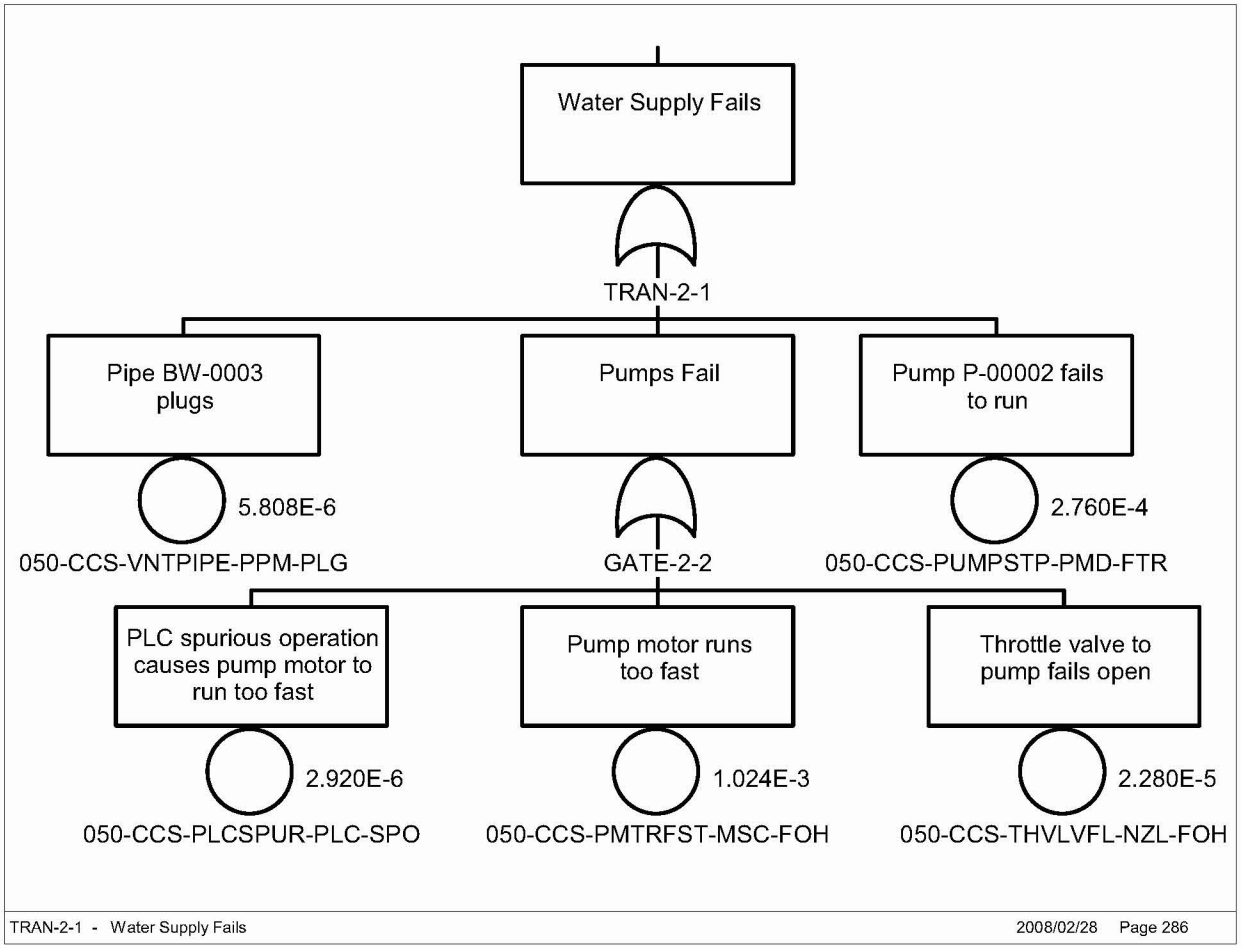
INTENTIONALLY LEFT BLANK



Source: Original

Figure B5.4-9. Fault Tree for a Cask/Sample Line Over-pressurized Rupture (Transfer 2-1)

INTENTIONALLY LEFT BLANK

B6 SITE TRANSPORTER FAULT TREE ANALYSIS

B6.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of this document. There are no superseded or cancelled documents associated with the modifications that led to the issuance of this revision. Cancelled or superseded documents associated with the portions of this document for which the snapshot has not yet been updated are designated herein with a dagger (†).

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designed categories described in Section 4.1, relative to suitability for intended use.

B6.1.1 †BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report – Site Transporter.* 170-30R-HAT0-00100-000-000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.

B6.1.2 BSE 2007. *Exhibit D, Statement of Work for Mechanical Handling Equipment Design.* 000-3SW-MGR0-00100-000 Rev. 003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070904.0031.

B6.1.3 Morris Material Handling 2007. *P&ID Site Transporter.* V0-CY05-QHC4-00459-00049-001 Rev. 004. Oak Creek, Wisconsin: Morris Material Handling. ACC: ENG.20071022.0012.

B6.2 SITE TRANSPORTER DESCRIPTION

The site transporter is a diesel/electric self-propelled tracked vehicle that is designed to transport a cylindrical concrete and steel ventilated aging overpack. The transport occurs both Intra-Site and within the CRCF, the WHF, and the RF[2]. In the WHF, the site transporter is used to deliver aging overpacks with a DPC, for loading an aging overpack with a DPC or TAD canister, and for removing the loaded aging overpacks from the facility.

Movement of the site transporter within the WHF is limited to the Loading Room and the Site Transporter Vestibule.

[2] Variations in the use of the site transporter for Intra-Site, RF and CRCF are addressed in their respective volumes.

B6.2.1 Overview

The interface between the site transporter and the aging overpack is via two parallel rectangular lift slots that pass through the containers near their lower ends. Orientation of the aging overpack is such that the axis of the aging overpack is vertical with lid, at the top. Access to the top of the aging overpack is unobstructed.

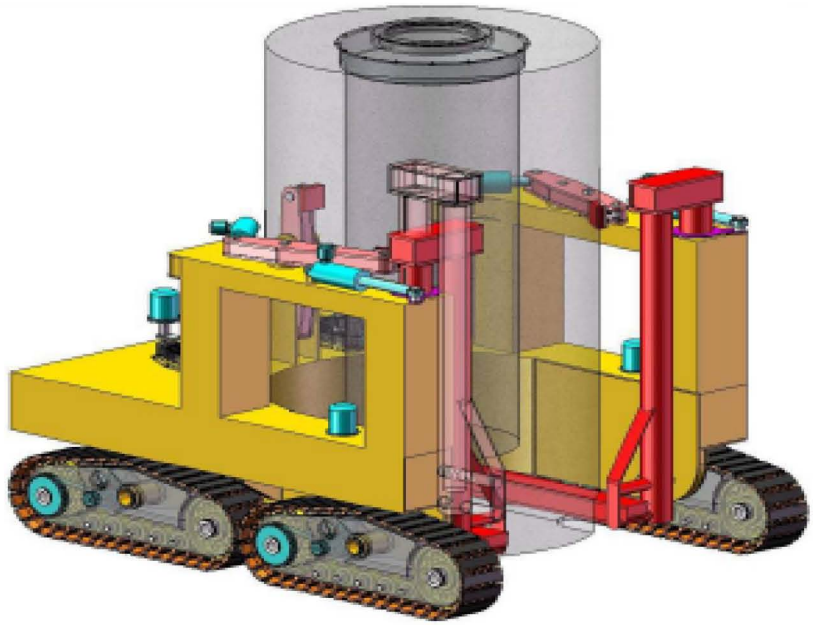
An integrated diesel powered electric generator and diesel fuel provides the electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable (or remote control) from the facility main electrical supply (Ref, B6.1.1, Section 2.1).

The site transporter is a track driven vehicle with four synchronized tracks (two on each side of the site transporter). The components of the drive system (i.e., tumblers, idlers, rollers) are not included in this analysis since these components are not ITS.

A rear fork assembly consists of a pair of arms that extend to the front of the site transporter. These forks move up and down for the purpose of raising, lowering, and supporting the aging overpack during movement. A pair of support arms is located at the front of the site transporter which is moved into position around the forks to provide support and assistance during the lifting and lowering of the aging overpack.

A passive restraint system provides stabilization during aging overpack movement. There are two mechanisms that control aging overpack movement on the pitch and roll axis. These restraints are not engaged until the aging overpack has been raised to the desire height. Once engaged, three pins are inserted, one in each restraint arm that keep the restraints in place should there be a failure of the electromechanical assembly used to position and secure the restraint device. They also serve as an interlock that prevents movement of a loaded site transporter if they are not properly installed.

Control of the site transporter is provided by a wireless remote control or a wired pendant. Although these devices only provide a subset of the controls and indicators that are available on the control console located on the site transporter, they do contain all the necessary controls and indicators to perform and monitor the operation state of the site transporter during normal operations. The site transporter is shown in Figure B6.2-1.



Source: Ref. B6.1.1

Figure B6.2-1. Site Transporter

The site transporter system is composed of six subsystems (Ref. B6.1.1):

1. Crawler Tracks Subsystem—Four crawlers, two on each side of the site transporter, are used to move the vehicle. These crawlers use tracks with chamfered flat steel plates mounted to double grouser shoes on a continuous chain.

2. Power Plant Subsystem—a diesel engine, generator, and diesel fuel tank are enclosed in the back of the site transporter. During Intra-Site Operations, the diesel engine drives the generator, which provides the required 480 V, 3-phase, 60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480 V, 3-phase, 60 Hz AC power is supplied to operate the vehicle.

3. Rear Lift Fork Subsystem—site transporter contains a pair of arms that extend forward from the site transporter through slots in the aging overpack. The lift/lower drive system utilizes an ACME type nut that changes the elevation of the fork as the screw lift mechanism turns through the ACME nut. A lift synchronizer controls the lift/lower operation.

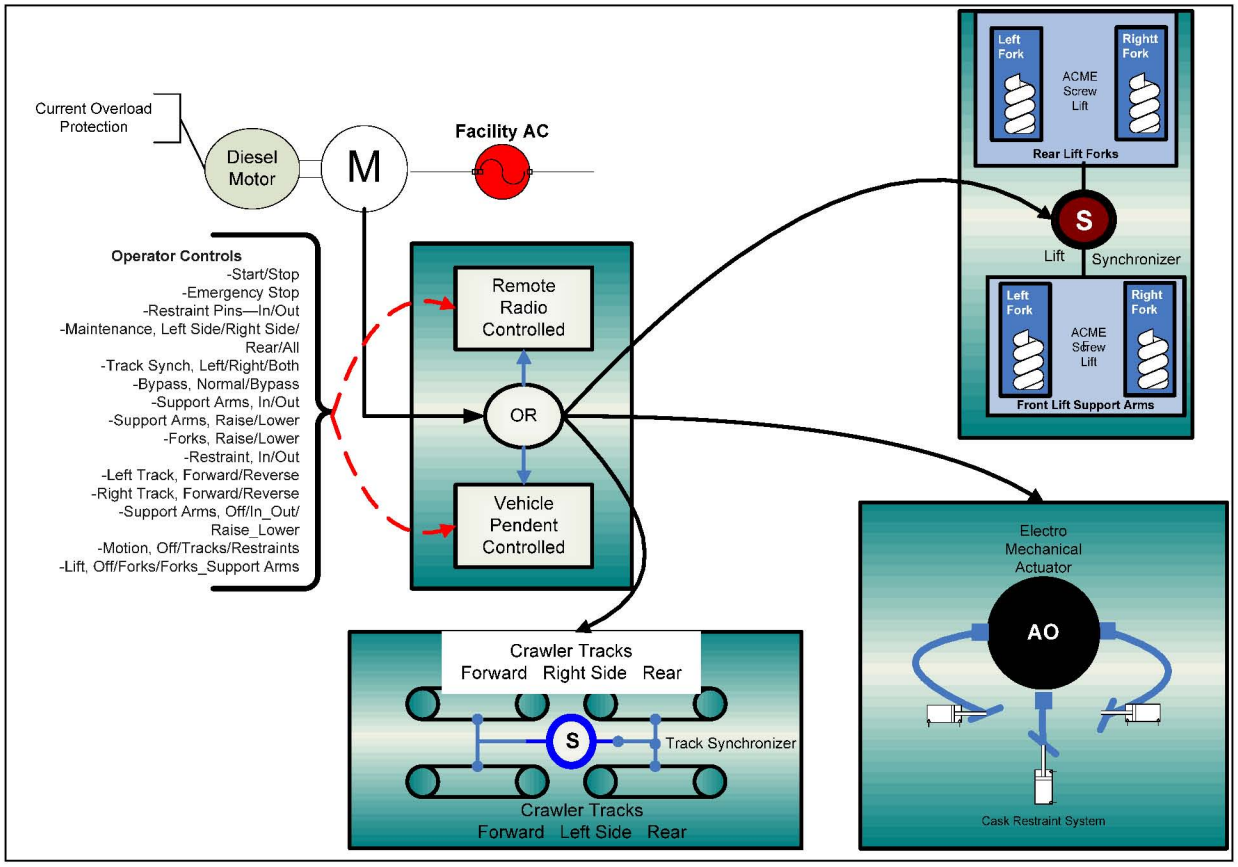
4. Lift Support Arms Subsystem—two support arms with electromechanical actuators are located on the front of the site transporter. These support arms are rotated 90 degrees to provide support and stabilization for the lift forks during lifting/lowering/moving operations. ACME nuts are used on these arms and synchronized with the lift forks during lifting/lowering/moving.

5. Restraint Subsystem—a two axis restraint system is incorporated to stabilize the aging overpack during site transporter movement. The restraints are emplaced/retracted with electromechanical actuators. These restraints when positioned against the aging overpacks will be secured with a locking pin. The three locking pins serve as an interlock and must be properly installed before the site transporter can be moved.

6. Vehicle Controls Subsystem—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.

Note: in addition to the six subsystems identified above, *Mechanical Handling Design Report – Site Transporter* (Ref. B6.1.1) also includes a description of the site transporter "car body." Events associated with car body failure are screened from this analysis based on the results of the stress analysis contained in this reference.

A simplified block diagram of the functional subsystems on the site transporter is shown in Figure B6.2-2.



NOTE: AO = aging overpack; M = motor; S = synchronizer.

Source: Original

Figure B6.2-2. Simplified Block Diagram of the Site Transporter Subsystems

B6.2.1.1 Site Transporter Crawler Tracks Subsystem Description

The site transporter moves by four tracks mounted on the crawler frames with two on each side of the vehicle to increase stability when traversing terrain that includes sudden changes in elevation such as a drainage trough or curb. The site transporter is designed to negotiate roadways with a 5% grade and up to a 2% cross-slope (Ref. B6.1.2, Section 7.2.2-11). Special pads are included on the tracks to reduce the wear and tear on concrete or roadways.

Each track is driven by its own electric motor (50 hp @ 900 rpm) through its own gear reduction and final chain drive reduction. During forward operations, motors on both sides of the machine drive are synchronized. During turns, the outside tracks are driven faster and for very sharp turns the tracks are counter-rotated to turn the site transporter about its own vertical centerline (Ref. B6.1.1, Section 2.1.2).

B6.2.1.2 Power Plant Subsystem Description

The power plant subsystem supplies the site transporter with 480 volts AC, 3-phase power at 60 Hz. Because of the risk of contamination from their various fluids, there are no storage batteries or capacitors in the system. The generator is sized approximately 110% more than the highest power requirement for the vehicle.

The 150 kW generator is sized for seven hours of continuous operation with a fuel tank containing 99 gallons of diesel fuel (Ref. B6.1.1, Section 2.2.3). The fuel tank capacity is sized to minimize the amount of fuel taken inside the facilities but sufficient to transport a loaded aging overpack three miles and return to the site transporter's point of origin without refueling (Ref. B6.1.2, Section 7.2.2.2).

When entering a building the generator is shut down and a power source from the building is plugged into the site transporter integral receptacle to allow the site transporter to operate inside the building without a source of combustion.

The motor drive and current over load protection system prevents the site transporter from exceeding 2.5 mph (Ref. B6.1.1, Section 3.2.1).

B6.2.1.3 Rear Lift Forks Subsystem Description

The rear forks are only capable of moving up or down. Each fork is driven by its own gear reduction and 16 HP, 900 rpm electric motor. The output of the drive is a rotating ACME type screw which, as it turns inside the rear fork lift tube, drives an ACME nut that raises or lowers the fork. The height of the rear lift fork is controlled by limit switches as well as being mechanically unable to lift an aging overpack height more than 12 inches above the floor/ground (Ref. B6.1.1, Sections 2.1.4 and 2).

B6.2.1.4 Lift Support Arms Subsystem Description

The front support arms have constrained movement which consists of a clockwise/counterclockwise rotation and up and down movement. The right and left assemblies

are mirror images of one another and move as a synchronous pair although they are each driven by its own gear reduction and 20 hp, 900 rpm electric motor (Ref. B6.1.1, Section 2.1.5).

The operator positions the lift support arms around the lifting forks. After the site transporter has been positioned properly around the aging overpack or shielded transfer cask (STC), the rear forks are raised to contact the bottom of the aging overpack's lifting slots. Limit and position switches ensure the lift support arms are in the correct position. Additional limit switches prevent the support arms from exceeding the 12-inch lift.

B6.2.1.5 Restraints Subsystem Description

When the load on the site transporter is ready to be lifted, the three arms of the restraint system are activated and moved to a location "near" the aging overpack. This location is determined by a combination of operator observation and integral limit switches.

After the aging overpack has been raised to the specified transportation height, the restraint arms are engaged to hold the aging overpack in place during movement. The arms are moved by linear electromechanical actuators. In addition, a locking pin is utilized to take extreme loads as well as serve as an interlock device. The three restraint arms must be properly pinned before the interlock will allow the site transporter to be moved (Ref. B6.1.3).

B6.2.1.6 Vehicle Controls Subsystem Description

The site transporter can be operated in two modes: a remote (wireless) control and an operator controlled pendant (Ref. B6.1.1, Section 2.1.7). Both of these devices have the same capability. Table B6.2-1 contains a list of controls that are available on the controller and the corresponding activation device (Ref. B6.1.3, Sheet 3 of 3).

Table B6.2-1. Site Transporter Remote or Pendant Controls

Site Transporter Operation	Activation Device on Controller
Start/Stop	Pushbutton
Emergency stop	Palm button
Restraint pin—Engage(In)/Disengage (Out)	Selector switch
Maintenance--left side/right side/rear/all	Keyed selector switch
Track synch—left/right/both	Selector switch
Bypass—Normal/bypass	Keyed selector switch
Support arms—in/out	Induction pushbutton
Support arms—raise/lower	Induction pushbutton
Forks—raise/lower	Induction pushbutton
Restraint—in/out	Induction pushbutton
Left Track—forward/reverse	Induction pushbutton
Right Track—forward/reverse	Induction pushbutton
Support Arms—off/in_out/raise_lower	Selector switch
Motion—off/tracks/restraints	Selector switch
Lift—off/forks/forks_support arms	Selector switch

Source: Original

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.

B6.2.2 Normal Operations

Once the lift has been 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. Once the site transporter arrives at the facility, the operator stops the vehicle outside the Site Transporter Vestibule and turns off the diesel generator. An electrical umbilical cord is manually retrieved from inside the building and attached to the site transporter. The site transporter is never operated inside the WHF on diesel power.

Once inside the building, the operator positions the site transporter in the Loading Room. When work is being performed on the aging overpack, the site transporter operator will remove the pins from the restraint arms and disengage them from the aging overpack. The movement interlock is engaged when the pins are removed. The operator lowers the aging overpack to the floor. The procedure is reversed when it is necessary to move the site transporter again inside the facility: the pins will be inserted, the restraints will be engaged, the aging overpack is raised from the floor and the umbilical cord attached.

The operations used to move an unloaded aging overpack are identical but not considered in this analysis.

B6.2.3 Site Transporter Off-Normal Operations

There are four off nominal conditions that could occur during the movement of an aging overpack in the WHF. When any of these occur, the operator response encompasses only those actions to return the aging overpack to a safe state. These are:

1. Lowering the forks without electrical power
2. Rotating the lift support arms without electrical power
3. On-board generator fails to operate
4. Track belt fails.

In the event of a loss of power, the site transporter is designed to stop, retain its load and enter a "lock mode" safe state. Upon the restoration of power the site transporter shall stay in the "lock mode" safe state until operator action is taken (Ref. B6.1.2, Section 7.2.3-5).

B6.2.4 Site Transporter Testing and Maintenance

Testing and maintenance of the site transporter is done on a periodic basis and does not affect the normal operations of the site transporter. Testing and/or maintenance are not performed on a site transporter loaded with an aging overpack or an STC. A site transporter that has malfunctioned or has a warning light lit on the site transporter will be deemed unserviceable and turned in for maintenance. Unserviceable vehicles will not be used.

If an unserviceable state is identified during a lift/lower or movement activity, the site transporter shall immediately be placed in a safe state (as quickly as possible) and recovery actions for the site transporter will be invoked.

B6.2.5 Site Transporter System/Pivotal Event Success Criteria

A site transporter failure is the initiating event in three event sequences in the WHF as shown in Table B6.2-2.

Table B6.2-2. Site Transporter Initiating Events by ESD

Site Transporter Initiating Event	Affected ESD
Site transporter collision	ESD03: Receipt of AO within WHF ESD11: Movement of the ST in the WHF or Export of AO from WHF
Site transporter rollover	ESD03: Receipt of AO within WHF ESD11: Movement of the ST in the WHF or Export of AO from WHF
Site transporter spurious movement	ESD13: Lifting and lowering a canister during transfer with CTM

NOTE: AO = aging overpack; CTM = canister transfer machine; ESD = event sequence diagram; ST = site transporter; WHF = Wet Handling Facility.

Source: Original

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals can not be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

Requirements

Two means of stopping the site transporter are incorporated in the controllers. One is the normal stop button and the other shall consist of an emergency stop that is the equivalent of a dead man switch.

On the loss of AC power derived from the facility, the site transporter shall immediately enter the "lock mode" safe state. The "lock mode" safe state shall not be reversible without specific operator action.

There is no testing or maintenance permitted on a site transporter loaded with an aging overpack.

Since the dominant contributor to site transporter collision in the facility is human error, no priority shall be given to either the remote or the pendant controllers.

Design Features

Stopping the site transporter is accomplished by pushing the "stop" button on the remote or pendant controller. The site transporter, upon receiving a stop command from either control source immediately responds by removing power from the propulsion system.

The site transporter is only able to perform one function at any time. It can lift a aging overpack or it can move it, but it can not perform both functions at the same time. This feature is accomplished by interlock and by power limitations inherent in the sizing of the power plant that ensures a limited amount of power for each of the electromechanical devices and drive system.

B6.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

Dependencies are broken down into five categories with respect to their interactions with system, structures, and components. The five areas considered are addressed in Table B6.3-1 with the following dependencies:

1. Functional dependence
2. Environmental dependence
3. Spatial dependence
4. Human dependence
5. Failures based on external events.

Table B6.3-1. Dependencies and Interactions Analysis

Systems, Structures, Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Lift booms	Material failure ACME screw/nut	—	—	—	—
Lift support arms	Material failure ACME screw/nut	—	—	—	—
Restraint arms	Material failure	—	—	—	—
Power plant	Current overload protection fails Safe state on	—	—	Failure to stop Failure to remove power cable	—
Remote control	Spurious commands	—	—	Improper command	Collide with crane rigging
Tracks	—	—	—	Failure to stop	—

Source: Original

B6.4 RELATED FAILURE SCENARIOS

There are three basic site transporter fault trees developed for the WHF. The top events for these fault trees are:

1. Site transporter collides with WHF structures
2. Site transporter rollover
3. Site transporter spurious movement during canister transfer.

A fourth scenario, site transporter load drop, was screened from further consideration in the WHF; see Table 6.0-2.

B6.4.1 Site Transporter Collides with WHF Structures (ESD-03, -11)

B6.4.1.1 Description

The fault trees for the collision events are identical. Collisions can occur as a result of human error or mechanical failures (human error events are uniquely identified but all have the same screening value of 3E-3 with a lognormal error factor of 5). Mechanical failures leading to a collision consist of: the site transporter fails to stop when commanded, the site transporter exceeding a safe speed, or the site transporter moves in the wrong direction.

B6.4.1.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the site transporter for mechanical failures. The site transporter operator continuously maintains situational awareness and proper control of the movement of the site transporter. To avoid collisions, the site transporter must stop when commanded, be prevented from entering a runaway situation or respond correctly to a site transporter movement command.

The site transporter is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the site transporter 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 site transporter will immediately stop all movement and enters into a "lock mode" safe state. The site transporter will remain in this "lock mode" safe state until power is returned and the operator restarts the site transporter.

Runaway situations on the site transporter are prevented by mechanical constraints. The maximum speed of the site transporter is limited by motor current overload protection (Ref. B6.1.1, Section 3.2.1). The site transporter motor speed and gearing prevents the site transporter from exceeding 2.5 mph.

The prevention of site transporter movements in the wrong direction is prevented by the limitation of the power plant that prevents simultaneous operations.

B6.4.1.3 Design Requirements and Features

Requirements

The site transporter has two off-equipment control devices that have complete control over the site transporter.

Features

Drive system consists of an electric motor and a transmission constraint which limits the maximum speed of the site transporter to 2.5 mph.

B6.4.1.4 Fault Tree Model

The fault tree model for "Site Transporter Collides with WHF Structures in the WHF" accounts for the both human error and/or site transporter mechanical problems that could result in collision. There are three distinct movements within the WHF which are reversed if an aging overpack is picked up in the WHF and taken to the aging pads. Movement within the facility is restricted and even at low speeds a collision can occur.

The fault tree considers mechanical failures that fail to stop the site transporter, events that could cause the site transporter to exceed a safe speed, and events that could cause the site transporter to move in the wrong direction.

B6.4.1.5 Basic Event Data

Table B6.4-1 lists the basic events used in the "Site Transporter Collides with WHF Structures" fault tree.

Table B6.4-1. Basic Event Probability for Site Transporter Collides with WHF Structures

BASIC EVENTS PROBABILITY REPORT					
Project: Yucca-Mountain ST Collision in Facility		**Case: Current Units: Per Hour**			
Name	**Calculation Type[a]**	**Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time[a]**
050-OPSTCOLLIDE3-HFI-NOD	1	3.00E-03	3.00E-03	—	—
050-ST---BRK001--BRK-FOD	1	1.46E-06	1.46E-06	—	—
050-ST---CBP004-CBP--OPC	3	9.13E-08	—	9.13E-08	1.00E+00
050-ST---CBP004-CBP--SHC	3	1.88E-08	—	1.88E-08	1.00E+00
050-ST---CT000---CT--FOD	1	4.00E-06	4.00E-06	—	—
050-ST---CT002---CT--FOH	3	6.88E-05	—	6.88E-05	1.00E+00
050-ST---HC001--HC--FOD	1	1.74E-03	1.74E-03	—	—
050-ST---HC002---HC--SPO	3	5.23E-07	—	5.23E-07	1.00E+00
050-ST---MOE000--MOE-FSO	3	1.35E-08	—	1.35E-08	1.00E+00
050-ST---MOE021--MOE-FSO	3	1.35E-08	—	1.35E-08	1.00E+00
050-ST---SC021---SC--FOH	3	1.28E-04	—	1.28E-04	1.00E+00
050-ST---SC021---SC--SPO	3	3.20E-05	—	3.20E-05	1.00E+00
050-ST---SEL021--SEL-FOH	3	4.16E-06	—	4.16E-06	1.00E+00
LOSP-4	1	4.1E-06	4.1E-06	—	—

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

ST = site transporter.

Source: Original

B6.4.1.5.1 Human Failure Events

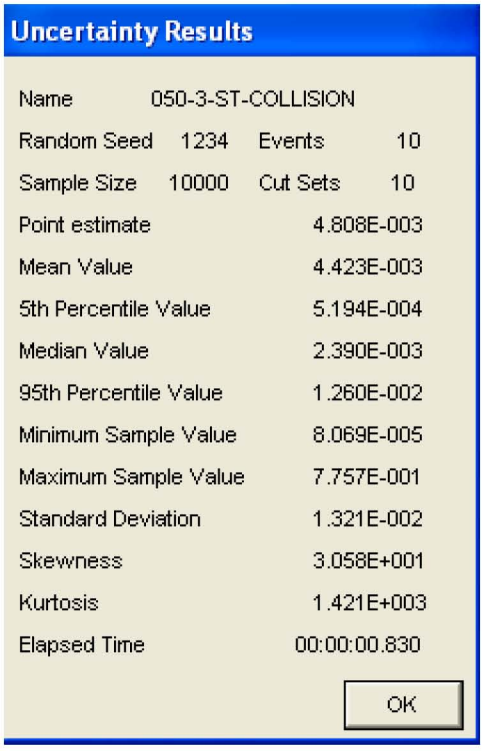
There is one human event in the collision trees for the site transporter and accounts for the site transporter operator causing the collision. This human error is set at the screening value of 3E-03 for all three ESD events.

B6.4.1.5.2 Common-Cause Failures

There are no CCF events identified for this fault tree.

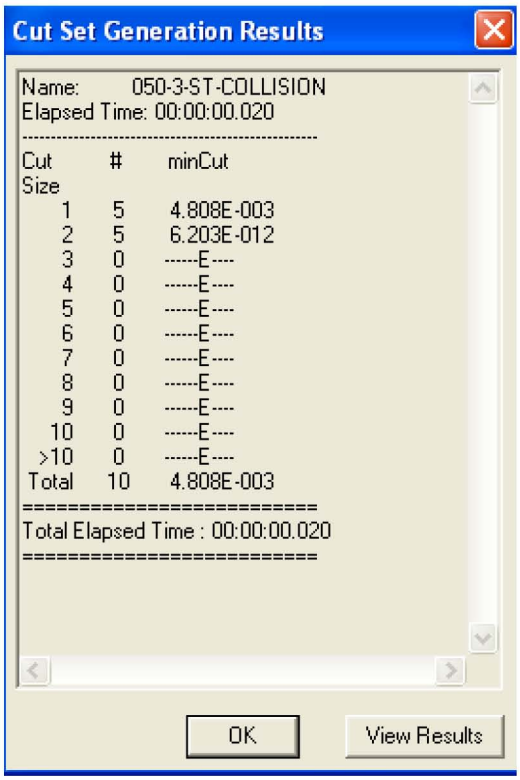
B6.4.1.6 Uncertainty and Cut Set Generation

Figures B6.4-1 and B6.4-2 contain the uncertainty and the cut set generation results for site transporter collision in facility using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-1. Uncertainty Results for the "Site Transporter Collides with WHF Structures" Fault Tree



Source: Original

Figure B6.4-2. Cut Set Generation Results for the "Site Transporter Collides with WHF Structures" Fault Tree

B6.4.1.7 Cut Sets

Table B6.4-2 contains the cut sets for "Site Transporter Collides with Facility Structures" fault tree.

Table B6.4-2. Cut Sets for the Site Transporter Collides with Facility Structures

Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
050-3-ST-COLLISION	62.40	3.000E-003	050-OPSTCOLLIDE3-HFI-NOD	Operator Error Causes Collision	3.0E-003
	36.19	1.740E-003	050-ST---HC001--HC--FOD	Remote Control Transmits Wrong Signal	1.7E-003
	1.43	6.880E-005	050-ST---CT002---CT--FOH	Direction Controller Fails	6.9E-005
	0.08	4.000E-006	050-ST---CT000---CT--FOD	ST Primary Stop Switch Fails	4.0E-006
	0.01	5.230E-007	050-ST---HC002---HC--SPO	Spurious Command to Lift/Lower AO or STC	5.2E-007
	0.00	5.986E-012	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006
			LOSP-4	Failure of Off Site Power	4.1E-006

Table B6.4-2. Cut Sets for the Site Transporter Collision in Facility (Continued)

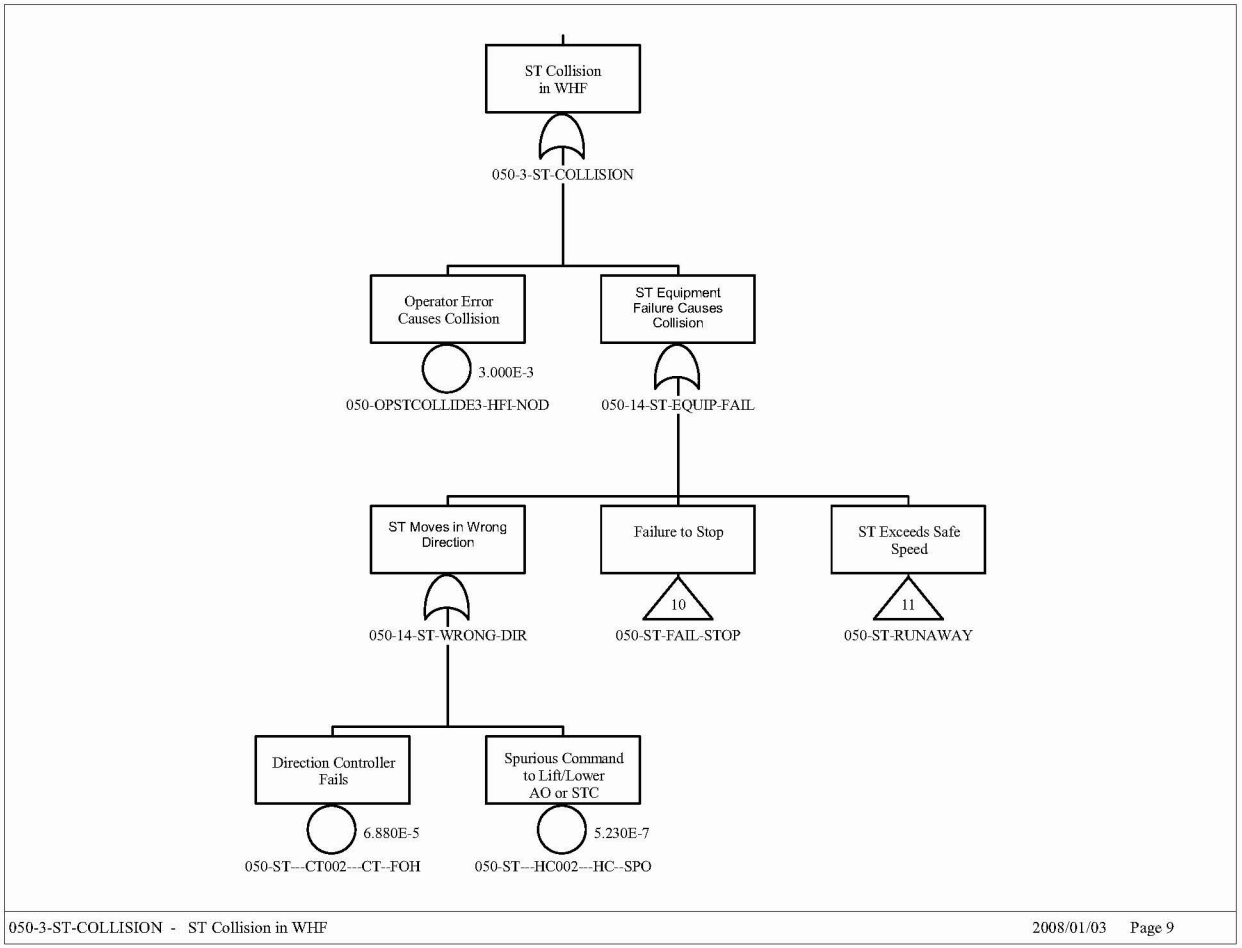
Fault Tree	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
050-3-ST-COLLISION	0.00	1.333E-013	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006
			050-ST---CBP004-CBP--OPC	ST Power Cable - Open Circuit	9.1E-008
	0.00	5.535E-014	050-ST---MOE000--MOE-FSO	ST Lock Mode State Fails on Loss of Power	1.4E-008
			LOSP-4	Failure of Off Site Power	4.1E-006
	0.00	2.745E-014	050-ST---BRK001--BRK-FOD	ST Fails to Stop on Loss of Power	1.5E-006
			050-ST---CBP004-CBP--SHC	ST Power Cable Short Circuit	1.9E-008
	0.00	1.233E-015	050-ST---CBP004-CBP--OPC	ST Power Cable - Open Circuit	9.1E-008
			050-ST---MOE000--MOE-FSO	ST Lock Mode State Fails on Loss of Power	1.4E-008
	4.808E-003			= Total	

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask.

Source: Original

B6.4.1.8 Fault Tree

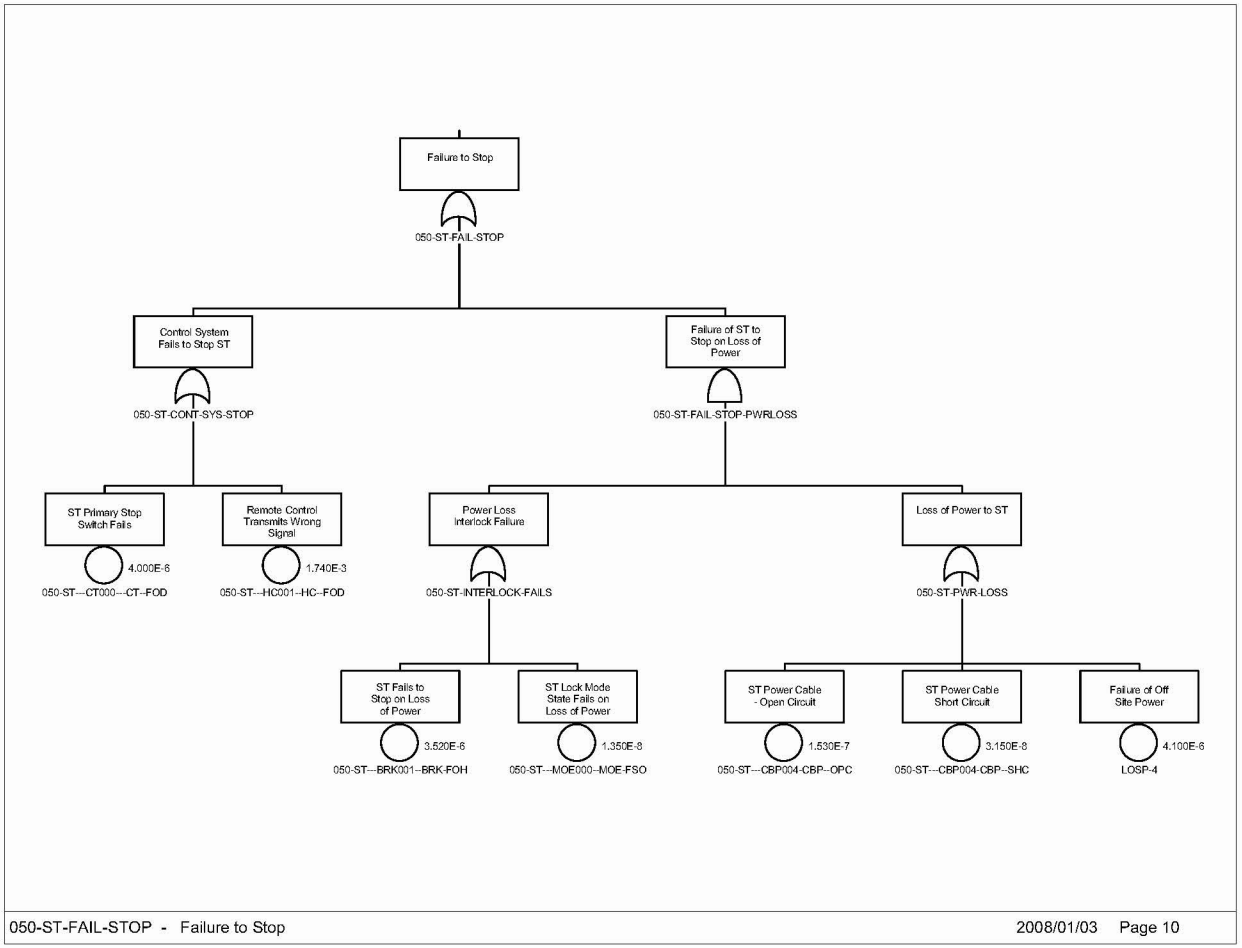
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-3. Site Transporter Collision in the WHF

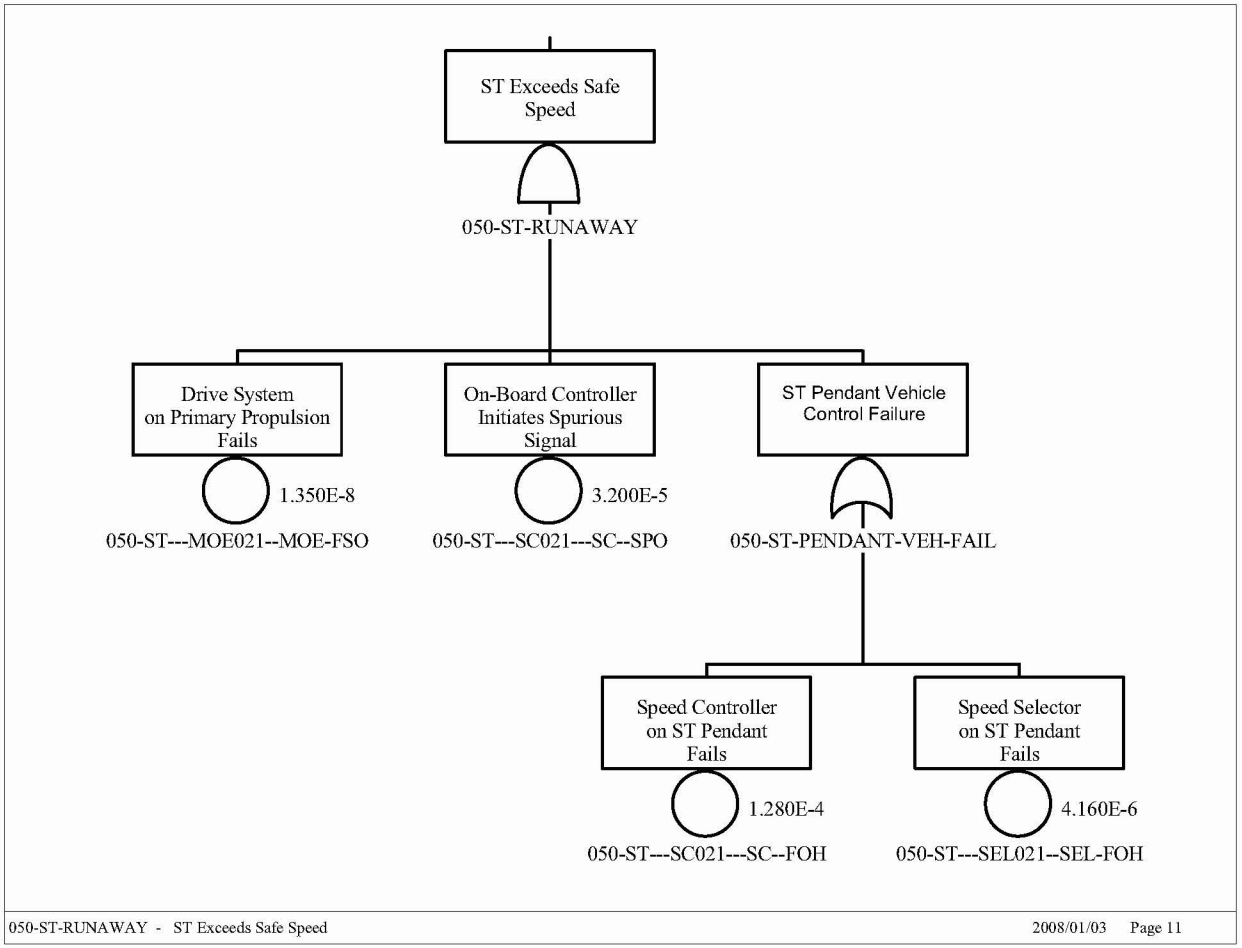
INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-4. Failure to Stop

INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-5. Site Transporter Exceeds Safe Speed

INTENTIONALLY LEFT BLANK

B6.4.2 Site Transporter Rollover (Tip-over) (ESD-03, -11)

B6.4.2.1 Description

Although the site transporter has been designed to have a low center of gravity and a wide footprint, there is a possibility of a rollover caused by a track failure with a subsequent operator failure to stop the site transporter upon loss of a track. The track would have to fail in a manner such that it binds (i.e., rolls up), the site transporter drives over the failed track, and the site transporter tilts to an angle that results in a tipover condition.

B6.4.2.2 Success Criteria

The design of the site transporter prevents the majority of scenarios that could potentially cause a site transporter rollover. The site transporter is designed to negotiate a 5% grade and a 2% cross-slope. In addition, the aging overpack is physically prevented from being lifted more than 12 inches. The combination of the low lift of the aging overpack or STC, the low center of gravity, and wide footprint of the site transporter results in stable platform during movements.

During movement, a site transporter track failure could result in a potential tip-over situation. There is no design constraint for this failure mode, preventing this situation relies on an operator awareness and response time to this situation to initiate an emergency stop command. The operator has several seconds to respond to the track failure; however, since this is a recovery action, no credit is taken for the operator response.

B6.4.2.3 Design Requirements and Features

Requirements

Operator shall have the capability of stopping the site transporter in sufficient time to keep the site transporter from running off the end of a broken track.

Features

The center of gravity of a loaded site transporter with aging overpack ensures stability.

The site transporter operator has the capability to stop the operation of the site transporter during abnormal conditions.

B6.4.2.4 Fault Tree Model

Human error is conservatively postulated to result in a rollover/tip-over if the operator does not stop the site transporter in sufficient time to prevent the site transporter from running off the broken track.

B6.4.2.5 Basic Event Data

Table B6.4-3 lists the basic events used in the site transporter drop load during lift/movement fault tree.

Table B6.4-3. Basic Event Probability for the Site Transporter Rollover

BASIC EVENTS PROBABILITY REPORT					
Project: Yucca-Mountain ST Rollover Name	**Calculation Type[a]**	**Case: Current Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time[a]**
050-CRWT-TRD0001-TRD-FOH	3	5.890E-007	—	5.890E-007	1.000E+000
050-CRWT-TRD0002-TRD-FOH	3	5.890E-007	—	5.890E-007	1.000E+000
050-CRWT-TRD0003-TRD-FOH	3	5.890E-007	—	5.890E-007	1.000E+000
050-CRWT-TRD0004-TRD-FOH	3	5.890E-007	—	5.890E-007	1.000E+000
050-OPFAILSTOP-HFI-FOD	1	1.000E+000	1.000E+000	—	—

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.

ST = site transporter.

Source Original

B6.4.2.5.1 Human Failure Events

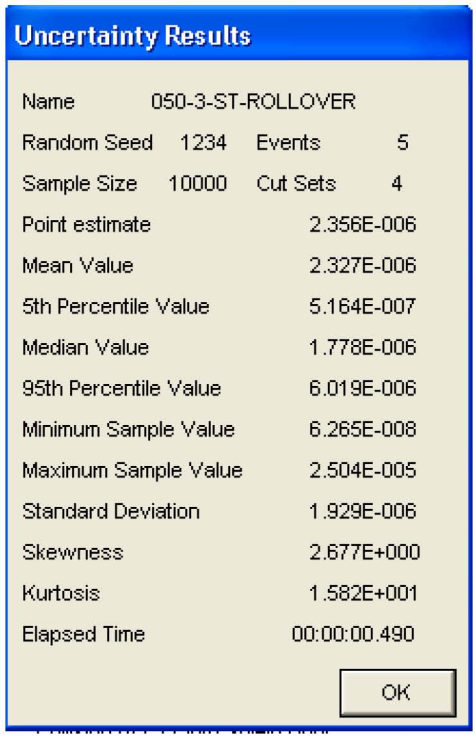
There is one human error failure event included in this model. It is conservatively set to a value of 1E+0 because unsafe actions that require an equipment failure to cause an initiating event are generically assigned a screening human error probability (HEP) of 1.0 (see Attachment E, Table E6.4-1).

B6.4.2.5.2 Common Cause Failures

There are no CCFs identified for this fault tree.

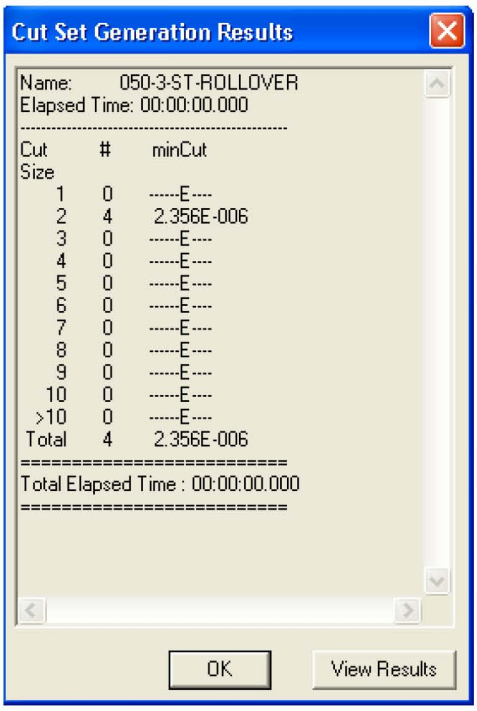
B6.4.2.6 Uncertainty and Cut Set Generation

Figures B6.4-6 and B6.4-7 contain the uncertainty and the cut set generation results for "Site Transporter Rollover (tip-over)" fault tree using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-6. Uncertainty Results from “Site Transporter Rollover” Fault Tree



Source: Original

Figure B6.4-7. Cut Set Generation Results from "Site Transporter Rollover" Fault Tree

B6.4.2.7 Cut Sets

Table B6.4-4 contains the cut sets for "Site Transporter Rollover."

Table B6.4-4. Cut Sets for the Site Transporter Rollover (Tip-over)

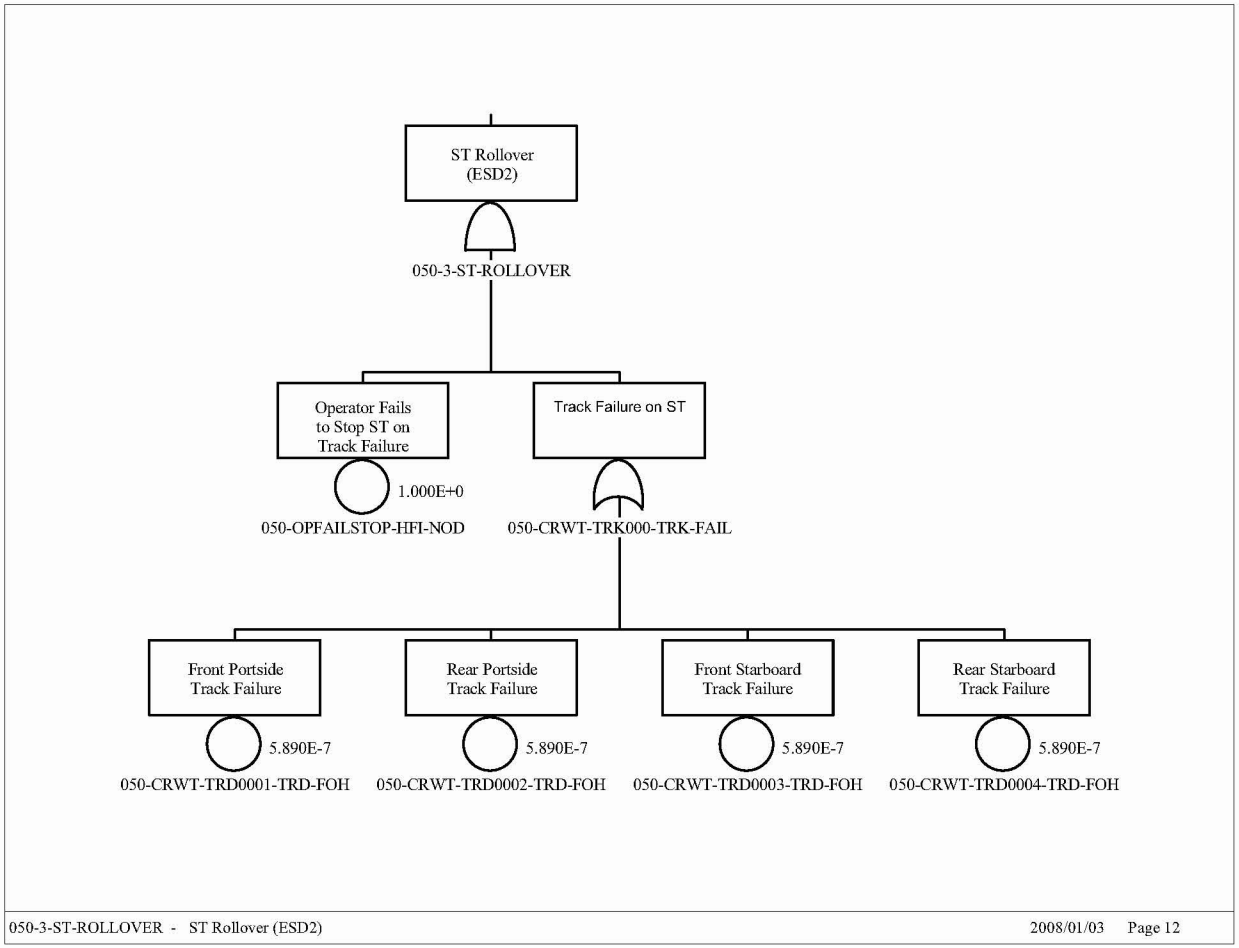
Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-3-ST-ROLLOVER	25.00	5.890E-007	050-CRWT-TRD0001-TRD-FOH	Front Portside Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0002-TRD-FOH	Rear Portside Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0003-TRD-FOH	Front Starboard Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
	25.00	5.890E-007	050-CRWT-TRD0004-TRD-FOH	Rear Starboard Track Failure	5.9E-007
			050-OPFAILSTOP-HFI-NOD	Operator Fails to Stop ST on Track Failure	1.0E+000
2.356E-006 = Total					

NOTE: ST = site transporter.

Source Original

B6.4.2.8 Fault Tree

INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-8. Site Transporter Rollover Fault Tree

INTENTIONALLY LEFT BLANK

B6.4.3 Site Transporter Spurious Movement (ESD-13)

B6.4.3.1 Description

The fault tree for "Site Transporter Spurious Movement" in this event sequence addresses activities associated with transfers of canisters from or to aging overpacks in the Loading Room.

B6.4.3.2 Success Criteria

Spurious movement of the site transporter is prevented by the inherent design constraints of the site transporter. There is only sufficient electrical power to perform one type of operation at a time. For example, it is not possible to command a lift/lower of the aging overpack when the site transporter is moving. Spurious signals cannot be generated when primary power is removed from the site transporter (i.e., diesel engine shut down and/or facility electrical power cord disconnected). There are no batteries or capacitors in the site transporter that can store electrical energy.

B6.4.3.3 Design Requirements and Features

Requirements

Site transporter power and the remote control pendant shall be removed from the site transporter when it has been positioned within the Loading Room.

Facility power and the control pendant are removed from the site transporter when it has been properly position within the Loading Room.

On removal of AC power derived from the facility, the site transporter immediately enters the "lock mode" safe state. The "lock mode" safe state is not be reversible without specific operator action.

Features

There are no electrical storage devices capable of propelling the site transporter with electrical energy when the AC power cable is removed. When the AC power cable is removed, the on-board diesel generator must be operating to cause the site transporter to move.

A shield door interlock shall be designed to ensure facility power has been removed from the site transporter.

B6.4.3.4 Fault Tree Model

The fault tree model for "Site Transporter Spurious Movement" in the Loading Room accounts for failure to remove facility power and the possibility of the site transporter receiving a spurious movement command for the remote control device.

B6.4.3.5 Basic Event Data

Table B6.4-5 lists the basic events used in the "Site Transporter Spurious Movement" fault tree.

Table B6.4-5. Basic Event Probability for Site Transporter Spurious Movement

BASIC EVENTS PROBABILITY REPORT					
Project: Yucca-Mountain ST Spurious Movement Name	**Case: Current Calculation Type[a]**	**Units: Per Hour Calculation Probability**	**Failure Probability**	**Lambda**	**Mission Time[a]**
050-CR---IEL001--IEL-FOD	1	2.75E-05	2.75E-05	—	—
050-CR---IEL002--IEL-FOD	1	2.75E-05	2.75E-05	—	—
050-CR---IELCCF--IEL-FOH	C	1.29E-06	—	—	—
050-OPNOUNPLUGST-HFI-NOD	1	1.00E-03	1.00E-03	—	—
050-ST---HC000--HC--SPO	3	5.23E-07	—	5.23E-07	1.00E+00
050-ST---SC002--SC--FOH	3	1.28E-04	—	1.28E-04	1.00E+00
050-ST---SC021---SC--SPO	3	3.20E-05	—	3.20E-05	1.00E+00

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time. See Table 6.3-1 for definitions of calculation types.

ST = site transporter.

Source: Original

B6.4.3.5.1 Human Failure Events

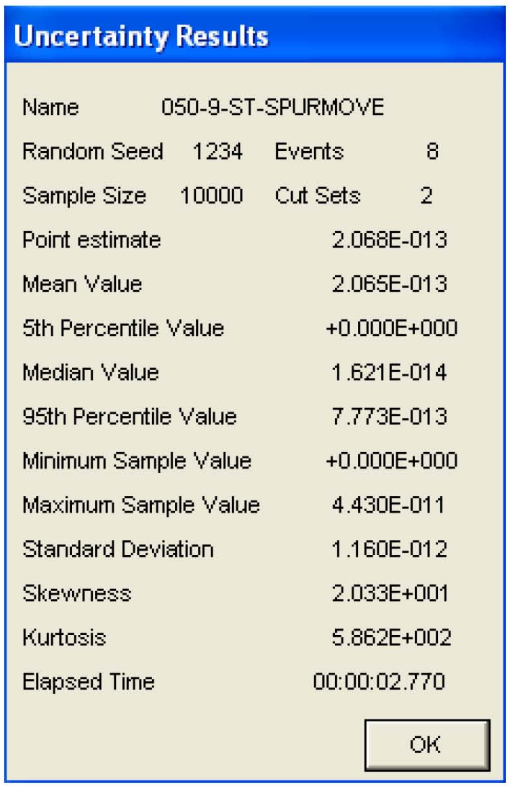
There is one human error associated with this fault tree that addresses an operator failure to unplug the site transporter power cable after it has been parked in the Loading Room.

B6.4.3.5.2 Common Cause Failures

There is one CCF associated with two interlock failures on the slide gates. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criteria (see Attachment C, Table C3-1, CCCG = 2).

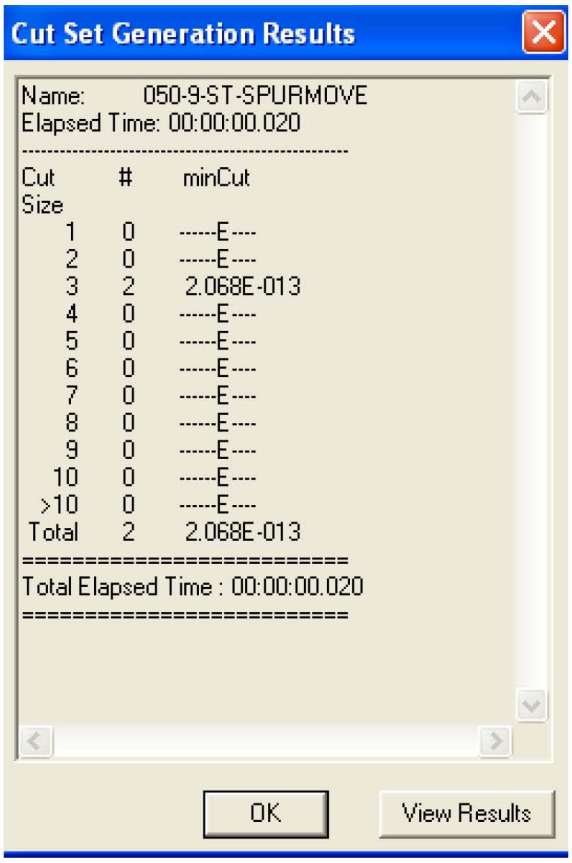
B6.4.3.6 Uncertainty and Cut Set Generation

Figures B6.4-9 and B6.4-10 contain the uncertainty and the cut set generation results for "Site Transporter Spurious Movement" using a cutoff probability of 1E-15.



Source: Original

Figure B6.4-9. Uncertainty Results for the "Site Transporter Spurious Movement" Fault Tree



Source: Original

Figure B6.4-10. Cut Set Generation Results for the "Site Transporter Spurious Movement" Fault Tree

B6.4.3.7 Cut Sets

Table B6.4-6 contains the cut sets for the "Site Transporter Spurious Movement" fault tree.

Table B6.4-6. Cut Sets for the Site Transporter Spurious Movement

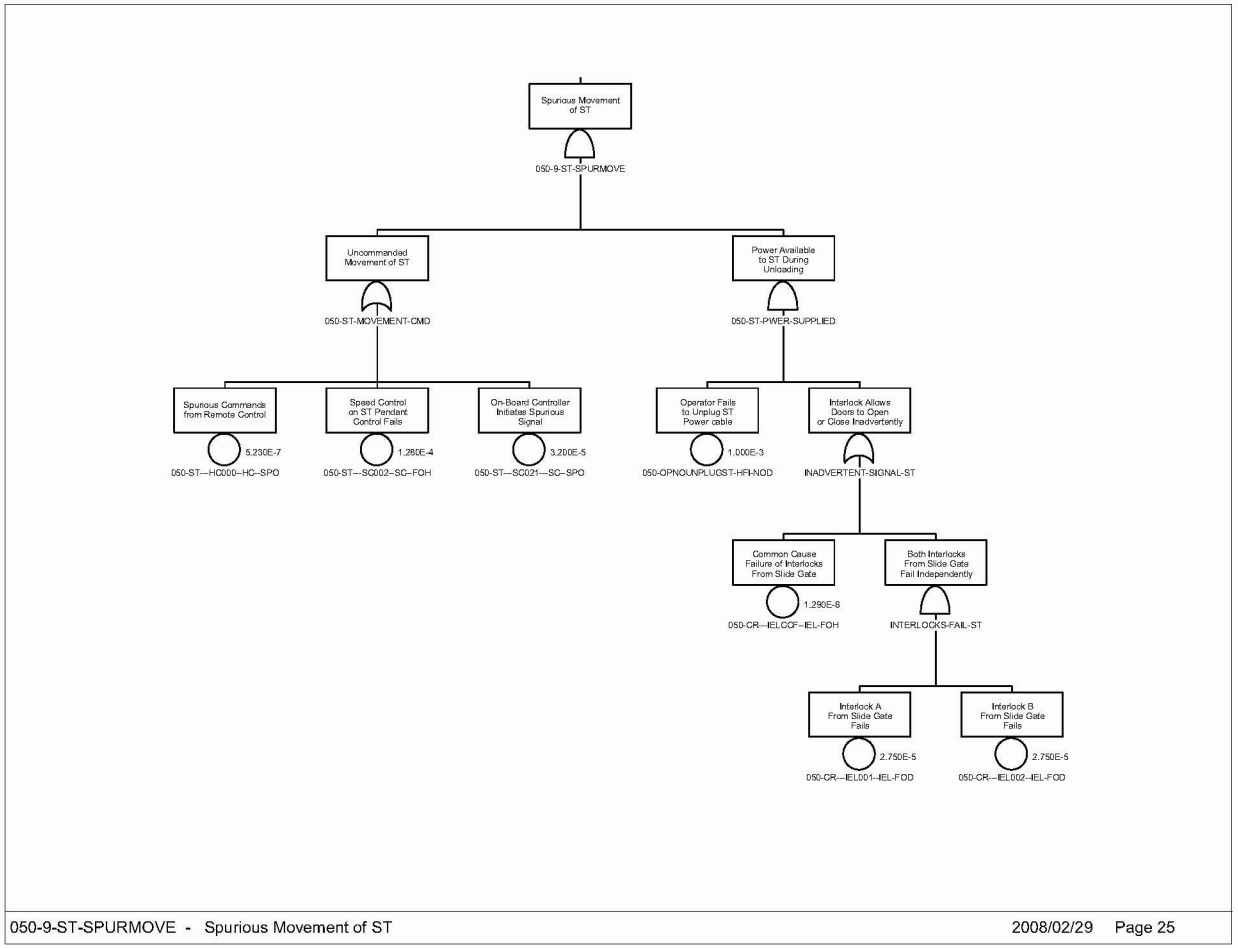
Fault Tree	Cut Set %	Probability /Frequency	Basic Event	Description	Probability
050-9-ST-SPURMOVE	79.98	1.654E-013	050-CR---IELCCF--IEL-FOH	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			050-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			050-ST---SC002--SC--FOH	Speed Control on ST Pendant Control Fails	1.3E-004
	20.00	4.136E-014	050-CR---IELCCF--IEL-FOH	Common Cause Failure of Interlocks From Slide Gate	1.3E-006
			050-OPNOUNPLUGST-HFI-NOD	Operator Fails to Unplug ST Power cable	1.0E-003
			050-ST---SC021---SC--SPO	On-Board Controller Initiates Spurious Signal	3.2E-005
				2.068E-013	

NOTE: ST = site transporter.

Source Original

B6.4.3.8 Fault Tree

INTENTIONALLY LEFT BLANK



Source: Original

Figure B6.4-11. Site Transporter Spurious Movement

INTENTIONALLY LEFT BLANK

B7 HEATING, VENTILATION, AND AIR CONDITIONING FAULT TREE ANALYSIS

B7.1 REFERENCES

Design Inputs

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an asterisk (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

B7.1.1 BSC 2007. *WHF Equipment Sizing and Selection Calculation (ITS)*. 050-M8C-VC00-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071031.0001.

B7.1.2 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System—Train A Ventilation & Instrumentation Diagram*. 050-M80-VC00-00102-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0014.

B7.1.3 BSC 2007. *Wet Handling Facility ITS Confinement Areas HEPA Exhaust System—Train B Ventilation & Instrumentation Diagram*. 050-M80-VC00-00103-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071204.0015.

B7.1.4 *BSC 2007. *Wet Handling Facility Composite Vent Flow Diagram Tertiary Confinement Non-ITS HVAC Supply & Exhaust System.* 050-M50-VCT0-00101-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0002.

Design Constraints

B7.1.9 NRC (Nuclear Regulatory Commission) 2007. *Preclosure Safety Analysis - Dose Performance Objectives and Radiation Protection Program.* HLWRS-ISG-03. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20070918.0096.

B7.2 IMPORTANT TO SAFETY HEATING, VENTILATION, AND AIR CONDITIONING DESCRIPTION

B7.2.1 Overview

The ITS heating, ventilation, and air conditioning (HVAC) provides high-efficiency particulate air (HEPA) filtered exhaust from the WHF waste handling areas denoted as tertiary confinement (C2) zones. This minimizes the potential of discharging radioactive material released during waste handling operations into the environment. The ITS HVAC system consists of two identical trains. Each train consists of one exhaust fan, three parallel HEPA filtered exhaust plenums, isolation and backdraft dampers, and associated instrumentation and controls. The normal system lineup is with one train operating and the other train in standby. Each HVAC train exhausts air through separate discharge ducts into the atmosphere. A backdraft damper is used on each train to ensure there is no airflow from the atmosphere back through the standby train.

A simplified schematic of the system and its associated controls is given in Figure B7.2-1. The source of information for Figure B7.2-1 is Refs. B7.1.1 and B7.1.2. The general location of the major HVAC components and the general direction of air flow through the waste handling areas are depicted in Figure B7.2-1.

Air distribution, ventilation rates, and transport velocities required to maintain design negative pressures and flows within the C2 zones are provided in *WHF Equipment Sizing and Selection Calculation (ITS)* (Ref. B7.1.1, Section 6.1).

Major components comprising the HVAC system include: a series of dampers that isolate components, and prevent reverse flow through the system; six HEPA filter plenums (three in each train) that remove particulate matter from the exhaust; and two exhaust fans (one in each train). Normal system control is provided by the digital control and management information system (DCMIS) through ASDs associated with each fan. ITS controls are hardwired bypassing the DCMIS to the fan ASD.

B7.2.2 Dampers

The ITS HVAC system uses manual, backdraft, and tornado dampers to control flow and pressure inside the containment area, isolate components, and prevent backflow through the standby system. With the exception of the tornado and backdraft dampers, all control dampers in the ITS HVAC system are manual dampers. These dampers may be closed when maintenance is required on the standby train.

Manual dampers are located on the input and output sides of the HEPA filter plenum. These dampers are used to isolate the HEPA filter plenum, if required, during maintenance. There is a manual damper on the input side of the exhaust fan that is used to isolate the entire HEPA filter subsystem for maintenance on the HEPA filters or the exhaust fan. One additional manual damper is located between the backdraft and the tornado damper which can be used to isolate the entire train.

A backdraft damper is located on the exhaust side of the fan. This damper is normally open for the operating train and closed on the standby train. This damper prevents reverse airflow through the standby system as a result of the negative delta pressure in the C2 areas.

A tornado damper is used to control airflow automatically to prevent the transmission of tornado pressure surges from outside the facility.

Failure modes considered for these dampers are summarized in the following table (Table B7.2-1).

Table B7.2-1. HVAC Damper Failure Modes

Damper Type	Failure Mode	Discussion
Manual Dampers	Fail to remain open	These dampers are normally open dampers that are used to isolate equipment. They will block flow within a train if they fail to a closed position or were not restored to an open position if they were closed to isolate a component for maintenance.
Backdraft Dampers	Fail to open	Back draft dampers close when the exhaust fan is not running to prevent backflow through the system. They are supposed to open when the exhaust fan starts. If the damper fails to open flow will be blocked, failing the train.
	Fail to remain open	If the backdraft damper fails to remain open while the exhaust fan is running, flow through the train will be lost.
Tornado Dampers	Fail to remain open	The tornado damper is intended to close and isolate its associated HVAC train from pressure transients caused by a tornado. If it closes at any time other than when tornado conditions exist it will block flow and defeat the train. If it operates as it is supposed to when tornado conditions exist it will close, blocking flow and defeating its associated HVAC train. Both conditions are captured in the tornado damper fails closed event in the HVAC fault tree.
	Fail to close	If the tornado damper fails to close when tornado conditions exist it would allow pressure transients within the train that could damage ducting or components.

NOTE: HVAC = heating, ventilation, and air conditioning.

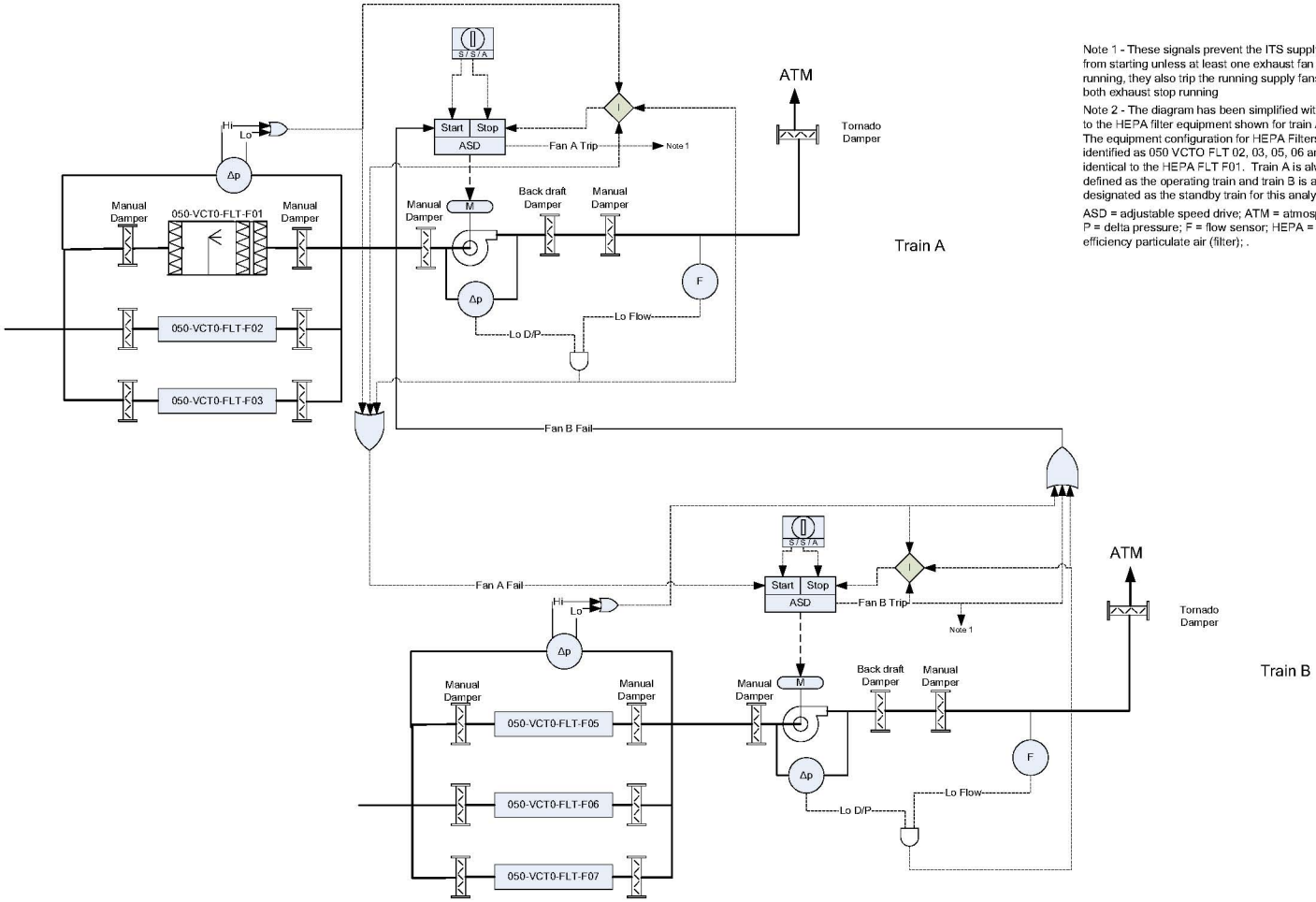
Source Original

B7.2.3 HEPA Filter Plenums

In each train there are three parallel HEPA filter plenums. Each plenum contains a preliminary bank of medium-efficiency roughing filters; followed by two banks of high-efficiency filters for particulate removal. The unit also contains a mister/demister for maintaining proper humidity levels and a water deluge system for fire suppression. The HEPA plenums also contain an inlet test section, a combination test section, and an outlet test section; these sections and the deluge system are not modeled in the fault tree analysis.

The preliminary bank of roughing filters consists of a 3 × 3 array (nine filters). The roughing filters are followed by two banks of HEPA filters. Each bank consists of 3 × 3 array (nine filters) for a total of 18 filters.

INTENTIONALLY LEFT BLANK



NOTE: The diagram has been simplified with respect to the HEPA filter equipment shown for Train A and B. The equipment configuration for HEPA filters identified as 050 VCTO FLT 02, 03, 05, 06 and 07are identical to the HEPA FLT 01. In addition, Train B has the same input/output dampers shown for Train A.

Source: Original

Figure B7.2-1. Block Diagram of the WHF ITS HVAC System

INTENTIONALLY LEFT BLANK

Failure modes associated with the filter plenums considered in the analysis includes the HEPA filter bank for plugs and leaks, mister/demister for humidity control, and the medium roughing filter. A bag-in/bag-out procedure is used to replace the HEPA filters.

Table B7.2-2. HEPA Plenum Failure Modes

Plenum Component	Failure Mode	Discussion
Mister/Demister	Plugs	The demister removes entrained moisture from the air by causing the air to rapidly change direction as it flows through the demister panel. This panel can become plugged with a combination of particulates and moisture over time.
Filters including the HEPA and roughing filters	Plug	Plugging of the filters will reduce flow, failing the train. When the supply fans are operating the flow rates require all three filter plenums to be operating in parallel to maintain the desired Δp. If the supply fans are inoperable the flow rates required to maintain the desired Δp are low enough that only two of the three filter plenums need to be in operation.
	Leak	Leaks through the filters can be from catastrophic failures that will be indicated by a large decrease in Δp across the filter plenum which would cause the control system to stop the operating train and start the standby train. Small leaks, such as those that might occur around the filter housing seals, however, may not be accompanied by a decrease in plenum Δp of sufficient magnitude to initiate an automatic switch over to the standby system. In this case the reduced Δp could be accompanied by increased radiation levels indicated in the discharge ducting. In this particular case the operator must recognize the indications of a small leak and initiate a manual switch over. Because leak data is does not differentiate between small and large leaks the leak failure modeled in the fault tree is accompanied by either a failure of the Δp sensing system or a failure of the operator to recognize the leaking condition.

NOTE: HEPA = high-efficiency particulate air; Δp = delta pressure.

Source Original

B7.2.4 Direct Drive Exhaust Fan and Motor

The exhaust fan and motor are sized to provide sufficient flow to meet delta pressure and air flow requirements for the WHF.

The exhaust fan motor speed is controlled by the ASD. The ASD adjusts the speed to maintain delta pressure when facility doors are opened; HEPA filters lose efficiency, or when external winds affect room pressures within the facility.

The failure modes for the exhaust fans are fail to start and fail to run.

B7.2.5 Supply Fans

Two parallel air handling units (AHUs) supply ventilation to the Waste Package Loadout Room (Room 1015) and two parallel AHUs supply ventilation to the Cask Preparation Room (Room 1026). These AHUs mix air recalculated from their associated areas with outside air to replenish leakage air flow that is exhausted by the ITS HVAC exhaust system. These systems are

considered non-ITS and are not necessary for the successful operation of the ITS HVAC exhaust system. They do, however, determine the amount of air that must be exhausted by the operating ITS HVAC exhaust system to maintain cascaded air flow and Δp within the C2 zone. When the supply fans are operating more air must be exhausted by the operating exhaust fan and all three filter plenums in the operating exhaust train must be operating to maintain the required flow. When the supply fans are not operating, less air needs to be exhausted and the flow through two HEPA plenums in the operating train are sufficient to maintain cascaded flow and Δp.

B7.2.6 Control Circuitry

Normal operation of the HVAC system is controlled by the DCMIS which controls each trains operating mode as determined by the operator (start, stop or auto). The DCMIS also controls fan speed through an ASD to maintain facility flow and pressures within normal operating limits. Functions considered ITS such as auto start of the standby train when the operating train fails are provided by hardwired interlocks that bypass the normal controls provided by the DCMIS.

The exhaust fan speed is controlled by an ASD which receives duct differential pressure signals from the DCMIS. The non-programmable ASD adjusts the exhaust fan speed to maintain these parameters within the specified operating band.

ASDs associated with the supply fans adjust the fans speed in response to temperature monitored in the room they supply. ((Ref. B7.1.2), (Ref. B7.1.3), and (Ref. B7.1.4)). The supply fans are used to stabilize the airflow within the WHF. Although these fans are non-ITS their operation impacts the air flow required to maintain Δp; consequently they are accounted for in the loss of HEPA filter plenum section of the fault tree model.

Automatic transfer from the operating train to the standby train is accomplished when the following conditions are sensed in the operating train:

- Low flow sensed in the discharge plenum occurring concurrently with a low Δp sensed across the exhaust fan, or
- Operating fan trip signal provided by the operating fan ASD indicating the fan has tripped, or
- High Δp across the operating train filter plenums indicating the plenum is plugged, or
- Low Δp across the operating train filter plenums, indicating the plenum is leaking.

B7.2.7 ITS HVAC Normal Operations

Under normal operations with non-ITS supply fans working, all three HEPA filter plenums in the train must be working to achieve the required exhaust air flow rate. The design has some reserve capacity but not enough to maintain the required delta pressure if one of the HEPA filters fails when the supply fans are operating. Under normal operations, system redundancy is provided by the second standby train.

B7.2.8 ITS HVAC Degraded Operations

The ITS HVAC system maintains proper Δp throughout designated containment areas. Exhausted air from the WHF is made-up from opening/closing doors to the outside, leaks in the structure and from one of two supply fans which are controlled by the ASD on the operating train. One of these fans in conjunction with other air makeup sources can provide sufficient airflow through the containment areas for the HVAC to maintain Δp. These supply fans are not ITS and therefore, they are not connected to the ITS power system for the WHF. Should these fans shut down, it becomes possible to maintain delta pressure with two of three HEPA filters. This special case has been added to the fault trees for the failure to maintain Δp in the WHF. In this case, there is redundancy within the train and a common-cause failure mode has been added to the fault tree.

B7.2.9 ITS HVAC Testing and Maintenance

Under normal operations Train A continues to operate until a failure is detected or the train is shut down for maintenance. Normal maintenance renders Train B unavailable 40 hours per year (the majority of operational-level maintenance can be performed on the operational train and therefore does not affect the overall availability of the standby train). During maintenance, the Train B "start/stop/auto" switch is placed in the stop position. When maintenance is completed, the standby system (Train B) is started and operational system (Train A) is shut down and is now considered to be the standby train (Train A). Maintenance may be scheduled consecutively for this train or at some future date. Under normal operations, maintenance does not result in the loss of/or the inability of the operating train to perform its intended function.

Testing is considered part of routine maintenance. When the maintenance has been completed, maintenance personnel turn the standby train on and check for normal operations including delta pressure, flow rate, and that all failure indicators are reset/off. Maintenance personnel also observe the forced shutdown of the operating system as the standby train is turned on.

Flow rates are monitored as part of testing to ensure that airflow balance is maintained.

B7.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components. The five areas considered are addressed in Table B7.3-1 with the following dependencies:

1. Functional dependence
2. Environmental dependencies
3. Spatial dependence
4. Human dependence
5. Failures based on external events.