted during the preclosure operations and the conditional probability of the top event. Such values for the expected number

of canister drops are not, however, developed directly. Instead, the initiating event tree in SAPHIRE links the various fault tree logic models to the canister, or other waste form, and the throughput values to generate the initial portions of event sequence cut sets that are subsequently processed as part of the solution of the complete event sequence that includes pivotal events.

In general, each of the FTAs in Attachment B is developed to include both 1) HFEs, and 2) mechanical failures that result in the occurrence of the top event. The HFEs include postulated unintended operator actions that could potentially occur during the facility activity and, as applicable, hardware failures for those SSCs whose function is to prevent the top event from occurring given the unintended operator action occurs (e.g., interlock). Mechanical failures typically involve random component failures (e.g., electrical, mechanical) 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 cut set. For component failure data that is expressed as “failures per hour,” a “mission time” must be defined. In many instances in the FTA quantification, a mission time of one hour is used if this value is conservative. Where mission time is critical, appropriate times are justified and incorporated into the event sequence quantification. Hardware failure probabilities are taken from the reliability analysis data discussed in Sections 6.3. HFE probabilities are taken from the HFE analysis discussed in Section 6.4.

Uncertainties in the probabilities of basic events are included in the inputs to the SAPHIRE 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 |
- Support systems and subsystems such as transporters (site prime mover, cask transfer trolley), electrical, etc.
- System interactions
- HFEs
- Control logic malfunctions.

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

- Physical description
- Operation
- Control system
- System/pivotal event success criteria
- Mission time
- Fault tree results.

6.2.2 Summary of Fault Tree Analysis

6.2.2.1 Site Prime Mover Fault Tree Analysis

The FTA is detailed in Attachment B, Section B1. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B1 for sources of information on the physical and operational characteristics of the site prime mover (SPM).

6.2.2.1.1 Physical Description

The SPM is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs for both the Intra-Site and within the IHF. A speed limiter is used on the SPM to ensure the maximum speed does not exceed 9 miles per hour. Movement of the SPM with railcars (termed site prime mover railcar (SPMRC)) or SPM with truck trailers (termed site prime mover truck trailer (SPMTT)) within the IHF is limited to the Cask Preparation Area. Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations. The driving and braking power comes directly from the road tires, as they are in contact with the rails. A diesel engine provides the energy to operate the SPM outside the facilities. Inside, the SPM is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

6.2.2.1.2 Operations

In-facility SPM operations begin after the SPM has positioned the railcar or truck trailer outside the IHF. The site prime mover diesel engine is shut down and the outer door is opened. Facility power is connected to the SPM for all operations inside the facility. The operator connects the pendant controller or uses a remote (wireless) controller to move the SPM to push the railcar or truck trailer into the Cask Preparation Area.

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

6.2.2.1.3 Control System

A simplified block diagram of the functional components on the SPMRC/truck trailer is shown in Attachment B, Section B1, Figure B1.2-1.

The control system provides features for preventing initiating events:

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

6.2.2.1.4 System/Pivotal Event Success Criteria

Success criteria for the SPM are the following:

- Prevent SPMRC and SPMTT collisions
- Prevent SPMRC derailments
- Prevent SPMTT rollovers.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event of a fault tree for the SPM.

6.2.2.1.5 Mission Time

A nominal one-hour mission time is used to calculate the failure probability for components having a time-based failure rate. One hour is conservative because it does not require more than one hour to disconnect the SPM from the railcar and remove it from the facility. Otherwise, failure-on-demand probabilities are used.

For railcar derailment, the probability is based on the distance traveled inside the IHF, 0.04 miles, and industry data derailment rate of 1.18E-05 per mile traveled (Attachment C, Table C4-1, DER-FOM).

6.2.2.1.6 Fault Tree Results

The detailed description in Attachment B, Section B1, documents the application of basic event data, CCFs, and HRA.

The SPMRC or SPMTT has three credible failure scenarios:

1. SPM collides with IHF structures for naval and HLW transportation casks.
2. SPMRC derails for both naval and HLW rail transportation casks.
3. SPMTT rollover for only HLW truck transportation casks.

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

Table 6.2-1. Summary of Top Event Quantification for the SPM on a per Cask Basis

Top Event	Mean Probability	Standard Deviation
SPM collides with IHF structures (NVL or HLW on RC or TT)	4.6E-03	1.4E-02
SPMRC derailment (NVL or HLW on RC)	4.7E-07	7.4E-9
SPMTT rollover (HLW on TT)	0.0E+00	0.0E+00

NOTE: IHF = Initial Handling Facility; NVL = naval; HLW = high-level radioactive waste; RC = railcar; SPM = site prime mover; TT = truck trailer.

Source: Attachment B, Figures B1.4-1, B1.4-6, B1.4-12 and B1.4-15

6.2.2.2 Cask Transfer Trolley Fault Tree Analysis

The FTA for the CTT 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 CTT.

6.2.2.2.1 Physical Description

The CTT is an air-powered machine that will be used to transport various vertically oriented transportation casks from the Cask Preparation Area to the Canister Transfer Area. The trolley consists of a platform, a cask support assembly, a pedestal assembly, a seismic restraint system, and an air system.

The CTT will handle a number of different casks, so several different pedestals are used to properly position the cask height. Each pedestal subcomponent is designed for its respective cask to sit down in a “cavity.” In addition, the cask is restrained in the longitudinal and transverse directions by the cavity walls and restrained in the vertical down direction by the pedestal itself. This design also ensures the cask is positioned correctly. The trolley is positioned within a set tolerance under the cask port in the Canister Transfer Area using bumpers and stops that are bolted to the floor of the Cask Unloading Room and which are designed with bolts that would break to allow the CTT to slide during a seismic event.

In addition, the cask is restrained by two electric powered linkage systems that prevent side motions during a seismic event. Different cask diameters are handled by bolting unique interface clamps on the seismic restraints. When the restraint system is properly positioned next to the cask, two locking pins are pneumatically actuated to secure the position of the system. If the locking pins are not secured, the CTT will not be able to power up and move/levitate.

The facility compressed air supply inflates air casters beneath the trolley platform, which allow the CTT to rise above the steel floor. The platform mounted hose reel has an air-powered return, a ball valve shut-off, quick disconnect fittings, and a safety air fuse. A main “off/on” control valve and separate flow control/monitoring valves for each air bearing allow adjustment and verification of pressure/flow for each individual bearing. Interlocks for the air are provided to

verify the main incoming pressure is not too high, and to verify that all bearings have sufficient air pressure.

End mounted turtle style drive units that are 360-degrees steerable are used to steer the CTT. Traction is produced by down-pressure on the wheels provided by a small air bag on each drive unit.

The CTT is evaluated for a collision with another object while carrying the cask. The maximum speed of the drives, 10 feet per minute (ft/min), has been set so that the forces the cask experiences during a seismic event would envelope a collision. The speed is controlled in two ways. First, the electrical control system is designed to provide a proportional control signal to the air valve that produces a speed range of 0 to 10 ft/min. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, restricts the air flow to prevent a “run-away” condition.

6.2.2.2.2 Operation

Initially, the CTT is located in the Cask Preparation Area with the battery fully charged, the seismic restraints retracted, and with no air or electrical power connected. Based on the next planned cask to be loaded onto the trolley, the corresponding pedestal components are installed into the base, and bumpers are bolted onto the seismic restraints and supports. The air hose is then connected to the CTT.

The overhead crane moves a cask onto the pedestal. With the cask still attached to the crane, the operator remotely operates the seismic restraints and secures the cask to the CTT. When the restraints are in place, the locking pins are pneumatically inserted remotely. With the cask secured to the CTT, the overhead crane is disengaged from the cask.

When the locking pins are inserted properly, an interlock allows the air bearings and drive motors to be operated. Once all preparations of the cask are complete, the CTT can be raised and moved to the Cask Unloading Room. Guides bolted to the floor ensure that the CTT can only move forward and back, and will position the CTT so that the cask is directly below the transfer port. Once in position, the air pressure to the bearings is stopped and the CTT rests in position. The shield doors that separate the Cask Preparation Area from the Cask Unloading Room are then closed.

6.2.2.2.3 Control System

The control system is relay-based and includes a pendant station as its operator interface.

No programmable logic controller (PLC) is used – all interlocks are hard wired. The pendant is a standard crane pendant that has all of the controls for the unit including:

- Deadman handle – The operator presses both handles simultaneously to allow air to flow to the CTT system to allow the CTT to levitate or move horizontally.
- Emergency stop button – The operator presses the emergency stop button on the pendant control to stop the CTT (Section B2.2.2).

- Clockwise/counterclockwise momentary switch – The operator turns this switch to turn the drive units for horizontal movement. This rotational characteristic is used to move the CTT to storage or maintenance location after it leaves the Cask Preparation Area.
- Forward/reverse switch – The operator uses the forward/reverse switch to determine the direction of the drive units.
- Variable speed control switch – The operator use the variable speed control switch to adjust the CTT drive speed.
- Cask restraint – The operator uses the selector switch to actuate the motor to close the restraints and automatically engage the locking pin.

During normal operations, the controls operate off a battery system contained on the CTT. Only one operator is needed to drive the CTT since it only travels in one direction when it is carrying a cask.

The main air supply valve is a pilot operated solenoid valve that is fail safe (i.e., it is a spring valve that closes upon loss of electrical power or loss of air pressure). The air supply valve opens when the locking pins actuate the limit switches and the pendant deadman switches are actuated.

6.2.2.2.4 System/Pivotal Event Success Criteria

Success criteria for the CTT are the following:

- Ensure the CTT remains stationary with no spurious movement during transportation cask placement onto the CTT, transportation cask preparation, or during unloading
- Prevent collisions while moving the CTT with cask from the Cask Preparation Area to the Cask Unloading Room.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event of a fault tree for the CTT.

6.2.2.2.5 Mission Time

In all cases a conservative mission time of one hour per cask transfer is used for each fault tree.

6.2.2.2.6 Fault Tree Results

The detailed analysis is presented in Attachment B, Section B2.

There are four fault trees associated with the CTT:

1. Spurious movement in the Cask Preparation Area while loading a cask onto the CTT
2. Spurious movement in the Cask Preparation Area during unbolting and lid adapter installation
3. Spurious movement in the Cask Unloading Room while unloading canisters from the CTT
4. Collision with an object or structure while moving a cask from the Cask Preparation Area to the Cask Unloading Room.

The results of the analysis are summarized in Table 6.2-2. Four fault trees were developed where the top events correspond to one of the scenarios listed above.

Table 6.2-2 Summary of Top Event Quantification for the CTT

Top Event	Mean Probability	Standard Deviation
Spurious movement of the CTT during cask loading	1.7E-9	7.8E-9
Spurious movement of the CTT during cask preparation	1.2E-4	2.0E-4
CTT collision into structure	1.0E-3	1.2E-3
Spurious movement during canister transfer	<1E-9	<1E-9

NOTE: CTT = cask transfer trolley.

Source: Attachment B, Figures B2.4-1, B2.4-5, B2.4-8 and B2.4-12

6.2.2.3 Slide Gate and Shield Door Fault Tree Analysis

The IHF Cask Unloading Room and Waste Package Loading Room have a port slide gate providing access to the Canister Transfer Area. There is a shield door between the Cask Preparation Area and the Cask Unloading Room, between the Waste Package Loading Room and the Waste Package Positioning Room, and between the Waste Package Positioning Room and the Waste Package Loadout Room. The shield doors and port slide gates provide shielding during canister unloading and loading.

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 equipment shield doors and slide gates.

6.2.2.3.1 Physical Description

The shield doors consist of a pair of large heavy doors that close together. The doors are operated by individual motors that have over-torque sensors to prevent crushing an object. Each door has two position sensors to indicate either a closed or open door, and an obstruction sensor prevents the doors from closing on an object. The shield doors and port slide gate are

interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand lever that must be enabled by an enable/disable switch. An emergency open switch exists enabling the doors to be opened in case of an emergency situation.

Similar to the shield doors, the port slide gate consists of two gates that close together between the loading/unloading rooms and the Canister Transfer Area. The gates are operated by individual motors that also have over-torque sensors. Each gate has limit switches to indicate open or closed gates. A CTM skirt-in-place switch is interlocked to the port slide gate to prevent the gates from opening without the CTM in place and a CTM in-place bypass hand switch exists for maintenance activities. Slide gate operation is controlled by a hand switch coupled with an enable/disable switch and shield door interlocks prevent the slide gate from opening when the shield door is open. Open/closed and CTM in-place indicators exist to assist operators in their activities.

6.2.2.3.2 Operation

The Cask Unloading Room shield doors are opened to allow the CTT to enter the room. Once the CTT is positioned properly in an unloading room, shield doors are shut in preparation for removing canisters from the cask. Once the shield doors are shut, the cask port slide gate may be opened to allow the CTM to perform cask unloading operations. Waste package loading operations in the Waste Package Loading Room are analogous to cask unloading operations. The waste package port slide gate may be opened to allow waste package loading access if the shield doors are closed. Once loading is complete and the slide gate is closed, the shield doors may be opened to allow the WPTT to carry the waste package into the Waste Package Positioning Room.

6.2.2.3.3 Control System

The control systems have hard-wired interlocks for the following functions:

- The shield door system will not have any test, maintenance, or other modes/settings that will allow bypass of interlocks
- A single interlock prevents the port slide gate from opening when the CTM skirt is not in place
- An obstruction sensor is provided to detect objects between the shield doors and prevent door closure initiation
- Motor over-torque sensors are provided to prevent shield doors from causing damage to casks or waste packages in the event of closure on a conveyance
- Shield doors and slide gates are equipped with redundant hardwired interlocks to prevent one from opening when the other is open.

6.2.2.3.4 System/Pivotal Event Success Criteria

Success criteria for the shield door and slide gate are the following:

- Prevent inadvertent opening of shield door
- Prevent inadvertent opening of the slide gate
- Prevent shield door closing on conveyance.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event for a fault tree for the CTT.

6.2.2.3.5 Mission Time

Most of the basic events in the fault tree models are “failure on demand” for equipment failures and “failure per operation” for HFEs. A mission time of one hour was used to calculate the probability of a spurious signal being sent due to PLC failure.

6.2.2.3.6 Fault Tree Results

The detailed analysis is presented in Attachment B3.

The slide gate and shield door system has three credible failure scenarios:

1. Inadvertent opening of the shield door
2. Inadvertent opening of the slide gate
3. Shield door closes on conveyance.

The results of the analysis are summarized in Table 6.2-3. Three fault trees were developed where the top events correspond to one of the scenarios listed above.

Table 6.2-3. Summary of Top Event Quantification for the Shield Doors and Slide Gate

Top Event	Mean Probability	Standard Deviation
Inadvertent Opening of the Shield Door	1.3E-6	3.3E-8
Inadvertent Opening of the Slide Gate (electromechanical failures only)	<1E-9	<1E-9
Shield Door Closes on Conveyance	3.1E-5	5.4E-5

Source: Attachment B, Figures B3.4-1, B3.4-4, B3.4-7, and (for HFEs associated with inadvertent opening of the slide gate) B6.4-1

6.2.2.4 Canister Transfer Machine Fault Tree Analysis

The FTA is detailed in Attachment B, Section B4. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B4 for sources of information on the physical and operational characteristics of the CTM.

6.2.2.4.1 Physical Description and Functions

The CTM is located and operated in the Canister Transfer Area of the IHF. The CTM is used to transfer waste canisters from a cask on the CTT to a waste package supported by the WPTT. The ports in the floor of the Canister Transfer Area provide access to the Cask Unloading Room and Waste Package Loading Room.

The CTM is an overhead crane bridge with two trolleys. The first is a canister hoist trolley with a grapple attachment and hoisting capacity of 70 tons. The second is a shield bell trolley that supports the shield bell. The bottom end of the shield bell is attached to a larger chamber to accommodate cask lids. The CTM bottom plate assembly supports a thick motorized slide gate. The CTM slide gate, when closed, provides bottom shielding for the canister once the canister is inside the shield bell. Around the perimeter of the bottom plate, a thick shield skirt is provided which can be raised and lowered to prevent lateral radiation shine during a canister transfer operation.

6.2.2.4.2 Operations

The CTM transfers waste canisters from the transportation cask to the waste package. For this operation, a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. In the case of the naval SNF canister, the lifting fixture has been affixed to the canister and it is ready to be grappled to the CTM. In the case of the HLW cask, the cask lid is in place but unbolted. Similarly, an empty waste package secured by the WPTT is positioned under the adjacent transfer port in the Waste Package Loading Room.

The CTM is moved to a position over the center of the port above the loaded cask. The shield skirt is lowered to rest on the floor, and the port slide gate is opened. The CTM slide gate is opened and the canister grapple is lowered through the shield bell to engage and lift the cask lid. The port slide gate is closed and the shield skirt is raised so the CTM can be moved to a cask lid staging area to set down the lid.

The CTM is moved back over the port above the loaded cask to align the canister grapple. The shield skirt is lowered, the port slide gate is opened, and the grapple is lowered to engage the canister lifting feature. The canister is raised into the shield bell. The CTM slide gate and the port slide gate are closed and the shield skirt is raised so the CTM can be moved to the port above the empty waste package. The waste package loading operations are essentially the reverse of the cask unloading.

The CTM canister grapple is used for handling naval canisters. Other grapples are used to access the smaller diameter HLW canisters. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Area floor and lowering the CTM hoist until the CTM grapple is accessible in the room below.

The CTM is normally controlled from the facility operations room (also referred to in this document as the control room), but a local control station is also provided.

Generally, under off-normal conditions, the CTM is not in operation. Following a loss of alternating current offsite power, all power to the CTM motors (e.g., hoist, bridge, trolley, and

bell trolley) is lost. If a transfer is underway when power is lost, all of the CTM motors stop and the hoist holding brake engages. Operations are suspended until power is restored and the load can be safely moved. Under other off-normal conditions, transfer operations would be suspended and the CTM would remain idle.

6.2.2.4.3 Control System

Hard-wired interlocks are provided to:

- Prevent bridge and trolley movement when the CTM shield skirt is lowered
- Prevent raising the shield bell skirt when the port slide gate is open
- Prevent hoist movement unless the grapple is fully engaged or disengaged
- Stop the hoist and erase the lift command when a canister clears the CTM slide gate
- Stop a lift before upper lift height limits are reached (two interlocks are provided for this function)
- Prevent opening of the port slide gate unless the CTM shield skirt is lowered and in position
- Prevent hoist movement unless the CTM shield skirt is lowered
- Prevent lifting of a load that exceeds the operational weight limit of the CTM (load cells).

Some of these interlocks can be bypassed during maintenance. The most significant of these interlocks that can be bypassed is the interlock between the CTM shield skirt position and the position of the port slide gate (The shield skirt cannot be raised unless the slide gate is closed or the maintenance bypass is engaged.). The design of the grapple interlock ensures that the bypass is voided when a canister is grappled.

Many of the operational controls are provided by non-ITS PLCs. Spurious or failed operation of the PLCs is in the FTA when such operation may contribute to a drop or collision event.

6.2.2.4.4 System/Pivotal Event Success Criteria

Success criteria for the CTM are the following:

- Prevent a canister drop from a height below the design basis height for canister damage from any cause during the lifting, lateral movement, and lowering portions of the canister transfer
- Prevent a canister drop from above the canister design limit drop height from any cause during the lifting, lateral movement, and lowering portions of the canister transfer

- Prevent a drop of any object onto the canister from any cause during the lifting, lateral movement, and lowering portions of the canister transfer
- Prevent a collision between the canister and the shield bell or Canister Transfer Area floor from any cause during the lifting, lateral movement, and lowering portions of the canister transfer
- Prevent CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the IHF.

The failure to achieve each success criterion defines the top event for a fault tree for the CTM.

6.2.2.4.5 Mission Time

The mission time for the ITS CTM is set to one hour.

6.2.2.4.6 Fault Tree Results

The analysis is detailed in Attachment B, Section B4.

There are five scenarios associated with the CTM that represent potential initiating events:

1. The CTM drops a canister from a height below the design basis height for canister damage (this includes canister drops within the shield bell once the CTM slide gate has been closed and drops through a Canister Transfer Area port to the loading or unloading room that can occur before the CMT slide gate is closed).
2. The CTM drops a canister from a height above the design basis height for canister damage.
3. The CTM drops an object onto a canister.
4. The CTM, while carrying a canister, moves in such a manner (spurious movements, exceeding bridge or trolley end of travel limits) as to cause an impact of the canister with the shield bell.
5. The CTM moves when the canister being transferred is being lifted and is between the IHF floors resulting in shear forces being applied to the canister.

The results of the analysis are summarized in Table 6.2-4. Five fault trees were developed. The top events correspond, to the five potential initiating events defined above.

Table 6.2-4. Summary of Top Event Quantification for the CTM

Top Event	Mean Probability	Standard Deviation
CTM drop below the design basis height	2.1E-4	2.3E-4
CTM high drops from two blocking events	2.8E-8	1.6E-7
Drop of object onto cask	1.4E-5	1.2E-5
CTM collision results in an impact to canister	3.9E-6	2.7E-7
CTM Shear	6.7E-9	1.4E-8

NOTE: CTM = canister transfer machine.

Source: Attachment B, Figures B4.4-1, B4.4-15, B4.4-20, B4.4-34, and B4.4-41

6.2.2.5 Waste Package Transfer Trolley Fault Tree Analysis

The FTA for the WPTT is detailed in Attachment B, Section B5. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification. See Attachment B, Section B5 for sources of information on the physical and operational characteristics of the WPTT.

6.2.2.5.1 Physical Description and Functions

The WPTT is an electrically powered machine used to transport the waste package containing various waste canisters from the Waste Package Loading Room to the Waste Package Positioning Room and then to the waste package transfer carriage docking station in the Waste Package Loadout Room. The WPTT consists of a shielded enclosure that holds the waste package, waste package pallet, waste package transfer carriage, and pedestal. The shielded enclosure acts as a radiation shield to minimize radiation to the surroundings. The enclosure pivots between a vertical and horizontal position for waste package loading and unloading.

The WPTT travels on rails between the Waste Package Loading Room and the docking station. The crane rails supporting the WPTT are gapped in multiple locations. Power is supplied to the motor by a third rail system and the maximum speed is less than 20 ft/min, as required by ASME NOG-1-2004 (Ref. 2.2.7) and established by the size of the drive motor and the gear drive system. The WPTT includes seismic rail clamps and rails anchored to the floor to ensure the stability of the WPTT during a seismic event.

The rotation of the shielded enclosure from vertical to horizontal is driven by worm gear mechanisms and is also powered by the third rail system. Each of the rotation mechanisms is sized to rotate the full design load (no greater than 178,200 lbs) on its own and at a speed no faster than 18-degrees per minute. The worm gear mechanism has the inherent property to self lock to prevent uncontrolled tilt down.

The waste package transfer carriage is a wheeled platform which carries the waste package pallet and waste package. The transfer carriage is moved by a mechanical screw-driven carriage retrieval assembly that places an empty waste package in the shielded enclosure and retrieves the loaded and sealed waste package from the shielded enclosure for interfacing with the TEV.

6.2.2.5.2 Operation

The waste package loadout operation begins with an empty waste package being loaded into the WPTT. The WPTT is locked into the waste package transfer carriage docking station and rotated to the horizontal position. The transfer carriage with an empty waste package and pallet is moved into the shielded enclosure of the WPTT via the waste package transfer carriage docking station's waste package retrieval assembly. The shielded enclosure is rotated into the vertical position and the shield ring is lowered and locked into position on top of the shielded enclosure by the waste package handling crane.

The WPTT is unlocked from the waste package transfer carriage docking station and is remotely driven into the Waste Package Loading Room. The WPTT is situated so that the empty waste package is directly beneath the center of the port slide gate that separates the Waste Package Loading Room from the Canister Transfer Area.

The WPTT is positioned in the Waste Package Loading Room and the port slide gate is opened to allow the waste canister(s) to be lowered into the empty waste package using the CTM.

After the waste package is loaded, the inner lid is placed onto the waste package, and the port slide gate closed, the WPTT moves to the Waste Package Positioning Room. At this station, the inner lid is welded in place, and the weld is inspected. The air within the waste package is replaced by helium with a helium purging operation. After the inner lid is inspected for leakage, the outer lid is positioned and welded in place. The welds of the outer lid are inspected to ensure the waste package is properly sealed.

After the waste package is sealed, the WPTT is moved into the Waste Package Loadout Room where it is locked into the waste package transfer carriage docking station. The shield ring is remotely removed with the waste package handling crane and the shielded enclosure is rotated into the horizontal position. The waste package carriage retrieval assembly is then retracted to pull the carriage and waste package out of the shielded enclosure to a position where the TEV is able to lift the waste package and pallet off the carriage.

6.2.2.5.3 Control System

Interlocks prevent translational or rotational motion of the WPTT while a canister is being loaded into the waste package (i.e., when the waste package slide gate is open) or while the waste package is being withdrawn from the shielded enclosure on the transfer carriage. The shielded enclosure is not able to rotate in either direction unless the WPTT is locked into the waste package transfer carriage docking station and the waste package carriage retrieval assembly is completely extended or retracted. Interlocks also prevent over-travel of the trolley and travel through portals when the shield doors are closed. Manually actuated, hardwired emergency stop buttons are available at all control locations to allow power to be removed from the drive motors.

6.2.2.5.4 System/Pivotal Event Success Criteria

Success criteria for the WPTT are the following:

- Ensure the WPTT in the Waste Package Loading Room remains stationary with no movement while loading a canister onto the shielded enclosure.
- Ensure the WPTT travels at a speed no greater than 40 ft/min and that the operator is in control and able to stop the WPTT as required.
- Ensure the WPTT does not derail during the transport process.
- Prevent premature tilt-down of the shielded enclosure during transfer.
- Prevent premature tilt-up or WPTT departure during loadout operations.

Various design features are provided to achieve each of the success criteria. The failure to achieve each success criterion defines the top event for a fault tree for the WPTT.

6.2.2.5.5 Mission Times

A conservative mission time of one hour per canister was used for canister and waste package transfers through the process for each fault tree.

6.2.2.5.6 Fault Tree Results

The WPTT fault tree analysis is detailed in Attachment B, Section B5.

There are five fault trees associated with the WPTT that represent potential initiating events:

1. Spurious movement in the Waste Package Loading Room while loading a canister into the waste package.
2. Impact of the WPTT with a structure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
3. Derailment of the WPTT while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
4. Premature tilt-down of the shielded enclosure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
5. WPTT or carriage malfunctions while extracting the carriage and waste package from the shielded enclosure at the Waste Package Loadout Room.

The results of the analysis are summarized in Table 6.2-5.

Table 6.2-5. Summary of Top Event Quantification for the WPTT

Top Event	Mean Probability	Standard Deviation
Spurious movement of the WPTT in the loading area while loading the WP with canisters	<1E-9	<1E-9
Impact of the WPTT with a structure	3.0E-3	3.5E-3
Derailment of the WPTT	4.7E-7	7.4E-9
Premature tilt-down of the shielded enclosure	2.7E-5	3.3E-5
Malfunction of WPTT or WP transfer carriage	1.0E-3	1.1E-3

NOTE: WP = waste package; WPTT = waste package transfer trolley.

Source: Attachment B, Figures B5.4-1, B5.4-7, B5.4-11, B5.4-14 and B5.4-17

6.2.2.6 Site Transporter Fault Tree Analysis

The site transporter is not used in the IHF.

6.2.2.7 HVAC Fault Tree Analysis

The HVAC in the IHF is not designated as ITS equipment and therefore does not provide confinement capability in the event of a release.

6.2.2.8 AC Power Fault Tree Analysis

There are no ITS AC power requirements for the IHF.

6.2.2.9 Potential Moderator Sources

6.2.2.9.1 Internal Floods

Internal floods are potential sources of moderator addition into a canister associated with pivotal events in the event sequences included in Section 6.1. The internal flooding analysis considers all waste handling facilities.

During most of its handling at the repository, a canister is surrounded by at least one other barrier to water intrusion: a transportation cask, 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-interlock preaction sprinkler system in areas where waste forms are handled (Ref. 2.2.16, Ref. 2.2.29, Ref. 2.2.25, and Ref. 2.2.34). Such systems, which require both actuation of smoke and flame detectors to allow the preaction valve to open and heat actuation of a fusible link sprinkler head to initiate suppression, have a very low frequency of spurious operation. A 30-day period from the occurrence of the canister breach to the time definitive action can be taken to prevent introduction of water into the canister is reasonable and is the same as the period used to assess dose for a radiological release. The spurious actuation frequency over a 30-day mission time after a breach is calculated below.

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

- Spurious preaction valve opens before canister breach \times failure of a sprinkler head during post-breach mission time (30 days)
- Failure of a sprinkler head during building evacuation \times water left in dry piping after last test (1st quarter following annual test).

The probability of sprinkler failure is estimated using an individual sprinkler head failure frequency of $1.6\text{E-}6/\text{yr}$ (Ref. 2.2.12, Table 1), the estimated number of sprinklers (1 per 130 ft^2 based on NFPA 13 (Ref. 2.2.55, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2.21)). For example, the area of CRCF Waste Package Loadout Room 1015 is listed as $7,470\text{ ft}^2$ in *Liquid Low-Level Waste Collection Calculation (C2 and C3 Contamination Zone)* (Ref. 2.2.21). At $130\text{ ft}^2/\text{sprinkler}$, 58 sprinklers are estimated. The failure of any sprinkler in the room is then estimated to be $58 \times 1.6\text{E-}6/\text{yr} \times 1/8760\text{ hrs/yr}$, or $1.1\text{E-}8/\text{hr}$.

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

The value of the first cut set is $(1.6\text{E-}6/\text{yr} \times 1/8760\text{ hr/yr} \times 720\text{ h}) \times (8.1\text{E-}7/\text{hr} \times 720\text{ h}) = 8\text{E-}11/\text{sprinkler head}$. The second cut set is more significant: 0.025 (human error screening value) $\times (1.6\text{E-}6/\text{yr} \times 1/8760\text{ hr/yr} \times 720\text{ h}) = 3\text{E-}9/\text{sprinkler head}$.

Applying the sum of these values, $3\text{E-}9/\text{sprinkler head}$, to the number of sprinklers calculated for the waste handling areas of the four facilities results in the following estimates of the probability of spurious sprinkler actuation found in Table 6.2-6.

Table 6.2-6. Probability of Spurious Sprinkler Actuation

Facility	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, IHF = Initial Handling Facility, RF = Receipt Facility, WHF = Wet Handling Facility.

Source: Ref. 2.2.21 for area

Piping carrying water is present in the waste form handling areas of the CRCF, IHF and WHF. Piping lengths in these areas of the CRCF and WHF are below 100 feet per facility. For the IHF, approximately 6,800 feet of piping runs no closer than 60 feet of the cask unbolting area (Ref. 2.2.79). Even the length of piping in the IHF has little impact post-breach, as the probability of a pipe crack or rupture in a 30-day period following a potential breach is 1.4E-03. (Due to the early nature of the design, the only available reference for the length of pipe is this interoffice memorandum. Due to the conservatisms used to determine the length of pipe, this information does not require verification.)

The probability of a pipe crack in a 30-day period was estimated using the pipe leak data from *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928* (Ref. 2.2.39, 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 of the conditioning applied to the fluids in the systems will be that typical of the commercial nuclear power plant:

External leak small (1 to 50 gallon/min): Leak rate = 2.5E-10 hr⁻¹ft⁻¹

External leak large (> 50 gallon/min): Leak rate = 2.5E-11 hr⁻¹ft⁻¹

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

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

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

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

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

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

The above applies to event sequences that do not involve fires as an initiating event. During fire initiating event sequences, fire suppression would actuate in the locations sufficiently heated by the fire. The fire initiating event analysis is described in Section 6.5, and the conditional probability of canister failure owing to fires is described in Section 6.3. The analysis is performed without the salutary effects of fire suppression in order to demonstrate large margins of safety during fire event sequences. Furthermore, the location of each fire is analyzed as around the outer shell of the overpack that surrounds the canister which neither accounts for the CTT or WPTT enclosures that surround the overpack nor the elevated position of the canisters with respect to a fire on the floor. The frequency of containment breach due to fire is significantly overestimated because of this conservative approach.

6.2.2.9.2 Lubricating Fluid

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a gearbox with a leak pan below it capable of capturing the entire gearbox fluid inventory. An estimate of the leakage rate through the gearbox and drip pan is found by multiplying the all-modes gearbox, motor failure frequency of $0.88\text{E-}06$ per hour (Ref. 2.2.36, p. 2-104 and Section 6.3) over 50 years by the conditional probability of oil pan failure. A loss of lubrication would fail the crane operation and also be detected by oil-pressure indicators. The conditional probability of oil pan failure may be estimated by analogy to receiver tank leakage during the interval between gearbox failure and detection. The interval is conservatively estimated to be 30 days. The all-modes failure rate of a receiver tank is $0.34\text{E-}06$ per hour (Ref. 2.2.36, p. 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:

$$0.88\text{E-}06/\text{hr} \times 50 \text{ yrs} \times 8760 \text{ hr/yr} \times 0.34\text{E-}06/\text{hr} \times 720 \text{ hr} = 9\text{E-}05 \text{ over the preclosure period.}$$

This probability is conservatively 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.

6.3 DATA UTILIZATION

6.3.1 Active Component Reliability Data

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

6.3.1.1 Industry-wide Reliability Data for Active Components

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

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

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

Given the fact that the YMP is a relatively unique facility (although portions are similar to the spent fuel handling and storage areas of commercial nuclear plants), the data development perspective is to collect as much relevant failure estimate information as possible to cover the spectrum of equipment operational experience. It is reasonable to expect that the YMP

equipment would fall within this spectrum (Section 3.2.1). The scope of the sources selected for this data set is therefore deliberately broad to take advantage of the combined experience of many facilities, not a single plant. It is then intended to provide a combined estimate that reflects as best as possible the uncertainty ranges of the individual estimates. This ensures that the data are not skewed towards the possibly atypical behavior of one particular plant, industry or operating environment. The combinatorial process, utilizing Bayes' theorem, is discussed in the following subsection.

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

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

6.3.1.2 Application of Bayes' Theorem to PCSA Database

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

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, NUREG/CR-6823 (Ref. 2.2.10). For the PCSA, the method known as "parametric empirical Bayes" is primarily used. This permits a variety of different sources to be statistically combined and compared, whether the inputs are expressed as the number of failures and exposure time or demands, or as means and lognormal error factors.

A typical application of Bayes' theorem is illustrated as follows. A failure rate for a given component is needed for a fault tree, e.g., a fan motor in the HVAC system. There is no absolute value for the failure rate, but there are several data sources for the same kind of fan and/or

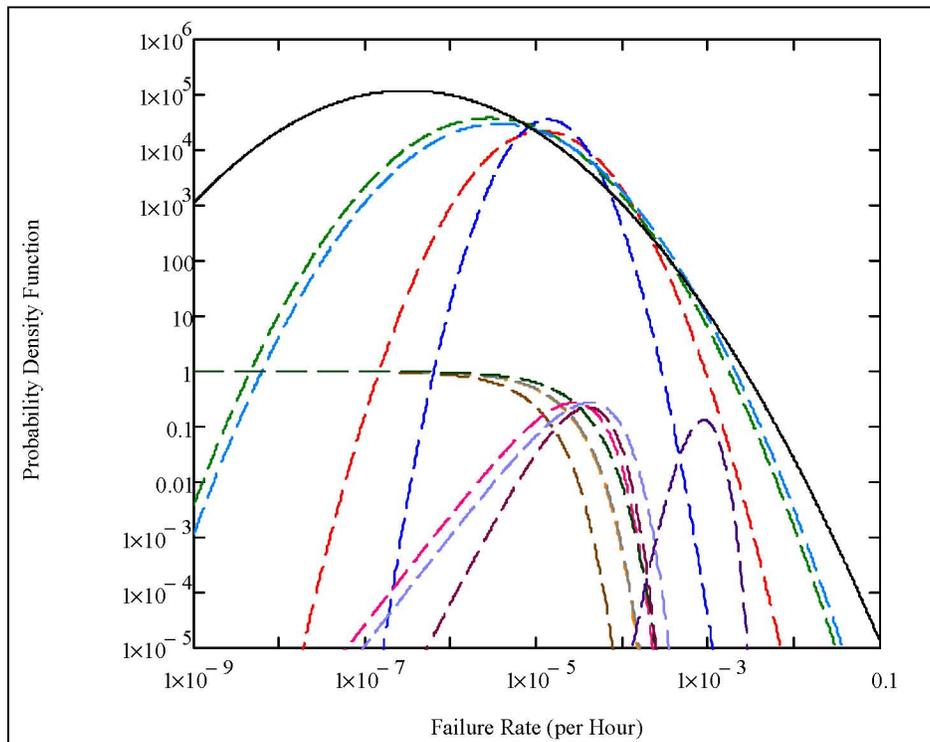
similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data to the YMP introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying available data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the “prior” probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.
2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trials if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur over a certain exposure, operational, or test duration.
3. Update the probability distribution for the failure rate based on the new body of evidence.

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

For the analysis presented herein, MathCad is used to calculate the population-variability (prior) distributions of active components. As described in Attachment C, Section C2.1, the method of “The Combined Use of Data and Expert Estimates in Population Variability Analysis” (Ref. 2.2.49, 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, ν and τ , respectively the mean and standard deviation of the associated normal distribution, are determined. Calculating ν 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 ν 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 ν 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 Jeffreys' noninformative prior distribution (i.e., gamma for time-related failure modes and beta for demand based failure modes).

Example implementations of the methods used for these cases are provided in Attachment C.

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. 2.2.44), the Multiple Greek Letter method (Ref. 2.2.53), which is an extension of the Beta Factor method, and the Alpha Factor method (Ref. 2.2.54). In a parametric model, the probability of two or more components failing by a CCF is estimated by use of the equations provided in Section 4.3.3.3.

For the PCSA, common-cause failure rates or probabilities are estimated using the alpha factor method (Ref. 2.2.54) because it is a method that includes a self-consistent means for development of uncertainties.

The data analysis reported in NUREG/CR-5485 (Ref. 2.2.54) 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 C3).
4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produces prior distributions for the alpha factors. The results are the mean alpha factors and uncertainty bounds, reported in NUREG/CR-5485 (Ref. 2.2.54, Table 5-11) and reproduced in Attachment C, Table C3-1.

These alpha-factors values are used directly for failure-on-demand events (e.g., pump failure to start). For failure-to-operate events (e.g., pump fails to run), the alpha factor provided is divided by 2. 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) is 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 common-cause failure probability.

Similarly, for the two-out-of-two operational failure, the mean alpha factor identified above is divided by 2 (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 4

(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 275 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 IHF Analysis

Table 6.3-1 summarizes the active component reliability data used in each basic event of the IHF 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 Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CR--IEL001--IEL-FOD	Interlock A from Slide Gate Fails	1	2.75E-05	–	–
51A-CR--IEL00A--IEL-FOD	Interlock A from Slide Gate Fails	1	2.75E-05	–	–
51A-CR--IEL00B--IEL-FOD	Interlock B from Slide Gate Fails	1	2.75E-05	–	–
51A-CR--IELCCF--IEL-CCF	Common Cause Failure of Interlocks from Slide Gate	C	1.29E-06	–	–
51A-CR--PLC001--PLC-SPO	Inadvertent Signal Sent Due to PLC Failure	3	3.65E-07	3.65E-07	1
51A-CR-IEL001-IEL-FOD	Interlock A from Slide Gate Fails	1	2.75E-05	–	–
51A-CR-IEL002-IEL-FOD	Interlock B from Slide Gate Fails	1	2.75E-05	–	–
51A-CR-IELCCF-IEL-FOD	Common Cause Failure of Interlocks from Slide Gate	C	1.29E-06	–	–
51A-CR-PLC001-PLC-SPO	Inadvertent Signal Sent due to PLC Failure	3	3.65E-07	3.65E-07	1
51A-CRN-BRIDGMTR-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
51A-CRN-BRIDGMTR-MOE-SPO	Crane Bridge Motor (Electric) Spurious Operations	3	6.74E-07	6.74E-07	1
51A-CRN-HSTTRLMO-MOE-FSO	Crane Hoist Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
51A-CRN-PLC0101--PLC-SPO	Crane Bridge Motor PLC Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CRN3-2-BLOCK-CRN-TBK	300-Ton Crane 2-Block Drop	1	4.41E-07	–	–
51A-CRN3-2BLKDON-CRN-TBK	300-Ton Crane 2-Block Crane Drop On	1	4.41E-07	–	–
51A-CRN3-DROPHLW-CRN-DRP	300-Ton Crane - Drop of HLW	1	3.16E-05	–	–

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CRN3-DROPNVL-CRN-DRP	300-Ton Crane - Drop of Naval Cask	1	3.16E-05	–	–
51A-CRN3-DROPON--CRN-DRP	300-Ton Crane Drop On	1	3.16E-05	–	–
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield Skirt Position Switch 0112 Fails	3	5.78E-05	7.23E-06	8
51A-CTM-#ZSH0112-ZS-FOH	Shield Skirt Position Switch Fails	3	5.78E-05	7.23E-06	8
51A-CTM--121122-ZS--CCF	CCF CTM Upper Limit Position Switches	C	1.38E-05	–	–
51A-CTM--330121--ZS--FOD	CTM Hoist First Upper Limit Switch 0121 Failure on Demand	1	2.93E-04	–	–
51A-CTM--330122--ZS--FOD	CTM Final Hoist Upper Limit Switch 0122 Failure Demand	1	2.93E-04	–	–
51A-CTM--CBL0001-CBL-FOD	CTM Hoist Wire Rope Breaks	1	2.00E-06	–	–
51A-CTM--CBL0001-WNE-BRK	CTM Hoist Wire Rope Breaks	1	2.00E-06	–	–
51A-CTM--CBL0002-CBL-FOD	CTM Hoist Wire Rope Breaks	1	2.00E-06	–	–
51A-CTM--CBL0002-WNE-BRK	CTM Hoist Wire Rope Breaks	1	2.00E-06	–	–
51A-CTM--CBL0102-WNE-CCF	CCF CTM Hoist Wire Ropes Break	C	9.40E-08	–	–
51A-CTM--DRTRN-CT--FOD	CTM Drive Train Protection and Fail Detection Controller Failure	1	4.00E-06	–	–
51A-CTM--DRUM001-DM--FOD	Hoisting Drum Structural Failure	1	4.00E-08	–	–
51A-CTM--DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Failure on Demand	1	5.02E-05	–	–
51A-CTM--DRUMBRK-BRP-FOH	CTM Drum Brake (Pneumatic) Failure to Hold	3	2.01E-04	8.38E-06	24
51A-CTM--EQL-SHV-BLK-FOD	Equalizer Sheaves Structural Failure	1	1.15E-06	–	–
51A-CTM--GRAPPLE-GPL-FOD	Grapple Failure on Demand	1	1.15E-06	–	–

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CTM--HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	3	6.50E-06	6.50E-06	1
51A-CTM--HOLDBRK-BRK-FOD	Brake Failure on Demand	1	1.46E-06	–	–
51A-CTM--HOLDBRK-BRK-FOH	CTM Holding Brake (Electric) Fails to Hold	3	3.52E-05	4.40E-06	8
51A-CTM--IMEC125-IEL-FOD	CTM Hoist Motor Control Interlock Fails on Demand	1	2.75E-05	–	–
51A-CTM--LOWERBL-BLK-FOD	CTM Lower Sheaves Structural Failure	1	1.15E-06	–	–
51A-CTM--MISSPOOL-DM-MSP	CTM Miss-Spool Event	3	6.86E-07	6.86E-07	1
51A-CTM--OVERSP--ZS--FOD	CTM Hoist Motor Speed Limit Switch Failure on Demand	1	2.93E-04	–	–
51A-CTM--OVERSP--ZS-FOD	Hoist Motor Speed Limit Switch Fails	1	2.93E-04	–	–
51A-CTM--PORTGT1-MOE-SPO	Spurious Port Gate 1 Motor Operation	3	6.74E-07	6.74E-07	1
51A-CTM--PORTGT1-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CTM--PORTGT2-MOE-SPO	Spurious Port Gate 2 Motor Operation	3	6.74E-07	6.74E-07	1
51A-CTM--PORTGT2-PLC-SPO	Programmable Logic Controller Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CTM--TROLLY-MOE-SPO	Trolley Motor Spurious Operation	3	6.74E-07	6.74E-07	1
51A-CTM--UPPERBL-BLK-FOD	Upper Sheaves Structural Failure	1	1.15E-06	–	–
51A-CTM--WT0125--SRP-FOD	Pressure Sensor Fails on Demand	1	3.99E-03	–	–
51A-CTM--WTSW125-ZS--FOD	Load Cell Limit Switch Fails	1	2.93E-04	–	–
51A-CTM--YS01129-ZS--FOD	CTM Drum Brake Control Circuit Limit Switch 1129 Failure	1	2.93E-04	–	–
51A-CTM--ZSH0111-ZS--SPO	Grapple-Engaged Limit Switch Spurious Operation	3	1.28E-06	1.28E-06	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CTM-ASD0122#-CTL-FOD	CTM Hoist Adjustable Speed Drive Controller Fails	1	2.03E-03	–	–
51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge Motor Torque Limiter Failure	3	2.86E-02	8.05E-05	360
51A-CTM-BREDGMTR-PR-FOH	Bridge Passive Restraints (end stops) Fail	3	1.95E-06	4.45E-10	4380
51A-CTM-BRIDGETR-#PR-FOH	Passive Restraint (Bumper) Failure	3	1.95E-06	4.45E-10	4380
51A-CTM-BRIDGETR-MOE-FSO	Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
51A-CTM-BRIDGMTR-IEL-FOD	CTM Shield Skirt-Bridge Motor Interlock Failure	1	2.75E-05	–	–
51A-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation - Shear	3	6.74E-08	6.74E-07	0.1
51A-CTM-BRIDTR-CT-FOD	CTM Bridge Motor Controller Failure	1	4.00E-06	–	–
51A-CTM-DRTRN-CT-FOD	CTM Drive Train Protection and Fail Detection Controller Failure	1	4.00E-06	–	–
51A-CTM-DRUMBRK-BRP-FOD	CTM Drum Brake (Pneumatic) Fails on Demand	1	5.02E-05	–	–
51A-CTM-HC0104###-HC-FOD	Handheld Radio Remote Controller Failure to Stop (on Demand)	1	1.74E-03	–	–
51A-CTM-HOISTMT-MOE-FTR	CTM Hoist Motor (Electric) Fails to Run	3	6.50E-06	6.50E-06	1
51A-CTM-HOISTMTR-MOE-FSO	CTM Hoist Motor (Electric) Fails to Shut Off	3	1.35E-08	1.35E-08	1
51A-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation	3	6.74E-08	6.74E-07	0.1
51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist Motor Torque Limiter Failure	3	2.86E-02	8.05E-05	360
51A-CTM-HSTTRLLY-IEL-FOD	CTM Shield Skirt Hoist Trolley Motor Interlock Failure	1	2.75E-05	–	–

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CTM-HSTTRLLY-MOE-SPO	Hoist Trolley Motor (Electric) Spurious Operation	3	6.74E-07	6.74E-07	1
51A-CTM-IMEC125-IEL-FOD	CTM Hoist Motor Controller Interlock Fails on Demand	1	2.75E-05	–	–
51A-CTM-OPSENSOR-SRX-FOH	Canister Above CTM Slide Gate Optical Sensor Fails	3	4.70E-06	4.70E-06	1
51A-CTM-PLC0101-PLC-SPO	CTM Bridge Motor PLC Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation - Shear	3	3.65E-08	3.65E-07	0.1
51A-CTM-PLC01021-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operations	3	3.65E-07	3.65E-07	1
51A-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation - Shear	3	3.65E-08	3.65E-07	0.1
51A-CTM-PLC0103-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation - Shear	3	3.65E-08	3.65E-07	0.1
51A-CTM-SBELTRLS-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operation - Shear	3	6.74E-08	6.74E-07	0.1
51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque Limiter Failure	3	2.86E-02	8.05E-05	360
51A-CTM-SBELTRLY-IEL-FOD	CTM Shield Bell Trolley Interlock Failure	1	2.75E-05	–	–
51A-CTM-SBELTRLY-MOE-SPO	CTM Shield Bell Trolley Motor (Electric) Spurious Operations	3	6.74E-07	6.74E-07	1
51A-CTM-SKRTCTCT-SRP-FOD	CTM Skirt Floor Contact Sensors Fail	1	3.99E-03	–	–
51A-CTM-SLIDEGT-MOE-SPO	CTM Slide Gate Motor (Electric) Spurious Operation	3	6.74E-07	6.74E-07	1

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CTM-SLIDEGT-PLC-SPO	CTM Slide Gate PLC Spurious Operation	3	3.65E-07	3.65E-07	1
51A-CTM-SLIDEGT1-IEL-FOD	CTM Slide Gate Interlock Fails	1	2.75E-05	–	–
51A-CTM-SLIDGT2-SRX-FOD	CTM Slide Gate Position Sensor Fails on Demand	1	1.10E-03	–	–
51A-CTM-TROLLEYT-MOE-FSO	Trolley Motor (Electric) Fails to Shut Off	3	1.08E-07	1.35E-08	8
51A-CTM-TROLLYTR--PR-FOH	CTM Trolley End Run Stops Failure	3	1.95E-06	4.45E-10	4380
51A-CTM-TROLT1-HC-FOD	Controller Failure to Stop (on Demand)	1	1.74E-03	–	–
51A-CTM-WT0125-SRP-FOD	CTM Load Cell Pressure Sensor Fails on Demand	1	3.99E-03	–	–
51A-CTM-WTSW125-ZS-FOD	CTM Load Cell Limit Switch Failure on Demand	1	2.93E-04	–	–
51A-CTM-YS01129-ZS-FOD	CTM Drum Brake Controller Circuit Limit Switch 1129 Fails	1	2.93E-04	–	–
51A-CTM-ZSL0111-ZS--SPO	Grapple Disengaged Limit Switch Spurious Operation	3	1.28E-06	1.28E-06	1
51A-CTT--CT001---CT--SPO	On-Board Controller Initiates Spurious Signal	3	2.27E-05	2.27E-05	1
51A-CTT--DSW000--ESC-CCF	Common Cause Failure of Deadman Switches	C	1.18E-05	–	–
51A-CTT--DSW001--ESC-FOD	Deadman Switch #1 Fails Closed	1	2.50E-04	–	–
51A-CTT--DSW002--ESC-FOD	Deadman Switch #2 Fails Closed	1	2.50E-04	–	–
51A-CTT--HC001---HC--SPO	Handheld Controller Initiates Spurious Signal	3	5.23E-07	5.23E-07	1
51A-CTT--HC021---HC-FOD	Remote Controller Transmits Wrong Instruction	1	1.74E-03	–	–
51A-CTT--SV601---SV--FOD	Main Air Supply Valve Fails on Demand	1	6.28E-04	–	–
51A-CTT--SV602---SV--FOD	Solenoid Valve Fails to Close	1	6.28E-04	–	–

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-CTT--ZS301---ZS--FOD	Pin Limit Switch #1 Fails	1	2.93E-04	–	–
51A-CTT--ZS302---ZS--FOD	Pin Limit Switch #2 Fails	1	2.93E-04	–	–
51A-CTT-FWDREVM1-SV-FOH	Failure of Supply Valve Providing Forward/Reverse to Motor 1	3	4.87E-05	4.87E-05	1
51A-CTT-FWDREVM2-SV-FOH	Failure of Supply Valve Providing Forward/Reverse to Motor 2	3	4.87E-05	4.87E-05	1
51A-CTT-PIN-LIMIT-CCF	Common Cause Failure of Limit Switches	C	1.38E-05	–	–
51A-CTT-SV301---SV--SPO	Air Supply Solenoid Valve Spurious Operations	3	4.09E-07	4.09E-07	1
51A-CTT-SV401-SV-FOH	Failure of Air Supply Solenoid Valve for Air Bags	3	4.87E-05	4.87E-05	1
51A-CTT-SVROTM1-SV-FOH	Failure of Supply Valve Providing Rotation to Motor 1	3	4.87E-05	4.87E-05	1
51A-CTT-SVROTM2-SV-FOH	Failure of Supply Valve Providing Rotation to Motor 2	3	4.87E-05	4.87E-05	1
51A-FL---SC001---SC--FOH	Forklift Speed Control Fails	3	1.28E-04	1.28E-04	1
51A-PMRC-DERAIL-DER-FOM	Derailment of a Railcar per Mile	3	1.18E-05	1.18E-05	1
51A-PORTSLIDEGTE-IEL-FOD	Port Slide Gate Interlock Fails	1	2.75E-05	–	–
51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	1	2.75E-05	–	–
51A-RC---BRP001--BRP-FOD	SPMRC Brake Failure	1	5.02E-05	–	–
51A-RHS-2BLKDON-CRW-TBK	RHS (Non-SFP) Crane Two-Block Drop	1	4.59E-05	–	–
51A-RHSCRN-DRPON-CRW-DRP	RHS (Non-SFP) Crane Drop	1	1.07E-04	–	–
51A-SD---PLC001--PLC-SPO	Spurious Signal from PLC Closes Door	3	3.65E-07	3.65E-07	1
51A-SD---SRU001--SRU-FOH	Ultrasonic Obstruction Sensor Fails	7	2.08E-02	9.62E-05	438

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

Basic Event Name	Basic Event Description	SAPHIRE Calculation Type ^a	Basic Event Mean Failure Probability ^b	Mean Failure Rate ^b	Mission Time ^a (Hours)
51A-SD---TL000---TL--CCF	Common Cause Failure of Over-Torque Sensors	C	6.68E-04	–	–
51A-SD---TL001---TL--FOH	Motor #1 Over-Torque Sensor Fails	7	2.84E-02	8.05E-05	720
51A-SD---TL002---TL--FOH	Motor #2 Over-Torque Sensor Fails	7	2.84E-02	8.05E-05	720
51A-SLDGATE-IEL-FOD	Slide gate Interlock Fails	1	2.75E-05	–	–
51A-SPMRC-BRK000-BRP-FOD	Pneumatic Brakes on SPMRC Fail on Demand	1	5.02E-05	–	–
51A-SPMRC-BRP000-BRP-FOD	SPMRC Fails to Stop on Loss of Power	1	5.02E-05	–	–
51A-SPMRC-CBP001-CBP-OPC	Power Cable to SPMRC - Open Circuit	3	9.13E-08	9.13E-08	1
51A-SPMRC-CBP001-CBP-SHC	SPMRC Power Cable Short Circuit	3	1.88E-08	1.88E-08	1
51A-SPMRC-CPL00-CPL-FOH	SPMRC Automatic Coupler System Fails	3	1.91E-06	1.91E-06	1
51A-SPMRC-CT000--CT--FOD	SPMRC Primary Stop Switch Fails	1	4.00E-06	–	–
51A-SPMRC-CT001--CT-SPO	Controller Spurious Operation	3	2.27E-05	2.27E-05	1
51A-SPMRC-CT001-CT-FOD	On-Board Controller Fails to Respond	1	4.00E-06	–	–
51A-SPMRC-CT002--CT--FOH	Pendant Direction Controller Fails	3	6.88E-05	6.88E-05	1
51A-SPMRC-DERAIL-DER-FOM	Derailment of SPMRC per Mile	3	1.18E-05	1.18E-05	1
51A-SPMRC-G6500--G65-FOH	SPMRC Speed Control (Speed Limiter) Fails	3	1.16E-05	1.16E-05	1
51A-SPMRC-HC001--HC--SPO	Spurious Command from Pendant Controller	3	5.23E-07	5.23E-07	1
51A-SPMRC-HC001-HC--FOD	Pendant Control Transmits Wrong Signal	1	1.74E-03	–	–
51A-SPMRC-IEL011-IEL-FOD	Failure of Mobile Platform Anti-Collision Interlock	1	2.75E-05	–	–
51A-SPMRC-MOE000-MOE-FSO	SPMRC Lock Mode State Fails on Loss of Power	3	1.35E-08	1.35E-08	1