

Source: Original

Figure B4.4-40. CTM Collision Sheet 5

INTENTIONALLY LEFT BLANK

B4.4.5 CTM Movement Subjects Canister to Shearing Forces

B4.4.5.1 Description

A fault tree was developed to address the potential for movement of the CTM when the canister being transferred is being lifted and is between the IHF floors. Movement initiated by the bridge or trolley motors could result in shear forces being applied to the canister should it be lifted when the CTM moves away from the floor port opening.

B4.4.5.2 Success Criteria

Success criteria for the CTM is the prevention of CTM movement that could result in a shearing force being applied to the canister when the canister is being lifted and is between the first and second floors of the IHF during the lift portions of the canister transfer.

B4.4.5.3 Design Requirements and Features

Requirements

Hard-wired interlocks are used to prevent inadvertent actions during CTM transfer operations. These include the following:

- An optical sensor at the bottom of the shield bell that, once it is cleared, stops the hoist and erases the lift command (can only lower hoist). This interlock is used only when lifting a canister
- Above the ASD stop point is an upper limit switch which, when reached, stops the hoist from lifting. This first limit switch (first hoist upper limit) effectively erases the lift command (the hoist still has power) and the operator can only lower the hoist. Roughly a foot above that limit switch is another limit switch (final hoist upper limit) that, when reached, cuts off the power to the CTM hoist
- An interlock between the shield skirt and port gate which requires the shield skirt to be lowered in order for the port gate to open. There is a bypass for this interlock
- An interlock between the CTM bridge/trolley travel and shield skirt position. Neither the CTM bridge nor the trolley can travel while the skirt is lowered
- An interlock between the slide gate and shield skirt – the shield skirt cannot be raised unless the slide gate is closed. This interlock can be bypassed, to allow the CTM to move with the slide gate open during lid removal
- Interlocks preventing improper hoist movement. The hoist cannot move unless the shield skirt is lowered. This interlock is based on hoist movement, not position, so movement with the hoist too low is not precluded

- The load cells cut off power to the hoist when the crane capacity is exceeded
- An interlock between the grapple position (fully engaged or fully disengaged) and hoist movement. The grapple automatically engages/disengages with a given object. The grapple must be positively engaged for the grapple engagement indicator to give a positive indication.

Design Features

Bridge and trolley motors are sized to limit lateral travel to less than 20 ft/min, sufficient to ensure that in the event of an impact, impact forces are below the design limits of the canister. |

The shield bell slide gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

The floor port gate motors are sized so that they are incapable of exerting sufficient force to damage any canister given an inadvertent closure of the gate when a canister is suspended in the gate closure path.

Hard-wired interlocks used to prevent inadvertent actions during CTM transfer operations are ITS; PLCs are not ITS equipment.

The end stops for both the bridge and trolley end of travel end stops are capable of stopping the bridge/trolley at their maximum speed and preclude impact with any permanent structure.

The interlock between the grapple position and the operation of the hoist motor cannot be bypassed during CTM canister transfer operations.

B4.4.5.4 Fault Tree Model

The top event in this fault tree is “CTM Movement Subjects Canister to Shearing Forces.” The fault tree includes events (mechanical control failures and human actions, considered in conjunction with the interlocks intended to prevent the erroneous human action) that can initiate a spurious movement of the CTM trolley or bridge while the canister is between the first and second floors of the IHF.

B4.4.5.5 Basic Event Data

Table B4.4-12 contains a list of basic events used in the “CTM Movement Subjects Canister to Shearing Forces” fault tree. Included are the human failure events and the common-cause failure events identified in the following two sections. There are no maintenance failures associated with the CTM. The CTM is not in service while it is undergoing maintenance. Sensor failures that could be associated with the failure to restore from maintenance are not expected to contribute significantly to the overall sensor availability. |

Table B4.4-12. Basic Event Probabilities for the CTM Movement Subjects Canister to Shearing Forces Fault Trees

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹) ^a	Miss. Time (hr) ^a
51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	3	5.784E-05	—	7.230E-06	8
51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	3	2.856E-02	—	8.050E-05	360
51A-CTM-BRIDGMS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation - shear	3	6.740E-08	—	6.740E-07	0.1
51A-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	3	6.740E-08	—	6.740E-07	0.1
51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	3	2.856E-02	—	8.050E-05	360
51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation - shear	3	3.650E-08	—	3.650E-07	0.1
51A-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3	3.650E-08	—	3.650E-07	0.1
51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation - shear	3	3.650E-08	—	3.650E-07	0.1
51A-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	3	6.740E-08	—	6.740E-07	0.1
51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	3	2.856E-02	—	8.050E-05	360
51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	1	4.000E-08	4.000E-08	—	—

NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

CCF = common-cause failure; CTM = canister transfer machine; PLC = programmable logic controller.

Source: Original

The shear impact drop probability modeled by the fault tree is evaluated over a mission time of one-tenth of an hour (limited to the time the canister is being lifted and is between the first and second floors). A longer mission time is also considered for specific components. For example, the fault tree accounts for the failure of standby components whose potential malfunction would remain hidden until they are tested. They are consequently evaluated over the interval of time between their tests, and the mission time is assigned a value of the average fault exposure time, half the test interval.

B4.4.5.5.1 Human Failure Events

One basic event is associated with human error: 51A-OPCTMIMPACT1-HFI-COD (Operator moves trolley/crane with canister below floor). This event addresses the possible operator initiated movement of the bridge or trolleys while a canister is being lifted and is between IHF floors.

B4.4.5.5.2 Common-Cause Failures

No common-cause failures apply to this fault tree.

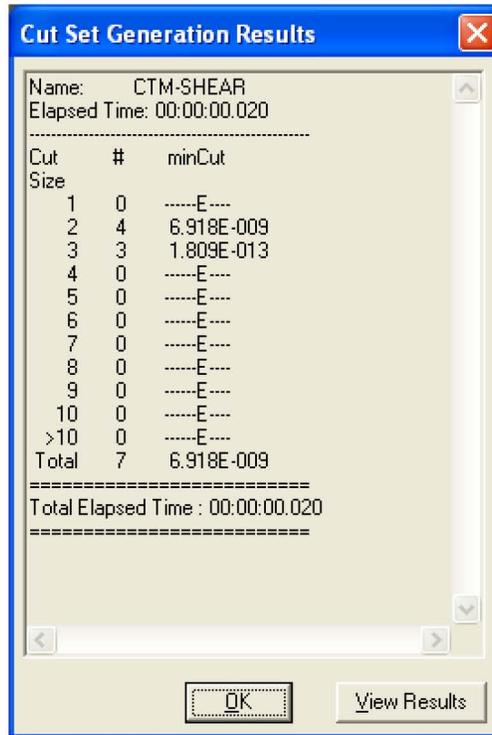
B4.4.5.6 Uncertainty and Cut Set Generation

Figure B4.4-41 contains the uncertainty results obtained from running the fault trees for “CTM Movement Subjects Canister to Shearing Forces.” Figure B4.4-42 provides the cut set generation results for the “CTM Movement Subjects Canister to Shearing Forces” fault tree.

Uncertainty Results	
Name	CTM-SHEAR
Random Seed	1234 Events 11
Sample Size	10000 Cut Sets 7
Point estimate	6.918E-009
Mean Value	6.739E-009
5th Percentile Value	5.109E-010
Median Value	3.120E-009
95th Percentile Value	2.257E-008
Minimum Sample Value	3.126E-011
Maximum Sample Value	4.229E-007
Standard Deviation	1.409E-008
Skewness	1.118E+001
Kurtosis	2.212E+002
Elapsed Time	00:00:00.750
OK	

Source: Original

Figure B4.4-41. Uncertainty Results of the CTM Movement Subjects Canister to Shearing Forces Fault Tree



Source: Original

Figure B4.4-42. Cut Set Generation Results for the CTM Movement Subjects Canister to Shearing Forces Fault Tree

B4.4.5.7 Cut Sets

Table B4.4-13 contains the cut sets for the “CTM Movement Subjects Canister to Shearing Forces” fault tree.

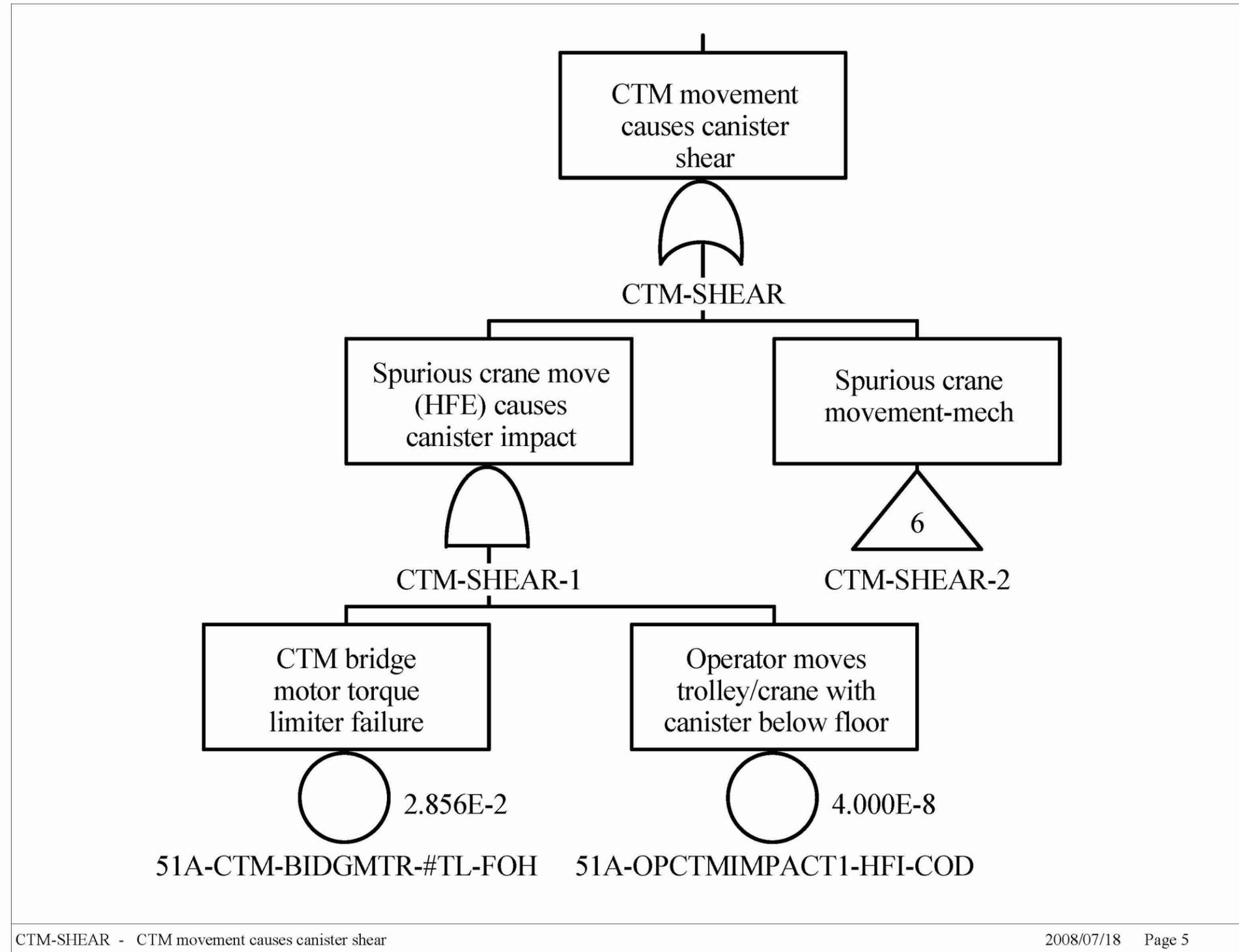
Table B4.4-13. Cut Sets for the CTM Movement Subjects Canister to Shearing Forces Fault Tree

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
27.83	27.83	1.925E-009	51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.9E-002
			51A-CTM-BRIDGMTS-MOE-SPO	CTM Bridge Motor (Electric) Spurious Operation -shear	6.7E-008
55.66	27.83	1.925E-009	51A-CTM-HSTTRLLS-MOE-SPO	CTM Hoist Trolley Motor (Electric) Spurious Operation m- shear	6.7E-008
			51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.9E-002
83.49	27.83	1.925E-009	51A-CTM-SBELTRLS-MOE-SPO	CTM shield Bell trolley Motor (Electric) spurious operation-shear	6.7E-008
			51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.9E-002
100.00	16.51	1.143E-009	51A-CTM-BI DGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.9E-002
			51A-OPCTMIMPACT1-HFI-COD	Operator moves trolley/crane with canister below floor	4.0E-008
100.00	0.00	6.030E-014	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.8E-005
			51A-CTM-BIDGMTR-#TL-FOH	CTM Bridge motor Torque limiter Failure	2.9E-002
			51A-CTM-PLC0101S-PLC-SPO	CTM Bridge Motor PLC Spurious Operation -shear	3.7E-008
100.00	0.00	6.030E-014	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.8E-005
			51A-CTM-HSTTRLLY-#TL-FOH	CTM Hoist motor Torque limiter Failure	2.9E-002
			51A-CTM-PLC0103S-PLC-SPO	CTM Hoist Trolley PLC Spurious Operation -shear	3.7E-008
100.00	0.00	6.030E-014	51A-CTM-#ZSH0112-1ZS-FOH	CTM Shield skirt position switch 0112 fails	5.8E-005
			51A-CTM-PLC0102S-PLC-SPO	CTM Shield Bell Trolley PLC Spurious Operation -shear	3.7E-008
			51A-CTM-SBELTRLY-#TL-FOH	CTM Shield Bell Motor Torque limiter Failure	2.9E-002

NOTE: CCF =common-cause failure; CTM =canister transfer machine; PLC = programmable logic controller.

Source: Original

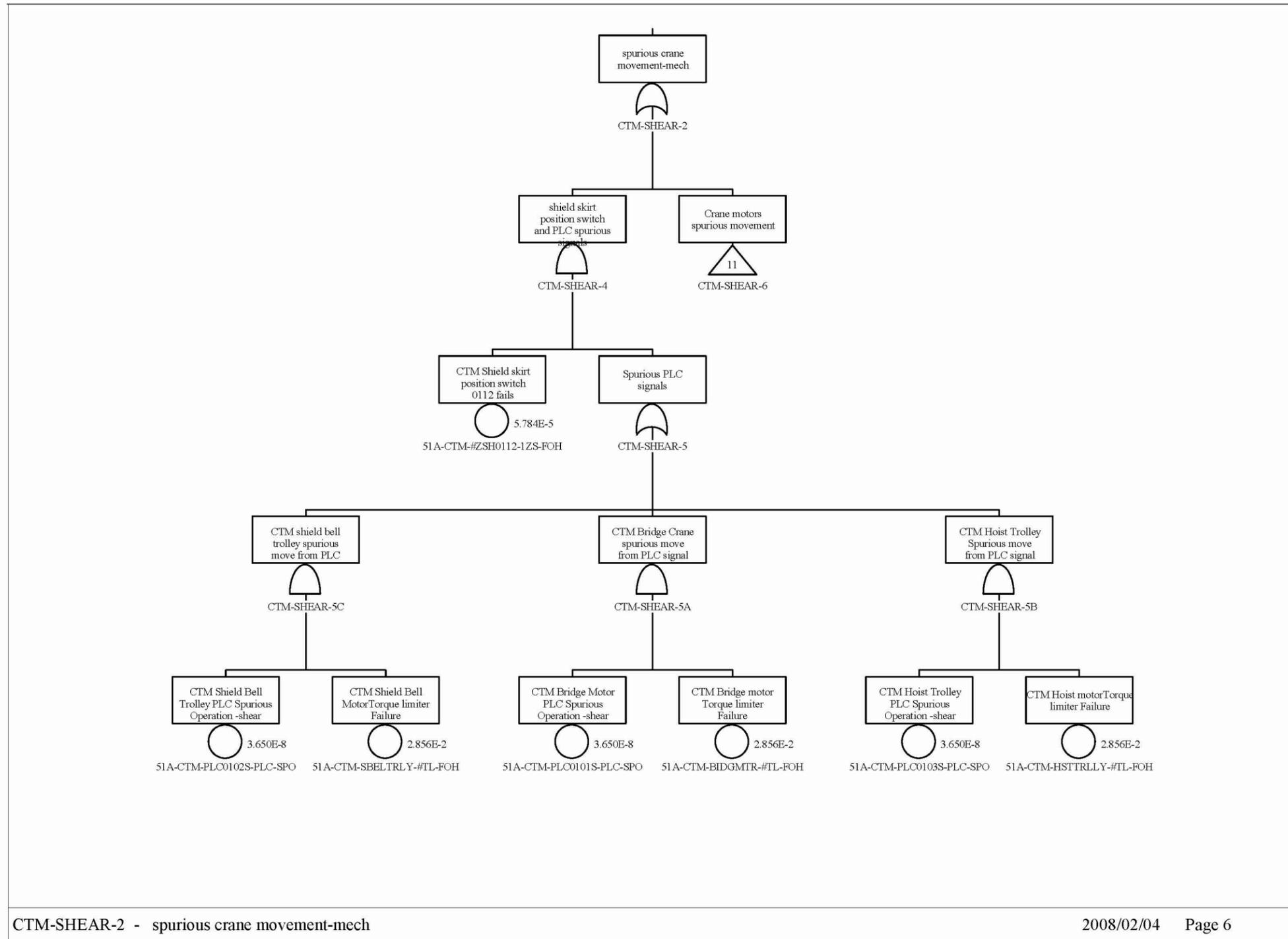
B4.4.5.8 Fault Tree



Source: Original

Figure B4.4-43. CTM Shear Sheet 1

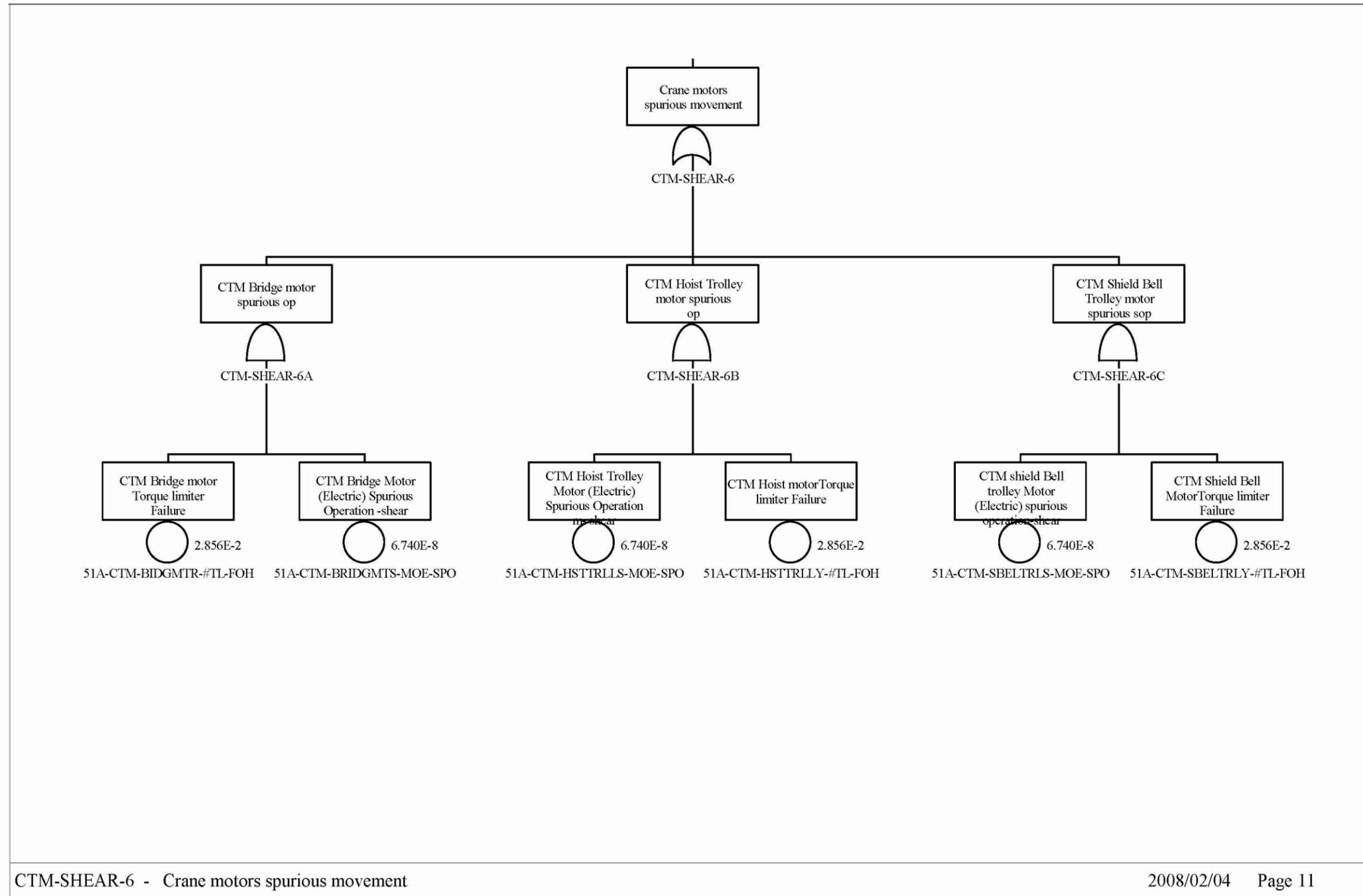
INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-44. CTM Shear Sheet 2

INTENTIONALLY LEFT BLANK



Source: Original

Figure B4.4-45. CTM Shear Sheet 3

INTENTIONALLY LEFT BLANK

B5 WASTE PACKAGE TRANSFER TROLLEY ANALYSIS – FAULT TREES

B5.1 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), Sections 3.2.1 and 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 designated categories described in Section 4.1, relative to suitability for intended use.

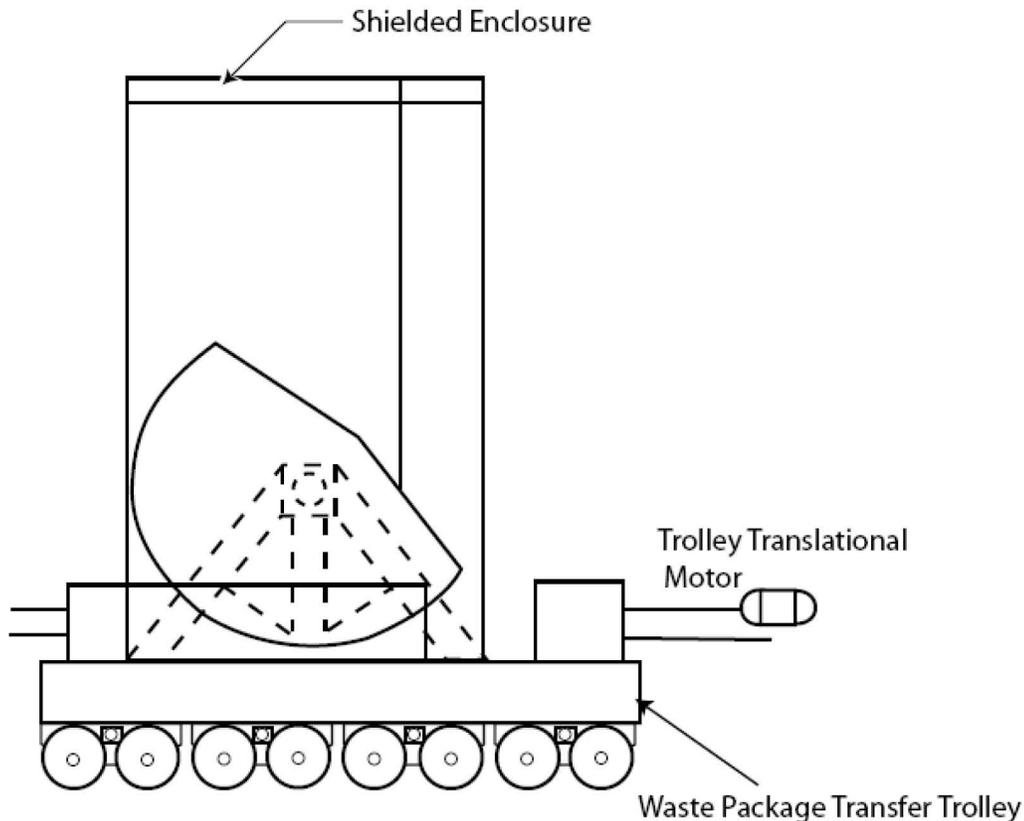
- B5.1.1 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.
- B5.1.2 Not Used.
- B5.1.3 Not Used.
- B5.1.4 BSC 2007. *CRCF and IHF WP Transfer Trolley Process & Instrumentation Diagram*. 000-M60-HL00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0013.
- B5.1.5 *BSC 2007. *CRCF-1 and IHF WP XFR Carriage Docking Sta Mechanical Equipment Envelope Plan, Elevation, & Section*. 000-MJ0-HL00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0018.
- B5.1.6 *BSC 2007. *CRCF and IHF WP XFR Carriage Docking Sta Process & Instrumentation Diagram*. 000-M60-HL00-00301-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071027.0014.
- B5.1.7 †BSC 2007. *Mechanical Handling Design Report – Waste Package Transfer Trolley*. 000-30R-WHS0-01200-000 REV 000. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071006.0001.
- B5.1.8 *BSC 2007. *Preliminary Throughput Study for the Initial Handling Facility*. 51A-30R-IH00-00100-000. REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071102.0021.

B5.1.9 BSC 2008. *Nuclear Facilities Slide Gate Process and Instrumentation Diagram*. 000-M60-H000-00201-000 REV 00E. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080123.0025.

B5.1.10 BSC 2008. *Waste Package Transfer Trolley Calculation*. 000-M0C-HL00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080207.0002.

B5.2 SYSTEM DESCRIPTION

This system description is derived from *CRCF and IHF WP XFR Carriage Docking Sta Process & Instrumentation Diagram* (Ref. B5.1.6), *CRCF-1 and IHF WP XFR Carriage Docking Sta Mechanical Equipment Envelope Plan, Elevation, & Section* (Ref. B5.1.5), *CRCF and IHF WP Transfer Trolley Process & Instrumentation Diagram* (Ref. B5.1.4), *Mechanical Handling Design Report – Waste Package Transfer Trolley* (Ref. B5.1.7) and *Waste Package Transfer Trolley Calculation* (Ref. B5.1.10). The Waste Package Transfer Trolley (WPTT), shown in Figure B5.2-1 is an electrically powered machine that is used to transport the waste package containing various waste canisters from the Waste Package Loading Room to the Waste Package Positioning Room and then to the waste package transfer carriage docking station in the Waste Package Loadout Room. The WPTT consists of the trolley and the shielded enclosure that holds the waste package, waste package pallet, waste package transfer carriage, and pedestal. The shielded enclosure acts to minimize radiation to the surroundings. The enclosure pivots between a vertical and horizontal position for waste package loading and unloading. The center of gravity of the shielded enclosure is positioned such that the vertical position is the most stable position.



Source: Derived from CRCF and IHF WP Transfer Trolley Process & Instrumentation Diagram (Ref. B5.1.4)

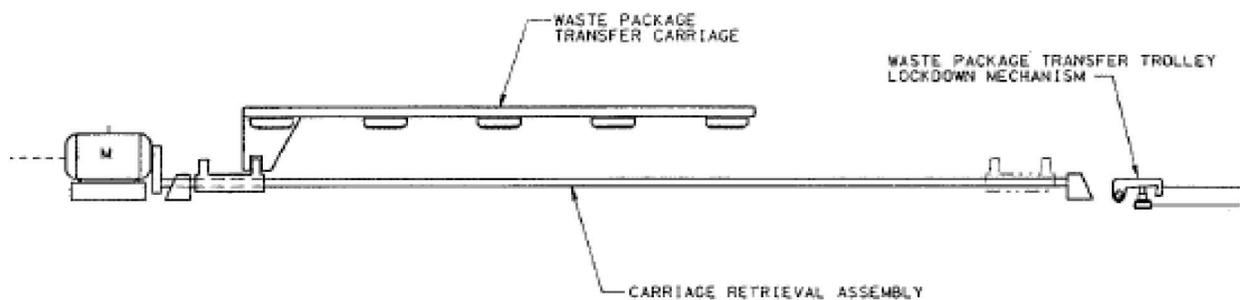
Figure B5.2-1. Waste Package Transfer Trolley

The WPTT travels on rails between the Waste Package Loading Room and the docking station using 24" double-flanged crane wheels. The total travel distance between these rooms is approximately 118 ft. Rail sweeps are used in front of each trolley wheel to brush away any object that might fall onto the trolley rails. The crane rails supporting the WPTT are gapped in multiple locations (as much as 16") to accommodate shield doors between rooms. Power is supplied to the motor by a third rail system and the maximum speed is less than 40 ft/min (Ref. B5.1.7, Section 3.2.4) established by the size of the drive motor and the gear drive system. The WPTT includes seismic rail clamps and rails anchored to the floor to ensure the stability of the WPTT during a seismic event.

The rotation of the shielded enclosure, which is also powered by the third rail system, is controlled by two rotation mechanisms, each consisting of a motor and a mechanical worm gear system. Each rotation mechanism is sized to rotate at a rate of 90-degrees per hour (Ref. B5.1.10, Section 6.15), and the worm gear mechanism has the inherent property to self lock to prevent uncontrolled tilt down. Within the shielded enclosure is a pedestal where the waste package sits during transfer operations that allow the waste package to be at the correct height for loading and sealing operations. There are interchangeable pedestals of different sizes which are for the loading operations of different sized waste packages.

The motor power for the trolley and the shielded enclosure is such that the canister cannot be breached through a shear failure in the event of spurious signals during canister transfer into the waste package. Either the drive train or rotational motors trip off before the canister is breached.

The waste package transfer carriage shown in Figure B5.2-2 is a wheeled platform that carries the waste package pallet and waste package. The transfer carriage is moved by a mechanical screw driven carriage retrieval assembly which places the carriage with an empty waste package into the shielded enclosure and retrieves the carriage with a loaded waste package in the Waste Package Loadout Room after the waste package has been loaded and sealed. Once removed from the shielded enclosure, the transport and emplacement vehicle (TEV) is able to pick up the loaded waste package and pallet by lifting features on the waste package pallet.



Source: Derived from CRCF and IHF WP XFR Carriage Docking Sta Process & Instrumentation Diagram (Ref. B5.1.6)

Figure B5.2-2. Waste Package Transfer Carriage

B5.2.1 Control System

Interlocks prevent translational or rotational motion of the WPTT while a canister is being loaded into the waste package (i.e., when the waste package slide gate is open) or while the waste package is being withdrawn from the shielded enclosure on the transfer carriage (Ref. B5.1.6), (Ref. B5.1.9), and (Ref. B5.1.4). The shielded enclosure is not able to rotate in either direction unless the WPTT is locked into the waste package transfer carriage docking station and the waste package carriage retrieval assembly is completely extended or retracted. Interlocks also prevent over-travel of the trolley and travel through portals when the shield doors are closed. Manually actuated, hardwired emergency stop buttons are available at all control locations to allow power to be removed from the drive motors. However, because the emergency stop function is a recovery action performed by the operator and requires operator intervention, these functions were not modeled in the analysis. A schematic of the control system and interlocks is shown in Figure B5.2-3.

The following controls are incorporated in the design of the rotation mechanism of the shielded enclosure:

- Rotation start and stop

- End of travel limit switches
- Motor amperage readout
- Interlocks to prevent movement of the shielded enclosure unless the trolley is locked down at the docking station and the waste package carriage retrieval assembly is completely extended or retracted.

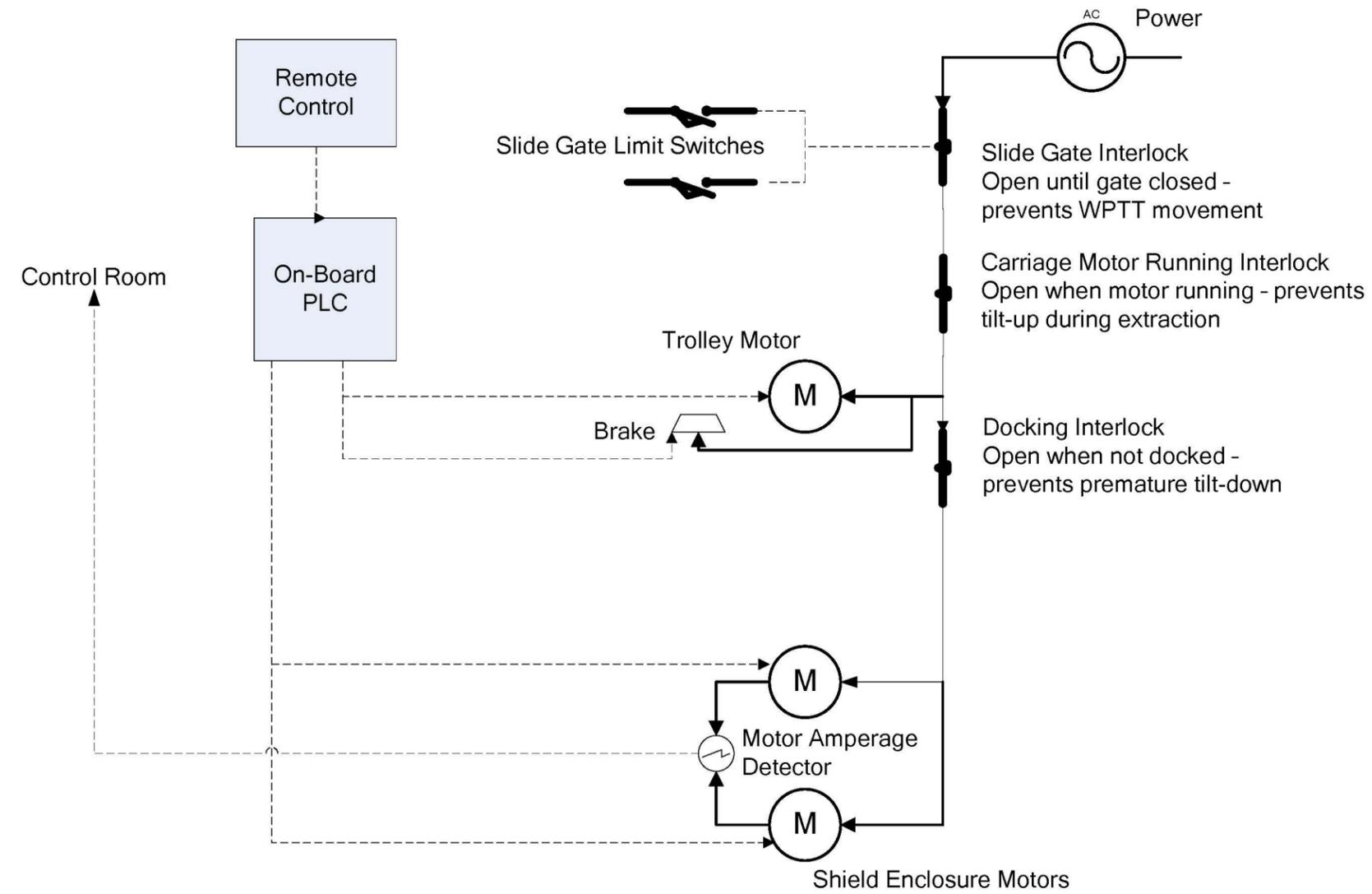
The following controls are provided for operation of the trolley system:

- Trolley start (forward and reverse) and stop
- Forward and reverse end of travel limit switches
- Motor amperage readout
- Forward and reverse range detectors, interlocked with the motors through a PLC
- Interlock to prevent movement of the trolley when the waste package slide gate is opened
- Position indication along the travel rail.

The following controls are provided for operation of the docking station system:

- Waste package retrieval system start (forward and reverse) and stop
- Raise and lower motions for the WPTT locking mechanisms
- Interlock between the locking mechanisms and the shielded enclosure to prevent unlocking the trolley from the docking station unless the enclosure is in the vertical position
- Interlock between the retrieval system and the power feed to the WPTT to prevent operation of the WPTT during waste package retrieval
- Motor amperage readout
- Position indication of the waste package as it is being retrieved from the WPTT.

INTENTIONALLY LEFT BLANK



NOTE: AC = alternating current; M = motor; PLC = programmable logic controller; WPTT = waste package transfer trolley.

Source: Original

Figure B5.2-3. Schematic of the Waste Package Transfer Trolley Control System

INTENTIONALLY LEFT BLANK

B5.2.2 Operation

B5.2.3 Initial Conditions

The waste package loading operation begins with an empty waste package being loaded into the WPTT on the pallet while the WPTT is locked into the waste package transfer carriage docking station and in the horizontal position. The transfer carriage with an empty waste package on the pallet is moved into the shielded enclosure of the WPTT via the waste package transfer carriage docking station's waste package retrieval assembly. Once the retrieval assembly is fully extended and the carriage and empty waste package are positioned within the WPTT, the shielded enclosure is rotated into the vertical position. A visual inspection of the waste package is then performed to ensure the positioning is correct within the shielded enclosure. When the waste package is correctly placed in the vertically oriented shielded enclosure the shield ring is lowered and locked into position on top of the shielded enclosure by the waste package handling crane equipped with the shield ring lift beam. Again a visual inspection is performed to ensure the shield ring is properly seated.

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

B5.2.4 Waste Package Loading

Once in position in the loading room, the slide gate is opened to allow the waste canister(s) to be lowered into the empty waste package using the canister transfer machine (CTM). The waste is contained in canisters during the entire process; these canisters are either HLW canisters or naval canisters.

B5.2.5 Waste Package Transfer

After the waste package is loaded and the slide gate closed, an operator in the control room provides power to the WPTT to move it to the Waste Package Positioning Room.

B5.2.6 Waste Package Closure

After the waste package is loaded and the slide gate closed, the WPTT moves to the Waste Package Positioning Room. The WPTT is positioned under the opening to the Waste Package Closure Room so that the top of the waste package is accessible through the opening. At this station the inner lid is placed on the waste package, welded in place, and the weld's integrity inspected. The air within the waste package is replaced by helium with a helium purging operation. Once the inner lid is inspected for leakage, the outer lid is positioned and welded in place. The welds of the outer lid are inspected to ensure the waste package is properly sealed.

B5.2.7 Waste Package Transfer Trolley Loadout

After the waste package is sealed, the WPTT is moved into the Waste Package Loadout Room where it is locked into the waste package transfer carriage docking station. The shield ring is remotely removed with the waste package handling crane and the shielded enclosure is rotated into the horizontal position. The waste package carriage retrieval assembly engages the carriage interface and retracts guiding the carriage and waste package out of the shielded enclosure. During the transfer from the WPTT to the TEV, video cameras allow operators to inspect the waste package surface for damage. The waste package is positioned such that the TEV is able to lift the waste package and pallet off the carriage. From here the TEV transports the waste package into the repository for emplacement.

Upon the WPTT reaching the loadout area, the TEV is in place and the carriage retrieval assembly is completely retracted. The WPTT links to the docking mechanism of the waste package retrieval system closing an interlock and allowing the shielded enclosure to be rotated to the horizontal position. The retrieval system links with the carriage assembly within the shielded enclosure. During extraction of the waste package carriage an interlock interrupts the power feed to the WPTT to prevent operation of the WPTT during the retrieval operation. When the carriage retrieval system is fully retracted the waste package has been removed from the shielded enclosure, an interlock is closed, and the shielded enclosure can now be raised to the vertical position. When the enclosure is vertical, the trolley can be unlocked from the docking station and moved back.

B5.3 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 B5.3-1 with the following dependencies:

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

Table B5.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environmental	Spatial	Human	External Events
Electric Power	Provides motive force	—	—	—	—
Trolley motor and gear drive	Limits maximum speed	—	—	—	—
Shielded enclosure motor and gear drive	Limits rotational speed and prevents slapdown	—	—	—	—
Interlocks	Prevent spurious movement	—	—	—	Fire or explosion can cause loss of power

Table B5.3-1. Dependencies and Interactions Analysis (Continued)

Structures, Systems, and Components	Dependencies & Interactions				
	Functional	Environmental	Spatial	Human	External Events
Rails	Prevent movement in wrong direction	—	—	—	—
Control room	Controls direction and speed and initiates movement	—	—	Wrong instructions	Fire or explosion can cause loss of power
Emergency stop	Stops WPTT	—	—	Fail to energize	—
Structure	Constrains and supports canisters and WP	—	—	—	Seismic causes impact
Shield door	Opens for WPTT to pass through	—	—	Close door inadvertently	Closes on WPTT

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

Source: Original

B5.4 RELATED FAILURE SCENARIOS

There are five fault trees associated with the WPTT:

1. Spurious movement of the WPTT in the loading area while loading the waste package with canisters—while loading a cask onto the WPTT, and spurious movement into the Waste Package Loadout Room while extracting the waste package carriage from the shielded enclosure.
2. Impact of the WPTT with a structure—while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
3. Derailment of the WPTT—while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
4. Premature tiltdown of the WPTT—premature tiltdown of the shielded enclosure while moving from the Waste Package Loading Room to the Waste Package Positioning Room and then to the Waste Package Loadout Room.
5. Malfunction of WPTT or waste package transfer carriage—while extracting the carriage and waste package from the shielded enclosure at the Waste Package Loadout Room.

An additional fault tree associated with damage to the waste package at the positioning and closure area satisfies ESD-09 and is also described in Attachment A and B6. These fault trees involve waste package failure due to the welding process or drop of an object on the WP.

In all cases a conservative mission time of 1 hour per canister was used for canister and waste package transfers through the process for each fault tree. The time required to lower a canister

into the waste package by the CTM is approximately 20 minutes, the time required to move the trolley from the loading area to the positioning area and then to the Waste Package Loadout Room is approximately 35 minutes, and the time required to extract the carriage from the shielded enclosure is also approximately 15 minutes (Ref. B5.1.8, Appendix A). Therefore, a one hour mission time is considered a conservative value for each fault tree.

Although the time in the Waste Package Positioning Room is approximately 40 hours, there are no WPTT failures that would damage the canister in this area.

B5.4.1 Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

B5.4.1.1 Description

This fault tree describes spurious movement of the WPTT during canister loading of the waste package to satisfy ESD-07, pivotal event “Canister Impact due to Movement of CTM, CTT, or WPTT During Lift.” The top event is “Spurious Movement of the WPTT While Loading the Waste Package with Canisters” which is defined as unplanned movement of the WPTT while canisters are being loaded into the waste package. This fault tree is shown in Figures B5.4-3, B5.4-4, B5.4-5 and B5.4-6.

Spurious movement may involve movement of the trolley or the shielded enclosure and may be caused by multiple equipment failures, or by a combination of equipment failure and operator error. For equipment failures to cause spurious movement the controls (remote or on-board) must emit a spurious signal, and the gate interlocks must fail for trolley movement, or the gate and docking interlocks must fail for shielded enclosure movement. For the operator to initiate spurious movement, the interlocks must fail as described above for the trolley or shielded enclosure to move.

B5.4.1.2 Success Criteria

Success criteria for loading a canister onto the shielded enclosure of the WPTT at the loading area require that the WPTT remain stationary during these operations. Interlocks prevent rotational movement of the shielded enclosure unless the trolley is locked down at the docking station in the Waste Package Loadout Room, and port slide gate interlocks interrupt all power to the WPTT to prevent any movement of the trolley or shielded enclosure when the slide gate is opened.

B5.4.1.3 Design Requirements and Features

Design features include the interlock that interrupts all power to the WPTT when it is in the loading room, and the slide gate interlocks that interrupt all power to the WPTT while the slide gate is open during the canister loading process. The docking interlock is another feature that prevents rotation of the shielded enclosure unless the WPTT is at the docking station in the Waste Package Loadout Room.

Requirements include sizing of the motor and gearing system such that the canister cannot be breached through a shear failure in the event of spurious signals during canister transfer into the

waste package. Either the drive train or rotational motors must trip before the canister is breached

B5.4.1.4 Fault Tree Model

The top event in Figure B5.4-3 is spurious movement of the WPTT during the canister loading process. This may occur due to initiation of a spurious signal due to equipment failure or operator error coupled with the failure of an interlock that interrupts all power to the WPTT while the WPTT is in the loading position. Power can be provided to the WPTT only through operator action to reset the interlock after loading is completed.

Spurious movement due to equipment failure, shown in Figures B5.4-4 and B5.4-5, may occur from initiation of spurious signals from the control system and failure of the gate and docking interlocks. Failure modes of the gate interlocks are shown in Figure B5.4-6.

B5.4.1.5 Basic Events

Basic events for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters” are shown in Table B5.4-1.

Table B5.4-1. Basic Event Probabilities for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹) ^a	Miss. Time (hr) ^a
51A-WPTT-IME001--IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-WPTT-ZS000---ZS--CCF	C	1.380E-005	—	—	—
51A-WPTT-ZS001---ZS--FOD	1	2.930E-004	2.930E-004	—	—
51A-WPTT--ZS002--ZS--FOD	1	2.930E-004	2.930E-004	—	—
51A-OPTILTDOWN01-HFI-NOD	1	1.000E+000	1.000E+000	—	—
51A-PWRPRTGATINT-IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-WPTT--HC001--HC--SPO	3	5.230E-007	—	5.230E-007	1
51A-WPTT-HC002-HC-SPO	3	5.230E-007	—	5.230E-007	1
51A-WPTT-IELDK3--IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-WPTT-PLC001-PLC-SPO	3	3.650E-007	—	3.650E-007	1
51A-WPTT-PLC002-PLC-SPO	3	3.650E-007	—	3.650E-007	1
51A-OPWPTTSPUR01-HFI-NOD	1	1.000E-003	1.000E-003	—	—

NOTE: ^aFor Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B5.4.1.5.1 Human Failure Events

Two operator errors involve initiation of spurious movement of the trolley 51A-OPWPTTSPUR01-HFI-NOD or shielded enclosure 51A-OPTILTDOWN01-HFI-NOD which involves initiation of a tiltdown.

B5.4.1.5.2 Common-Cause Failure

One common-cause failure (CCF) was added to the tree to account for failure of both gate closed limit switches. An alpha factor of 0.047 was used to determine the common-cause value using two of two as the failure criterion (Section C3).

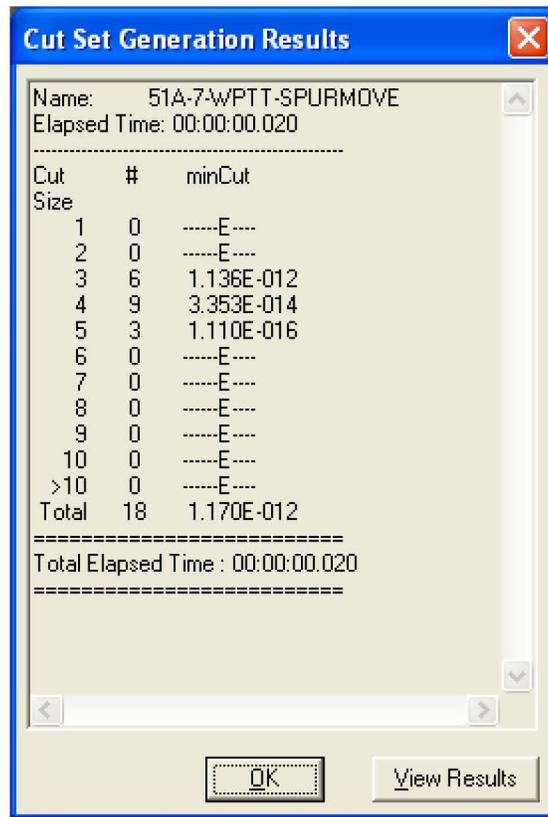
B5.4.1.6 Uncertainty and Cut Set Generation

Figure B5.4-1 contains the uncertainty results obtained from running the fault trees for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters.” Figure B5.4-2 provides the cut set generation results for “Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters”.



Source: Original

Figure B5.4-1. Uncertainty Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters



Source: Original

Figure B5.4-2. Cut Set Generation Results for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

B5.4.1.7 Cut Sets

Table B5.4-2 contains the cut sets for spurious movement of the WPTT during canister loading. The total probability per cask loading is 1.169E -12.

Table B5.4-2. Cut Sets for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
51A-7-WPTT-SPURMOVE	64.66	7.563E-013	51A-OPWPTTSPUR01-HFI-NOD	Operator Initiates Spurious Movement of Trolley	1.0E-003
			51A-PWRPRTGATINT-IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005
			51A-WPTT-IME001--IEL-FOD	Interlock Failure on Demand	2.8E-005
	32.38	3.787E-013	51A-OPWPTTSPUR01-HFI-NOD	Operator Initiates Spurious Movement of Trolley	1.0E-003

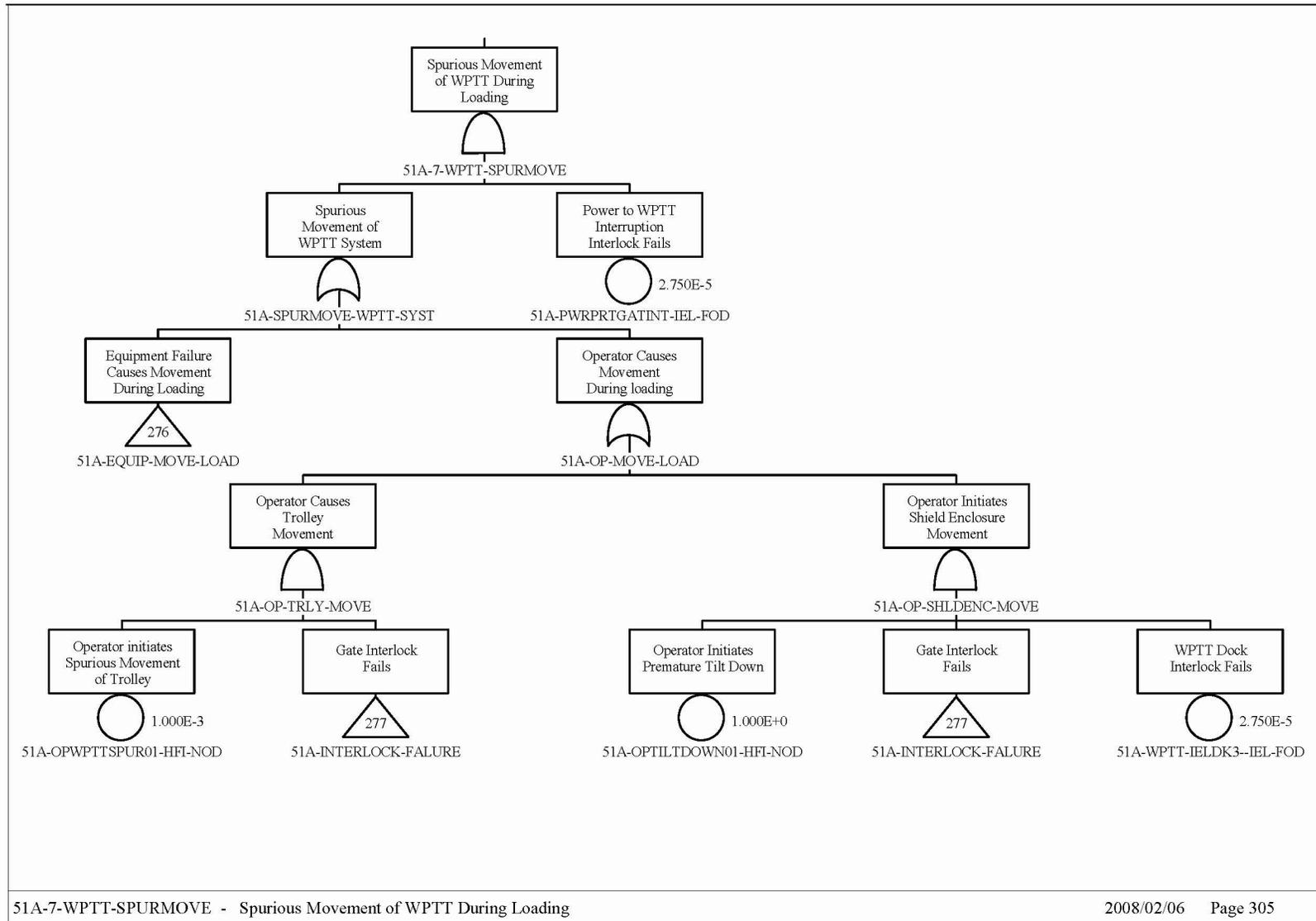
Table B5.4-2. Cut Sets for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability	
(continued)	(continued)	(continued)	51A-PWRPRTGATINT- IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005	
			51A-WPTT-ZS000---ZS- -CCF	CCF of Gate Closed Limit Switches	1.4E-005	
	1.78	2.080E-014	51A-OPTILTDOWN01- HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000	
			51A-PWRPRTGATINT- IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005	
			51A-WPTT-IELDK3-- IEL-FOD	WPTT Dock Interlock Fails	2.8E-005	
			51A-WPTT-IME001-- IEL-FOD	Interlock Failure on Demand	2.8E-005	
	0.89	1.041E-014	51A-OPTILTDOWN01- HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000	
			51A-PWRPRTGATINT- IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005	
			51A-WPTT-IELDK3-- IEL-FOD	WPTT Dock Interlock Fails	2.8E-005	
			51A-WPTT-ZS000---ZS- -CCF	CCF of Gate Closed Limit Switches	1.4E-005	
	0.20	2.361E-015	51A-OPWPTTSPUR01- HFI-NOD	Operator initiates Spurious Movement of Trolley	1.0E-003	
			51A-PWRPRTGATINT- IEL-FOD	Power to WPTT Interruption Interlock Fails	2.8E-005	
			51A-WPTT--ZS002--ZS- -FOD	Gate Closed Limit Switch #2 Spurious Transfer	2.9E-004	
			51A-WPTT-ZS001---ZS- -FOD	Gate Closed Limit Switch #1 Spurious Transfer	2.9E-004	
	1.169E-012 = Total					

NOTE: CCF = common-cause failure; Freq. = frequency; Prob. = probability; WPTT = waste package transfer trolley.

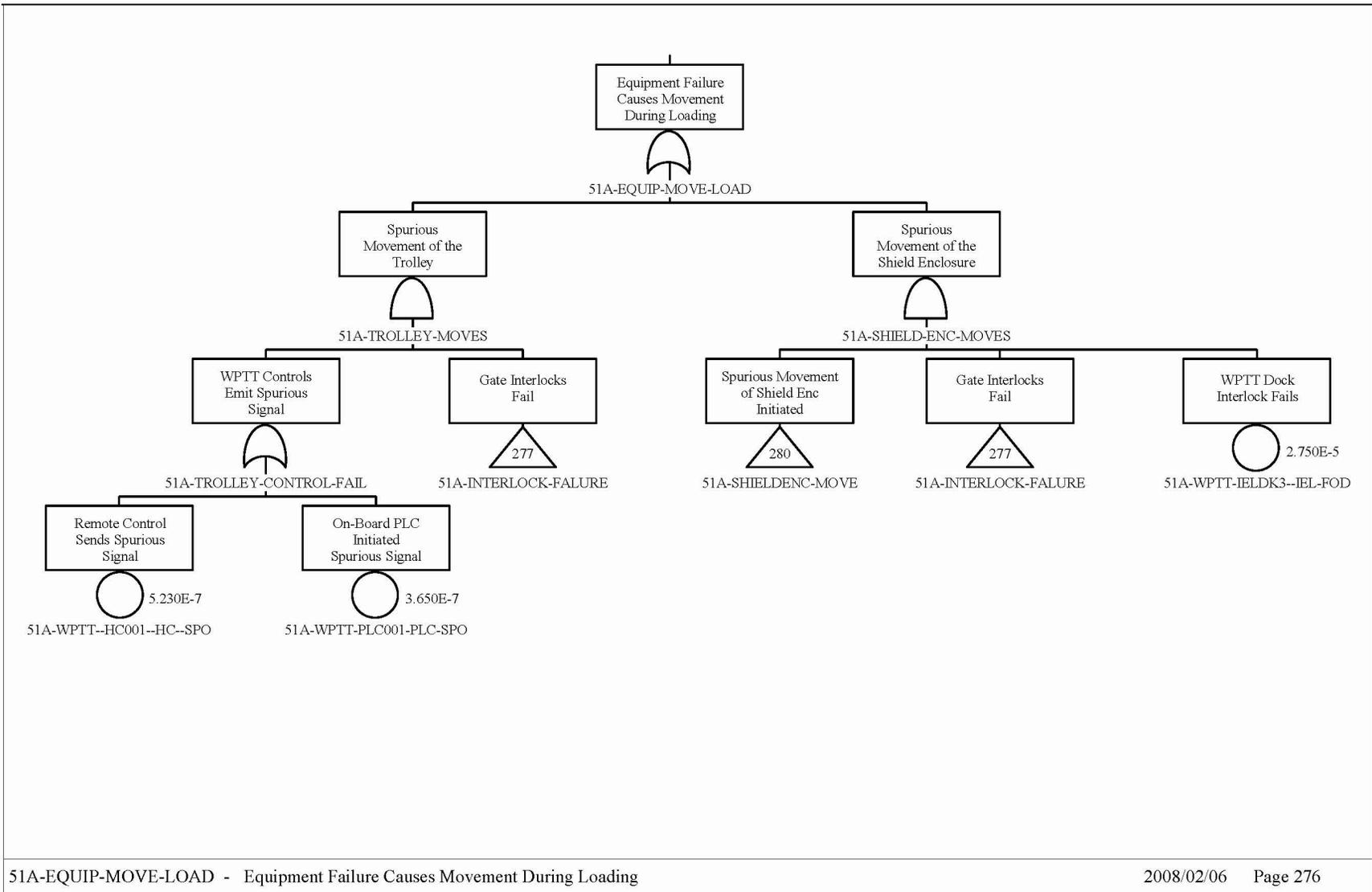
Source: Original

B5.4.1.8 Fault Tree



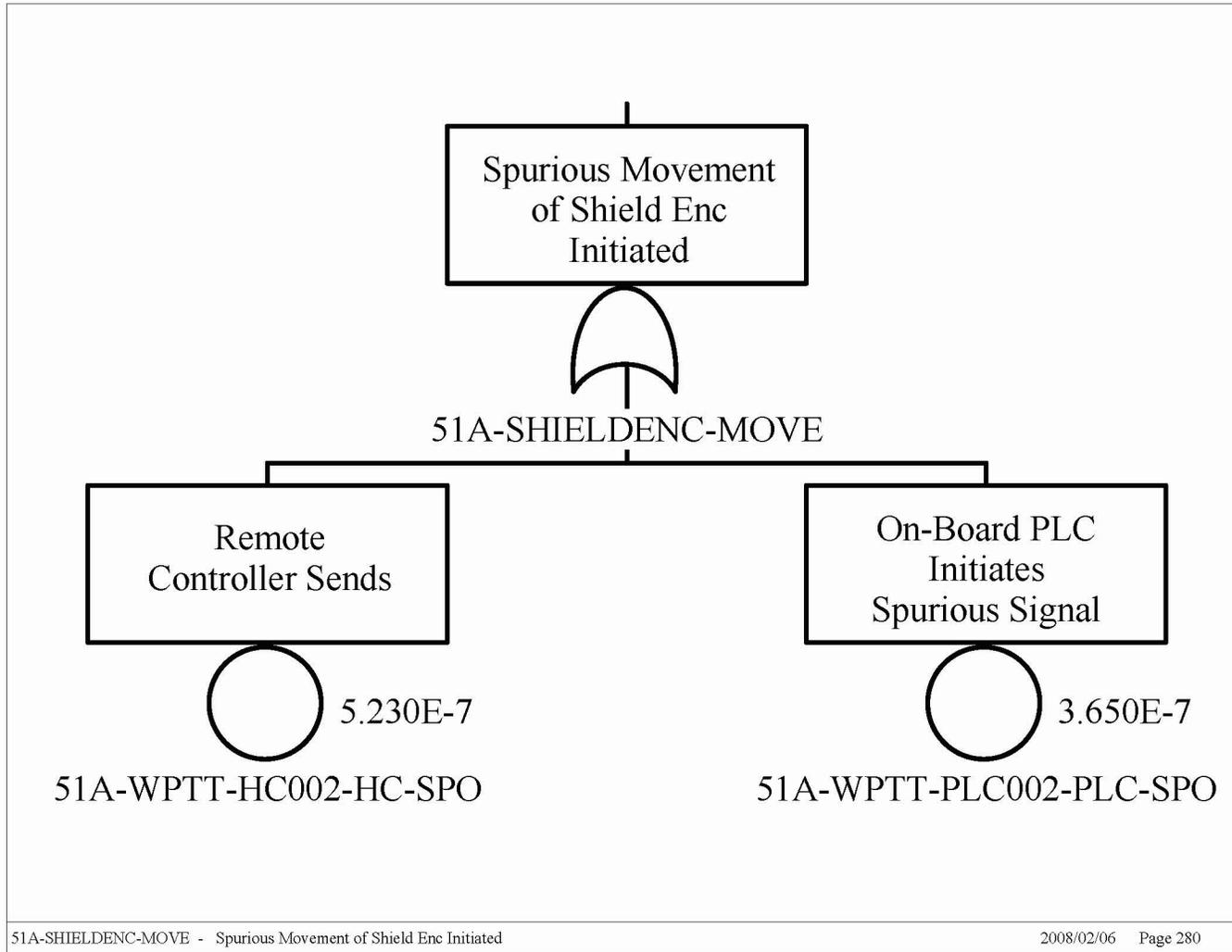
Source: Original

Figure B5.4-3. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters



Source: Original

Figure B5.4-4. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued)

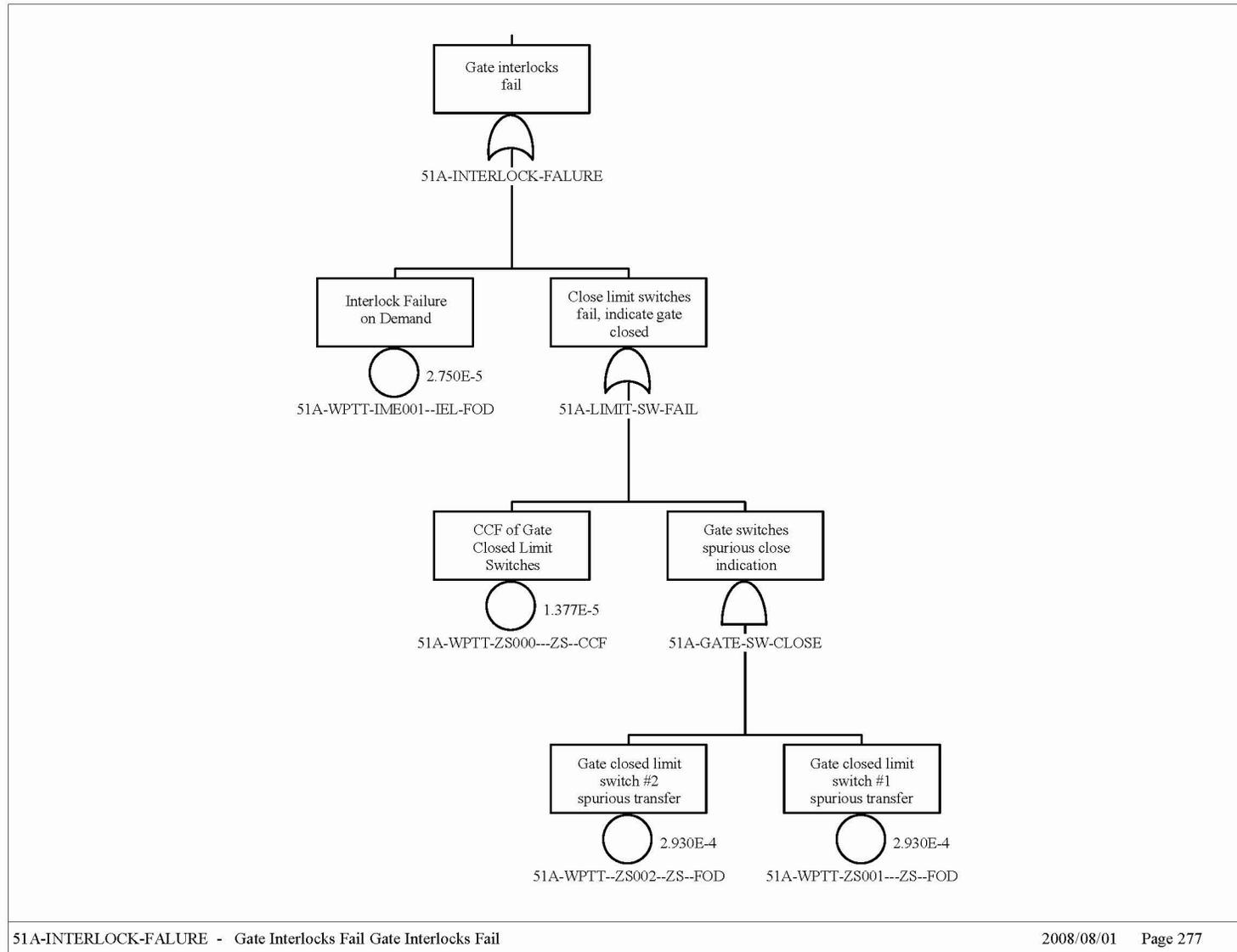


B5-19

Source: Original

Figure B5.4-5. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued)

November 2008



Source: Original

Figure B5.4-6. Fault Tree for Spurious Movement of the WPTT in the Loading Area While Loading the Waste Package with Canisters (Continued)

B5.4.2 Impact of the WPTT with a Structure

B5.4.2.1 Description

This fault tree considers the potential for the WPTT to collide with a structure or object while moving the waste package from the loading area to the positioning area to satisfy ESD-08 pivotal event “Collision of WPTT with facility structure or equipment.” The top event is “WPTT Collides Trip Loading Rm to Positioning RM.” This fault tree is shown in Figures B5.4-9 and B5.4-10.

The fault tree is more general than the name of the top event implies. The same fault tree considers the potential for the WPTT to collide into a structure or object while moving the waste package from the Waste Package Positioning Room to the docking station to satisfy ESD-10, pivotal event “WPTT Collision.”

Two primary causes of a collision are operator initiated (possibly through inattention) or failure of the WPTT to stop. Movement in the wrong direction as a contributing factor is negated by the use of rails forcing the WPTT to only move forward and backward. A runaway condition is prevented by the sizing of the electrical motor and drive gears to limit the speed to less than 40 ft/min.

Failure to stop requires failure of the brake or failure of the motor to shut off. The emergency stop buttons in the control room must also fail; however, because these are recovery actions to be taken by the operator the emergency stop functions are not credited in the fault tree.

B5.4.2.2 Success Criteria

Success criteria for moving the WPTT with a waste package from the loading area to the Waste Package Positioning Room and then to the Waste Package Loadout Room requires the WPTT travel at a speed no greater than 40 ft/min and the operator be in control and able to stop the WPTT as required. The WPTT is stopped to prevent a collision into a closed shield door or other object by the operator speed controls in the control room, or by the emergency stop buttons in the control room that remove power to the WPTT. When moving the waste package between the loading area and the Waste Package Loadout Room, movement in the wrong direction is prevented by the rails on which the WPTT travels. This forces the WPTT to move only in a straight line forward and backward between the two areas. Runaway of the WPTT is prevented by the limited motor power and gear drive system such that the maximum speed allowable is less than 40 ft/min.

B5.4.2.3 Design Requirements and Features

The design feature is the size of the motor that limits the speed of the WPTT to 40 ft/min. The requirement is that the speed of the WPTT does not exceed 40 ft/min.

B5.4.2.4 Fault Tree Model

The fault tree is shown in Figures B5.4-9 and B5.4-10. The top event is “WPTT Collides Trip Loading Rm to Positioning RM” and may be caused by operator error of failure to stop. Failure to stop may be caused by equipment failure shown in Figure B5.4-10.

B5.4.2.5 Basic Event Data

Table B5.4-3 contains a list of basic events used in the fault tree for an impact of the WPTT with a structure while moving the waste package from the loading area to the loadout room.

Table B5.4-3. Basic Event Probabilities for Impact of the WPTT with a Structure

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹) ^a	Miss. Time (hr) ^a
51A-WPTT-BRK401--BRK-FOD	1	1.460E-006	1.460E-006	—	—
51A-WPTT-MOE001-MOE-FSO	3	1.350E-008	—	1.350E-008	1
51A-OPWPCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	—	—

NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B5.4.2.5.1 Human Failure Events

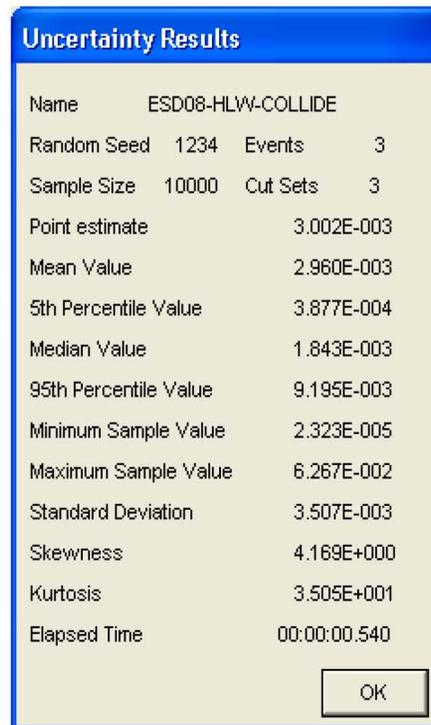
One operator error (51A-OPWPCOLLIDE1-HFI-NOD) involves causing a collision of the WPTT.

B5.4.2.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

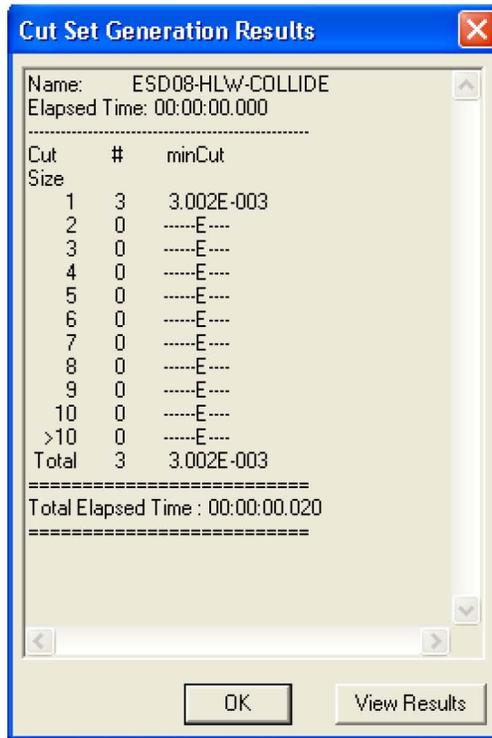
B5.4.2.6 Uncertainty and Cut Set Generation

Figure B5.4-7 contains the uncertainty results for impact of the WPTT with a structure. Figure B5.4-8 provides the cut set generation results for impact of the WPTT with a structure during movement.



Source: Original

Figure B5.4-7. Uncertainty Results for Impact of the WPTT with a Structure Fault Tree



Source: Original

Figure B5.4-8. Cut Set Generation Results for Impact of the WPTT with a Structure Fault Tree

B5.4.2.7 Cut Sets

Table B5.4-4 contains the cut sets for impact of the WPTT with a structure during waste package transfer. The total probability per cask is 3.002E-003 with operator error the dominant cause of collision.

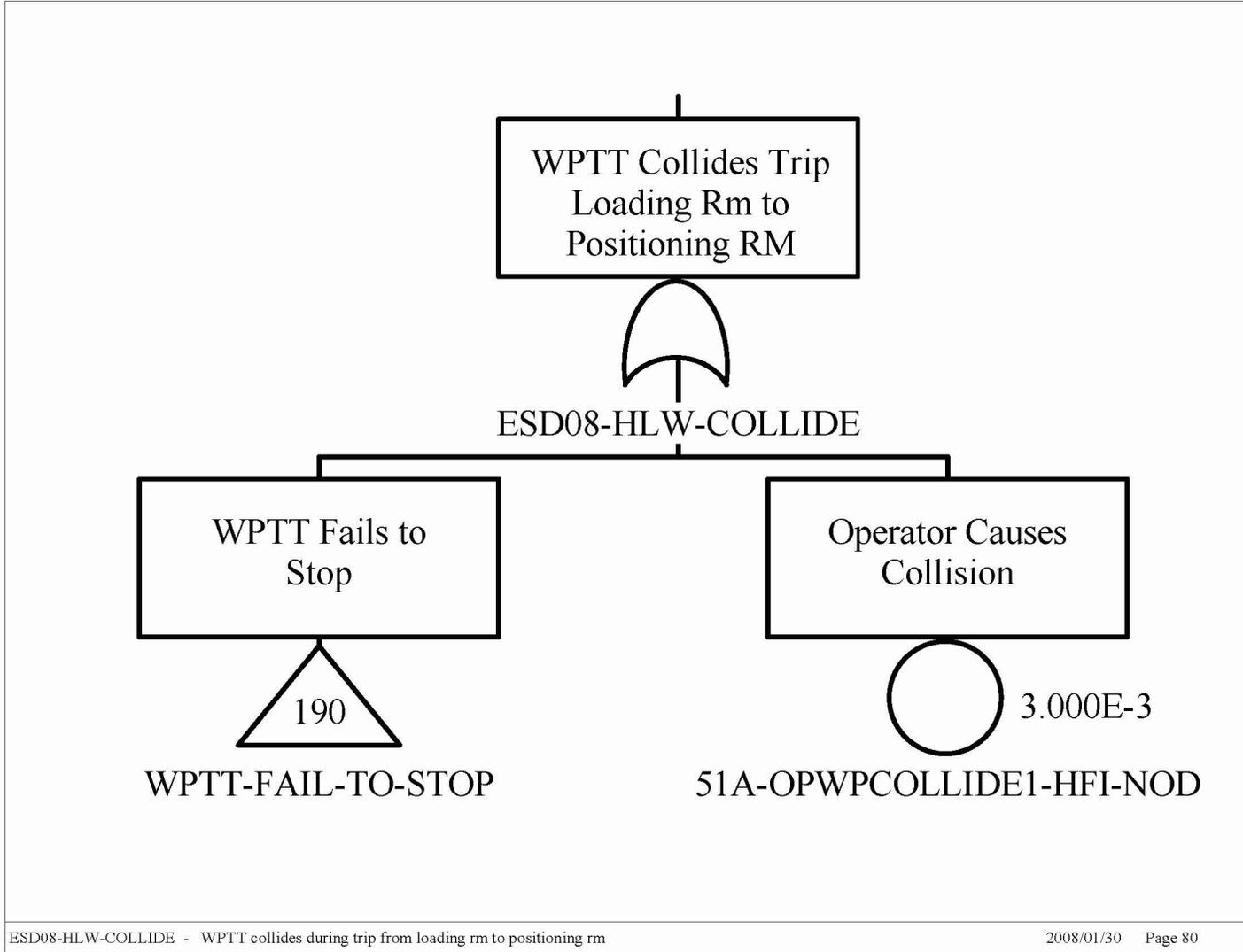
Table B5.4-4. Cut Sets for Impact of the WPTT with a Structure

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW-COLLIDE	99.95	3.000E-003	51A-OPWPCOLLIDE1-HFI-NOD	Operator Causes Collision	3.0E-003
	0.05	1.460E-006	51A-WPTT-BRK401--BRK-FOD	Brakes Fail	1.5E-006
	0.00	1.350E-008	51A-WPTT-MOE001-MOE-FSO	Motor (Electric) Fails to Shut Off	1.4E-008
3.001E-003 = Total					

NOTE: Freq. = frequency; Prob. = probability.

Source: Original

B5.4.2.8 Fault Tree

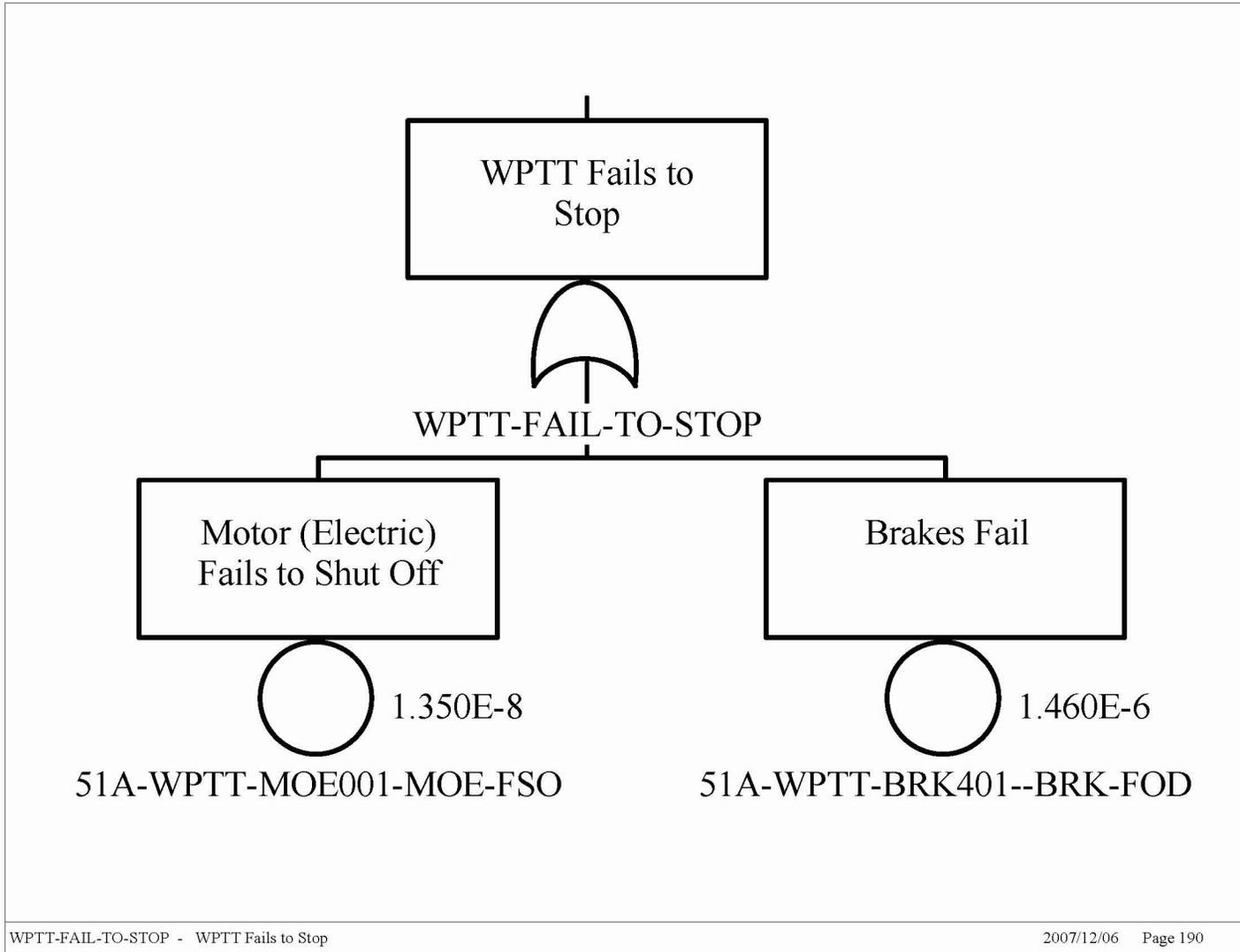


B5-25

November 2008

Source: Original

Figure B5.4-9. Fault Tree for Impact of the WPTT with a Structure



Source: Original

Figure B5.4-10. Fault Tree for Impact of the WPTT into a Structure during Waste Package Transfer (Continued)

B5.4.3 Derailment of the Waste Package Transfer Trolley

B5.4.3.1 Description

This fault tree considers the potential for the WPTT to derail during movement from loading area to the Waste Package Positioning Room (ESD-08) and during movement from the Waste Package Positioning Room) to the docking station (ESD-10). For both ESDs, the pivotal event is “Derailment of WPTT.” The top event is “WPTT Derails.” This fault tree is shown in Figure B5.4-13.

The probability of derailment is based on historical data for train derailment at low speeds and is discussed in the section on data development. The probability of derailment per mile is multiplied by the number of miles the WPTT travels from the loading area to the Waste Package Loadout Room (approximately 4E-2 miles).

B5.4.3.2 Success Criteria

The success criterion is that the WPTT does not derail during the transport process.

B5.4.3.3 Design Features and Requirements

There are no design features or requirements.

B5.4.3.4 Fault Tree Model

The fault tree model is shown in Figure B5.4-13 with “WPTT Derails” as the top event.

B5.4.3.5 Basic Event Data

Table B5.4-5 contains a list of basic events used in the “Derailment of the WPTT” fault tree.

Table B5.4-5. Basic Event Probabilities for Derailment of the WPTT During Waste Package Transfer

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹) ^a	Miss. Time (hr) ^a
51A-WPTT-DERAIL-DER-FOM	3	1.180E-005	—	1.180E-005	1
51A-WPTT-MILES-IN-IHF	V	4.000E-002	4.000E-002	—	—

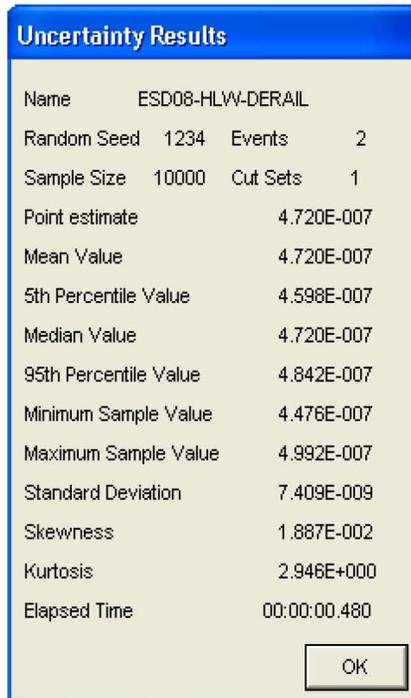
NOTE: ^a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. Calculation Type V (for “value”) indicates direct numerical entry, where the number is not necessarily a probability and is therefore allowed to be greater than 1. In this case the value is the number of miles travelled by the SPM in the IHF. See Table 6.3-1 for definitions of other calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability; V = value.

Source: Original

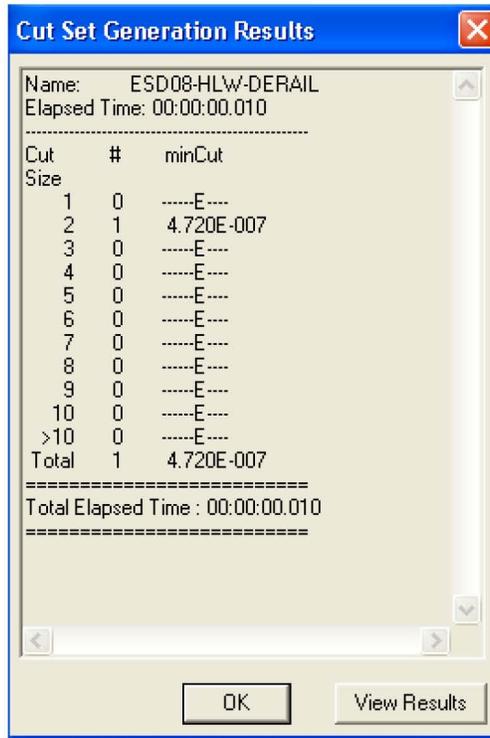
B5.4.3.6 Uncertainty and Cut Set Generation

Figure B5.4-11 contains the uncertainty results for “Derailment of the WPTT.” Figure B5.4-12 provides the cut set generation results obtained from running the fault trees for “Derailment of the WPTT” during waste package transfer.



Source: Original

Figure B5.4-11. Uncertainty Results for the Derailment of the WPTT Fault Tree



Source: Original

Figure B5.4-12. Cut Set Generation Results for the Derailment of the WPTT Fault Tree

B5.4.3.7 Cut Sets

Table B5.4-6 contains the cut sets for “Derailment of the WPTT” during waste package transfer. The total probability per cask is 4.720E-007.

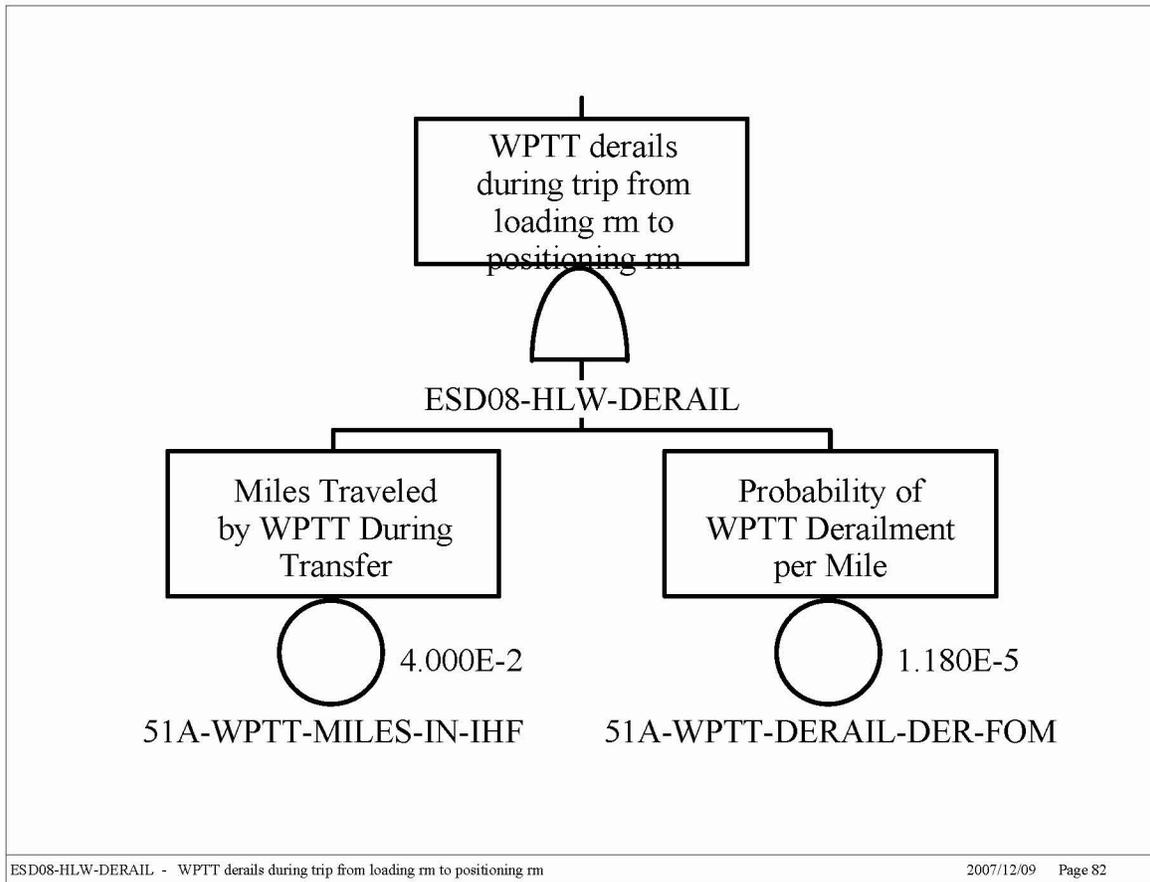
Table B5.4-6. Cut Sets for Derailment of the WPTT

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW-DERAIL	100.00	4.720E-007	51A-WPTT-DERAIL-DER-FOM	Probability of WPTT derailment per mile	1.2E-005
			51A-WPTT-MILES-IN-IHF	Miles traveled by WPTT during transfer	4.0E-002
4.720E-007 = Total					

NOTE: Freq. = frequency; Prob. Probability; WPTT = waste package transfer trolley.

Source: Original

B5.4.3.8 Fault Trees



Source: Original

Figure B5.4-13. Fault Tree for Derailment of the WPTT

B5.4.4 Premature Tilt-down of the WPTT

B5.4.4.1 Description

This fault tree considers the potential for the shielded enclosure to prematurely tilt down during movement of the WPTT from the loading area to the Waste Package Positioning Room (ESD-8) and during movement from the Waste Package Positioning Room to the docking station (ESD-10). For both ESDs, the pivotal event is “Premature Tilt-down of WPTT.” The top event is “Premature Tilt-down of WPTT.” This fault tree is shown in Figure B5.4-16.

Premature tilt-down may occur due to operator error, failure of the control system, or structural failure of the mechanical components supporting the shielded enclosure. Operator or control system initiated tilt-down must coincide with failure of the docking interlock that must engage for power to be supplied to the shielded enclosure motors. Structural failure requires failure of either the gear box or shaft on both sides of the shielded enclosure since each side is designed to

support the shielded enclosure independently. If inadvertent tiltdown does begin, the gear system on each side is designed to provide a slow tiltdown and prevent slapdown.

B5.4.4.2 Success Criteria

Premature tiltdown of the shielded enclosure is prevented during this transfer by interlocks that prevent power to the shielded enclosure motors until the WPTT is docked.

B5.4.4.3 Design Features and Requirements

The design feature is the gearing system on each side of the shielded enclosure that prevents slapdown and which can support the shielded enclosure independently. An additional design feature is the docking interlock that must be engaged for power to be provided to the shielded enclosure motors. There are no requirements.

B5.4.4.4 Fault Tree Model

The top event of the fault tree, shown in Figure B5.4-16, is premature tiltdown during movement of the WPTT from the loading area to the loadout room. Premature tiltdown may occur due to operator error or spurious signals from the control system coupled with the failure of the docking interlock.

B5.4.4.5 Basic Events

Table B5.4-7 contains a list of basic events used in the fault tree for “Premature Tiltdown of the WPTT” during waste package transfer.

Table B5.4-7. Basic Event Probabilities for Premature Tilt-down of the WPTT

Name	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda (hr ⁻¹) ^a	Miss. Time (hr) ^a
51A-WPTT-HC002---HC--SPO	3	5.230E-007	—	5.230E-007	1
51A-WPTT-PLC002--PLC-SPO	3	3.650E-007	—	3.650E-007	1
51A-WPTT-IEL001-IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-OPTILTDOWN01-HFI-NOD	1	1.000E+000	1.000E+000	—	—

NOTE: a For Calc. Type 3 with an unspecified mission time or a mission time specified as 0, SAPHIRE performs the quantification using the system mission time, 1 hr. The mission time used by SAPHIRE is listed here regardless of whether it is specified explicitly in the SAPHIRE basic event or the system mission time is used as a default. See Table 6.3-1 for definitions of calculation types.

Calc. = calculation; Fail. = failure; Miss. = mission; Prob. = probability.

Source: Original

B5.4.4.5.1 Human Failure Events

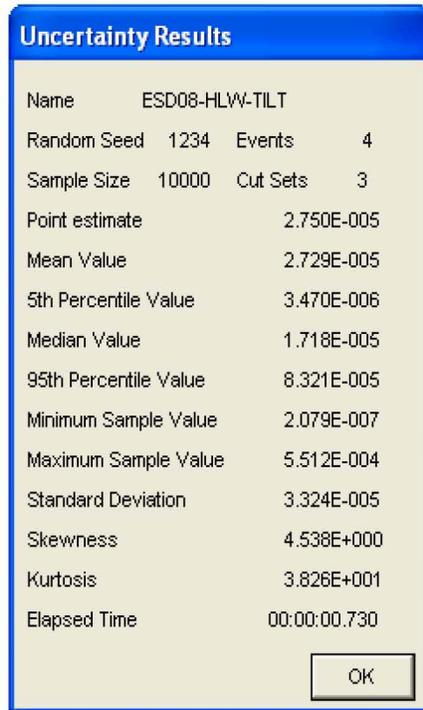
One operator error (51A-OPTILTDOWN01-HFI-NOD) involves initiation of tilt-down.

B5.4.4.5.2 Common-Cause Failures

There are no CCFs identified for this fault tree.

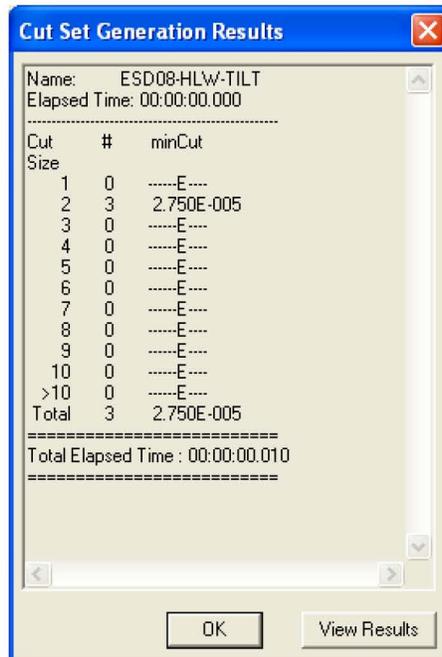
B5.4.4.6 Uncertainty and Cut Set Generation

Figure B5.4-14 contains the uncertainty results for “Premature Tilt-down of the WPTT.” Figure B5.4-15 provides the cut set generation results obtained from running the fault trees for “Premature Tilt-down of the WPTT” during waste package transfer.



Source: Original

Figure B5.4-14. Uncertainty Results for the Premature Tilt-down of the WPTT Fault Tree



Source: Original

Figure B5.4-15. Cut Set Generation Results for the Premature Tilt-down of the WPTT Fault Tree

B5.4.4.7 Cut Sets

Table B5.4-8 contains the cut sets for “Premature Tilt-down of the WPTT” during waste package transfer. The total probability per cask is 2.750E-005 with the major contributor being an operator initiation of premature tilt-down coinciding with the failure of the docking interlock.

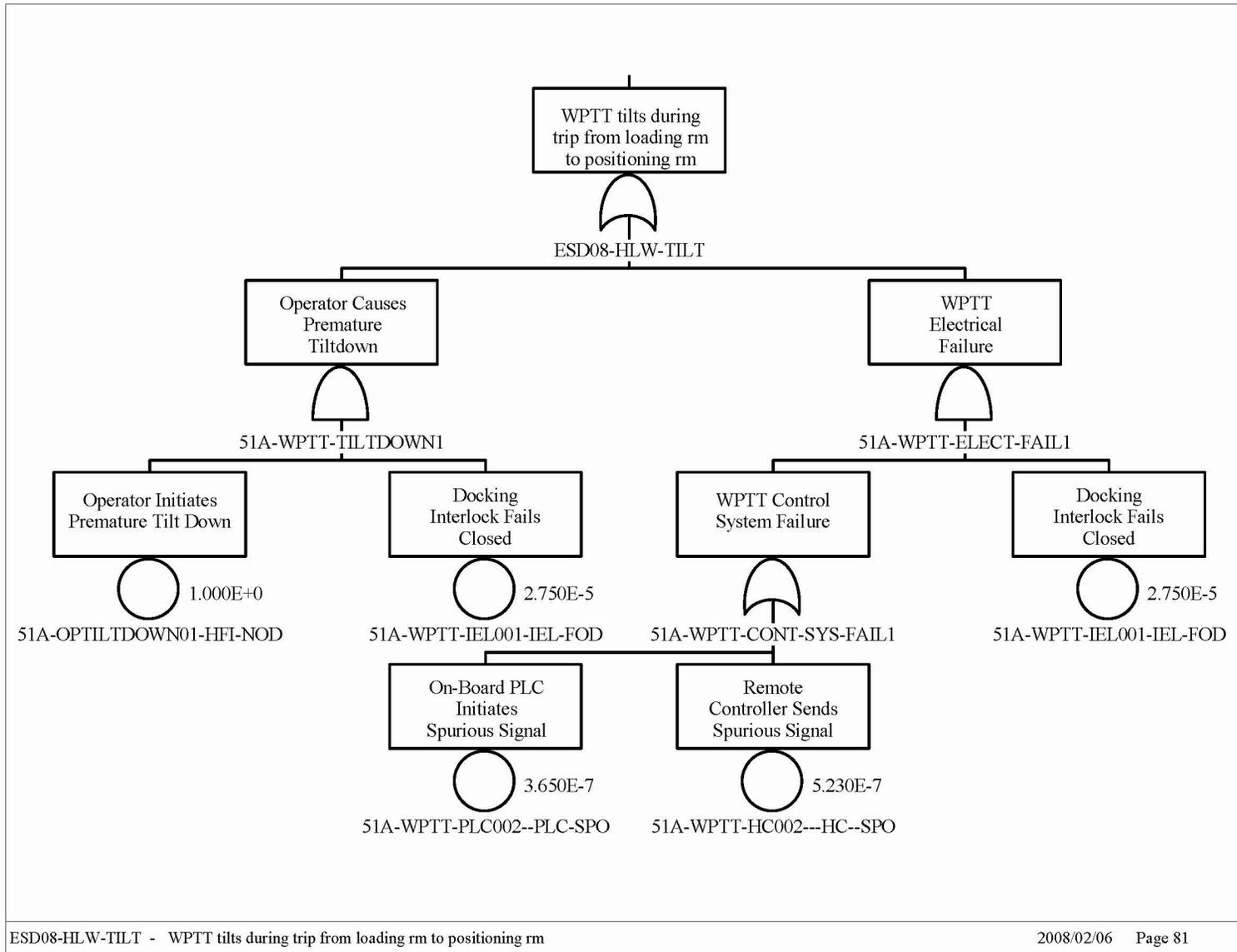
Table B5.4-8. Cut Sets for Premature Tilt-down of the WPTT

Fault Tree	Cut Set %	Prob./Freq.	Basic Event	Description	Probability
ESD08-HLW-TILT	100.00	2.750E-005	51A-OPTILTDOWN01-HFI-NOD	Operator Initiates Premature Tilt Down	1.0E+000
			51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
	0.00	1.438E-011	51A-WPTT-HC002---HC--SPO	Remote Controller Sends Spurious Signal	5.2E-007
			51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
	0.00	1.004E-011	51A-WPTT-IEL001-IEL-FOD	Docking Interlock Fails Closed	2.8E-005
			51A-WPTT-PLC002--PLC-SPO	On-Board PLC Initiates Spurious Signal	3.6E-007
2.750E-005 = Total					

NOTE: Freq. = frequency; Prob. Probability; WPTT = waste package transfer trolley.

Source: Original

B5.4.4.8 Fault Trees



B5-35

November 2008

Source: Original

Figure B5.4-16. Fault Tree for Premature Tiltdown of the WPTT

B5.4.5 Malfunction of WPTT or Waste Package Transfer Carriage

B5.4.5.1 Description

This fault tree describes unplanned movements of the WPTT or carriage leading to impacts to the waste package during extraction of the waste package from the shielded enclosure in the Waste Package Loadout Room. This fault tree satisfies ESD-11, pivotal event “Exposure due to Malfunction of WPTT or the Waste Package Transfer Carriage.” The top event is “WPTT or Carriage Malfunction During Export.” During the waste package extraction process, damage to the waste package may occur due to premature departure of the WPTT from the docking station, tilt-up of the shielded enclosure, or operator error initiating the extraction process before the TEV door is completely open and impacting the waste package with the TEV door. This fault tree is shown in Figures B5.4-19, B5.4-20 and B5.4-21.

Several mechanical or control system failures must occur for the WPTT to prematurely leave the docking station during extraction. The control system (on-board or remote systems) must initiate a spurious signal, the locking mechanism must fail, and the docking interlock between the retrieval system and the power feed to the WPTT must fail. For the shielded enclosure to tilt-up during extraction a tilt-up signal must be initiated (either through the control system or by the operator) and the motor running interlocks that close only when the waste package carriage retrieval assembly is completely extended or retracted must fail.

B5.4.5.2 Success Criteria

The success criteria are for the WPTT to remain motionless during the extraction process, and the extraction process start only after the TEV doors are completely open.

B5.4.5.3 Design Requirements and Features

The design features include the docking interlock that interrupts power to the trolley motor while the trolley is docked to prevent premature departure, and the carriage motor interlock that prevents power to the shielded enclosure motors unless the carriage retrieval assembly is completely extended or retracted. A requirement is that the extraction process is not initiated until the TEV doors are fully open.

B5.4.5.4 Fault Tree Model

The top event of the fault trees in Figure B5.4-19 is “Malfunction of WPTT or Waste Package Transfer Carriage” during export of the waste package from the shielded enclosure. This may occur due to premature departure of the WPTT from the docking station, premature tiltup of the shielded enclosure during extraction or premature extraction of the waste package before the TEV doors are open due to operator error.

Premature departure (Figure B5.4-20) may occur due to spurious signals from the control system couples with failure of the docking interlock and the mechanical locking mechanism at the docking station. Premature tiltup (Figure B5.4-21) may occur due to spurious signals from the control system or operator initiation of tiltup couples with failure of the carriage motor interlock.