

are developed, categorized, and documented in a separate analysis (Ref. 2.4.4). Loss of offsite power (LOSP) is treated together with internal causes of power loss in Section 6.0.2.2.

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

External Event Category	Retention Decision. If Not Retained, Basis for Screening.
Seismic activity	<b>YES.</b> Retained for further analysis.
Nonseismic geologic activity	<b>NO.</b> Except for one of the subcategories, drift degradation, the external events in this category are not applicable to the site or do not occur at a rate that could affect the repository during the preclosure period. The chance of drift degradation severe enough to affect the repository and its operation over the preclosure period is less than 1/10,000.
Volcanic activity	<b>NO.</b> The chance of volcanic activity occurring at the repository over the preclosure period is less than 1/10,000.
High winds / tornadoes	<b>NO.</b> The chance of a high wind or tornado event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
External floods	<b>NO.</b> The chance of a flood event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Lightning	<b>NO.</b> The chance of a lightning event severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Loss of power event	<b>YES.</b> Retained for further analysis. See Section 6.0.2.2 for a screening analysis of loss of electrical power as an initiating event.
Loss of cooling capability event	<b>NO.</b> The primary requirements for cooling water at the Yucca Mountain site during the preclosure period are makeup water for the Wet Handling Facility (WHF) pool and cooling of HVAC chilled water. The chance of a loss of cooling capability occurring at the repository over the preclosure period is less than 1/10,000.
Aircraft crash	<b>NO.</b> The chance of an accidental aircraft crash occurring at the repository over the preclosure period is less than 1/10,000.
Nearby industrial/military facility accidents	<b>NO.</b> The chance of an industrial or military facility accident occurring at the repository over the preclosure period is less than 1/10,000.
Onsite hazardous materials release	<b>NO.</b> The chance of an accident event sequence initiated by the release of onsite hazardous materials at the repository over the preclosure period is less than 1/10,000.
External fires	<b>NO.</b> The chance of an external fire severe enough to affect the repository and its operation occurring at the repository over the preclosure period is less than 1/10,000.
Extraterrestrial activity	<b>NO.</b> Extraterrestrial activity is defined as an external event involving objects outside the earth's atmosphere and enters the earth's atmosphere, survive the entry through the earth's atmosphere and strike the surface of the earth. Extraterrestrial activity include: meteorites, asteroids, comets, and satellites. The chance of an occurrence at the repository over the preclosure period is less than 1/10,000.

NOTE: The source document defines the categories.

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

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

### 6.0.2.2 Screening of Loss of Electrical Power as an Initiating Event

Loss of electrical power, whether caused by onsite or offsite failures, is expected to occur during the preclosure period. Conveyances, cranes, and CTMs that rely on electric power will stop upon loss of power, but are designed to hold loads indefinitely. A set of redundant emergency diesel generators and the associated ITS electrical distribution system would start upon LOSP in order to continue operation of the ITS HVAC confinement system.

LOSP is not shown as an initiating event in the event trees because, by itself, it does not cause mechanical handling equipment to malfunction in a way that causes a drop or other mechanical impact of a waste container. Therefore, load drop and LOSP may be treated as independent events. The following calculation demonstrates that a LOSP and coincident load drop is Beyond Category 2.

The LOSP frequency is estimated at 3.6E-02/yr (Ref. 2.2.46, Table 3-8), with a failure to recover power within 24 hours of 1.8E-02 (Ref. 2.2.46, Table 4-1). Thus, during the 50-yr portion of the preclosure period in which waste handling operations are conducted, the expected number of LOSP events is:

$$\begin{aligned} \text{LOSP \#} &= 3.6\text{E-}02 / \text{yr} \times 50 \text{ yr} \\ &= 1.8; \end{aligned}$$

The initiating frequency of a LOSP lasting more than 24 hours would be:

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

An independent load drop from a crane following a LOSP would probably be caused by crane holding and emergency brake failures or random hoist cable breaks (each CTM and crane uses multiple wire ropes) because no other movement induced failure modes have been identified. Crane brake failures are more frequent than wire rope breaks, and for this calculation, the brake failure rates are used to determine a load drop probability. Two failure modes for the brakes have been modeled: failure of the brake to set and failure of the brakes to hold for an extended period. As documented in Attachment C, Table C4-1, estimated crane brake failure rates are:

- Holding (pneumatic) brake (BRP-FOD & BRP-FOH): 5.0E-05 per demand (initial setting of the brake) and 8.4E-06 per hour (holding the load for the duration of the power loss)
- Emergency brake (BRK-FOD & BRK-FOH): 1.5E-06 per demand (initial setting of the brake) and 4.4E-06/hr (holding the load for the duration of the power loss).

The four components of LOSP and brake failures are:

1. Both the holding brake and emergency brake fail to set on a LOSP resulting in a load drop.

2. Holding brake fails to set at LOSP. Emergency brake sets at LOSP but fails to hold during an extended loss of power (720 hours) resulting in a load drop
3. Emergency brake fails to set at LOSP. Holding brake sets at LOSP but fails to hold during an extended loss of power (720 hours) resulting in a load drop
4. Both brakes set at LOSP but fail to hold during an extended loss of power (720 hours) resulting in a load drop.

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 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.2.2.46). 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. 2.2.10).

The probability of the fourth component described above – the combination of LOSP and load drop (brakes set but fail to hold over a 720 hour 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 the *Canister Receipt and Closure Facility Event Sequence Development Analysis* (Ref. 2.2.33) 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. 2.2.33, 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 No.)	Initiating Event Description	Screening Basis
<p>CRCF-ESD01-DSTD (#3) (Figure A5-4)</p> <p>CRCF-ESD01-HLW (#3) (Figure A5-5)</p> <p>CRCF-ESD01-MCO (#3) (Figure A5-6)</p>	<p>Rollover of a truck trailer carrying a transportation cask in the Entry Vestibule or Cask Preparation Room</p>	<p>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 Entry Vestibule or Cask Preparation Room. The area in question has 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 rooms are 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.</p>
<p>CRCF-ESD04-DPC (#2) (Figure A5-15)</p> <p>CRCF-ESD04-DSTD (#2) (Figure A5-16)</p> <p>CRCF-ESD04-HLW (#2) (Figure A5-17)</p> <p>CRCF-ESD04-MCO (#2) (Figure A5-18)</p> <p>CRCF-ESD04-TAD (#2) (Figure A5-19)</p>	<p>Operator drops cask during cask preparation activities</p>	<p>The 20-ton auxiliary crane, rather than the 200-ton crane, is used in the lid-removal operation. Because the cask is not intentionally lifted in this step, dropping the cask would require a series of extraordinary human failures.</p> <p>For DPCs, a cask drop would require a series of human failures as follows:</p> <p>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 20-ton crane would be incapable of lifting the cask). The crane operator and at least two other crewmembers stand 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.</p> <p>For casks other than DPC 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 casks other than DPC casks, is considered to be unrealizable.</p>

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
<p>CRCF-ESD06-DPC (#2) (Figure A5-22)</p> <p>CRCF-ESD06-DSTD (#2) (Figure A5-24)</p> <p>CRCF-ESD06-HLW (#2) (Figure A5-25)</p> <p>CRCF-ESD06-MCO (#2) (Figure A5-26)</p> <p>CRCF-ESD06-TAD (#2) (Figure A5-27)</p>	<p>Structural damage to transportation cask due to impact from the crane hook or rigging while under the cask preparation platform</p>	<p>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.</p>
<p>CRCF-ESD09-DPC (#7) (Figure A5-41)</p> <p>CRCF-ESD09-DSTD (#7) (Figure A5-42)</p> <p>CRCF-ESD09-HLW (#7) (Figure A5-43)</p> <p>CRCF-ESD09-MCO (#7) (Figure A5-44)</p> <p>CRCF-ESD09-TAD (#7) (Figure A5-45)</p>	<p>Canister dropped inside shield bell (with CTM slide gate closed)</p>	<p>Drops within the shield bell have been subsumed within event sequences 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.</p>
<p>CRCF-ESD09-HLW (#6) (Figure A5-43)</p> <p>CRCF-ESD09-DSTD (#6) (Figure A5-42)</p>	<p>Drop of a heavy object onto an HLW canister or onto a DOE SNF canister</p>	<p>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 or DOE SNF canister could jeopardize the canister's structural integrity. Divider plates in the codisposal waste package (part of the basket structure) extend higher than the canisters inside. Therefore, a dropped waste package lid would not impact the canisters. Transportation casks for HLW or DOE SNF canisters are designed such that a lid drop would not impact the canisters inside. (Drop of a HLW canister or DOE SNF canister onto a HLW canister is not screened out and is included in the model. However, the drop of a 24-in HLW canister onto an 18-in DOE SNF canister is screened out due to the difference in diameter and the presence of divider plates.) Thus, the drop of a heavy load does not have an adverse effect on the integrity of HLW or DOE SNF canisters and can be screened from further consideration.</p>
<p>CRCF-ESD09-DPC (#7) (Figure A5-41)</p> <p>CRCF-ESD09-DSTD (#7) (Figure A5-42)</p> <p>CRCF-ESD09-HLW (#7) (Figure A5-43)</p> <p>CRCF-ESD09-MCO (#7) (Figure A5-44)</p> <p>CRCF-ESD09-TAD (#7) (Figure A5-45)</p>	<p>Side impact from a slide gate</p>	<p>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.</p>

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
<p>CRCF-ESD11-WP-H&amp;D (#2) (Figure A5-50)</p> <p>CRCF-ESD11-WP-H&amp;M (#2) (Figure A5-51)</p> <p>CRCF-ESD11-WP-TAD (#2) (Figure A5-52)</p>	<p>Welding of the waste package lid causes canister breach</p>	<p>No plausible scenarios have been identified whereby the gas tungsten arc welding process could cause burn through of the waste package and canister (Ref. 2.2.15). Therefore, event sequences associated with this initiating event are considered to be physically unrealizable.</p>
<p>CRCF-ESD14-DPC (#3) (Figure A5-59)</p> <p>CRCF-ESD14-TAD (#3) (Figure A5-60)</p>	<p>Site transporter or aging overpack catches crane hook or rigging resulting in impact to the aging overpack</p>	<p>This initiating event is subsumed within the initiating event for site transporter collision (Branch #2 of the listed event tree in each case).</p>
<p>CRCF-ESD15-WP-H&amp;D (#2) (Figure A5-61)</p> <p>CRCF-ESD15-WP-H&amp;M (#2) (Figure A5-62)</p> <p>CRCF-ESD15-WP-TAD (#2) (Figure A5-63)</p>	<p>TEV collision with stationary waste package</p>	<p>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 can not cause a collision between the two because of the extremely slow speed of these vehicles. Therefore, event sequences associated with these initiating events are considered to be physically unrealizable.</p>
<p>CRCF-ESD13-H&amp;D (#4) (Figure A5-55)</p> <p>CRCF-ESD13-H&amp;M (#4) (Figure A5-57)</p> <p>CRCF-ESD13-TAD (#4) (Figure A5-58)</p>	<p>Tilt-down of WPTT at uncontrolled speed</p>	<p>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. 2.2.26, 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. 2.2.26, 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.</p>

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
<p>CRCF-ESD06-DPC (No applicable branch) (Figure A5-22)</p> <p>CRCF-ESD06-DSTD (No applicable branch) (Figure A5-24)</p> <p>CRCF-ESD06-HLW (No applicable branch) (Figure A5-25)</p> <p>CRCF-ESD06-MCO (No applicable branch) (Figure A5-26)</p> <p>CRCF-ESD06-TAD (No applicable branch) (Figure A5-27)</p>	<p>Tipover of CTT</p>	<p>The CTT is designed to prevent tip over. (Ref. 2.2.24, 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 normally set on the floor inside the cask preparation platform. As such, tip over 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 tip over. Therefore, tip over of the CTT is considered physically unrealizable for internal events. CTT tipover, however, is analyzed in the seismic event sequence and categorization analysis.</p>
<p>No applicable event trees</p>	<p>Conveyance carrying a waste form collides with a shield door, causing the door to dislodge from its supports and fall onto the waste form</p>	<p>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.</p>
<p>No applicable event trees</p>	<p>Canister dropped into the Cask Unloading Room or Waste Package Positioning Room with no waste package present</p>	<p>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. 2.2.37). 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.</p>
<p>No applicable event trees</p>	<p>Internal flooding</p>	<p>Internal flooding as an initiating event is screened from further analysis in Section 6.0.4.</p>

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	More than four standardized DOE SNF canisters in single location.	<p>Due to potential criticality implications, more than four standardized DOE SNF canisters must not be put in close proximity without controls on their interaction. The only places where more than four DOE SNF canisters can fit and reasonably be put in uncontrolled proximity is in a TAD waste package, a TAD canister staging rack, or an aging overpack. A series of human errors would be necessary for a misload of this type. For example, a TAD waste package could be erroneously staged in the Waste Package Positioning Room and loaded with multiple DOE SNF canisters (whereas the codisposal waste package is designed to accommodate only one standardized DOE SNF canister). The potential for misloads of this kind has been addressed by a reliance on a combination of human actions and design solutions. Although there are a number of potential locations where a misload of this kind could occur, the one that requires the least deviation from normal operations is staging the wrong waste package. For this case, a screening argument is provided below. The other cases are bounded by the analyzed case because they require a longer series of human failure events.</p> <p>There are approximately 385 transportation casks and 3,300 waste packages containing DOE SNF that are unloaded or loaded in the CRCF. The probability of an operator attempting to place more than one DOE SNF canister into a TAD waste package or into a TAD canister staging rack is estimated to be 1E-03 (060-OpDSNFLoad-HFI-NOD) per operation set (where an operation set is the loading of a waste package or the unloading of a transportation cask to the staging rack). To prevent this error, there is an interlock that allows a canister to be emplaced in the waste package or canister staging rack only if the CTM is centered with the receptacle. The demand failure rate for the interlock is 2.7E-06. This interlock is not bypassed during normal operations or regular maintenance. For a second DOE SNF canister to be placed in a TAD waste package or TAD staging rack, the interlock would have to fail. The expected number of occurrences of placing two DOE SNF canisters in a TAD waste package or a TAD canister staging rack is estimated as <math>[2.7E-06 \times 1E-03 \times (3300+385)]=1E-05</math> over the preclosure period. Thus, placing just two DOE SNF canisters in a TAD waste package is Beyond Category 2. Further errors of the same kind would have to be repeated to accumulate five or more canisters in the TAD waste package. The potential for criticality for five or more canisters applies to only a small fraction of DOE SNF canisters. The screening argument conservatively does not include this consideration, which would further lower the estimated event sequence frequency.</p>

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

Initiator Event Tree (Branch No.)	Initiating Event Description	Screening Basis
No applicable event trees	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.

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; H&D = HLW & DOE Standardized Canister; H&M = HLW & MCO; HLW = high-level radioactive waste; MCO = multicanister overpack; 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. 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 one 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.

The possibility of inadvertent direct exposure of workers due to internal flooding is considered next. 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, CTT, 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.

INTENTIONALLY LEFT BLANK

## 6.1 EVENT TREE ANALYSIS

The event trees that are quantified in this analysis were developed from ESDs in the *Canister Receipt and Closure Facility Event Sequence Development Analysis* (Ref. 2.2.33, 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 fault tree analysis (FTA) (Section 6.2 and Attachment B), HRA (Section 6.4 and Attachment E), and PEFA (Section 6.3 and Attachment D). The YMP preclosure handling is performed using four kinds of buildings as summarized below:

1. The Receipt Facility (RF) accepts DPC and TAD canisters and places them into aging overpacks, either destined for the aging pads or the CRCF.
2. The CRCF accepts all waste containers except those supplied by the Naval Nuclear Propulsion Program (NNPP) for placement into waste packages destined for emplacement in the repository emplacement drifts. Three CRCFs are currently considered. This analysis models throughput from all three CRCFs as if it goes through a single building.
3. The WHF accepts DPCs and transportation casks containing uncanistered commercial SNF, transfers the SNF to TAD canisters which are destined for the CRCF or the aging pads.
4. The Initial Handling Facility (IHF) accepts canisters from the NNPP and some canisters containing high-level radioactive waste for placement in waste packages destined for emplacement in the repository emplacement drifts.

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

Event sequences are developed for each of the four building types, TEV and Subsurface Operations, and Intra-Site Operations. Because each type of waste container in the CRCF has different characteristics that manifest during event sequences, separate event sequences are developed for each type of waste container. As described in the *Canister Receipt and Closure Facility Event Sequence Development Analysis* (Ref. 2.2.33), 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 end states:

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

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

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. SAPHIRE's 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. 2.2.33, Attachment F). An example is CRCF-ESD07-DPC, which is shown in Figure A5-28 in Attachment A. The feed on the left side of the event tree is an event that represents the frequency of the challenge to the successful operation of the process step represented in the event tree. In the example, the frequency of challenge is equal to the number of transportation casks containing DPCs 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. 2.2.33, 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, CRCF-ESD01-DPC, is shown in Figure A5-2 in Attachment A, and the corresponding system response event tree, RESPONSE-TCASK1, 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 DPCs that are received during the preclosure period. Initiator event trees do not end at end states but transfer to a system response event tree. The models to be used for the initiating events associated with each initiator event tree are specified in SAPHIRE “basic rules,” which are attached to the initiator event tree.

System response event trees contain only pivotal events. In accordance with the basic rules that are written for a given initiator event tree, the SAPHIRE program links specific fault tree model or basic event to a given pivotal event. For example, the system response tree in Figure A5-3 shows the system response event tree RESPONSE-TCASK1. 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. The models to be used for the pivotal events

associated with each initiating event and system response event tree are specified in SAPHIRE basic rules, which are attached to the associated 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 linkage or connector fault trees. 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 probabilities 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 CRCF. 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 CRCF Over the Preclosure Period

Waste Form Unit	CRCF Throughput Over Preclosure Period	Comments
HLW transportation cask	1,960 <sup>a</sup>	Five canisters per cask
Defense SNF (standardized) transportation cask	385 <sup>a</sup>	Five to nine canisters per cask
MCO transportation cask	113 <sup>a</sup>	Four canisters per cask
DPC transportation cask	346 <sup>a</sup>	One canister per cask
TAD canister transportation cask	6,978 <sup>a</sup>	One canister per cask
Aging overpacks containing a TAD canister (outgoing)	6,978 <sup>a</sup>	Bounding number based on every TAD canister arriving by transportation cask going to aging pad
Aging overpacks containing a TAD canister (incoming)	8,143 <sup>a</sup>	Includes TAD canisters from aging pad and from WHF

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

Waste Form Unit	CRCF Throughput Over Preclosure Period	Comments
HLW canisters	9,801 <sup>b</sup>	Bounding number based on all HLW canisters going through CRCF
DOE standardized canister transfers by CTM	3,300 <sup>b</sup>	—
MCOs	451 <sup>b</sup>	—
DPCs	346 <sup>a</sup>	Same as number of DPC casks
TAD canisters	6,978 <sup>a</sup>	Same as number of TAD canister casks
Aging overpacks containing DPC (outgoing)	346 <sup>a</sup>	Same as number of DPC casks
Waste packages containing 1 DOE standardized canister and 4 to 5 HLW canisters	3,300 <sup>a</sup>	—
Waste packages containing 2 HLW canisters and 2 MCOs	225 <sup>a</sup>	—
Waste packages loaded with a TAD canister	8,143 <sup>a</sup>	Includes TAD canisters from aging pad and from WHF
Waste packages (all types produced at canister receipt and closure facilities)	11,668 <sup>a</sup>	—

NOTE: CRCF = Canister Receipt and Closure Facility; CTM = canister transfer machine; DOE = U.S. Department of Energy; DPC = dual-purpose canister; HLW = high-level radioactive waste; MCO = multicanister overpack; SNF = spent nuclear fuel; TAD = transportation, aging, and disposal; WHF = Wet Handling Facility.

Source: <sup>a,b</sup> Ref. 2.2.31, <sup>b</sup>Table 3, <sup>a</sup>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. 2.2.33, 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
CRC-ESD-01	Event Sequences for Activities Associated with Receipt of TC in Transportation Cask Vestibule and Movement into Cask Preparation Room	CRCF-ESD01-DPC CRCF-ESD01-DSDT CRCF-ESD01-HLW CRCF-ESD01-MCO CRCF-ESD01-TAD	Figure A5-2 Figure A5-4 Figure A5-5 Figure A5-6 Figure A5-7	RESPONSE-TCASK1	Figure A5-3
CRC-ESD-02	Event Sequences for Activities Associated with Receipt of AO in Site Transporter Vestibule and Movement into Cask Preparation Room	CRCF-ESD02-TAD	Figure A5-8	RESPONSE-AO1	Figure A5-9
CRC-ESD-03	Event Sequences for Activities Associated with Removal of Impact Limiters, Upending and Transfer of TC to CTT	CRCF-ESD03-DPC CRCF-ESD03-DSTD CRCF-ESD03-HLW CRCF-ESD03-MCO CRCF-ESD03-TAD	Figure A5-10 Figure A5-11 Figure A5-12 Figure A5-13 Figure A5-14	RESPONSE-TCASK1	Figure A5-3
CRC-ESD-04	Event Sequences for Cask Preparation Activities Associated with Unbolting and Lid Adapter Installation	CRCF-ESD04-DPC CRCF-ESD04-DSTD CRCF-ESD04-HLW CRCF-ESD04-MCO CRCF-ESD04-TAD	Figure A5-15 Figure A5-16 Figure A5-17 Figure A5-18 Figure A5-19	RESPONSE-TCASK1	Figure A5-3
CRC-ESD-05	Event Sequences for AO Preparation Activities Associated with Unbolting and Lid Adapter Installation	CRCF-ESD05-TAD	Figure A5-20	RESPONSE-CANISTER1	Figure A5-21
CRC-ESD-06	Event Sequences Associated with Transfer of Cask on CTT or an AO on ST from Cask Preparation Room to Cask Unloading Room	CRCF-ESD06-DPC CRCF-ESD06-DSTD CRCF-ESD06-HLW CRCF-ESD06-MCO CRCF-ESD06-TAD	Figure A5-22 Figure A5-24 Figure A5-25 Figure A5-26 Figure A5-27	RESPONSE-TCASK2	Figure A5-23

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
CRC-ESD-07	Event Sequences Associated with Collision of CTT or ST with Cask Unloading Room Shield Door	CRCF-ESD07-DPC CRCF-ESD07-DSTD CRCF-ESD07-HLW CRCF-ESD07-MCO CRCF-ESD07-TAD CRCF-ESD07-WP-H&D CRCF-ESD07-WP-H&M CRCF-ESD07-WP-TAD	Figure A5-28 Figure A5-29 Figure A5-30 Figure A5-31 Figure A5-32 Figure A5-33 Figure A5-34 Figure A5-35	N/A	N/A
CRC-ESD-08	Event Sequences Associated with Collision of two CTMs Loaded with Canisters	CRCF-ESD08-DPC CRCF-ESD08-DSTD CRCF-ESD08-HLW CRCF-ESD08-MCO CRCF-ESD08-TAD	Figure A5-36 Figure A5-37 Figure A5-38 Figure A5-39 Figure A5-40	RESPONSE-CANISTER1	Figure A5-21
CRC-ESD-09	Event Sequences for Activities Associated with Lifting and Lowering a Canister during Transfer to or from Staging, TC, WP, or AO with CTM	CRCF-ESD09-DPC CRCF-ESD09-DSTD CRCF-ESD09-HLW CRCF-ESD09-MCO CRCF-ESD09-TAD	Figure A5-41 Figure A5-42 Figure A5-43 Figure A5-44 Figure A5-45	RESPONSE-CANISTER1	Figure A5-21
CRC-ESD-10	Event Sequences for Activities Associated with WP Transfer from WP Loading Room to Closing Position in WP Positioning Room below WP Closure Room	CRCF-ESD10-WP-H&D CRCF-ESD10-WP-H&M CRCF-ESD10-WP-TAD	Figure A5-46 Figure A5-48 Figure A5-49	RESPONSE-WP1	Figure A5-47
CRC-ESD-11	Event Sequences for Activities Associated with Assembly and Closure of WP	CRCF-ESD11-WP-H&D CRCF-ESD11-WP-H&M CRCF-ESD11-WP-TAD	Figure A5-50 Figure A5-51 Figure A5-52	RESPONSE-WP1	Figure A5-47
CRC-ESD-12	Event Sequences for Activities Associated with Assembly and Closure of AO	CRCF-ESD12-DPC CRCF-ESD12-TAD	Figure A5-53 Figure A5-54	RESPONSE-AO1	Figure A5-9
CRC-ESD-13	Event Sequences for Activities Associated with Transfer of WP from WP Closure Room to WPTT Docking Station	CRCF-ESD13-WP-H&D CRCF-ESD13-WP-H&M CRCF-ESD13-WP-TAD	Figure A5-55 Figure A5-57 Figure A5-58	RESPONSE-WP2	Figure A5-56

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
CRC-ESD-14	Event Sequences for Activities Associated with Transfer of AO from Cask Unloading Room to Cask Preparation Room	CRCF-ESD14-DPC CRCF-ESD14-TAD	Figure A5-59 Figure A5-60	RESPONSE-AO1	Figure A5-9
CRC-ESD-15	Event Sequences for Activities Associated with Exporting of WP from CRCF	CRCF-ESD15-WP-H&D CRCF-ESD15-WP-H&M CRCF-ESD15-WP-TAD	Figure A5-61 Figure A5-62 Figure A5-63	RESPONSE-WP2	Figure A5-56
CRC-ESD-16	Event Sequences for Activities Associated with Exporting of AO from CRCF	CRCF-ESD16-DPC CRCF-ESD16-TAD	Figure A5-64 Figure A5-65	RESPONSE-AO1	Figure A5-9
CRC-ESD-17	Event Sequences for Activities Associated with Direct Exposure During Cask Preparation Activities	CRCF-ESD17-DPC CRCF-ESD17-DSTD CRCF-ESD17-HLW CRCF-ESD17-MCO CRCF-ESD17-TAD	Figure A5-66 Figure A5-67 Figure A5-68 Figure A5-69 Figure A5-70	N/A	N/A
CRC-ESD-18	Event Sequences for Activities Associated with Direct Exposure During CTM Activities	CRCF-ESD18-DPC CRCF-ESD18-DSTD CRCF-ESD18-HLW CRCF-ESD18-MCO CRCF-ESD18-TAD	Figure A5-71 Figure A5-72 Figure A5-73 Figure A5-74 Figure A5-75	N/A	N/A
CRC-ESD-19	Event Sequences for Activities Associated with Direct Exposure During Closure and Exporting Loaded WP	CRCF-ESD19-WP H&D CRCF-ESD19- WP H&M CRCF-ESD19-WP-TAD	Figure A5-76 Figure A5-77 Figure A5-78	N/A	N/A
CRC-ESD-20	Event Sequences for Fire Occurring in Canister Receipt and Closure Facility	CRCF-ESD20-DPC CRCF-ESD20-DSTD CRCF-ESD20-HLW CRCF-ESD20-MCO CRCF-ESD20-TAD CRCF-ESD20-WP-H&D CRCF-ESD20-WP-H&M	Figure A5-79 Figure A5-81 Figure A5-82 Figure A5-83 Figure A5-84 Figure A5-85 Figure A5-86	RESPONSE-FIRE	Figure A5-80

NOTE: AO = aging overpack; CRCF = Canister Receipt and Closure Facility; CTM = canister transfer machine; CTT = cask transfer trolley; N/A = not applicable; ST = site transporter; TC = transportation cask; WP = waste package; WPTT = waste package transfer trolley.

Source: Attachment A, Table A5-1

## 6.2 ANALYSIS OF INITIATING AND PIVOTAL EVENTS

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

Section 4.3.2 provides a brief introduction to the application of fault tree analysis (FTA) for initiating and pivotal events, including an example fault tree. Many of the initiating events involve faults in complex machinery for which no historical data exists at the system level, an exception being historical data on 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 CRCF is also used in other surface facilities and the Intra-Site operations. Furthermore, a given system, such as the site transporter, may affect the event sequences for several operational nodes of the same facility or several kinds of waste forms, as it does for the CRCF. 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 B8, presents all of 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 B9, presents all linking fault trees used in the CRCF 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 criterion for a given SSC fails to be achieved. At least one success criteria is defined for each system. Multiple success criteria are defined for systems that perform multiple safety functions in the CRCF.

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 developed directly, however. 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.

By contrast, the top event for the confinement function of the HVAC represents the conditional probability that the confinement feature is not achieved for the required duration following an airborne release of radioactive material inside the CRCF. The quantification of the top event, as summarized in Section 6.2.2.7 and detailed in Attachment B7, is expressed as unavailability. The results provide insight into the reliability of the HVAC and its contribution to event sequence quantification. Again, the quantified top event is not used directly in the event sequence quantification. Instead, the fault tree logic for the HVAC is linked to event sequence analysis via SAPHIRE.

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

For quantification of the probability of the top event, failure probabilities are developed for each basic event (hardware or HFE) and are used to compute the probability of each 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, etc.
- Support systems and subsystems such as cooling (HVAC, cooling water), 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 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 SPM.

#### **6.2.2.1.1 Physical Description**

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

#### **6.2.2.1.2 Operations**

In-facility SPM operations begin after the SPM has positioned the railcar or truck trailer outside the CRCF. 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 vestibule.

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

#### **6.2.2.1.3 Control System**

A simplified schematic of the functional components on the SPMRC/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 perform a controlled stop. Once stopped, the SPM enters 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
- Prevented SPMRC derailment
- Prevent SPMTT rollover.

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 CRCF, 0.04 miles, and industry data derailment rate of 1.18E-5 per mile traveled (Attachment C, Table C4-1, DER-FOM).

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

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

The SPMRC or SPMTT has three credible failure scenarios:

1. SPM collides with CRCF structures (DPC on railcar or truck trailer)
2. SPMRC derailment (DPC on railcar)
3. SPMTT rollover (DPC on truck trailer).

Each failure mode may occur with various waste forms that are received in the 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

Top Event	Mean Probability	Standard Deviation
SPMRC collides with CRCF structures	4.3E-3	1.1E-2
SPMRC derailment	4.7E-7	7.4E-9
SPMTT rollover	0	0

NOTE: CRCF = Canister Receipt and Closure Facility; SPM = site prime mover; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailers.

Source: Attachment B, Section B1, Figures B1.4-1, B1.4-6, B1.4-11 and B1.4-14

### 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 is used to transport various vertically oriented transportation casks from the Cask Preparation Room to the Canister Transfer Room. 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 sub-component 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 Room 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 speed of the drives, 10 feet per minute (fpm), 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 only give a proportional signal to the air valve that produces a speed of 0 to 10 fpm. In the event this control system fails, a factory set mechanical throttle valve, in line with each motor drive, allows a maximum amount of air through at any time to prevent a “run-away” condition.

#### **6.2.2.2.2 Operation**

Initially, the CTT is located in the Cask Preparation Room 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 insure 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 Room from the Canister Transfer 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—operator must depress both handles to allow air to flow to the system so the CTT can levitate or move horizontally
- E-stop button on the pendant control and on the CTT
- Clockwise/counterclockwise momentary 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 Room
- Forward/reverse switch to determine direction of the drive units
- Drive speed—variable speed control switch
- Cask restraint—selector switch that actuates 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 Room 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 Room while loading a cask onto the CTT
2. Spurious movement in the Cask Preparation Room during unbolting and lid adapter installation
3. Spurious movement at 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 Room 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 during cask transfer	1.0E-3	1.2E-3
Spurious movement during canister transfer	3.0E-14	1.9E-13

NOTE: CTT = cask transfer trolley.

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

### 6.2.2.3 Shield Door and Slide Gate Fault Tree Analysis

Each of the CRCF Cask Unloading Rooms and Waste Package Positioning Rooms have a slide gate providing access to the Canister Transfer Room and a shield door providing access to either the Cask Preparation Room or the Waste Package Loadout Room. The shield doors and slide gates provide shielding during canister unloading and loading.

The FTA is detailed in Attachment B, Section B.3. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### 6.2.2.3.1 Physical Description

The Cask Unloading Rooms' shield doors are opened to allow cask-carrying equipment, such as the site transporter, to enter the room. Once equipment is positioned properly in a Cask Unloading Room, shield doors may be shut in preparation for removing canisters from the cask. Once the shield doors are shut, the slide gate may be opened, to allow the CTM to perform cask unloading operations. Waste package loading operations in the Waste Package Positioning Rooms are analogous to cask unloading operations.

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 of an object.

Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand lever that must be enabled by an enable/disable switch. An emergency open switch exists enabling the doors to be opened in case of an emergency situation.

Similar to the shield doors, the slide gate consists of two gates that close together between the Waste Package Loadout Room/Cask Unloading Room and the Canister Transfer Room. 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 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 cask-carrying equipment, such as the SPM, to enter the room. Once equipment 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 slide gate may be opened to allow the CTM to perform cask unloading operations. Waste package loading operations in the Waste Package Positioning Rooms are analogous to cask unloading operations. The 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 waste package removal.

#### **6.2.2.3.3 Control System**

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

- Redundant hardwire interlocks prevent the shield door from opening while the slide gate is open.
- 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 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 hardwire interlocks to prevent one another 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 concurrent opening of the shield door and slide gate when waste is present
- 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 is 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 B, Section 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-7	4.6E-7
Inadvertent Opening of the Slide Gate	3.6E-9	9.8E-9
Shield Door Closes on Conveyance	3.2E-6	5.6E-6

Source: Attachment B, Section B3, Figures B3.4-1, B3.4-4 and B3.4-7

#### 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 two identical CTMs operate in the Canister Transfer Room of the CRCF. Their function is to transfer waste canisters from a cask on a CTT or from any aging overpack on a site transporter to another cask or overpack, or to a waste package supported by a WPTT. The CTMs also have the capability to transfer canisters to staging areas for temporary staging for a later transfer to a waste package. The ports in the floor of the Canister Transfer Room provide access to the Cask Unloading Room and Waste Package Loading Room and access to the canister staging areas.

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 slide gate, when closed, provides bottom shielding of 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**

A typical CTM canister transfer operation is the transfer of a waste canister from a transportation cask to a waste package. For this operation, a loaded transportation cask, secured in the CTT, is positioned below the transfer port in the Cask Unloading Room. 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 Positioning 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 large diameter canisters such as TAD canisters and DPCs. Other grapples are used to access the smaller diameter DOE SNF, HLW canisters, and the MCOs. These grapples are attached to the CTM canister grapple by positioning the CTM over a hatch located in the Canister Transfer Room floor and lowering the CTM hoist until the CTM grapple is accessible in the room below.

Loading codisposal waste packages may require that a canister be moved from the loaded cask to a staging area as an interim step before the canister is placed into a waste package. For codisposal waste packages, a waste package inner lid (shield plug) is also placed using the CTM after the waste package is loaded.

The CTM is normally controlled from the facility operations room (also referred to 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 AC 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 would stop and the hoist holding brake engages. Operations would be 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 shield bell skirt is lowered
- Prevent raising the shield bell skirt when the slide gate is open
- Prevent hoist movement unless the grapple is fully engaged or disengage
- Stop the hoist and erase the lift command when a canister clears the shield bell slide gate
- Stop a lift before upper lift heights are reached (two interlocks are provided for this function)
- Prevent opening of the port gate unless the shield bell skirt is lowered and in position
- Prevent hoist movement unless the shield bell skirt is lowered
- Prevent a collision between the two CRCF CTMs
- Prevent lifting of a load beyond the operational 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 shield skirt position and the position of the 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.

Much 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 Room 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 CRCF
- Prevent CTM movement that could result in a collision between the two CTMs while either one is transferring a canister.

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 six 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 bell slide gate has been closed and drops through the Canister Transfer Room ports to the loading/unloading areas that can occur before the bell 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 CRCF floors resulting in shear forces being applied to the canister.
6. The CTM, while carrying a canister, moves in such a manner as to cause a impact of the collision with the second CTM.

These six scenarios apply to operations in all three CRCFs. The facilities and operations within each of these facilities is identical, therefore, only one set of fault trees have been developed to address operations within all three facilities.

The results of the analysis are summarized in Table 6.2-4. Six fault trees were developed. The top events correspond, to the six 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 from below the canister design-limit drop height	1.4E-5	1.5E-5
CTM high drops from above the canister design limit drop height	2.8E-8	1.6E-7
Drop of object onto cask	1.4E-5	1.3E-5
CTM collision results in an impact to canister	3.9E-6	2.7E-7
CTM shear	6.7E-9	1.4E-8
CTM collision with second CTM	3.2E-5	5.4E-5

NOTE: CTM = canister transfer machine.

Source: Attachment B, Section B4, Figures B4.4-1, B4.4-14, B4.4-19, B4.4-33, B4.4-40, and B4.4-45

### 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 Area to the Waste Package Closure Area 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 40 fpm, required by ASME NOG-1-2004 (Ref. 2.2.10), 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 at a speed no faster than 90-degrees per hour (Ref. 2.2.92). 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 Room 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 Loadout Room. The WPTT is situated so that the empty waste package is directly beneath the center of the slide gate that separates the Waste Package Loadout Room and Canister Transfer Room.

The WPTT is positioned in the Waste Package Loadout Room and the 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 and the slide gate closed, the WPTT moves to the Waste Package Closure Area. At this station, the inner lid is placed on top and 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 at the loading area remains stationary with no movement while loading a canister onto the shielded enclosure
- Ensure the WPTT travels at a speed no greater than 20 fpm and the operator be 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 shield 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 is 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 at the loading area while loading a cask onto the WPTT.
2. Impact of the WPTT with a structure while moving from the loading area to the Waste Package Positioning Room and then to the Waste Package Loadout Room
3. Derailment of the WPTT while moving from the loading area 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 loading area 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	2.7E-12	1.6E-11
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 WPTT	2.7E-5	3.3E-5
Malfunction of WPTT or WP transfer carriage	1.0E-3	1.3E-3

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

Source: Attachment B, Section B5, 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 FTA for the site transporter is detailed in Attachment B, Section B6. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### 6.2.2.6.1 Physical Description

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a concrete and steel ventilated aging overpack. The transport occurs both within the Intra-Site and within the CRCF. The analysis described herein is limited to movement of the site transporter within the CRCF: the Entry Vestibule, the Cask Preparation Room, and either of the two Cask Unloading Rooms.

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

buildings the site transporter is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

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

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

#### **6.2.2.6.2 Control System**

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

#### **6.2.2.6.3 Normal Operations**

The site transporter operator lines up the front opening of the site transporter to envelop the aging overpack and positions the rear fork down and in-line with the rectangular lifting slots near the bottom of the aging overpack and moves the site transporter forward until the aging overpack is centered in the interior of the site transporter.

The rear forks are raised to contact the bottom of the lift slots but do not attempt to lift the cask at this time. The operator and interlocks (torque and/or position) are incorporated to prevent lifting with the rear forms only.

The operator initiates the lift support arm's interface sequence with the rear forks and cask to prepare for lifting. After the operator and machine's switches have confirmed that the rear forks and lift support are properly aligned with one another, the lift sequence is initiated. The control system will sequence the lift motors so all screws operate together.

When the lift is completed, the operator performs the final positioning of the upper restraint arms and inserts a pin in each arm. When the pins are properly installed, the site transporter can move.

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

Once inside the building, the operator positions the site transporter in the Cask Preparation Room and in the Cask Unloading Rooms. During the various movements inside the CRCF, the

operator disengages the restraint arms for lower and lift operations at the various stations. Each time, the operator removes or replaces the pins from the restraint arms, as appropriate. The movement interlock is engaged when the pins are removed.

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

Success criteria for the site transporter are the following:

- Prevent a collision of the site transporter with objects, structures, or shield doors
- Prevent runaway situations
- Prevent site transporter movements in the wrong direction
- Preventing a rollover of the site transporter
- Prevent spurious site transporter movements
- Prevent a load drop during lift/lower or transport operations.

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 site transporter.

#### **6.2.2.6.5 Mission Time**

For quantification of the site transporter fault trees in Attachment B, Section B6, a mission time of one hour per cask transfer is used.

#### **6.2.2.6.6 Fault Tree Results**

There are five basic site transporter fault trees developed for the CRCF. The scenarios represented and the variations by these fault trees are the following:

1. Site transporter collides with CRCF structures:
  - A. Importing aging overpack to Cask Preparation Room
  - B. Transfer aging overpack from Cask Preparation Room to Cask Unloading Room
  - C. Transfer aging overpack from Cask Unloading Room to Cask Preparation Room
  - D. Export aging overpack from Cask Preparation Room.
2. Site transporter load drop during lift/lower
3. Site transporter rollover
4. Site transporter spurious movement during canister transfer by CTM
5. Site transporter spurious movement during preparation or closure of aging overpack.

The results of the analysis are summarized in Table 6.2-6 for the five fault trees.

Table 6.2-6. Summary of Top Event Quantification for the Site Transporter

Top Event	Mean Probability	Standard Deviation
Collides with CRCF structures	4.4E-3	1.3E-2
ST load drop during lift and movement	4.0E-8	1.2E-7
ST rollover	2.3E-6	1.9E-6
ST spurious movement (during canister transfer)	2.1E-13	1.2E-12
ST spurious movement (during preparation/closure)	2.6E-4	2.9E-4

NOTE: CRCF = Canister Receipt and Closure Facility; ST = site transporter.

Source: Attachment B, Section B6, Figures B6.4-1, B6.4-6, B6.4-20, B6.4-23 and B6.4-26

### 6.2.2.7 HVAC FAULT TREE ANALYSIS

The FTA is detailed in Attachment B, Section B7. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

#### 6.2.2.7.1 HVAC Description and Function

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

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

This HVAC system is composed of four subsystems:

- A series of dampers are used to control pressure, flow, as well as flow direction in this system.
- Three HEPA filters, each consisting of one medium efficiency roughing filter (60 to 90% efficiency), two high efficiency filters for particulate removal in air (99.97% efficiency), and a mister/demister for maintaining proper humidity levels.
- One exhaust fan with a rated capacity of 40,500 cubic feet per minute and an exhaust fan motor rated at 200 horsepower (hp).
- Control circuitry with logic contained in an erasable programmable read-only memory located in the adjustable speed drive controller used for controlling the speed of the operating fan and on fault detection, and for off-nominal conditions, shutting down the operating train and transmitting signals to the standby system to start.

#### **6.2.2.7.2 Success Criteria**

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

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

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

#### **6.2.2.7.3 Mission Time**

The mission time for the HVAC system is 720 hours (Attachment B, Section B7). However, the mission time for the backup system has been taken as, half of the active system, (i.e., 360 hours). This is to account for the difference in failure rates between active and passive systems.

#### **6.2.2.7.4 Fault Tree Results**

The system failure probability and standard deviation, including failure of electrical power, are as follows:

- The mean HVAC system probability of failure is 4.3E-02 (Figure B7.4-1)
- The standard deviation is 8.8E-02 (Figure B7.4-1).

These results are presented in Attachment B, Section B7, Figure B7.4-1

#### **6.2.2.8 AC Power Fault Tree Analysis**

The FTA is detailed in Attachment B, Section B8. The following is a summary of the design, operations, success criteria, and results of the fault tree quantification.

##### **6.2.2.8.1 System Description**

The ITS AC power system supplies power to the ITS systems (the HVAC Systems). The ITS power system consists of two elements; those used during normal operations and those used during off-normal conditions. During normal operations AC power is supplied from one of two offsite 138 kV offsite power lines through the 138 to 13.8 kV switchyard and then through the plant AC power distribution system to the various facilities throughout the site. Off-normal conditions for the distribution of AC power occur during a loss of offsite power (LOSP).

A LOSP may be the result of problems on the power grid, or may be the result of failures within the plant AC power systems. Under these conditions, the AC power source for the CRCF ITS equipment is two onsite ITS diesel generators. Power is supplied to ITS loads via the same onsite AC power distribution system that is used during normal operation. Each ITS diesel

generator supplies power to one division (A or B) of ITS systems. Each ITS diesel generator, its associate support systems, and the power distribution system are independent and electrically isolated from the other diesel generator, its support systems and power distribution system.

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

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

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

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

#### **6.2.2.8.2 Operations**

Under normal operating conditions, AC power is supplied from two 138 kV offsite power lines. Power is passed through the 138 to 13.8 kV switchyard to the two independent 13.8 kV ITS switchgear. From here, power is transmitted via separate lines to a 13.8 to 480 V transformers supporting divisions A and B of the CRCF. Power to individual ITS components within each facility is provided via 480 V ITS Load Centers and MCCs (one each for division A and one each for division B in each facility) powered through these transformers.

During a LOSP, both ITS diesel generators are required to start and accept loads in a timely manner. Upon a LOSP, the onsite power distribution system supporting ITS loads is disconnected from the switchyard; a circuit breaker between the 13.8kV ITS switchgear and the switchyard 13.8 kV switchgear in each division automatically opens. Both ITS diesel generators start automatically and are connected to the 13.8kV ITS switchgear when the connecting breaker

is closed by the load sequencer. The load sequencer then reconnects the CRCF loads to the 13.8kV ITS switchgear. Both ITS diesel generators continue to supply AC power until normal power is restored.

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

#### **6.2.2.8.3 Control System**

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

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

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

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

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

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

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

#### **6.2.2.8.5 Mission Time**

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

#### 6.2.2.8.6 Fault Tree Results

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

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

The results are essentially the same for either train:

- The mean probability of failure for either train value is 3.1E-02
- The standard deviation is 7.5E-02.

These results are presented in Attachment B, Section B8, Figure B8.4-1.

#### 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. Moderator addition into a canister can occur following a breach of the canister and a subsequent internal flood. The internal flooding analysis considers all waste handling facilities.

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

Each facility is equipped with a normally dry, double-preaction sprinkler system in areas where waste forms are handled (Ref. 2.2.19, Ref. 2.2.35, Ref. 2.2.29, and Ref. 2.2.41). 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 is developed using a simplified screening model that addresses 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 (1<sup>st</sup> quarter following annual test).

The frequency of sprinkler failure is estimated using an individual sprinkler head failure frequency of  $1.6E-6/\text{yr}$  (Ref. 2.2.14, Table 1), the estimated number of sprinklers (1 per  $130 \text{ ft}^2$  based on Ref. 2.2.64, Table 8.6.2.2.1(b)) and the applicable area (Ref. 2.2. 23). For example, the area of CRCF Waste Package Loadout Room 1015 is listed as  $7,470 \text{ ft}^2$  in (Ref. 2.2.23, Table 10). At  $130 \text{ ft}^2/\text{sprinkler}$ , 58 sprinklers are estimated. The failure of any sprinkler in the room is then estimated to be  $58 \times 1.6E-6/\text{yr} \times 1/8,760 \text{ hrs/yr}$ , or  $1.1E-8/\text{hr}$ .

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

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

Applying the sum of these values,  $3E-9/\text{sprinkler head}$ , to the number of sprinklers calculated for the waste handling areas of the four facilities results in the following estimates of the probability of spurious sprinkler actuation found in Table 6.2-7.

Table 6.2-7. Probability of Spurious Sprinkler Actuation

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

NOTE: <sup>a</sup> CRCF area based on room numbers 1005E, 1016-1026, 2004,2007, 2007A, and 2007B  
IHF area based on room numbers 1001-1003, 1006-1008, 1011,1012, 1026 and 2004  
RF area based on room numbers 1013, 1015, 1016, 1017, 1017A, and 2007  
WHF area based on room numbers 1007-1010, 1016, 2004, 2006, and 2008.

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

Source: Ref. 2.2. 23

Piping carrying water is present in the waste form handling areas of the CRCF, IHF and WHF. Piping lengths in these areas of the CRCF and WHF are below 100 feet per facility (Ref. 2.2.89). The probability of a pipe crack in a 30 day period is 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. 2.2.47, Table 5-1). Piping leaks and large break rates applicable to non-service water applications are used in the analysis. These values are considered appropriate for repository systems because the conditioning applied to the fluids in the systems is that typical of commercial nuclear power plants:

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

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

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

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

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

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

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

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

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

For fires that occur in locations that contain canisters sealed within bolted transportation casks, the fire location is floor level and the transportation casks rise as much as 20 feet above the floor. Casks are relatively thick walled compared to canisters and sustain a relatively small internal pressurization when compared to canisters. Therefore, if a fire is large enough, it will fail the internal canister first, as indicated in Attachment D. This will cause the bolted and sealed cask to bear the overpressure that is inside the canister. The cask bolts might act as elastic springs allowing the top to break the seal and relieve the internal pressure. This would be a mechanism that prevents cask breach. However, a hot fire may result in sufficient loss of strength of the bottom portion of the stainless steel cask such that it breaches. If failure occurs because of bolt stretching the cask lid remains on top of the cask preventing fire suppression water from entering. Commercial DPCs and TAD canisters will require at least 100 liters of water to enter the canister if optimally distributed among the fuel rods (Ref. 2.2.39, Section 2.3.10.1). Casks are raised above the floor. They lay on top of railcars, are lifted from there by cranes, sit inside a CTT, or lay sideways on a pallet. They are at least five feet from the floor. If the bottom portion of the canister breaches, there is no physical mechanism for this much water to enter the cask and then the canister, remain as water (not boil off), and optimally mix with the fuel rods.

This latter situation also applies to canisters sealed within a welded waste package. The waste package sits inside a WPTT or is inside a TEV. In the former case it is more than three feet from the floor (Ref. 2.2.20) and in the latter case about one foot from the floor (Ref. 2.2.21). In the latter case, however, the TEV offers an additional layer of protection against fires. In addition, it

is physically unrealistic for a sufficient amount of available fire suppression water to cause 100 liters to leak into a breached canister, but not extinguish the fire or at least reduce the severity of the fire such that a breach would not occur.

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

Upon failure of the canister inside the cask, the cask will not be susceptible to pressurization failures as above. Instead, water can only enter in a cask (or waste package) if the cask body melts through. Fires capable of melting stainless steel or Alloy 22, however, have an occurrence frequency within the waste handling facilities of less than 1E-05 over the preclosure period (Attachment D, Section D1.3). Thus, breach of the cask or waste package in a manner that would allow water to enter the canister is essentially not physically realizable.

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

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

#### **6.2.2.9.2 Lubricating Fluid**

Another source of moderation is lubricating fluid in cranes. Crane lube oil is of limited quantity (<150 gallons) and housed in a welded gear box with a leak pan below it capable of capturing the

entire gearbox fluid inventory. An estimate of the leakage rate through the gear box and drip pan is found by multiplying the gearcase motor failure frequency (all modes) of  $0.88E-06$  per hour (Ref. 2.2.43, Page 2-104 and Section 6.3) over the 50 years by the conditional probability of oil pan failure. A loss of lubrication would fail the crane operation and also be detected by oil pressure indicators. The conditional probability of oil pan failure may be estimated by analogy to receiver tank leakage during the interval between gearbox failure and detection. The interval is conservatively estimated to be 30 days. The all modes failure rate of a receiver tank is  $0.34 E-06$  per hour (Ref. 2.2.43, Page 2-213). Using an exposure interval of 50 years (which represents the operating life of the surface facilities), the conditional probability of lubricating fluid entering a breached canister would be less than:

$$0.88E-06/\text{hr} \times 50 \text{ yrs} \times 8760 \text{ hrs/yr} \times 0.34E-06/\text{hr} \times 720 \text{ hrs/30days} = 9.E-05 \text{ over the preclosure period.}$$

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

## **6.3 DATA UTILIZATION**

### **6.3.1 Active Component Reliability Data**

The fault tree models described in Section 6.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. The active component reliability estimates are developed by gathering and reviewing 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 activities are atypical of nuclear power plant activities and no operating history exists, it is necessary to develop the required data from the experience of other nuclear and non-nuclear equipment 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 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 industry-wide source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, is to evaluate the similarity between the YMP operating environment and that represented in each data source to ensure data appropriateness. This evaluation process is described in 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. 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 CRCF; 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 is made to find more than one data source for each component type and failure mode combination (TYP-FM), although multiple sources are not always available for a specific piece of equipment. When data was extracted from several sources, it was combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs are quantified with one data source, eight percent with two data sources, eight percent with three data sources, and 31%, are quantified 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. 2.2.12). 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