B1.3.1.2 Truck Trailers

The U.S. Department of Transportation has the primary responsibility for regulating the safe transport of radioactive materials in the United States. It sets the standards for packaging, transporting, and handling radioactive materials, including labeling, shipping papers, loading, and unloading requirements.

Trailers used for the movement of transportation casks are designed in accordance with the National Highway Traffic Safety Administration requirements as authorized by Title 49, U.S.C. 301, Standards and Compliance, (Ref. B1.1.3, Section 30111: Standards). The requirements are delineated in 49 CFR 571 (Ref. B1.1.2).

B1.3.1.3 Subsystems

The SPMRC and SPMTT systems are composed of four subsystems:

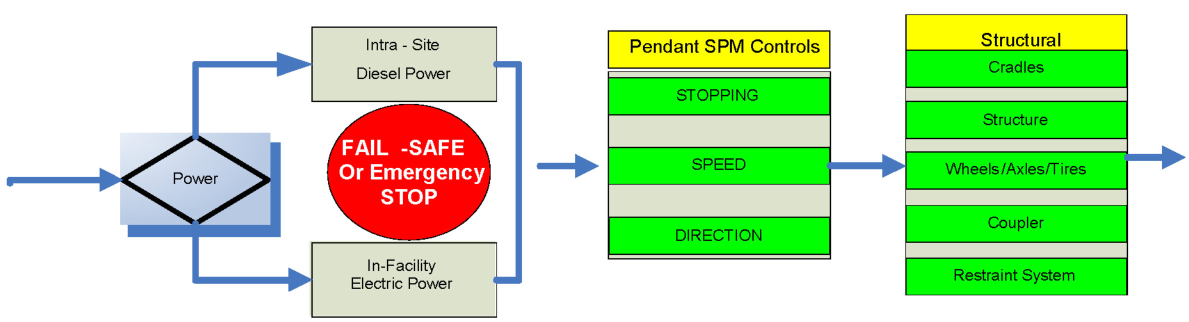
1. Power plant—A diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all Intra-Site Operations. For operations conducted inside facilities, the SPM is connected to facility 480 V, 3-phase 60 Hz power.

2. Vehicle controls—During Intra-Site Operations, the operator controls the SPM at the operator's console inside the SPM. For all operations inside of facilities, the operator controls the SPM with either a remote (wireless) controller or through a pendant connected to the vehicle.

3. Structural—Structural subsystems include restraints for securing the transportation casks to the railcar/truck trailer, automatic coupler hardware, cradles for supporting the transportation cask, and wheels/tires and axles.

4. Brakes—For the railcar, the brakes comply with FRA requirements; for the truck trailer the braking system complies with 49 CFR 571 (Ref. B1.1.2).

A simplified schematic of the functional components on the SPMRC/SPMTT is shown in Figure B1.3-1.



Source: Original

Figure B1.3-1. Site Prime Mover Simplified Schematic Intra-Site and In-Facility

B1.3.2 Operations

B1.3.2.1 Normal Operations

Intra-Site SPM operations begin once the railcar/truck trailer carrying a transportation cask arrives onsite at the receipt area. Receipt activities include the placement of temporary protective shielding around the railcar/truck trailer, inspection of the transportation cask, and connection of the railcar/truck trailer to the SPM. Once all receipt activities are completed the SPM with the railcar/truck trailer proceeds to the appropriate facility (CRCF, IHF, RF, or WHF).

In-facility SPM operations begin when the SPM has positioned the railcar/truck trailer outside the entry vestibule at the facility such that the railcar/truck trailer is pushed into the facility. The SPM diesel engine is shut down and the outer and inner vestibule doors are opened. Facility power is connected to the SPM for all operations inside the facility.[1]

The operator connects the pendant controller or uses a remote (wireless) controller to move the railcar/truck trailer into the vestibule. Once inside, the outer vestibule door is closed. The Cask Preparation Area Vestibule door is then opened and the SPM moves the railcar/truck trailer into position in the Cask Preparation Area. Once in position, the SPM is disconnected from the railcar/truck trailer and returns to the inner vestibule area. The Cask Preparation Area Vestibule door is then closed. The inner and outer vestibule doors can then be opened and the SPM exits the facility. Once outside, the SPM is shut down and the facility power is removed and the inner and outer vestibule doors are closed.

B1.3.2.2 Site Prime Mover Off-Normal Operations

In the event of loss of power, the SPM is designed to stop, retain control of the railcar/truck trailer, and enter a locked mode. Upon the restoration of power the SPM stays in the locked mode until operator action is taken to return to normal operations.

B1.3.2.3 Site Prime Mover Testing and Maintenance

Testing and maintenance of the SPM is done on a periodic basis and does not affect the normal operations of the SPM. Testing and/or maintenance are not performed on a SPM when it is coupled with a railcar/truck trailer. A SPM that has malfunctioned or has a warning light lit on the SPM is deemed unserviceable and turned in for maintenance. Unserviceable vehicles are not to be used.

If an unserviceable state is identified during movement, the SPM is immediately placed in a safe state (as quickly as possible) and recovery actions for the SPM are invoked.

[1] The SPM is never operated inside a facility using the diesel engine.

B1.4 DEPENDENCIES AND INTERACTIONS ANALYSIS

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 B1.4-1 with the following dependencies:

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

Table B1.4-1 Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environ-mental	Spatial	Human	External Events
Structural	Material failure Coupler Wheels/tires/axle	—	—	—	—
Brakes	Material failure	—	—	Failure to engage (set)	—
Power plant	Governor fails Safe state on	—	—	Failure to stop	—
Remote control	Spurious commands	—	—	Improper command	Collide with end stops

Source: Original

B1.5 SITE PRIME MOVER RELATED FAILURE SCENARIOS

There are two basic SPM fault trees developed for Intra-Site Operations. The top events for these fault trees are:

- SPMRC collision while entering facility (INT-1-SPMRC-COLLISION)
  - SPMRC with DPC collides with facility structures
  - SPMRC with a horizontal DPC collides with facility structures
  - SPMRC with MCO collides with facility structures
  - SPMRC with DSTD collides with facility structures
  - SPMRC with transportation, aging, and disposal canister collides with facility structures
  - SPMRC with Navy SNF collides with facility structures
  - SPMRC with HLW collides with facility structures

– SPMRC with uncanistered commercial SNF collides with facility structures.

- SPMTT collision while entering facility (INT-1-SPMTT-COLLISION)

  – SPMTT with MCO collides with facility structures
  – SPMTT with DSTD collides with facility structures
  – SPMTT with uncanistered commercial SNF collides with facility structures
  – SPMTT with HLW collides with facility structures.

B1.5.1 SPMRC Collision While Entering Facility (INT-1-SPMRC-COLLISION)

B1.5.1.1 Description

Collision can occur as a result of human error or hardware failures. Hardware failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

B1.5.1.2 Success Criteria

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

The SPM is designed to stop whenever commanded to stop or 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 any time there is a loss of power detected, the SPM immediately stops all movement and enters into a "lock mode" safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a governor on the diesel engine for outside facility movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

B1.5.1.3 Design Features and Requirements

Requirements

- Since the dominant contributor to a SPMRC collision in the facility is human error, no priority is given to either the remote or the pendant controllers.

- The SPM is operated on electrical power when inside the building.
- The SPM is disconnected from the railcar at the preparation area and moved out of the building before cask preparation activities begin.

Design Features

- The SPM has two off-equipment control devices that have complete control over the SPMRC.
- Drive system contains both a governor and a transmission constraint which limits the maximum speed of the SPM to 9.0 mph.
- There are no common-cause failures (CCFs) identified for the SPMRC.

System Configuration and Operating Conditions

Requirements

- Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a "deadman switch."
- On the loss of alternating current (AC) power derived from the facility (CRCF, RF, IHF, or WHF), the SPM immediately enters the lock mode state. The lock mode state is reversible without specific operator action.

Design Features and Inputs

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

Testing and Maintenance

Requirements

There shall be no maintenance or testing permitted on an SPM loaded with a transportation cask.

Design Feature

None

B1.5.1.4 Fault Tree Model

The fault tree model for "SPMRC Collision" while entering facility, "INT-1-SPMRC-COLLISION," accounts for both human error and/or SPMRC hardware problems that could result in a collision. Figure B1.5-1 contains the uncertainty results obtained from running the fault tree for INT-1-SPMRC-COLLISION. Figure B1.5-2 provides the cut set generation results for the INT-1-SPMRC-COLLISION fault tree. Figures B1.5-3 through B1.5-5 show the fault trees as modeled.

The fault trees for collisions involving the SPMRC and SPMTT are functionally identical. The fault tree for the SPMTT is discussed in the next section.

The fault tree for the top event is a collision of the SPMRC as shown in Figure B1.5-3 through B1.5-5. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop or exceeding a safe speed. Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

B1.5.1.5 Basic Event Data

Table B1.5-1 contains a list of basic events used in the SPMRC collision fault tree. The mission time has been set at one hour which allows sufficient time to move the SPMRC from the receipt area to the individual facilities (CRCF, IHF, RF, or WHF).

Table B1.5-1. Basic Event Probability for SPMRC Collision

Name	Description	Calc. Type [a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-OPRCCOLLIDE1-HFI-NOD	Operator causes collision	1	3.000E−03	3.000E−03	0.000E+00	0.000E+00
ISO-OPRCINTCOL01-HFI-NOD	Operator initiates runaway	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
ISO-PWR-LOSS	Loss of site power	1	4.100E−06	4.100E−06	0.000E+00	0.000E+00
ISO-SPMRC--CT001-CT--FOD	On-board controller fails to respond	1	4.000E−06	4.000E−06	0.000E+00	0.000E+00
ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	3	2.270E−05	0.000E+00	2.270E−05	1.000E+00[a]
ISO-SPMRC-BRP000-BRP-FOD	SPMRC brake 000 failure on demand	1	5.020E−05	5.020E−05	0.000E+00	0.000E+00
ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	1	5.020E−05	5.020E−05	0.000E+00	0.000E+00
ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC – open circuit	3	9.130E−08	0.000E+00	9.130E−08	1.000E+00[a]
ISO-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	3	1.880E−08	0.000E+00	1.880E−08	1.000E+00[a]
ISO-SPMRC-CPL000-CPL-FOH	Railcar automatic coupler system fails	3	1.910E−06	0.000E+00	1.910E−06	1.000E+00[a]

Table B1.5-1. Basic Event Probability for SPMRC Collision (Continued)

Name	Description	Calc. Type [a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-SPMRC-CT000--CT—FOD	SPMRC primary stop switch fails	1	4.000E−06	4.000E−06	0.000E+00	0.000E+00
ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	3	1.160E−05	0.000E+00	1.160E−05	1.000E+00[a]
ISO-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1	1.740E−03	1.740E−03	0.000E+00	0.000E+00
ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	3	1.350E−08	0.000E+00	1.350E−08	1.000E+00[a]
ISO-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	3	1.280E−04	0.000E+00	1.280E−04	1.000E+00[a]
ISO-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	3	4.160E−06	0.000E+00	4.160E−06	1.000E+00[a]

NOTE: [a] 1 is direct input probability; and 3 is lambda and mission time. For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time (1.00E+00).

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability; SPMRC = site prime mover railcar.

Source: Original

B1.5.1.5.1 Human Failure Events

Two human errors have been identified for this fault tree:

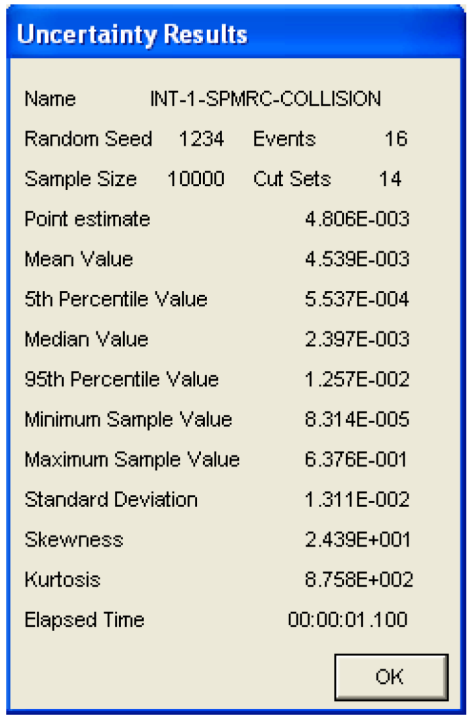
- Operator causes collision (INT-OPRCCOLLIDE1-HFI-NOD) is assigned a screening value of 3E−03.
- Operator initiates runaway (INT-OPRCINTCOL01-HFI-NOD) is assigned a screening value of 1.0.

B1.5.1.5.2 Common-Cause Failures

There are no CCFs.

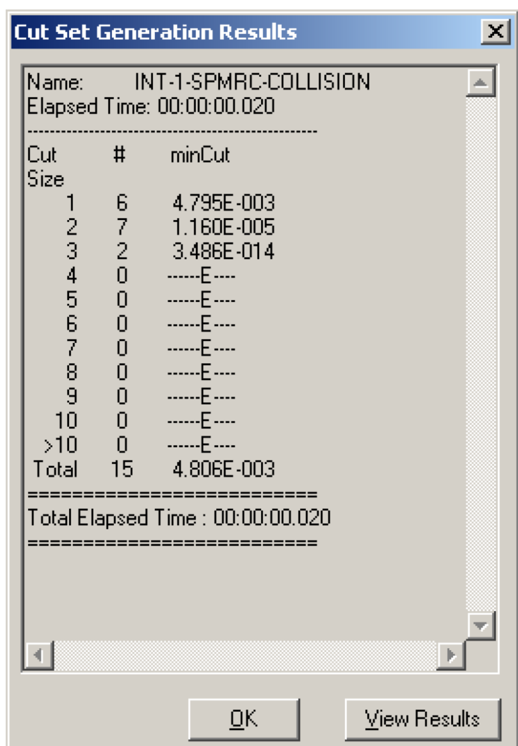
B1.5.1.6 Uncertainty and Cut Set Generation Results

As stated, figure B1.5-1 contains the uncertainty results obtained from running the fault tree for INT-1-SPMRC-COLLISION. Figure B1.5-2 provides the cut set generation results for the INT-1-SPMRC-COLLISION fault tree.



Source: Original

Figure B1.5-1. Uncertainty Results of the INT-1-SPMRC-COLLISION Fault Tree



Source: Original

Figure B1.5-2. Cut Set Generation Results for the INT-1-SPMRC-COLLISION Fault Tree

B1.5.1.7 Cut Sets

Table B1.5-2 contains the cut sets for INT-1-SPMRC-COLLISION.

Table B1.5-2. Cut Sets for INT-1-SPMRC-COLLISION

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
62.42	62.42	3.000E−03	ISO-OPRCCOLLIDE1-HFI-NOD	Operator causes collision	3.000E−03
98.62	36.20	1.740E−03	ISO-SPMRC-HC001-HC--FOD	Pendant control transmits wrong signal	1.740E−03
99.66	1.04	5.020E−05	ISO-SPMRC-BRP000-BRP-FOD	SPMRC brake 000 failure on demand	5.020E−05
99.90	0.24	1.160E−05	ISO-OPRCINTCOL01-HFI-NOD	Operator initiates runaway	1.000E+00
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E−05
99.98	0.08	4.000E−06	ISO-SPMRC--CT001-CT--FOD	On-board controller fails to respond	4.000E−06
100.00	0.08	4.000E−06	ISO-SPMRC-CT000--CT--FOD	SPMRC primary stop switch fails	4.000E−06
100.00	0.04	1.910E−06	ISO-SPMRC-CPL000-CPL-FOH	Railcar Automatic Coupler System Fails	1.910E−06
100.00	0.00	2.058E−10	ISO-PWR-LOSS	Loss of site power	4.100E−06
			ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E−05
100.00	0.00	4.583E−12	ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E−05
			ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	9.130E−08
100.00	0.00	9.438E−13	ISO-SPMRC-BRP001-BRP-FOD	SPMRC fails to stop on loss of power	5.020E−05
			ISO-SPMRC-CBP001-CBP-SHC	SPMRC power cable - short circuit	1.880E−08
100.00	0.00	5.535E−14	ISO-PWR-LOSS	Loss of site power	4.100E−06
			ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	1.350E−08
100.00	0.00	3.370E−14	ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	2.270E−05
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E−05
			ISO-SPMRC-SC021--SC--FOH	Speed controller on SPMRC pendant fails	1.280E−04
100.00	0.00	1.233E−15	ISO-SPMRC-CBP001-CBP-OPC	Power cable to SPMRC - open circuit	9.130E−08
			ISO-SPMRC-MOE000-MOE-FSO	SPMRC motor (electric) fails to shut off	1.350E−08
100.00	0.00	1.095E−15	ISO-SPMRC--CT003-CT--SPO	On-board controller initiates spurious signal	2.270E−05
			ISO-SPMRC-G65000-G65-FOH	SPMRC speed control (governor) fails	1.160E−05

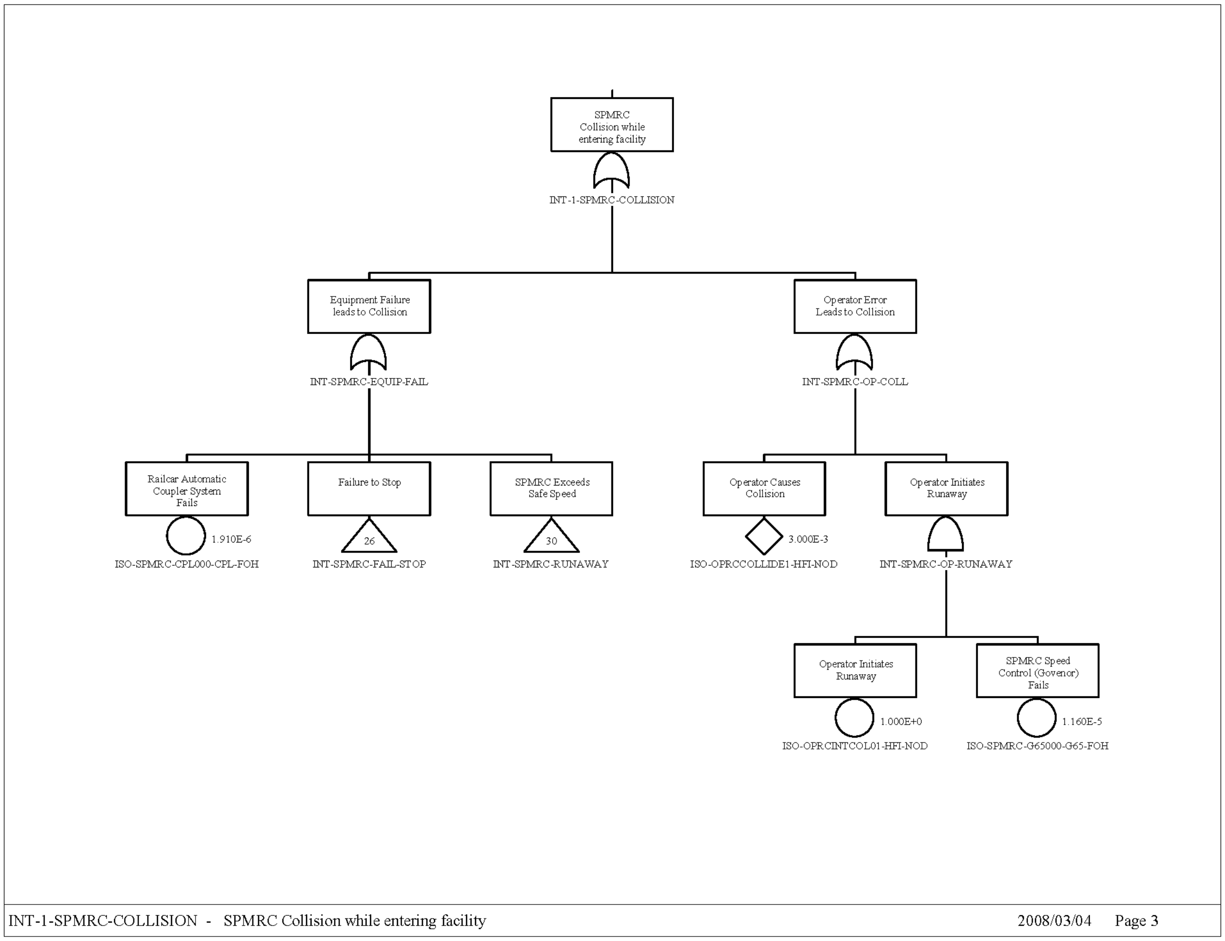
Table B1.5-2. Cut Sets for INT-1-SPMRC-COLLISION (Continued)

% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
100.00 (cont.)	0.00 (cont.)	1.095E−15 (cont.)	ISO-SPMRC-SEL021-SEL-FOH	Speed selector on SPMRC pendant fails	4.160E−06

NOTE: Prob. = probability; SPMRC = site prime mover railcar.

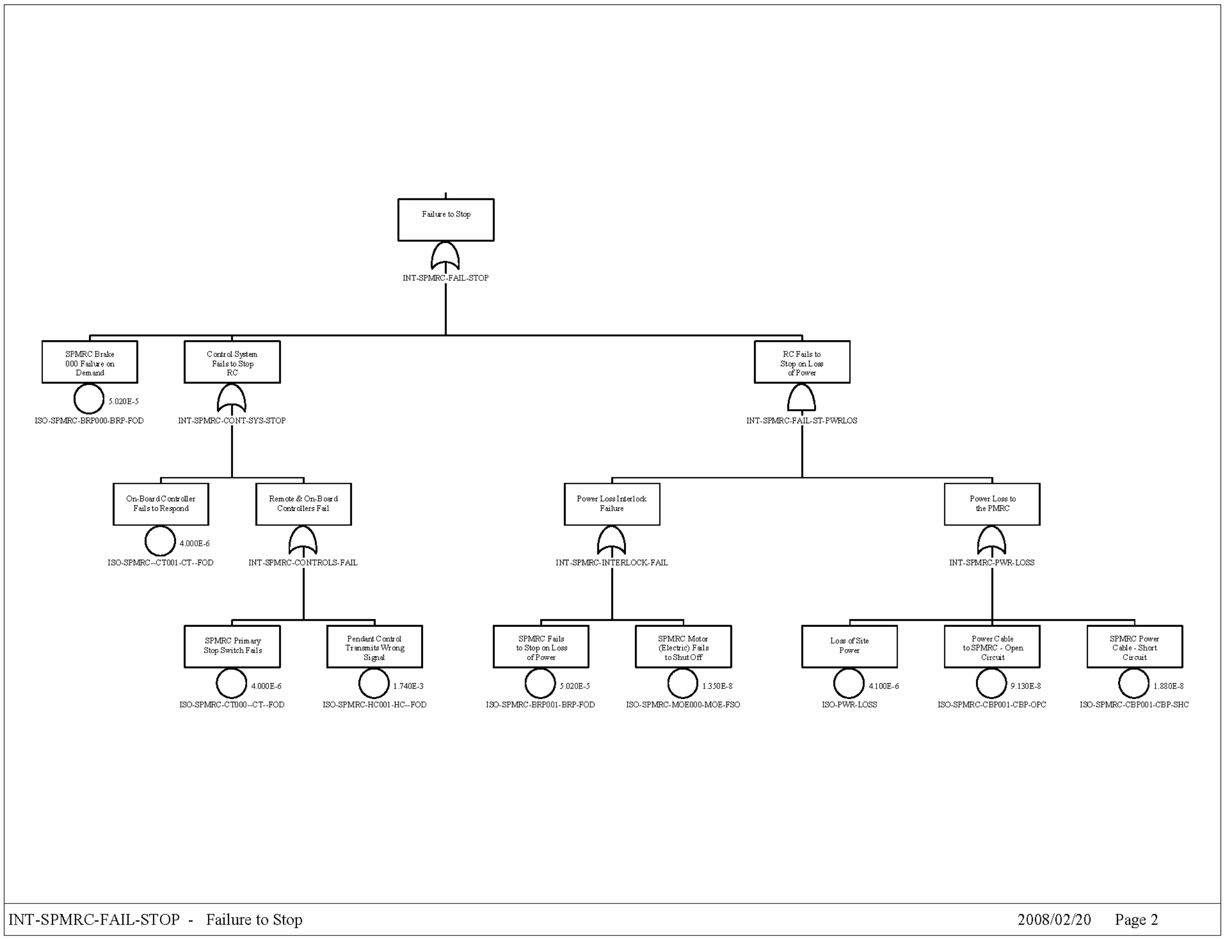
Source: Original

B1.5.1.8 Fault Trees



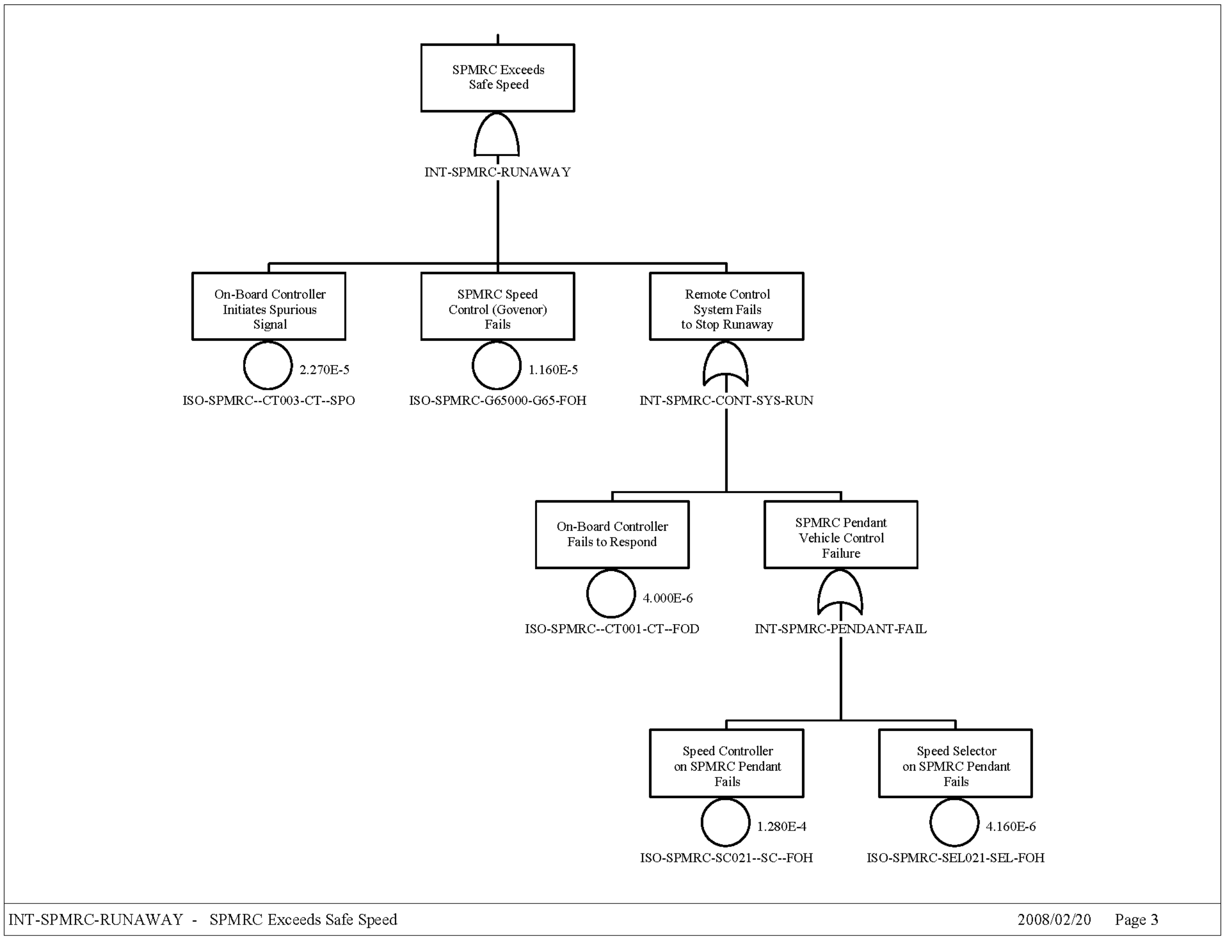
Source: Original

Figure B1.5-3. INT-1-SPMRC-COLLISION Sheet 1 of 3



Source: Original

Figure B1.5-4. INT-1-SPMRC-COLLISION Sheet 2 of 3



Source: Original

Figure B1.5-5. INT-1-SPMRC-COLLISION Sheet 3 of 3

B1.5.2 SPMTT Collision Entering Facility (INT-1-SPMTT-COLLISION)

B1.5.2.1 Description

Collision can occur as a result of human error or hardware failures. Hardware failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

The fault tree for collisions involving the SPMRC and SPMTT are functionally identical. The fault tree for the SPMRC was discussed in the previous section.

B1.5.2.2 Success Criteria

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

The SPM is designed to stop whenever commanded to stop or 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 performs a controlled stop. Once stopped, the SPM stops all movement and enters into "lock mode" safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM. The SPM remains in this fail safe mode until power is returned and restarted by the operator.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a governor on the diesel engine for outside movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 mph. The prevention of SPM movements in the wrong direction is prevented by the limitations of the power plant that prevents simultaneous operations.

B1.5.2.3 Design Features and Requirements

Requirements

- Since the dominant contributor to SPMTT collision in the facility is human error, no priority is given to either the remote or the pendant controllers.
- The SPM is operated on electrical power when inside the building.
- The SPM is disconnected from the railcar at the preparation area and moved out of the building before cask preparation activities begin.

Design Features

- The SPM has two off-equipment control devices that have complete control over the SPMTT.
- Drive system contains both a governor and a transmission constraint which limits the maximum speed of the SPM to 9.0 mph.
- There are no CCFs identified for the SPMTT.

System Configuration and Operating Conditions

Requirements

- Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that has the equivalent of a "deadman switch."

- On the loss of AC power derived from the facility, the SPM immediately enters the lock mode state. The lock mode state is not be reversible without specific operator action.

Design Features and Inputs

Stopping the SPM is accomplished by pushing the “stop” button on the remote or pendant controller. The SPM, upon receiving a stop command from either control source, is to immediately respond by removing power from the propulsion system.

Testing and Maintenance

Requirements

There is no maintenance or testing permitted on a SPM loaded with a transportation cask.

Design Feature

None.

B1.5.2.4 Fault Tree Model

The fault tree model for “SPM Collision” accounts for both human error and/or SPMTT hardware problems that could result in a collision.

The top event is a collision of the SPMTT and the fault tress are shown in Figure B1.5-8, B1.5-9, and B1.5-10. This collision may occur due to a human error coupled with the failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop or exceeding a safe speed. Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

B1.5.2.5 Basic Event Data

Table B1.5-3 contains a list of basic events used in the SPMTT collision fault trees. The mission time has been set at one hour which is conservative because it will not require more than one hour to disconnect the SPM from the railcar and remove it from the facility.

Table B1.5-3. Basic Event Probability for SPMTT Collision

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes collision of TT	1	3.000E−03	3.000E−03	0.000E+00	0.000E+00
ISO-OPTTINTCOL01-HFI-NOD	Operator initiates runaway	1	1.000E+00	1.000E+00	0.000E+00	0.000E+00
ISO-PWR-LOSS-2	Loss of power	1	4.100E−06	4.100E−06	0.000E+00	0.000E+00
ISO-SPMTT--CT001-CT--FOD	On-board controller fails to respond	1	4.000E−06	4.000E−06	0.000E+00	0.000E+00

Table B1.5-3. Basic Event Probability for SPMTT Collision (Continued)

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time
ISO-SPMTT--CT001-CT--SPO	On-board controller spurious operation	3	2.270E−05	0.000E+00	2.270E−05	1.000E+00
ISO-SPMTT-BRK000-BRP-FOD	Pneumatic brakes on SPMTT fail on demand	1	5.020E−05	5.020E−05	0.000E+00	0.000E+00
ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	1	5.020E−05	5.020E−05	0.000E+00	0.000E+00
ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	3	9.130E−08	0.000E+00	9.130E−08	1.000E+00[a]
ISO-SPMTT-CBP003-CBP-SHC	Cables (electrical power) short circuit	3	1.880E−08	0.000E+00	1.880E−08	1.000E+00[a]
ISO-SPMTT-CPL000-CPL-FOH	Truck trailer automatic coupler system fails	3	1.910E−06	0.000E+00	1.910E−06	1.000E+00[a]
ISO-SPMTT-CT000--CT--FOD	Controller mechanical jamming	1	4.000E−06	4.000E−06	0.000E+00	0.000E+00
ISO-SPMTT-CT002---CT-FOH	Controller failure	3	6.880E−05	0.000E+00	6.880E−05	1.000E+00[a]
ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	3	1.160E−05	0.000E+00	1.160E−05	1.000E+00[a]
ISO-SPMTT-HC001-HC--FOD	Remote control transmits wrong signal	1	1.740E−03	1.740E−03	0.000E+00	0.000E+00
ISO-SPMTT-HC002--HC--SPO	Spurious signal from pendant controller	3	5.230E−07	0.000E+00	5.230E−07	1.000E+00[a]
ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	3	1.350E−08	0.000E+00	1.350E−08	1.000E+00[a]
ISO-SPMTT-SC021--SC--FOH	Speed controller on SPMTT pendant fails	3	1.280E−04	0.000E+00	1.280E−04	1.000E+00[a]
ISO-SPMTT-SEL021-SEL-FOH	Speed selector on SPMTT pendant fails	3	4.160E−06	0.000E+00	4.160E−06	1.000E+00[a]
ISO-SPMTT-STU001-STU-FOH	SMPTT end stops fail	3	2.107E−04	0.000E+00	4.810E−08	4.380E+03

NOTE: [a] 1 is direct input probability; and 3 is lambda and mission time. For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time (1.00E+00).

Calc. calculation; Fail. = failure; Miss. = mission; Prob. = probability; SPMTT = site prime mover truck trailer; TT= truck trailer.

Source: Original

B1.5.2.5.1 Human Failure Events

Two human errors have been identified for this fault tree:

1. Operator causes collision (060-OPTTCOLLIDE1-HFI-NOD) is assigned a screening value of 5E−03.

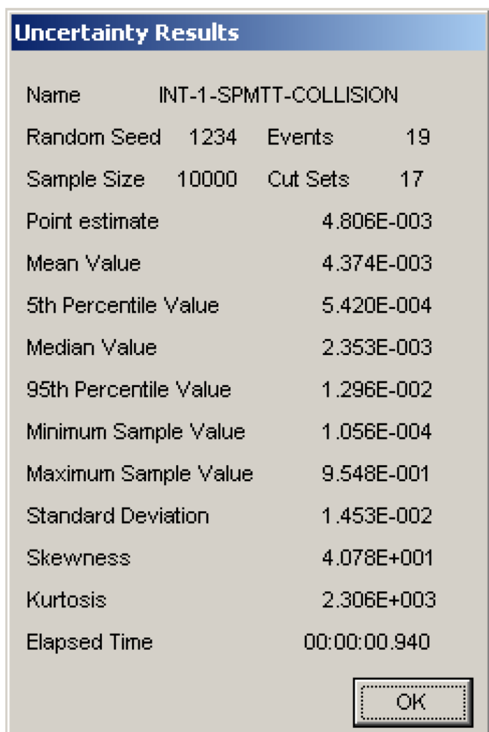
2. Operator initiates runaway (060-OPTTINTCOL01-HFI-NOD) is assigned a screening value of 1.0.

B1.5.2.5.2 Common-Cause Failures

There are no CCFs.

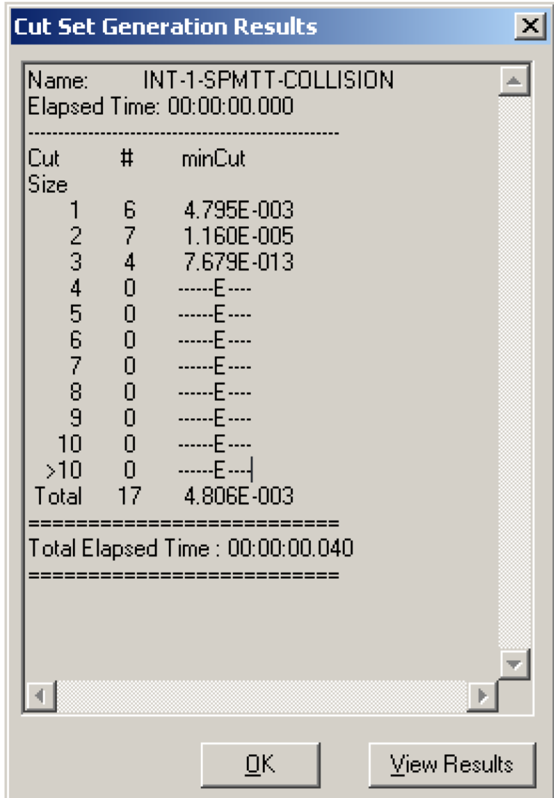
B1.5.2.6 Uncertainty and Cut Set Generation Results

Figure B1.5-6 contains the uncertainty results obtained from running the fault tree for SPMTT collision. Figure B1.5-7 provides the cut set generation results for the SPMTT collision fault tree.



Source: Original

Figure B1.5-6. Uncertainty Results of the SPMTT Collision Fault Tree



Source: Original

Figure B1.5-7. Cut Set Generation Results for the SPMTT Collision Fault Tree

B1.5.2.7 Cut Sets

Table B1.5-4 contains the cut sets for SPMTT collision.

Table B1.5-4. Cut Sets for SPMTT Collision

% Total	% Cut set	Probability/ Frequency	Basic Event	Description	Event Probability
62.42	62.42	3.000E−03	ISO-OPTTCOLLIDE1-HFI-NOD	Operator causes collision of TT	3.000E−03
98.62	36.20	1.740E−03	ISO-SPMTT-HC001-HC--FOD	Remote control transmits wrong signal	1.740E−03
99.66	1.04	5.020E−05	ISO-SPMTT-BRK000-BRP-FOD	Pneumatic brakes on SPMTT fail on demand	5.020E−05
99.90	0.24	1.160E−05	ISO-OPTTINTCOL01-HFI-NOD	Operator initiates runaway	1.000E+00
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E−05
99.98	0.08	4.000E−06	ISO-SPMTT--CT001-CT--FOD	On-board controller fails to respond	4.000E−06
100.00	0.08	4.000E−06	ISO-SPMTT-CT000--CT--FOD	Controller mechanical jamming	4.000E−06

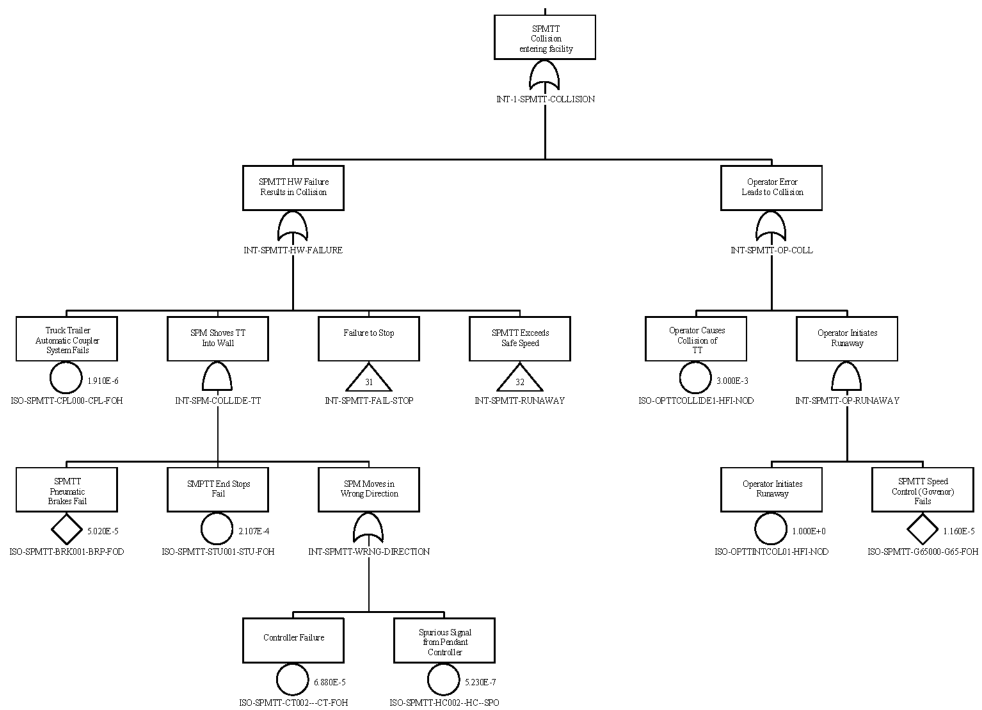
Table B1.5-4. Cut Sets for SPMTT Collision (Continued)

% Total	% Cut set	Probability/ Frequency	Basic Event	Description	Event Probability
100.00	0.04	1.910E−06	ISO-SPMTT-CPL000-CPL-FOH	Truck trailer automatic coupler system fails	1.910E−06
100.00	0.00	2.058E−10	ISO-PWR-LOSS-2	Loss of power	4.100E−06
			ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E−05
100.00	0.00	4.583E−12	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E−05
			ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	9.130E−08
100.00	0.00	9.438E−13	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E−05
			ISO-SPMTT-CBP003-CBP-SHC	Cables (electrical power) short circuit	1.880E−08
100.00	0.00	7.275E−13	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E−05
			ISO-SPMTT-CT002---CT-FOH	Controller failure	6.880E−05
			ISO-SPMTT-STU001-STU-FOH	SMPTT end stops fail	2.107E−04
100.00	0.00	5.535E−14	ISO-PWR-LOSS-2	Loss of power	4.100E−06
			ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	1.350E−08
100.00	0.00	3.370E−14	ISO-SPMTT--CT001-CT--SPO	On-board controller spurious operation	2.270E−05
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E−05
			ISO-SPMTT-SC021--SC--FOH	Speed controller on SPMTT pendant fails	1.280E−04
100.00	0.00	5.531E−15	ISO-SPMTT-BRK001-BRP-FOD	SPMTT pneumatic brakes fail	5.020E−05
			ISO-SPMTT-HC002--HC--SPO	Spurious signal from pendant controller	5.230E−07
			ISO-SPMTT-STU001-STU-FOH	SMPTT end stops fail	2.107E−04
100.00	0.00	1.233E−15	ISO-SPMTT-CBP002-CBP-OPC	SPMTT power cable - open circuit	9.130E−08
			ISO-SPMTT-MOE000-MOE-FSO	SPMTT motor (electric) fails to shut off	1.350E−08
100.00	0.00	1.095E−15	ISO-SPMTT--CT001-CT--SPO	On-board controller spurious operation	2.270E−05
			ISO-SPMTT-G65000-G65-FOH	SPMTT speed control (governor) fails	1.160E−05
			ISO-SPMTT-SEL021-SEL-FOH	Speed selector on SPMTT pendant fails	4.160E−06

NOTE: SPMTT = site prime mover tractor and trailer; TT = truck trailer.

Source: Original

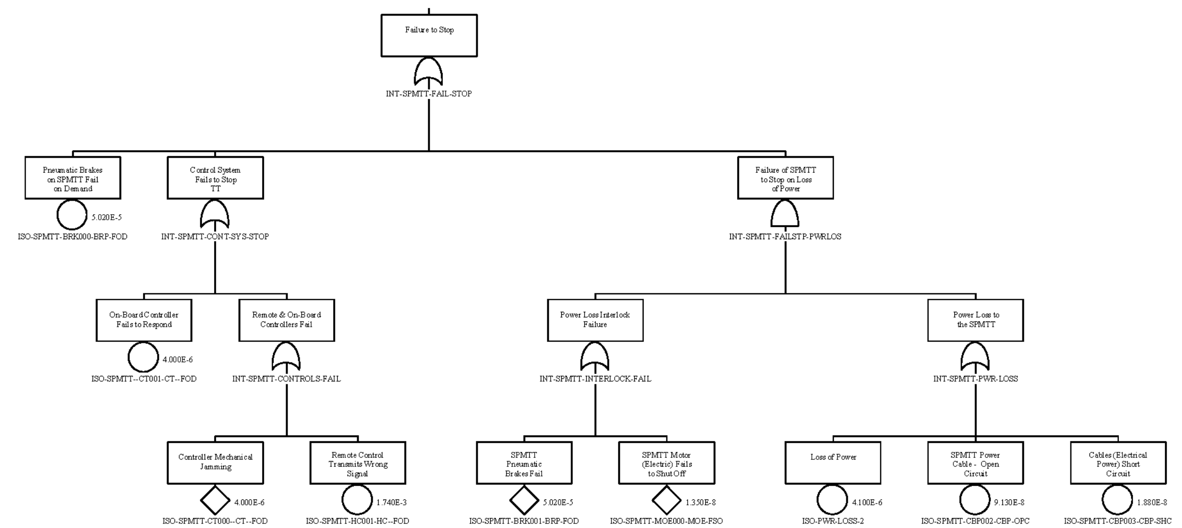
B1.5.2.8 Fault Trees



INT-1-SPMTT-COLLISION - SPMTT Collision entering facility 2008/03/04 Page 1

Source: Original

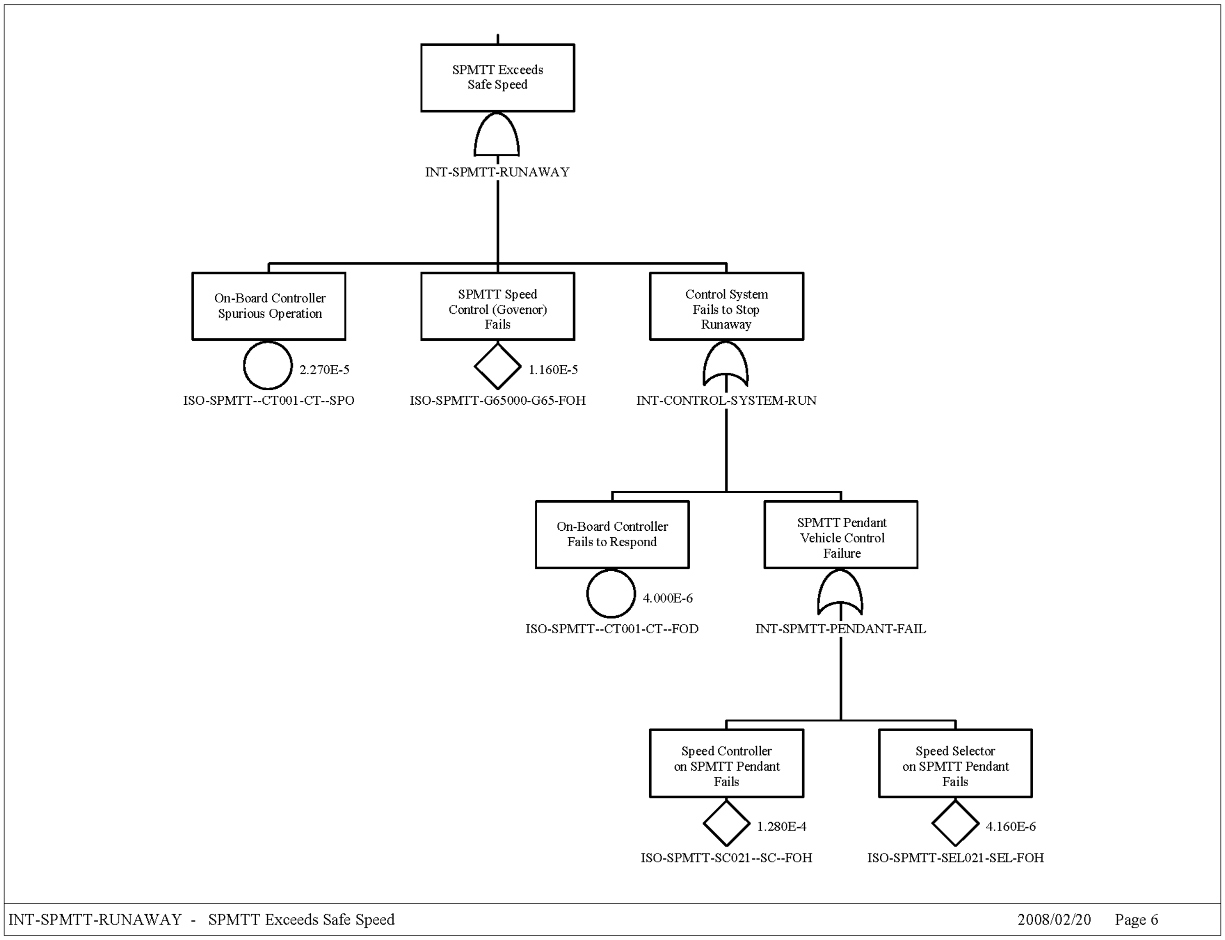
Figure B1.5-8. INT-1-SPMTT-COLLISION Sheet 1 of 3



INT-SPMTT-FAIL-STOP - Failure to Stop 2008/02/20 Page 5

Source: Original

Figure B1.5-9. INT-1-SPMTT-COLLISION Sheet 2 of 3



Source: Original

Figure B1.5-10. INT-1-SPMTT-COLLISION Sheet 3 of 3

B2 SITE TRANSPORTER - FAULT TREE ANALYSIS

B2.1 REFERENCES

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 the 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.

Design Inputs

B2.1.1 †BSC (Bechtel SAIC Company) 2007. *Mechanical Handling Design Report – Site Transporter*. 170-30R-HAT0-00100-000-Rev 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071217.0015.

B2.1.2 BSC 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.200770904.0031.

B2.1.3 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.

B2.2 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 or, for the Wet Handling Facility, a cylindrical-steel shielded transfer cask (STC). The site transporter is used for Intra-Site Operations and within the CRCF, the WHF, and the RF[2].

Movement of the site transporter within a facility is limited to a facility's Entrance Vestibule, Cask Preparation Area, and the Cask Unloading Rooms.

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

B2.2.1 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 the lid at the top. Access to the top of the aging overpack is unobstructed.

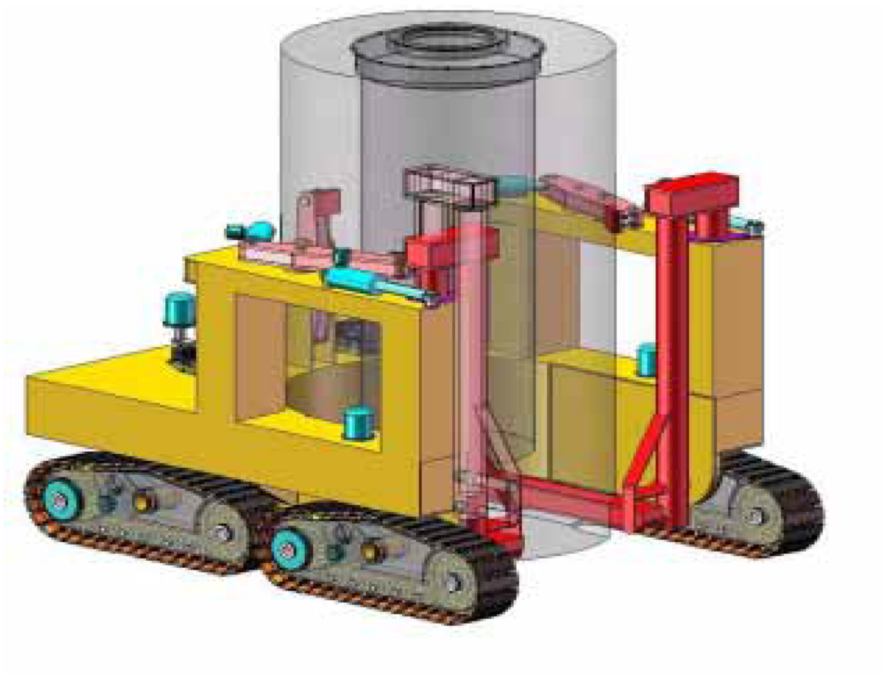
An integrated, diesel powered, electric generator provides electricity to operate the site transporter outside the facility building. Inside the facility buildings the site transporter is electrically driven via an umbilical cable (or remote control) from the facility main electrical supply. See *Mechanical Handling Design Report – Site Transporter* (Ref. B2.1.1, 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 important to safety.

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 stability 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 desired 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 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 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 B2.2-1.



Source: Ref. B2.1.1

Figure B2.2-1 Site Transporter

The site transporter system is composed of six subsystems (Ref. B2.1.1):

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 AC/3-phase/60 Hz power to the vehicle. During facility operations, the diesel engine is disabled and facility 480 V AC/3-phase/60 Hz power is supplied to operate the vehicle.

3. Rear Lift Fork Subsystem—The 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.

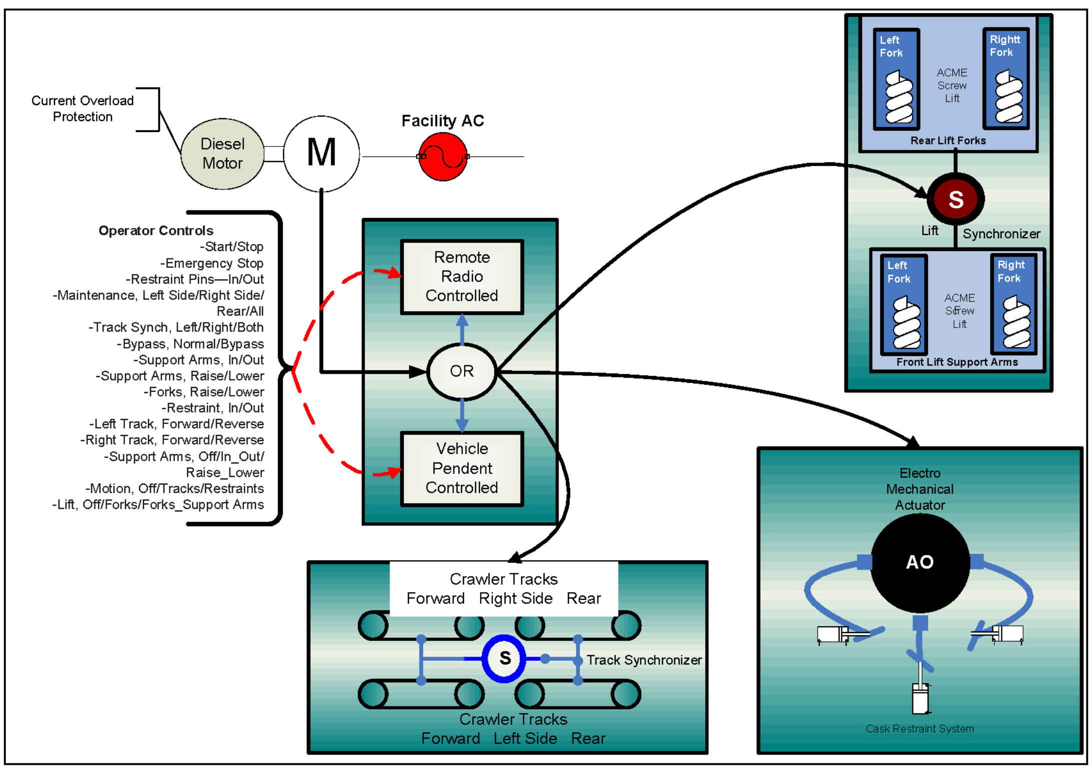
4. Lift Support Arms Subsystem—Two support arms with electromechanical actuators are located on the front of the site transporter. These support arms are rotated 90 degrees to provide support and stabilization for the lift forks during lifting/lowering/moving operations. ACME nuts are used on these arms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

5. Restraint Subsystem—A two axis restraint system is incorporated to stabilize the cask during site transporter movement. The restraints are emplaced/retracted with electromechanical actuators. These restraints, when positioned against the aging overpack are 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. B2.1.1) 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 B2.2-2.



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

Source: Original

Figure B2.2-2. Simplified Block Diagram of the Site Transporter Subsystems

B2.2.1.1 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. B2.1.2). 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 at 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. B2.1.1, Section 2.1.2).

B2.2.1.2 Power Plant Subsystem Description

The power plant subsystem supplies the site transporter with 480 V, 3-phase AC 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. B2.1.1, 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. B2.1.2, 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's integral receptacle to allow the site transporter to operate inside the building without a source of combustion.

The motor drive system and current overload protection system prevents the site transporter from exceeding 2.5 mph (Ref. B2.1.1, Section 3.2.1).

B2.2.1.3 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 in. above the floor/ground (Ref. B2.1.1, Sections 2.1.4 and 2).

B2.2.1.4 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 their own gear reduction and 20 HP, 900 rpm electric motor (Ref. B2.1.1, 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, 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-in. lift.

B2.2.1.5 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 and locked 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 allows the site transporter to be moved (Ref. B2.1.3, Sheet 1 of 3).

B2.2.1.6 Vehicle Controls Subsystem Description

The site transporter can be operated in two modes: a remote (wireless) control and an operator controlled pendant (Ref. B2.1.1, Section 2.1.7). Both of these devices have the same capability. Table B2.2-1 contains a list of controls that are available on the controller and the corresponding activation device (Ref. B2.1.3, Sheet 3 of 3).

Table B2.2-1. 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 programmable logic controller or computer is used to control the machine.

B2.2.2 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 Entry Vestibule and turns off the diesel generator. An electrical umbilical cable is manually retrieved from inside the building and attached to the site transporter. The site transporter is never operated inside a facility on diesel power.

Once inside the building, the operator positions the site transporter in the appropriate room associated with aging overpack loading or unloading activities. Before work is performed on the aging overpack, the site transporter operator removes the pins from the restraint arms and disengages them from the aging overpack. The movement interlock is engaged when the pins are removed. The operator then lowers the aging overpack to the floor. The procedure is reversed when it is necessary to move the site transporter again inside the facility. Once inside the appropriate room, the pins are removed, the restraints are disengaged, the aging overpack is lowered to the floor, and the umbilical cable is removed.

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

B2.2.3 Site Transporter Off-Normal Operations

There are four off-normal conditions that could occur during the movement of an aging overpack. When any of these occur, the operator response encompasses only those actions to return the aging overpack to a safe state. The off-normal conditions include the following:

- Loss of power while lowering the forks
- Loss of power while rotating the lift support arms
- On-board generator failing to operate
- Track belt failing.

In the event of a loss of power, the site transporter is designed to stop, retain its load, and enter a locked mode. Upon the restoration of power the site transporter stays in the locked mode until operator action is taken (Ref. B2.1.3, Section 7.2.3-5).

B2.2.4 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 is deemed unserviceable and turned in for maintenance. Unserviceable vehicles are not used.

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

B2.2.5 Site Transporter System Requirements and Design Features

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 cable 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 consists 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 performs a controlled stop. Once stopped the site transporter enters the “lock mode,” safe state. The “lock mode,” safe state is not 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 is 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 an 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.

B2.3 DEPENDENCIES AND INTERACTIONS ANALYSIS

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 B2.3-1 with the following dependencies:

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

Table B2.3-1. Dependencies and Interactions Analysis

Structures, Systems, and 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 - lock pin 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	Material failure	—	—	Failure to stop	—

Source: Original

B2.4 SITE TRANSPORTER FAILURE SCENARIOS

There are two basic site transporter fault trees developed for Intra-Site Operations. The top events for these fault trees and the variations are as follows:

1. Site transporter collision entering/leaving facility (INT-2-ST-COLLISION)
2. Site transporter drops load during lift/lower (INTRASITE-ST-AO-DROP).

Tipover of the site transporter was also considered, but is screened out as an initiating event (Table 6.0-2).

B2.4.1 Site Transporter Collision (INT-2-ST-COLLISION)

B2.4.1.1 Description

Collisions can occur as a result of human error or hardware failures (human error events are uniquely identified but all have the same screening value of 3E−3). Hardware failures leading to a collision consist of the site transporter fails to stop when commanded, the site transporter exceeds a safe speed, or the site transporter moves in the wrong direction.

B2.4.1.2 Success Criteria

The success criteria for preventing a collision include safety design features incorporated in the site transporter for hardware failures, and the site transporter operator 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 immediately stops all movement and enters into "lock mode" safe state. The site transporter remains in this locked mode 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. B2.1.1, 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.

B2.4.1.3 Design Features 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.

B2.4.1.4 Fault Tree Model

The fault tree model for a site transporter collision entering/leaving facility (INT-2-ST-COLLISION) accounts for the both human error and/or site transporter hardware problems that could result in a collision.

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

B2.4.1.5 Basic Event Data

Tables B2.4-1 lists the basic events used in the INT-2-ST-COLLISION fault tree.

Table B2.4-1. Basic Event Probability for INT-2-ST-COLLISION

Name	Description	Calc. Type[b]	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-LOSP-4	Failure of offsite power	1	4.100E−06	4.100E−06	0.000E+00	0.000E+00
ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes collision	1	3.000E−03	3.000E−03	0.000E+00	0.000E+00
ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1	1.460E−06	1.460E−06	0.000E+00	0.000E+00
ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	3	9.130E−08	0.000E+00	9.130E−08	1.000E+00
ISO-ST---CBP004-CBP--SHC	ST power cable short circuit	3	1.880E−08	0.000E+00	1.880E−08	1.000E+00
ISO-ST---CT000---CT--FOD	ST primary stop switch fails	1	4.000E−06	4.000E−06	0.000E+00	0.000E+00
ISO-ST---CT002---CT--FOH	Direction controller fails	3	6.880E−05	0.000E+00	6.880E−05	1.000E+00
ISO-ST---HC001--HC--FOD	Remote control transmits wrong signal	1	1.740E−03	1.740E−03	0.000E+00	0.000E+00
ISO-ST---HC002---HC--SPO	Spurious command to lift/lower AO or STC	3	5.230E−07	0.000E+00	5.230E−07	1.000E+00
ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	3	1.350E−08	0.000E+00	1.350E−08	1.000E+00
ISO-ST---MOE021--MOE-FSO	Drive system on primary propulsion fails	3	1.350E−08	0.000E+00	1.350E−08	1.000E+00 [a]
ISO-ST---SC021---SC--FOH	Speed controller on ST pendant fails	3	1.280E−04	0.000E+00	1.280E−04	1.000E+00 [a]
ISO-ST---SC021---SC--SPO	On-board controller initiates spurious signal	3	3.200E−05	0.000E+00	3.200E−05	1.000E+00 [a]
ISO-ST---SEL021--SEL-FOH	Speed selector on ST pendant fails	3	4.160E−06	0.000E+00	4.160E−06	1.000E+00 [a]

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time (1.00E+00).
AO = aging overpack; Calc. = calculation; ST = site transporter; STC = shielded transfer cask (used in WHF).
[b] 1 is direct input probability; and 3 is lambda and mission time.

Source: Original

B2.4.1.5.1 Human Failure Events

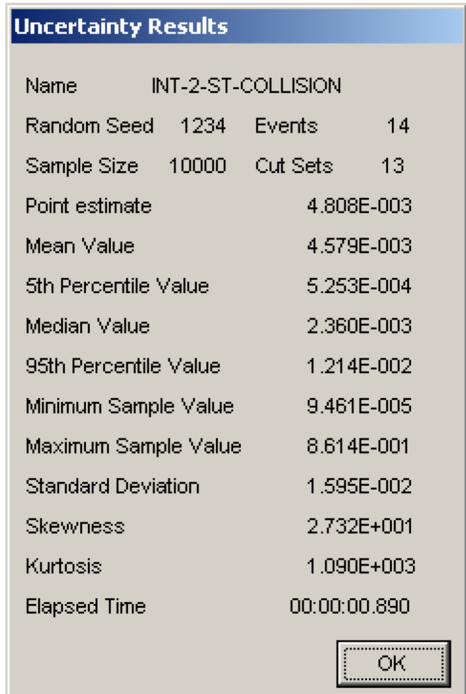
There is one human event (ISO-OPSTCOLLIDE2-HFI-NOD) in the collision trees for the site transporter and accounts for the site transporter operator causing the collision. This human error is set at the screening value of 3E−03.

B2.4.1.5.2 Common-Cause Failures

There are no CCF events identified for the site transporter collision events.

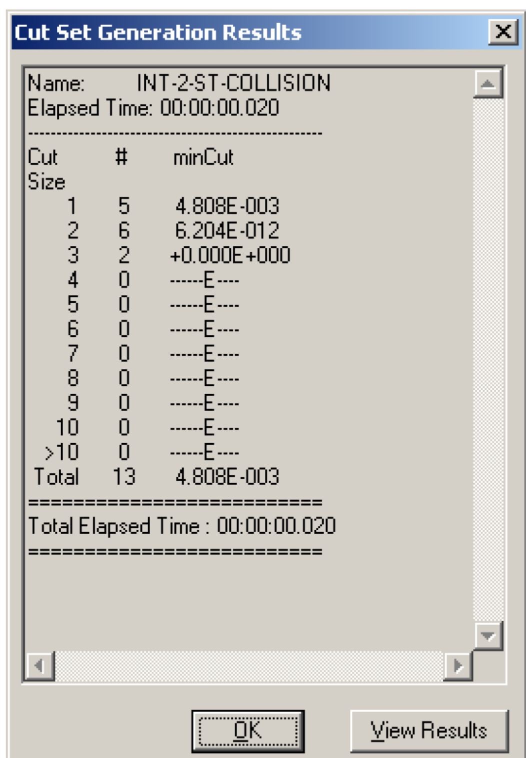
B2.4.1.6 Uncertainty and Cut Set Generation

Figures B2.4-1 and B2.4-2 contain the uncertainty and the cut set generation results for a site transporter collision.



Source: Original

Figure B2.4-1. Uncertainty Results Site Transporter Collision



Source: Original

Figure B2.4-2. Cut Set Generation Results

B2.4.1.7 Cut Sets

Table B2.4-2 provides the cut sets developed for the site transporter collision fault tree.

Table B2.4-2. Cut Sets for the Site Transporter Collision in Facility

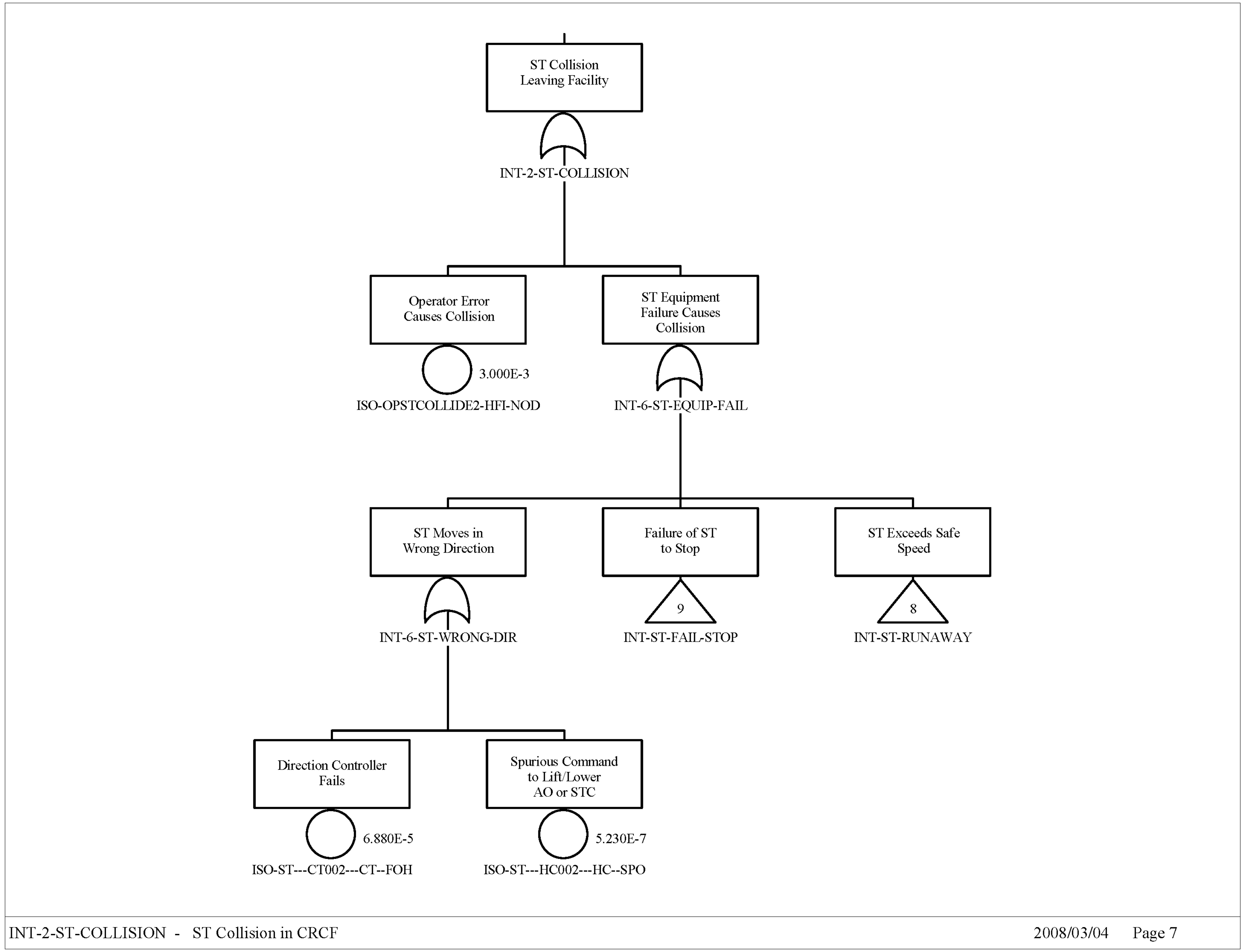
% Total	% Cut Set	Probability/ Frequency	Basic Event	Description	Event Probability
62.40	62.40	3.000E−03	ISO-OPSTCOLLIDE2-HFI-NOD	Operator error causes collision	3.000E−03
98.59	36.19	1.740E−03	ISO-ST---HC001--HC--FOD	Remote control transmits wrong signal	1.740E−03
100.00	1.43	6.880E−05	ISO-ST---CT002---CT--FOH	Direction controller fails	6.880E−05
100.00	0.08	4.000E−06	ISO-ST---CT000---CT--FOD	ST primary stop switch fails	4.000E−06
100.00	0.01	5.230E−07	ISO-ST---HC002---HC--SPO	Spurious command to lift/lower AO or STC	5.230E−07
100.00	0.00	5.986E−12	ISO-LOSP-4	Failure of offsite power	4.100E−06
			ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E−06
100.00	0.00	1.333E−13	ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E−06
			ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E−08
100.00	0.00	5.535E−14	ISO-LOSP-4	Failure of off site power	4.100E−06
			ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	1.350E−08
100.00	0.00	2.745E−14	ISO-ST---BRK001--BRK-FOD	ST fails to stop on loss of power	1.460E−06
			ISO-ST---CBP004-CBP--SHC	ST power cable short circuit	1.880E−08
100.00	0.00	1.233E−15	ISO-ST---CBP004-CBP--OPC	ST power cable - open circuit	9.130E−08
			ISO-ST---MOE000--MOE-FSO	ST motor (electric) fails to shut off	1.350E−08

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask (used in WHF)

Source: Original

B2.4.1.8 Fault Tree

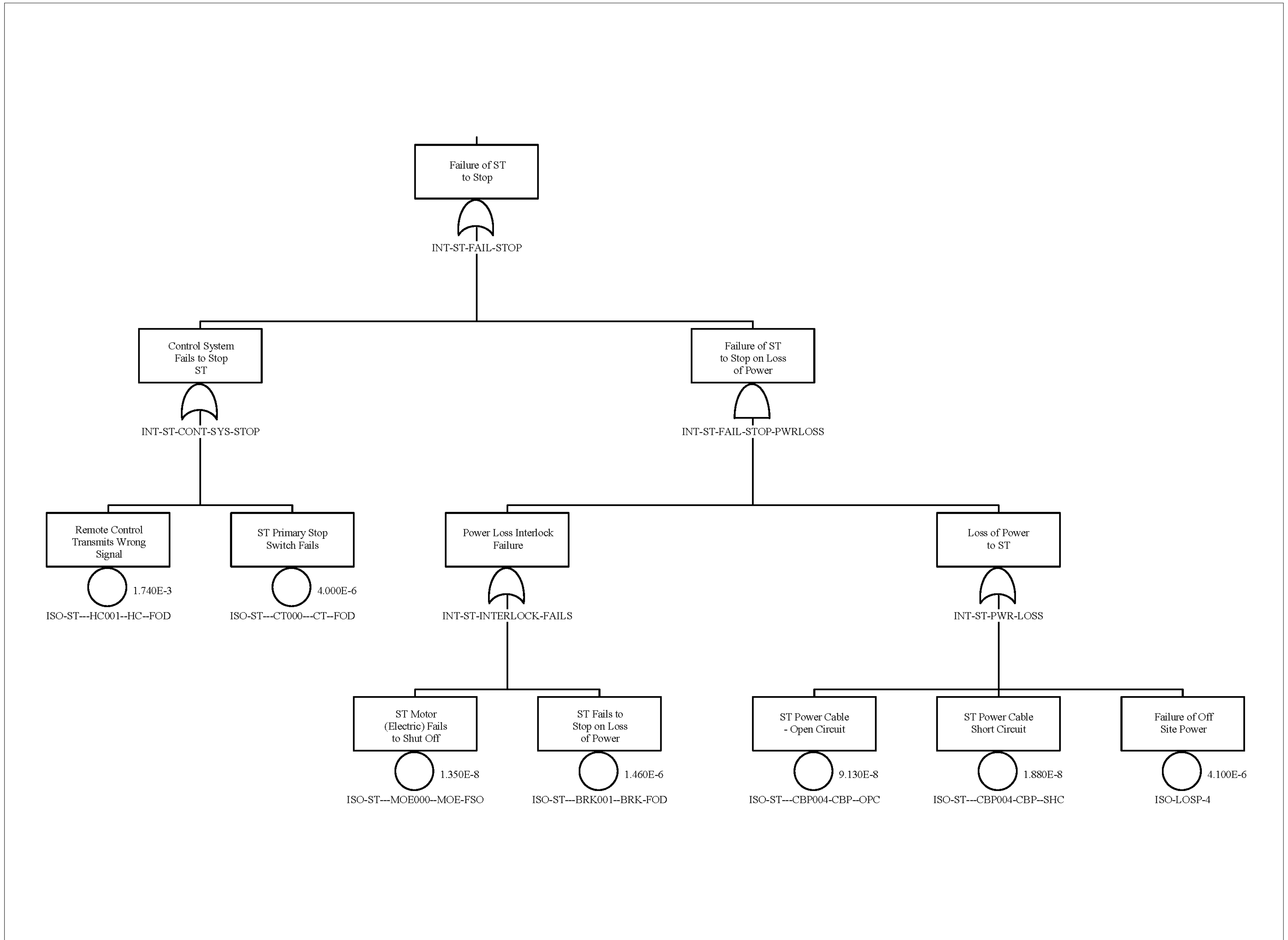
The fault trees for “Site Transporter Collision” are presented in Figures B2.4-3 through B2.4-5.



Source: Original

Figure B2.4-3. INT-2-ST-COLLISION -Site Transporter Collision Sheet 1 of 3

INTENTIONALLY LEFT BLANK

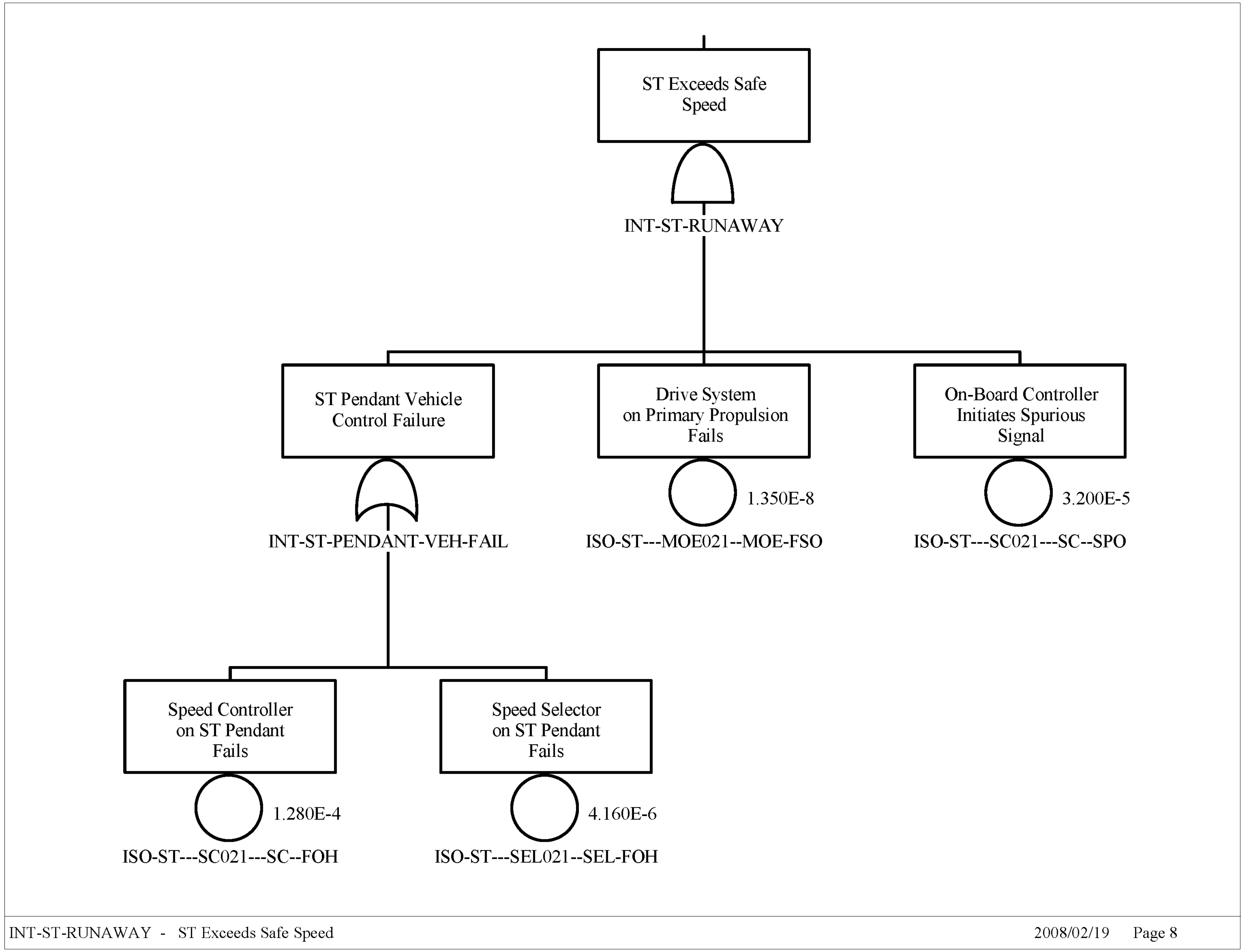


INT-ST-FAIL-STOP - Failure of ST to Stop 2008/02/20 Page 9

Source: Original

Figure B2.4-4. INT-2-ST-COLLISION Site Transporter Collision Sheet 2 of 3

INTENTIONALLY LEFT BLANK



Source: Original

Figure B2.4-5. INT-2-ST-COLLISION Site Transporter Collision Sheet 3 of 3

INTENTIONALLY LEFT BLANK

B2.4.2 Site Transporter Load Drop during Lift and Movement (INTRASITE-ST-AO-DROP)

B2.4.2.1 Description

The site transporter conducts lift/lowering and movement operations at the aging pads and inside the facilities. Since the site transporter is only capable of performing one operation at a time, it is not possible to move an aging overpack while it is being lifted/lowered. For activities associated with lifting the aging overpack, there are four distinct failure modes. Those associated with electrical failures, site transporter controller failures, mechanical failures during lifting/lowering, and mechanical failures during movement.

B2.4.2.2 Success Criteria

The potential for a load drop exists when there is a loss of site transporter power, a mechanical failure of the lift/lowering devices, aging overpack restraint device failure during movement, or a failure of the site transporter control system during these operations.

If there is a failure of the electrical system during lifting/lower or movement, the ACME screw/nuts prevent the rear forks and the lift support arms from moving.

The ACME devices also serve to prevent a load drop when there is a lift boom failure. There are four of these devices. One on each of the rear forks and one on each of the lift support arms.

The aging overpack restraint system is engaged after the lift has been accomplished and released prior to performing a lowering operation. These devices restrict the movement of the aging overpack during transport. There are three of these restraints that prevent/restrict movement in the roll-pitch-axis. Pins are used in these devices that prevent the release of the restraint in the advent of an electromechanical failure that controls the position of these devices.

There is an interlock built-in to the restraint system. Movement of the site transporter is prevented until the three pins in the restraint system have been properly installed. These pins also preclude an inadvertent release of the restraint system since they have to be removed from their engaged position before the restraints can be released.

The receipt of inadvertent command signals is also prevented in that the site transporter can only perform one operation at a time due to the limitations in the power plant.

B2.4.2.3 Design Requirements and Features

Requirements

On the loss or removal of AC power derived from the facility, the site transporter performs a controlled stop. Once stopped the site transporter enters the “lock mode,” safe state. The “lock mode,” safe state is not 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.

Two operators have the capability of stopping any operation performed by the site transporter when it is inside a facility.

B2.4.2.4 Fault Tree Model

The fault tree model for site transporter drop load during lift and movement addresses:

- Electrical failures, including motor and distribution events and the failure to enter a "lock mode," safe state.
- A load drop during the lifting or lowering of the aging overpack, which includes mechanical failure of the lifting booms and restraint/lifting arms.
- Failure of the aging overpack restraint subsystem during the lift/lowering/moving of the site transporter.
- Failure of the site transporter control subsystem.

NOTE: The fault tree defines the movement of the aging overpack in a three axis system as:

1. A roll movement side-to-side as the "R-axis"
2. A pitch movement front-to-back as the "P-axis"
3. An up or down movement as the "D-axis."

B2.4.2.5 Basic Events

Table B2.4-3 lists the basic events used in the "Site Transporter Load Drop during Lift and Movement" (INTRASITE-ST-AO-DROP) fault tree.

Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree

Name	Description	Calc Type[b]	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATB1011-AT--FOH	Screw actuator mechanism on lift boom #1 fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATB222-AT--FOH	Screw actuator mechanism on lift boom #2 fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATD03-AT--FOH	ST D-axis electrical actuator #1 movement fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATD04-AT--FOH	ST D-axis electrical actuator #2 movement fails	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATP002-AT--FOH	ST P-axis electrical failure during movement	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-ATR10002-AT-FOH	ST R-axis electrical actuator #1 fails movement	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00[a]
ISO-CRWT-BEA#1-BEA-BRK	Boom #1 fails during cask movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEA22-BEA-BRK	Boom #2 fails during cask lift	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEAB202-BEA-BRK	Boom #2 fails during cask movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEAD003-BEA-BRK	ST D-axis actuator structural arm #2 failure movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEAD006-BEA-BRK	ST D-axis actuator structural arm #1 failure movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEAP02-BEA-BRK	ST P-Axis mechanical failure during movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-BEAR103-BEA-BRK	ST R-axis actuator structural arm #1 failure movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]

Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree (Continued)

Name	Description	Calc Type[b]	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-BEAR204-BEA-BRK	ST R-axis actuator structural arm #2 failure movement	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00[a]
ISO-CRWT-CBP0000-CBP-OPC	Electrical power dist cable failure on ST	3	9.130E−08	0.000E+00	9.130E−08	1.000E+00[a]
ISO-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	3	7.140E−05	0.000E+00	7.140E−05	1.000E+00
ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	3	2.270E−05	0.000E+00	2.270E−05	1.000E+00[a]
ISO-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	3	2.400E−08	0.000E+00	2.400E−08	1.000E+00
ISO-CRWT-EATR2004-AT-FOH	ST R-axis electrical actuator #2 fails movement	3	7.540E−05	0.000E+00	7.540E−05	1.000E+00
ISO-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	3	1.790E−06	0.000E+00	1.790E−06	1.000E+00
ISO-CRWT-ELEC-MOE-FOD	ST electric motor failure	1	6.000E−05	6.000E−05	0.000E+00	1.000E+00
ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	1	2.750E−05	2.750E−05	0.000E+00	0.000E+00[a]
ISO-CRWT-LM000011-LC-FOD	ST lift/lower selector lever fails	1	6.250E−04	6.250E−04	0.000E+00	0.000E+00[a]
ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	3	2.100E−06	0.000E+00	2.100E−06	1.000E+00
ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	3	2.100E−06	0.000E+00	2.100E−06	1.000E+00
ISO-CRWT-PIND004-PIN-BRK	ST D-axis actuator pin #2 failure movement	3	2.120E−09	0.000E+00	2.120E−09	1.000E+00
ISO-CRWT-PIND005-PIN-BRK	ST D-axis actuator pin #1 failure movement	3	2.120E−09	0.000E+00	2.120E−09	1.000E+00
ISO-CRWT-PINP04-PIN-BRK	ST P-axis pin failure during movement	3	2.120E−09	0.000E+00	2.120E−09	1.000E+00
ISO-CRWT-PINR103-PIN-BRK	ST R-axis mechanical pin #1 failure during movement	3	2.120E−09	0.000E+00	2.120E−09	1.000E+00
ISO-CRWT-PINR202-PIN-BRK	ST R-axis mechanical pin #2 failure during movement	3	2.120E−09	0.000E+00	2.120E−09	1.000E+00
ISO-CRWT-SJKB011-SJK-FOH	Screw lift on boom #1 fails	3	8.140E−06	0.000E+00	8.140E−06	1.000E+00
ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	3	8.140E−06	0.000E+00	8.140E−06	1.000E+00
ISO-CRWT-SJKB202-SJK-FOH	Screw lift on boom #2 fails	3	8.140E−06	0.000E+00	8.140E−06	1.000E+00

Table B2.4-3. Basic Event Probability for the INTRASITE-ST-AO-DROP Fault Tree (Continued)

Name	Description	Calc Type[b]	Calculation Probability	Failure Probability	Lambda	Mission Time
ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	3	8.140E−06	0.000E+00	8.140E−06	1.000E+00
ISO-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	1	2.930E−04	2.930E−04	0.000E+00	0.000E+00[a]
ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	1	2.930E−04	2.930E−04	0.000E+00	0.000E+00[a]
ISO-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	1	2.930E−04	2.930E−04	0.000E+00	0.000E+00[a]
ISO-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	1	2.930E−04	2.930E−04	0.000E+00	0.000E+00[a]
ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	3	1.350E−08	0.000E+00	1.350E−08	1.000E+00

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time (1.00E+00).
[b] 1 is direct input probability; and 3 is lambda and mission time.

AO = aging overpack; Calc. = calculation; ST = site transporter; STC = shielded transfer cask (used in WHF).

Source: Original

B2.4.2.5.1 Human Failure Events

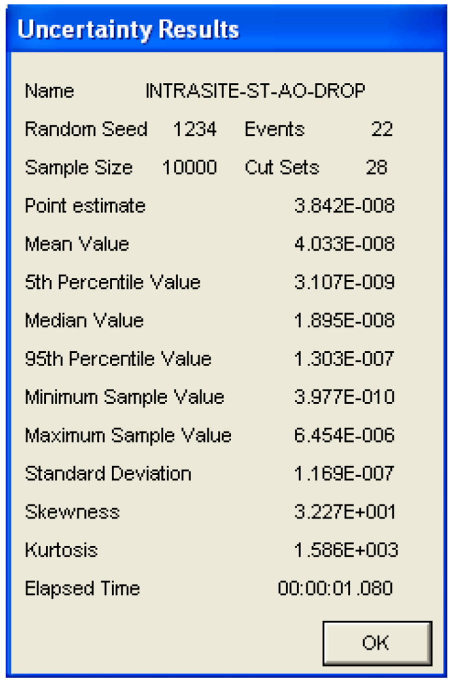
There are no human error events incorporated in the tree.

B2.4.2.5.2 Common-cause Failures

There are no CCFs identified in this fault tree.

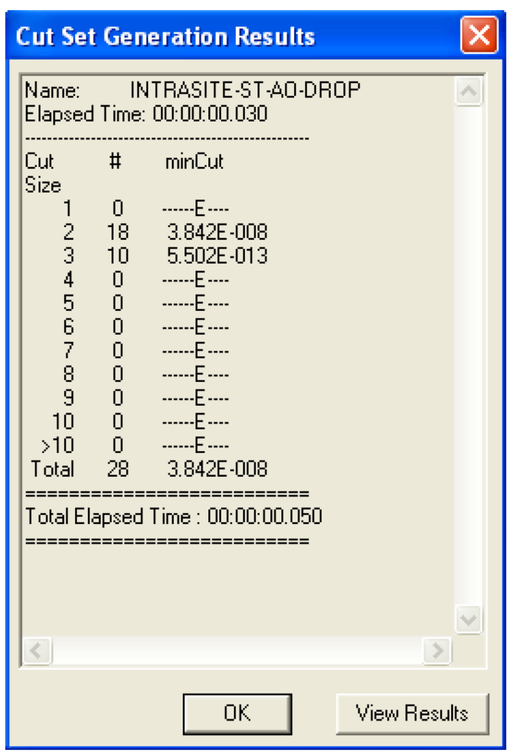
B2.4.2.6 Uncertainty and Cut Set Generation

Figures B2.4-6 and B2.4-7 contain the uncertainty and the cut set generation results for “Site Transporter Load Drop during Lift and Movement” fault tree using a cutoff probability of 1E−15.



Source: Original

Figure B2.4-6. Uncertainty Results for Site Transporter Load Drop during Lift/Movement Fault Tree



Source: Original

Figure B2.4-7. Cut Set Generation Results for Site Transporter Load Drop during Lift/Movement Fault Tree

B2.4.2.7 Cut Sets

Table B2.4-4 contains the top 25 cut sets for "Site Transporter Load Drop during Lift/Movement" (INTRASITE-ST-AO-DROP) fault tree.

Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree

% Total	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
36.92	36.92	1.419E−08	ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E−05
			ISO-CRWT-LM000011-LC-FOD	ST lift/lower selector lever fails	6.250E−04
57.89	20.97	8.057E−09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E−05
			ISO-CRWT-ZSR00005-ZS-FOD	ST R-axis position switch failure movement	2.930E−04
78.86	20.97	8.057E−09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E−05
			ISO-CRWT-ZSP00003-ZS-FOD	ST P-axis position switch failure during movement	2.930E−04
99.83	20.97	8.057E−09	ISO-CRWT-IEL0001-IEL-FOD	Restraint system interlock failure	2.750E−05
			ISO-CRWT-ZSD00005-ZS-FOD	ST D-axis position switch failure movement	2.930E−04
99.94	0.11	4.063E−11	ISO-CRWT-CTSHC000-CT-SPO	Spurious command to raise/lower AO or STC	2.270E−05
			ISO-CRWT-ECP0000-ECP-FOH	ST restraint arms position selector fails	1.790E−06
99.96	0.02	7.032E−12	ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E−08
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E−04
99.98	0.02	7.032E−12	ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E−08
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E−04
99.98	0.00	1.810E−12	ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E−05
			ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E−08
99.98	0.00	1.810E−12	ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E−05
			ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E−08
99.98	0.00	1.810E−12	ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E−05
			ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E−08
99.98	0.00	1.810E−12	ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E−05

Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree (Continued)

% Total	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
99.98 (cont.)	0.00 (cont.)	1.810E−12 (cont.)	ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E−08
99.98	0.00	9.639E−13	ISO-CRWT-CON0000-CON-FOH	Electrical power dist connectors fail on ST	7.140E−05
			ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E−08
99.98	0.00	8.100E−13	ISO-CRWT-ELEC-MOE-FOD	ST electric motor failure	6.000E−05
			ISO-ST-MOE0001-MOE-FSO	ST lock mode state fails on loss of power	1.350E−08
99.98	0.00	1.798E−13	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E−05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E−06
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E−04
99.98	0.00	1.798E−13	ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E−05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E−06
			ISO-CRWT-ZSD0006-ZS-FOD	ST D-axis position switch failure lift/lower	2.930E−04
99.98	0.00	5.040E−14	ISO-CRWT-DROP11-BEA-BRK	Boom #1 fails during cask lift	2.400E−08
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E−06
99.98	0.00	5.040E−14	ISO-CRWT-BEA22-BEA-BRK	Boom #2 fails during cask lift	2.400E−08
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E−06
99.98	0.00	5.040E−14	ISO-CRWT-DROP11-BEA-BRK	Boom#1 fails during cask lift	2.400E−08
			ISO-CRWT-LVRD01-LVR-FOH	ST D-Axis actuator structural arm #1 failure	2.100E−06
99.98	0.00	5.040E−14	ISO-CRWT-BEA22-BEA-BRK	Boom#2 fails during cask lift	2.400E−08
			ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	2.100E−06
99.98	0.00	4.627E−14	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E−05
			ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E−05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E−06
99.98	0.00	4.627E−14	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E−05

Table B2.4-4. Cut Sets for Site Transporter Load Drop during Lift/Movement Fault Tree (Continued)

% Total	Cut Set %	Probability/ Frequency	Basic Event	Description	Probability
99.98 (cont.)	0.00 (cont.)	4.627E-14 (cont.)	ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E−05
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E−06
99.98	0.00	4.627E−14	ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E−05
			ISO-CRWT-ATD001-AT--FOH	ST D-axis electrical actuator #1 fails lift/lower	7.540E−05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E−06
99.98	0.00	4.627E−14	ISO-CRWT-ATB2002-AT--FOH	Screw actuator mechanism on lift boom #2 fails	7.540E−05
			ISO-CRWT-ATD0002-AT--FOH	ST D-axis electrical actuator #2 fails lift/lower	7.540E−05
			ISO-CRWT-SJKB22-SJK-FOH	Screw lift on boom #2 fails	8.140E−06
99.98	0.00	1.289E−15	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E−05
			ISO-CRWT-LVRD02-LVR-FOH	ST D-axis actuator structural arm #2 failure	2.100E−06
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E−06
99.98	0.00	1.289E−15	ISO-CRWT-ATB1001-AT--FOH	Screw actuator mechanism on lift boom #1 fails	7.540E−05
			ISO-CRWT-LVRD01-LVR-FOH	ST D-axis actuator structural arm #1 failure	2.100E−06
			ISO-CRWT-SJKB101-SJK-FOH	Screw lift on boom #1 fails	8.140E−06

NOTE: AO = aging overpack; ST = site transporter; STC = shielded transfer cask (used in WHF).

Source: Original

B2.4.2.8 Fault Trees

The fault trees for "Site Transporter drop Load during Lift/Movement" are presented in Figures B2.4-8 through B2.4-19.