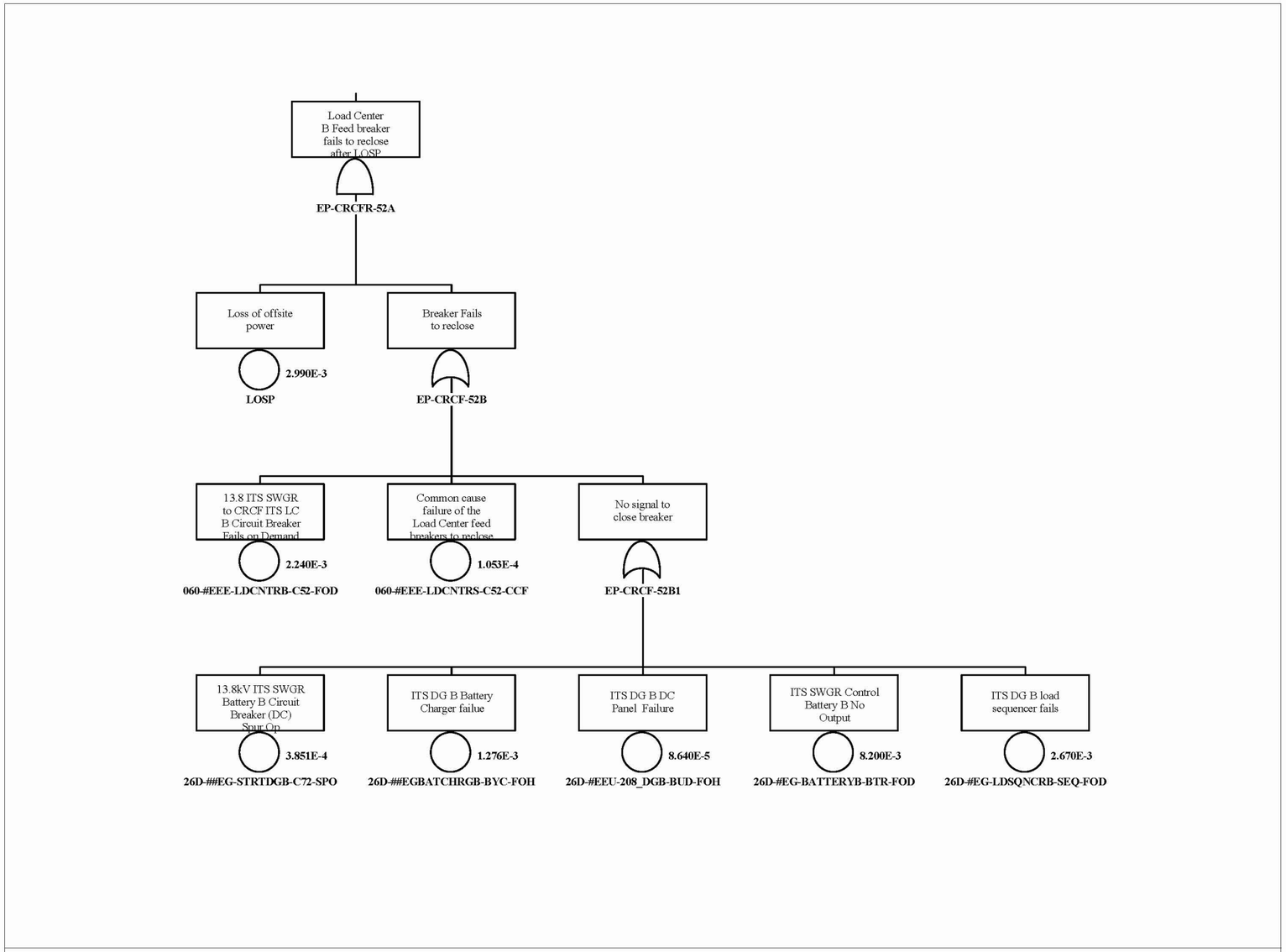
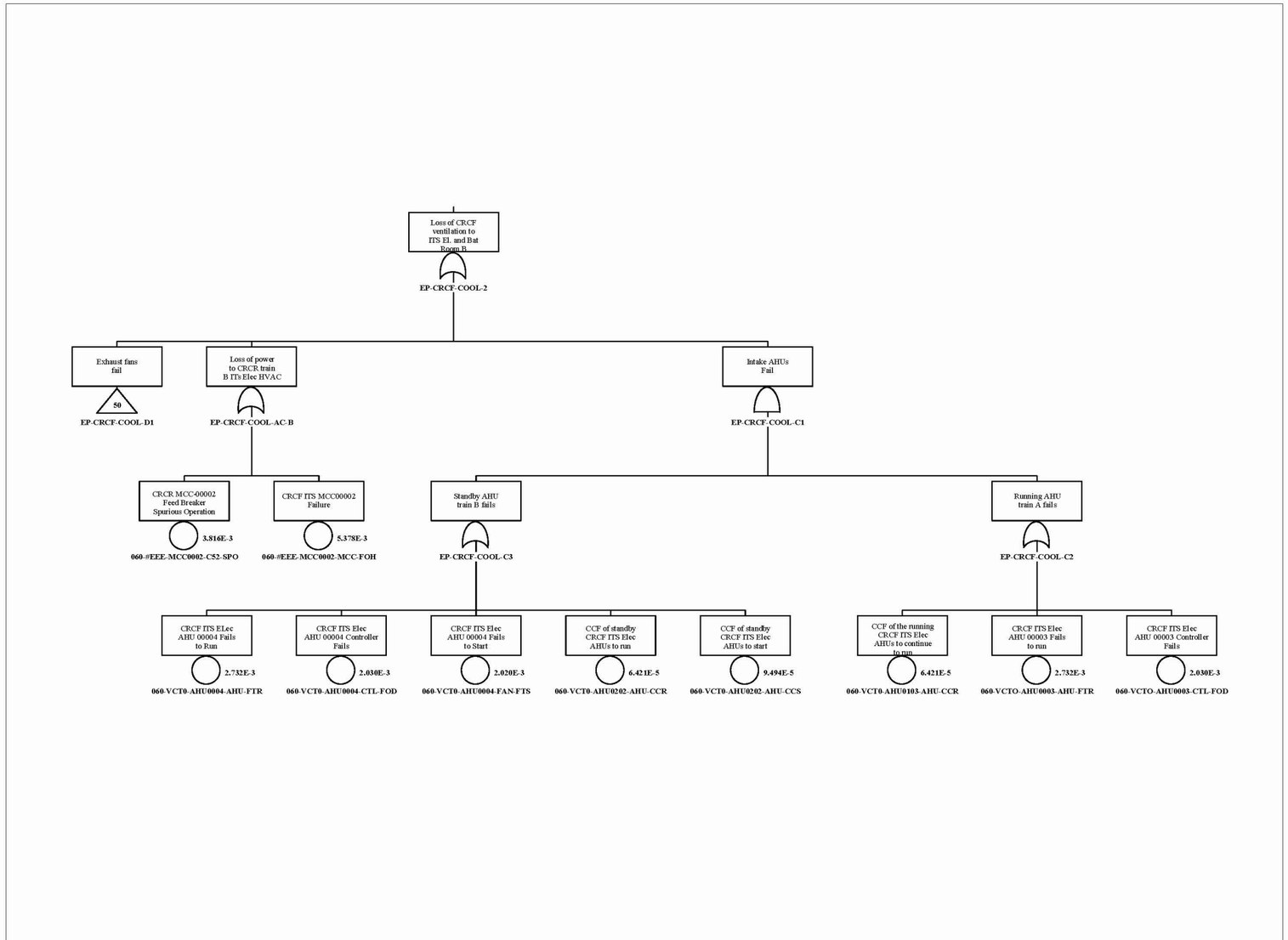


Source: Original

Figure B3.4-18. Loss of Power to CRCF ITS Load Center Train B (2 of 12)

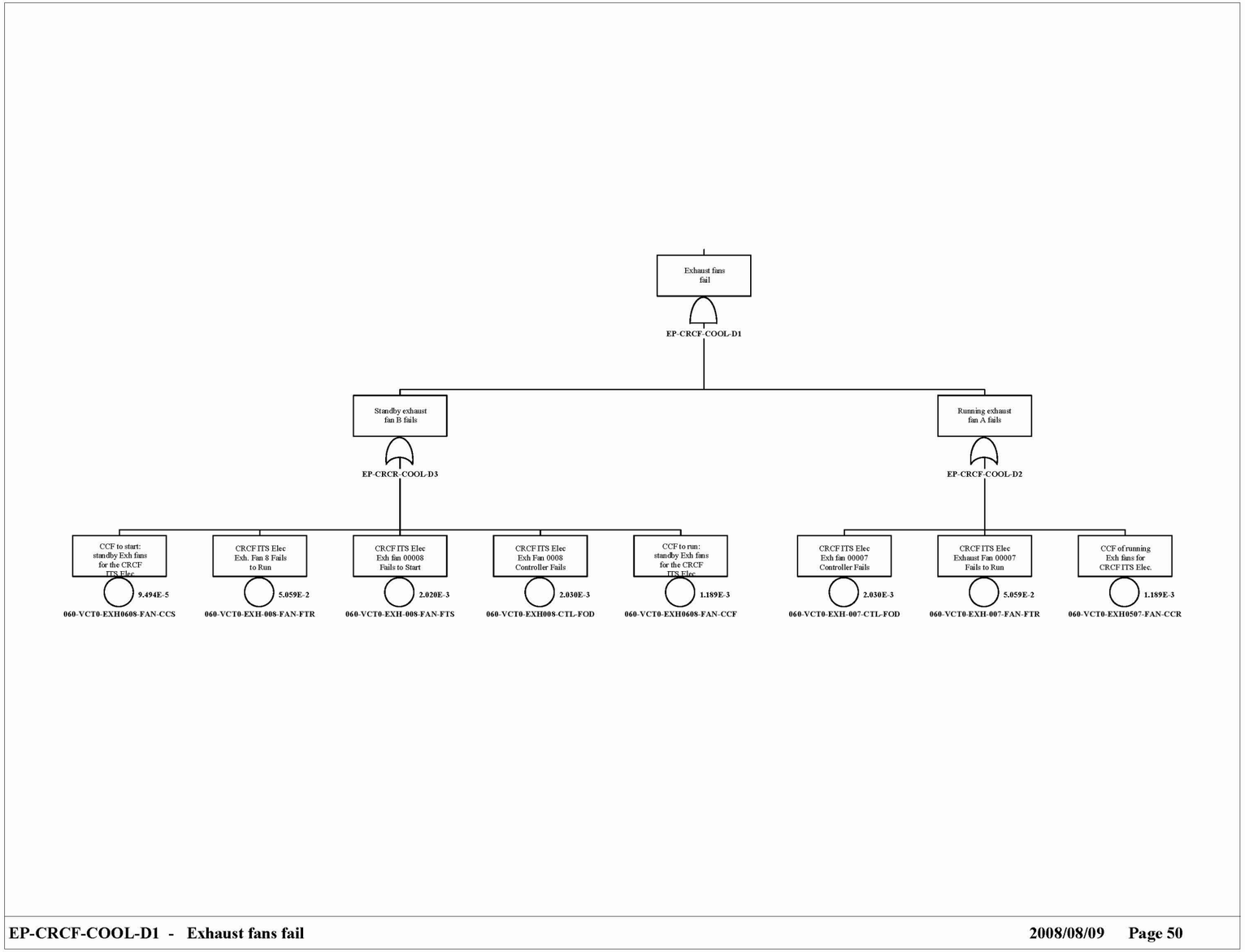
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-19. Loss of Power to CRCF ITS Load Center Train B (3 of 12)

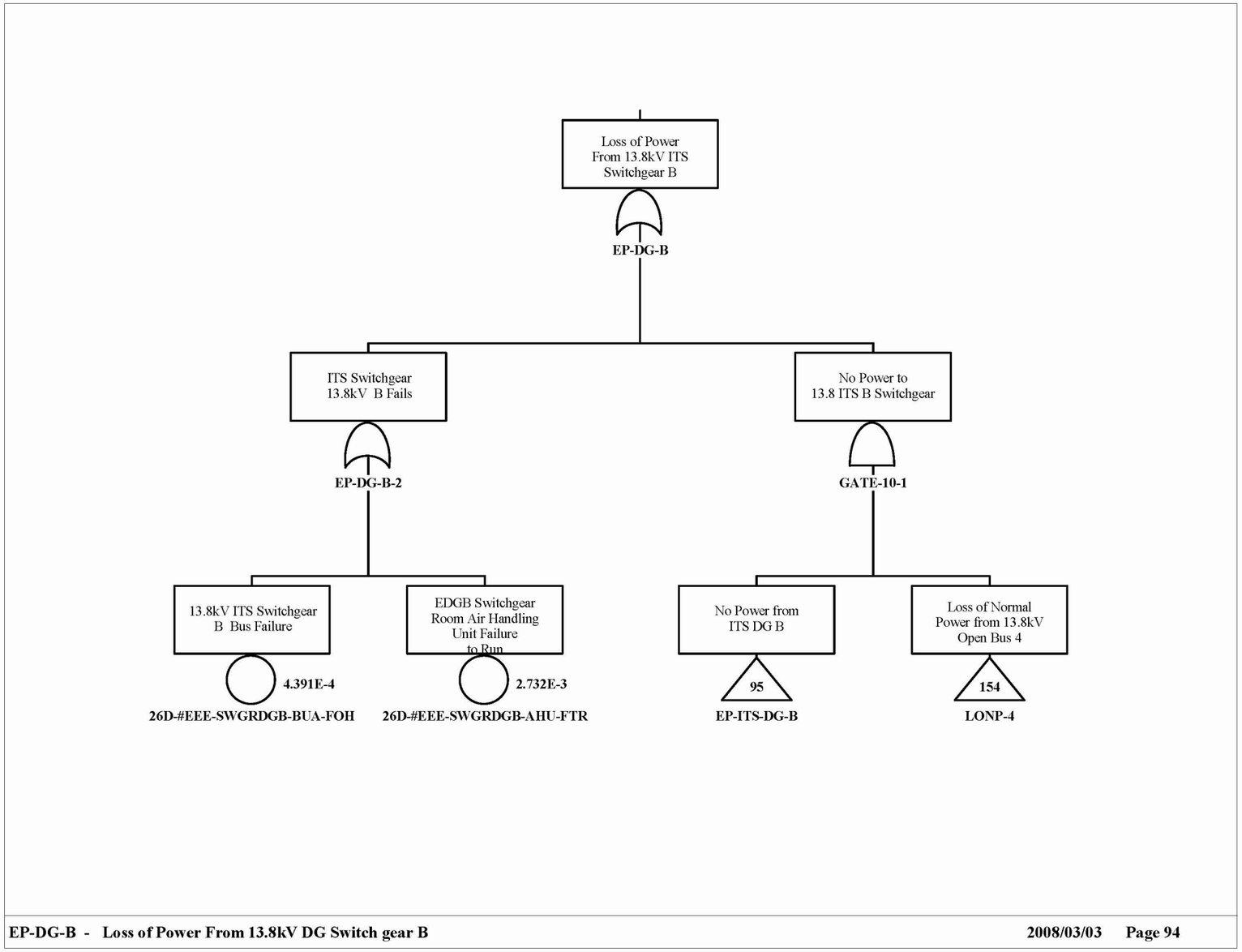
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-20. Loss of Power to CRCF ITS Load Center Train B (4 of 12)

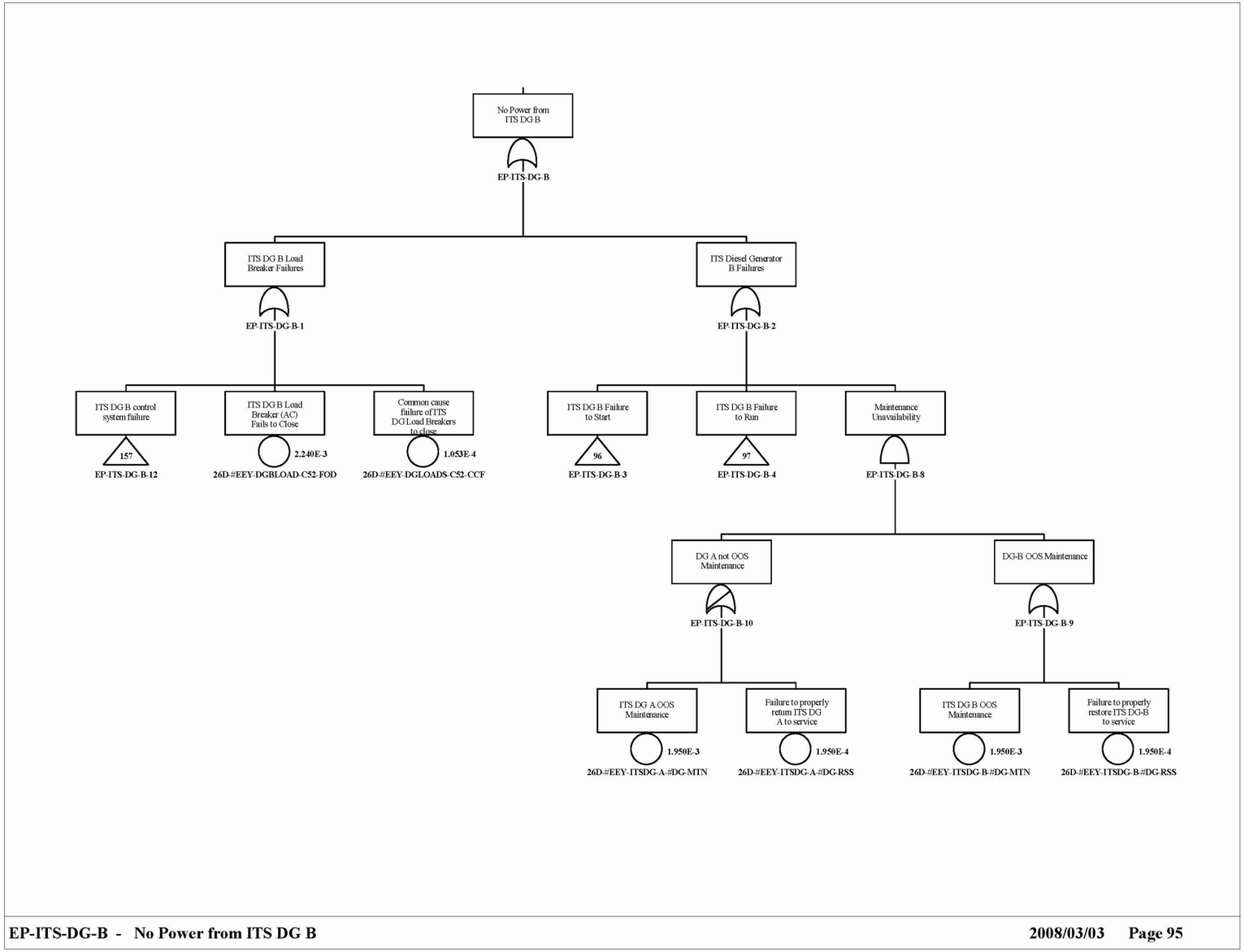
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-21. Loss of AC Power to CRCF ITS Load Center Train B (5 of 12)

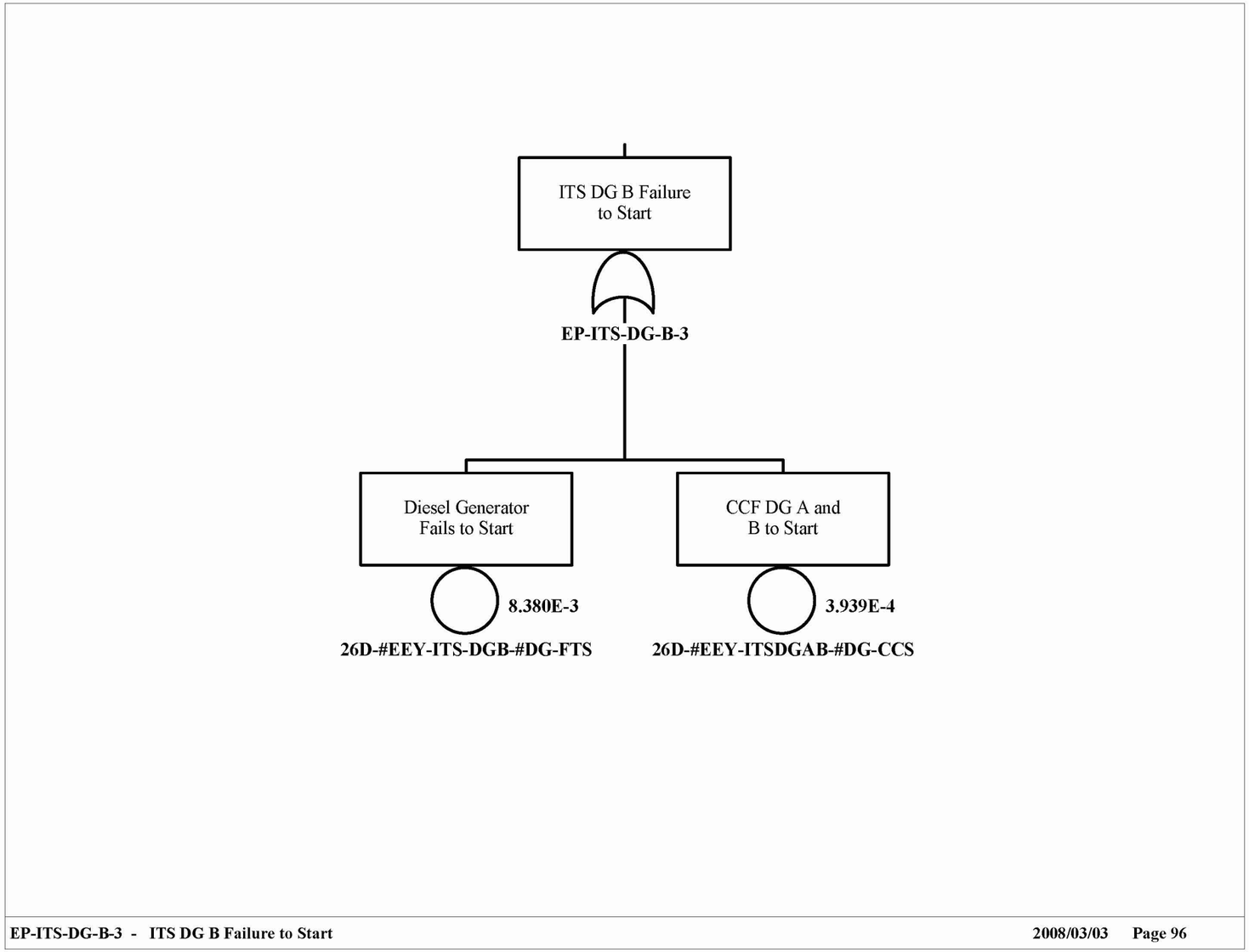
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-22. Loss of AC Power to CRCF ITS Load Center Train B (6 of 12)

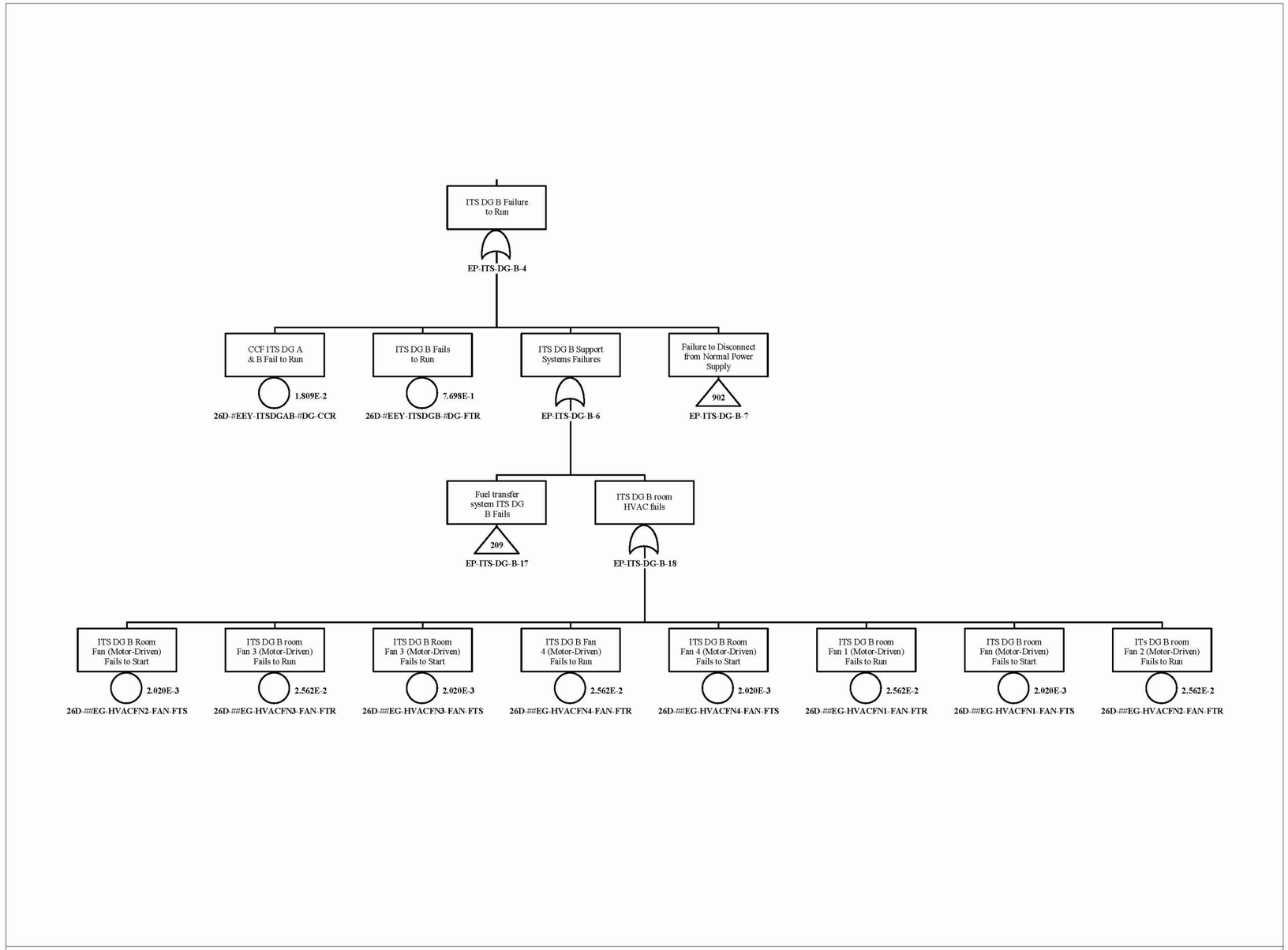
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-23. Loss of AC Power to CRCF ITS Load Center Train B (7 of 12)

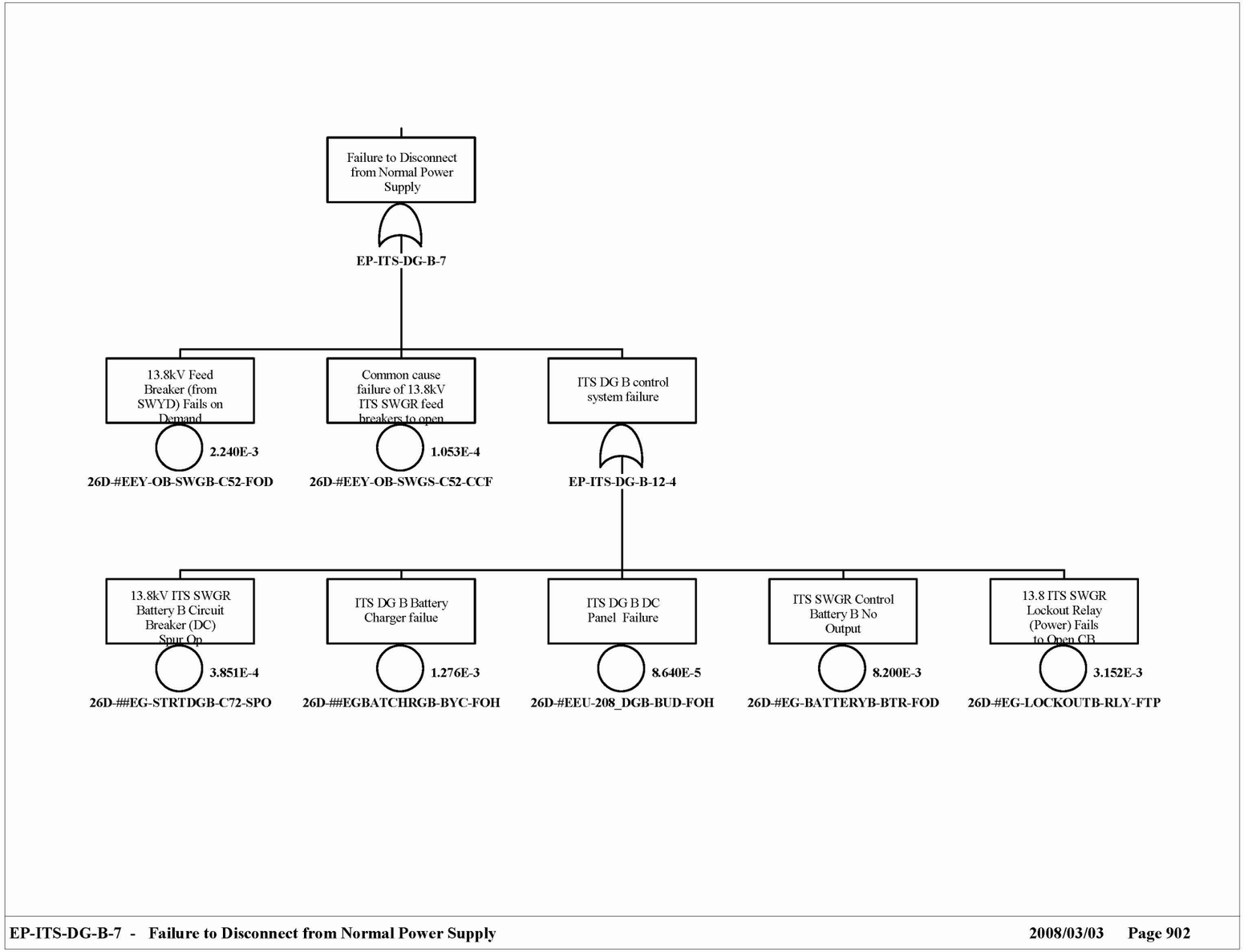
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-24. Loss of AC Power to CRCF ITS Load Center Train B (8 of 12)

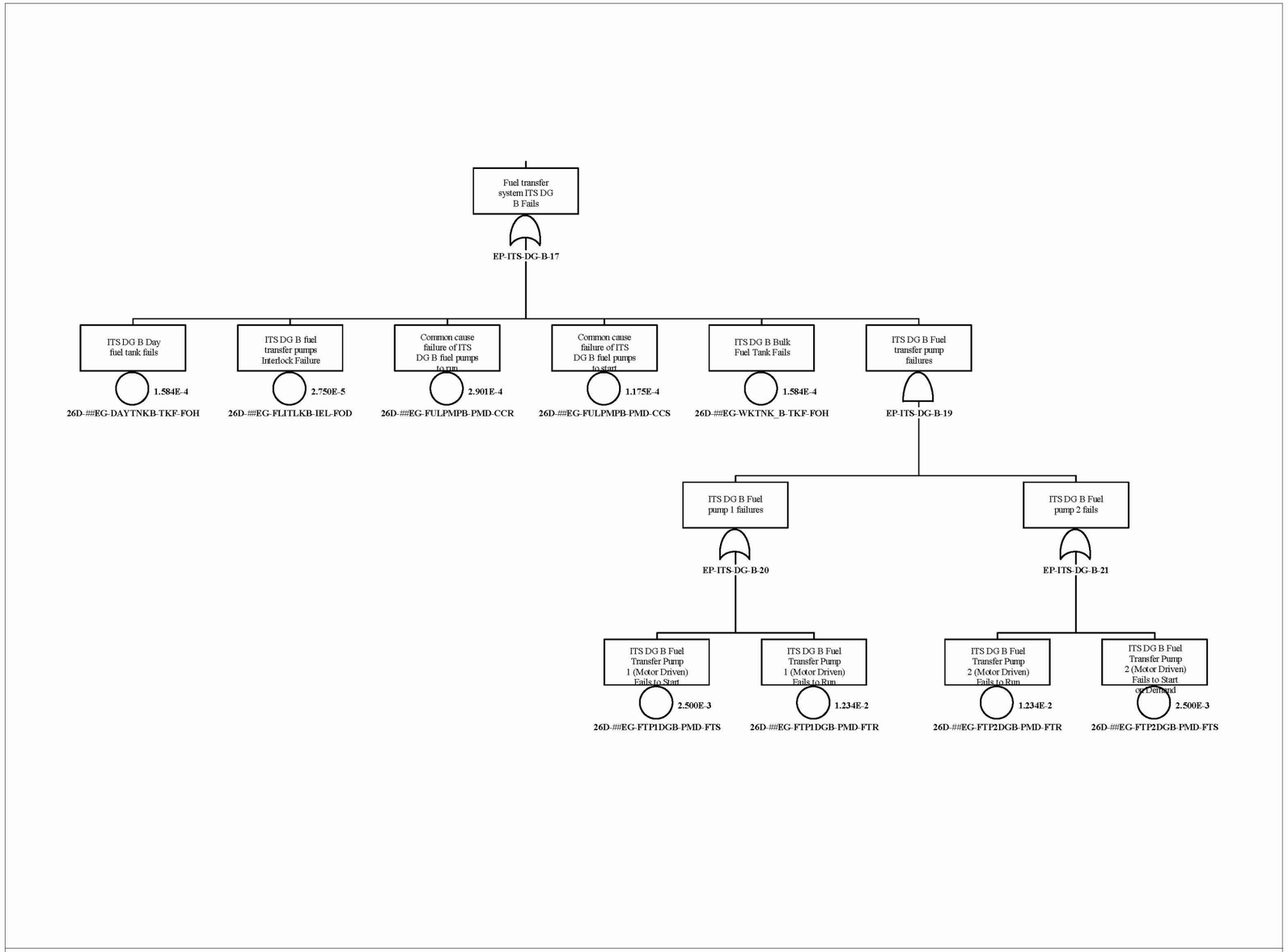
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-25. Loss of AC Power to CRCF ITS Load Center Train B (9 of 12)

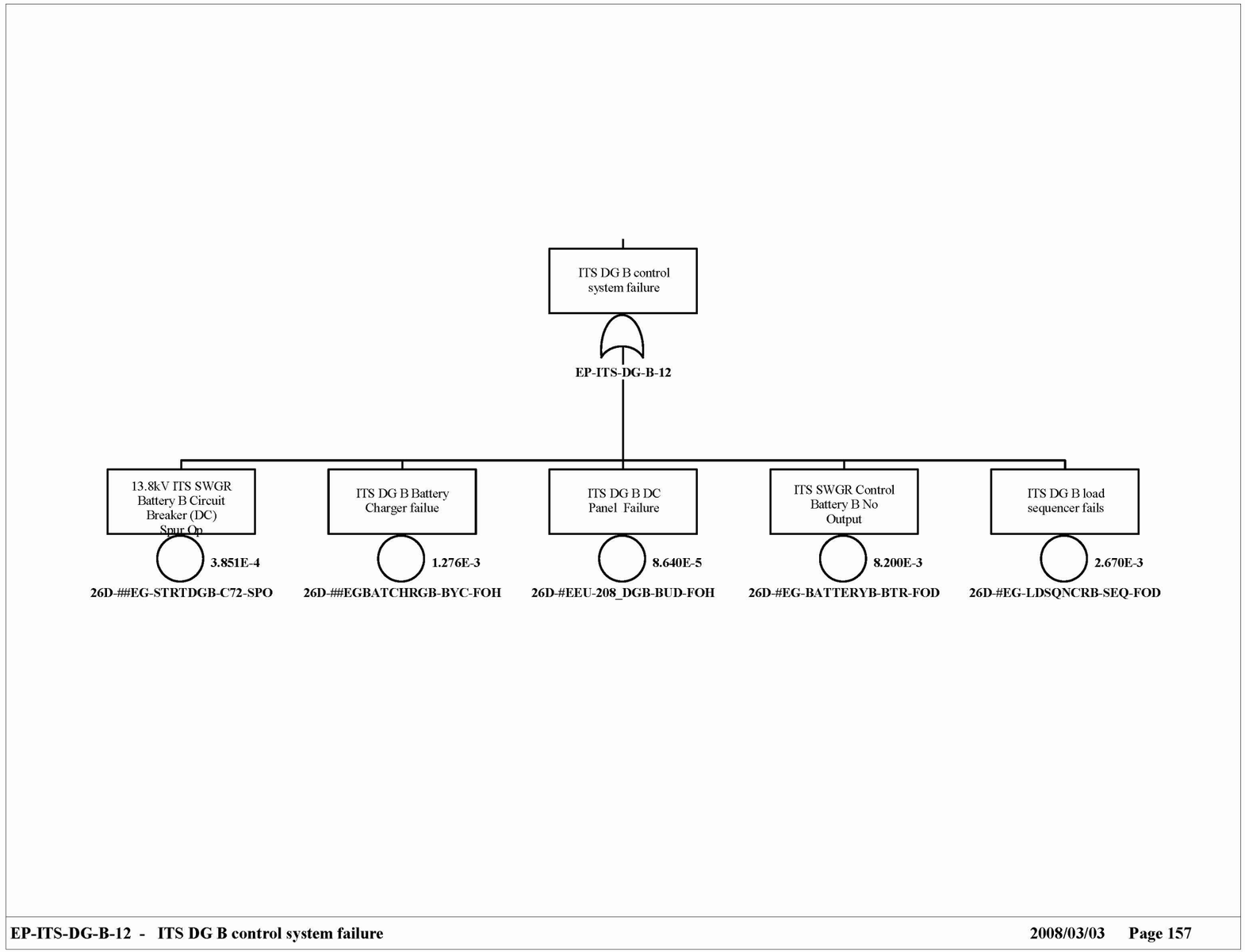
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-26. Loss of AC Power to CRCF ITS Load Center Train B (10 of 12)

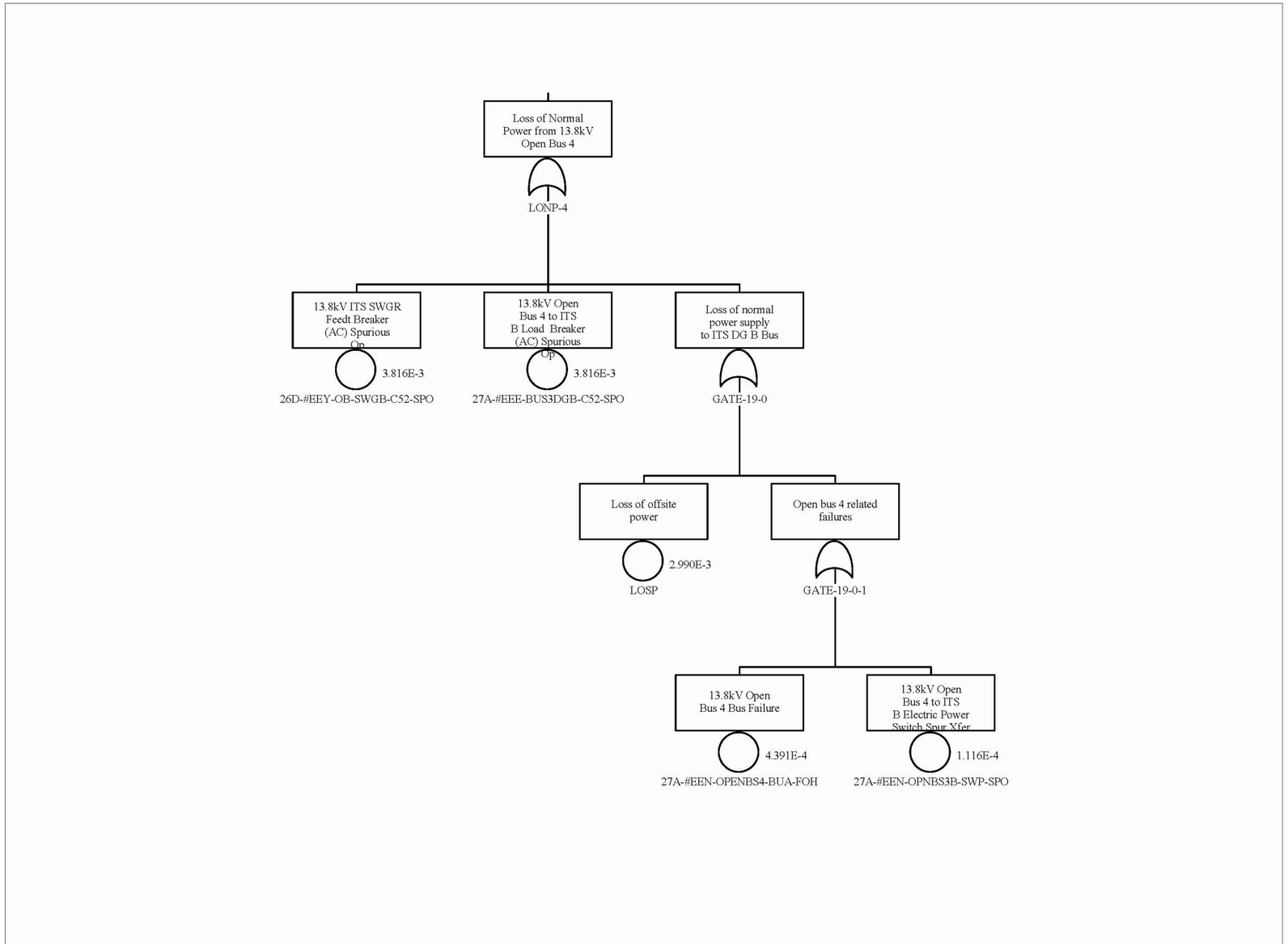
INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-27. Loss of AC Power to CRCF ITS Load Center Train B (11 of 12)

INTENTIONALLY LEFT BLANK



Source: Original

Figure B3.4-28. Loss of AC Power to CRCF ITS Load Center Train B (12 of 12)

INTENTIONALLY LEFT BLANK

B4 DRIP SHIELD EMPLACEMENT GANTRY—FAULT TREE ANALYSIS

B4.1 REFERENCES

Design Inputs

The PCSA is a safety analysis based on a snapshot of the design. The reference design documents are appropriately documented as design input 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, paragraph 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

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

B4.1.1 *BSC (Bechtel SAIC Company) 2007. *Concept of Operations for the Drip Shield Gantry.* 800-30R-HEE0-00200-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070810.0010.

B4.1.2 BSC 2007. *Drip Shield and Waste Package Emplacement Pallet Design Report.* 000-00C-SSE0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070810.0008.

B4.1.3 *BSC 2007. *Emplacement and Retrieval, Drip Shield Emplacement Gantry, Mechanical Equipment Envelope.* 800-MJ0-HE00-00201-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071026.0031.

B4.1.4 BSC 2007. *Interlocking Drip Shield Configuration.* 000-M00-SSE0-00101-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070409.0001.

B4.1.5 BSC 2007. *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3.* 800-MH0-HEE0-00201-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0034.

B4.1.6 *BSC 2008. *Drip Shield Gantry Mechanical Equipment Envelope Calculation.* 800-MQC-HEE0-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080125.0005.

B4.2 DRIP SHIELD OVERVIEW

Drip shields are placed over the waste packages within the emplacement drifts prior to closure of the Subsurface Facility. The purpose of the drip shield is to prevent any water seepage onto the waste packages after repository closure and to protect the waste package from the direct impact of a rockfall.

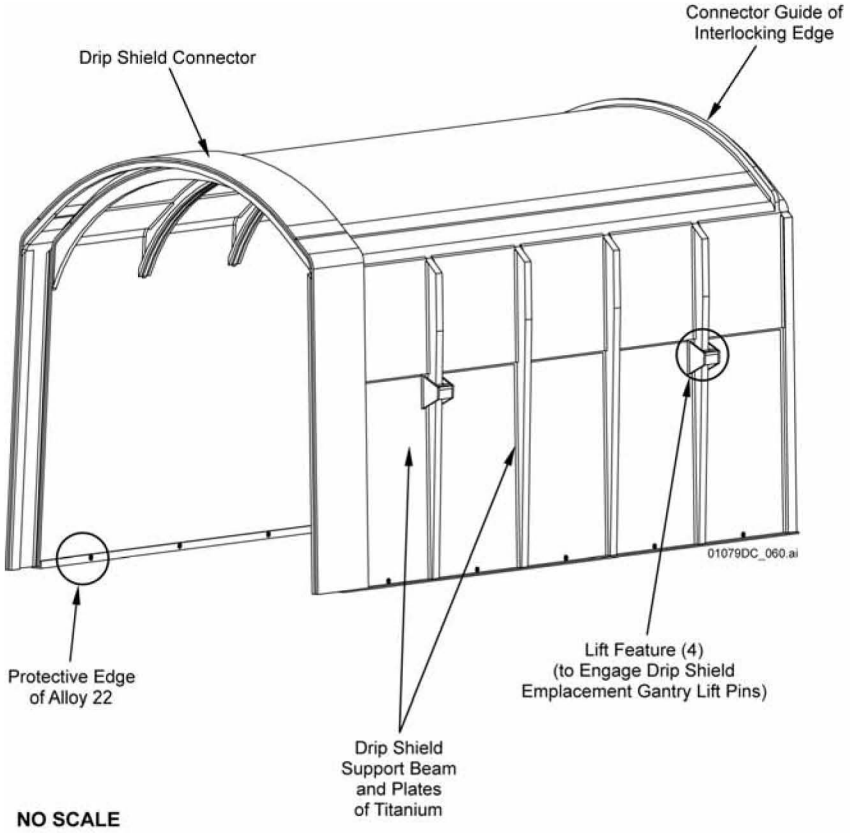
The inverted U-shaped drip shield (see Figure B4.2-1) is composed of titanium alloys (UNS R56404 and UNS R52400) with a protective base edge of Alloy 22. A drip shield segment is

approximately 2.9 m (9.5 ft) high and 5.8 m (19 ft) long and weighs approximately 5 metric tons (5.5 short tons). Each drip shield segment is designed to interlock with a previously emplaced drip shield segment. When properly interlocked, the drip shield does not contact the emplacement pallet, the waste package, the rock wall, or the runway beams of the invert.

B4.2.1 System Description

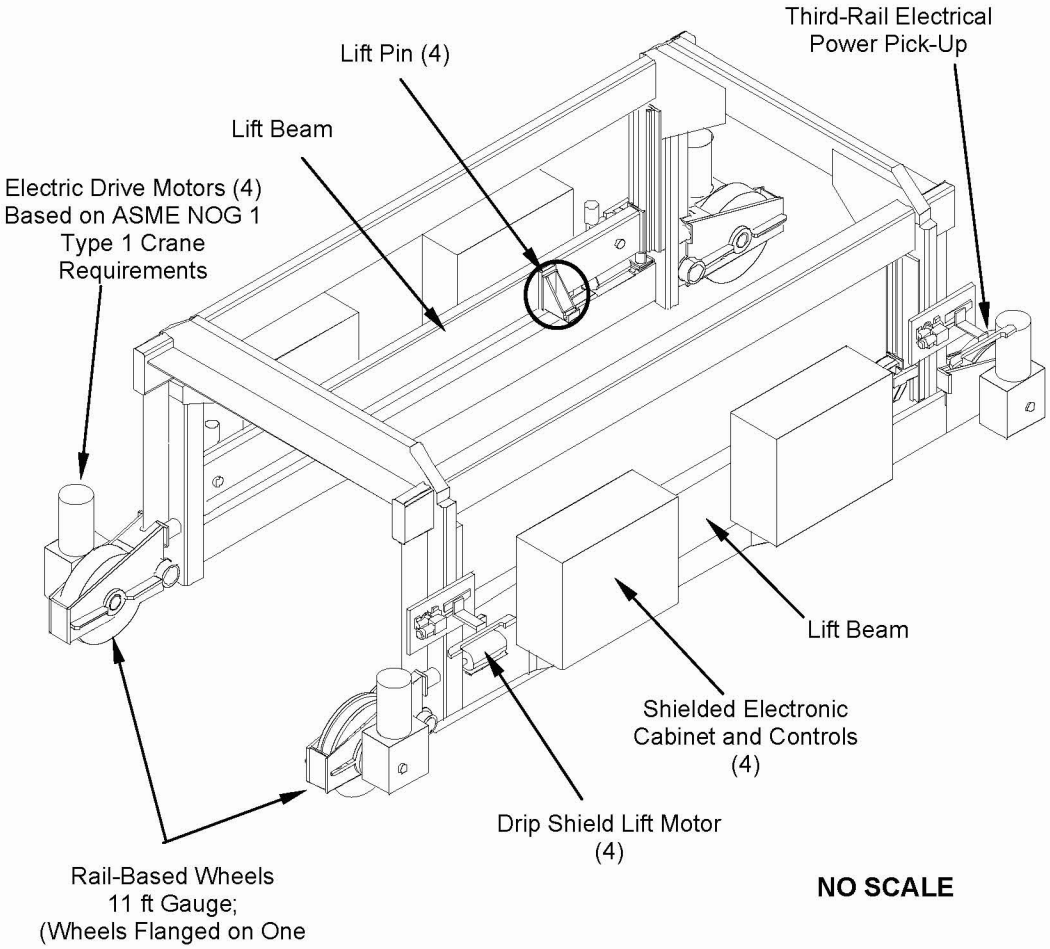
B4.2.1.1 Drip Shield Emplacement Gantry

The drip shield emplacement gantry is a remotely-operated vehicle that transports drip shields from the Heavy Equipment Maintenance Facility into emplacement drifts. The drip shield emplacement gantry is illustrated in Figure B4.2-2. Similar to the TEV, this gantry is a rail-based vehicle which is powered by a third rail electrical power system and contains PLCs for remote control of the device. In most cases the drip shield emplacement gantry operates under PLC control with only general oversight from the CCCF. Operations are performed under total manual control as needed.



Source: Modified from (Ref. B4.1.2) and (Ref. B4.1.4)

Figure B4.2-1. Illustration of a Drip Shield



Source: Modified from Ref. B4.1.3

Figure B4.2-2. Illustration of the Drip Shield Emplacement Gantry

The frame of the drip shield emplacement gantry is a steel structure designed to support its own weight and the weight of the drip shield. The gantry raises the lift beams upward to engage the lifting pin assemblies on the drip shield, thereby raising the shield into a carry position.

The drip shield emplacement gantry has four wheels (two on each side); each wheel is directly driven by an electric motor. The wheels on one side of the vehicle are double-flanged to limit derailment. Disc brakes are integral to the motors on each wheel. The wheels travel on 171 lb crane rail with a gauge of 3.35 m (11 ft). This track is the same track used by the TEV. The drip shield emplacement gantry carries an auxiliary (battery) backup power system to provide a limited supply of power in the event that third rail power is lost. Motors and gearboxes are sealed against environmental effects.

The drip shield emplacement gantry PLCs and other electronic controls are housed in separate equipment compartments (boxes) positioned at the sides of the gantry (Figure B4.2-2). Each compartment is insulated and contains equipment to maintain the operating environment for the control instrumentation as well as a fire suppression system.

The unloaded drip shield emplacement gantry weighs approximately 86 metric tons (95 short tons) and has a nominal height, width, and length of 3.5 × 4.9 × 9.4 m (11.6 × 16 × 31 ft), respectively.

Specific components of the TEV that are considered in fault trees are described in the following sections. The discussions are based on *Concept of Operations for the Drip Shield Gantry* (Ref. B4.1.1) and *Drip Shield Gantry Mechanical Equipment Envelope Calculation* (Ref. B4.1.6).

Drip Shield Lift System–The drip shield emplacement gantry lifts and lowers the drip shield using two moving lift beams (one on each side of the gantry). The drip shield has two lifting points (or features) on each side of the shield (Figure B4.2-1). Each gantry lift beam has two corresponding lift features (lift pins) (Figure B4.2-2). Four screw jacks power the lift beam and are used to lift the drip shield; each jack has a nominal capacity of 5 short tons (4.5 metric tons). A 3 hp (2.2 kW) motor or equivalent is used to drive the screw jack.

Drip Shield Emplacement Gantry Linear Drive Gear Motors–Each of the four gantry wheels are driven by a 12.5 hp (9.3 kW) linear drive gear motor featuring integral disc brakes.

B4.2.1.2 Operations

B4.2.1.3 Drip Shield Emplacement

The drip shield emplacement gantry transports a drip shield from the Heavy Equipment Maintenance Facility to a designated emplacement drift turnout using the same rail system as the TEV. After the gantry stops at the turnout, its positional sensors and devices enable it to calibrate and to establish a positional datum point. Once calibration is complete, the emplacement access door is opened and the gantry holding the drip shield proceeds through the door; the door is closed after the gantry has passed through.

The gantry proceeds down the turnout drift and enters the emplacement drift at an operational transit speed of approximately 2.7 km/hr (1.7 mph or 150 ft/min) to a predetermined position. Here the gantry stops and re-confirms its location. The gantry then moves forward at a slow speed, nominally 4.6 m/min (15 ft/min), to a predetermined position relative to the previously emplaced drip shield. Similar to the TEV, additional onboard positional sensors and devices are activated (e.g., lights, cameras, and ultrasonic sensors) and measurements are made to re-confirm the position of the gantry and drip shield in relation to a previously emplaced drip shield.

The gantry moves forward at a crawl speed, nominally 0.46 m/min (1.5 ft/min), until the required final position is achieved. Onboard cameras and sensors report the final position to the CCCF; some correction movement may be required to achieve the desired position. Once the final position is achieved, the gantry lowers the lift beams, thereby lowering the drip shield. The drip shield engages the previously emplaced drip shield interlock (if present) and it rests upon the steel frame of the emplacement drift invert.

The emplacement gantry lowers its lifting features to its travel height and moves at a crawl speed in a reverse direction from the newly emplaced drip shield to a predetermined distance and stops. Upon confirmation of emplacement status, the gantry slowly accelerates to the full operational

speed towards the emplacement access door. Once the gantry reaches the emplacement access door, the gantry again stops. The emplacement access door is opened and the gantry passes through the doorway.

Block diagrams of the drip shield emplacement gantry operations are provided in *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3* (Ref. B4.1.5).

B4.3 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 B4.3-1 with the following dependencies:

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

Table B4.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Third rail electrical power	Provides power for vehicle motion and controls	—	—	—	—
Programmable logic controllers	Provide local control of gantry mechanical systems	Failure due to high temperature or radiation	—	—	—
Linear-drive gear motors for wheels	Provides locomotive force for vehicle	—	—	—	—
Rail system (including switches)	Constrains and supports vehicle movement	—	Controls vehicle path	—	Seismic loading can fail rail system
Lift pin	Guide drip shield on drip shield emplacement gantry	Failure due to corrosion	Mates with lift features on drip shield	—	Seismic loading can cause failure
Lift beam	Provide lift for drip shield emplacement operations	Failure due to corrosion	Keeps lift pins in correct location	—	Seismic loading can cause failure
Drip shield lift motor / actuator	Moves lift beams up and down	Failure due to corrosion	—	—	—
Central control and communication system	Controls operation	—	—	Incorrect instruction	—
Manual controls	Controls operation	—	—	Incorrect instruction	—

Table B4.3-1. Dependencies and Interactions Analysis (Continued)

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Drip shield emplacement gantry frame	Constrains and supports lift beams and supports drip shield load	Failure due to corrosion or poor maintenance	Keeps lift beams in correct location	—	Seismic loading can cause failure

Source: Original

B4.4 DRIP SHIELD EMPLACEMENT GANTRY-RELATED FAILURE SCENARIOS

One scenario and fault tree associated with the drip shield emplacement gantry involves the drop of a drip shield onto a waste package.

The fault tree is described in the following subsection.

B4.4.1 Drop of Drip Shield onto a Waste Package

B4.4.1.1 Description

The scenario involves a drop of a drip shield onto a waste package (or packages) by the drip shield emplacement gantry while the gantry is transporting the drip shield into position within an emplacement drift. Just prior to closure, drip shields are transported and moved into emplacement drifts to provide for the long-term protection of the waste packages. The gantry moves a single drip shield in a raised position over a single waste package or a row of waste packages. It then lowers the drip shield in a position such that the shield interlocks with previously-emplaced drip shields (if present) to form a continuous barrier. Since a four-position lift system holds the drip shield during travel operations, at least two of the four lift positions must fail for the drip shield to fall and impact a waste package. The drip shield could potentially dig into the invert and rotate the drip shield if the gantry is moving when such a drop occurs. In addition, this failure may derail the drip shield emplacement gantry.

B4.4.1.2 Success Criteria

Success criteria for the drip shield emplacement gantry during the drip shield emplacement process require that the gantry subsystems operate without failure or spurious operations. During the emplacement operations, the gantry lift system should maintain the drip shield above the waste package as the gantry moves along the emplacement drift at an operational speed of 2.7 km/hr (1.7 mph).

B4.4.1.3 Design Features and Input

The following requirement is identified with respect to this scenario: Normal periodic maintenance and inspection activities are performed on the drip shield emplacement gantry. Specifically, the lift system and lift pins are maintained to allow for the safe operation of the gantry without dropping the drip shield during normal operation.

B4.4.1.4 Fault Tree Model

The fault tree model for the sequence is labeled as DRIPSHIELD-DROPPED. As shown in Figure B4.4-3, the fault tree describes the drop of the drip shield by the drip shield emplacement gantry onto a waste package in an emplacement drift. The top event is drop of the drip shield due to failure of at least two of the four lift pins or lift beam systems (rigs). This top event is realized by the occurrence of two of the four basic events through an OR gate; each basic event is the failure of one of the individual lift pins or lift beam systems.

B4.4.1.5 Basic Event Data

Table B4.4-1 contains a list of basic events used in the fault tree, DRIPSHIELD-DROPPED for impact on a waste package in an emplacement.

Table B4.4-1. Drip Shield Dropped on Waste package

Name	Description	Calc. Type[a]	Calc. Prob.	Probability/ Lambda	Miss. Time[a]
800-HEE0-DSLIFTC-LRG-CCF	Common-cause failure of 2 of 4 lifting rig or hooks	C	2.781E-08	—	—
800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	3	7.450E-07	7.450E-07	1.000E+00
800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	3	7.450E-07	7.450E-07	1.000E+00

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

Source: Original

B4.4.1.5.1 Human Failure Events

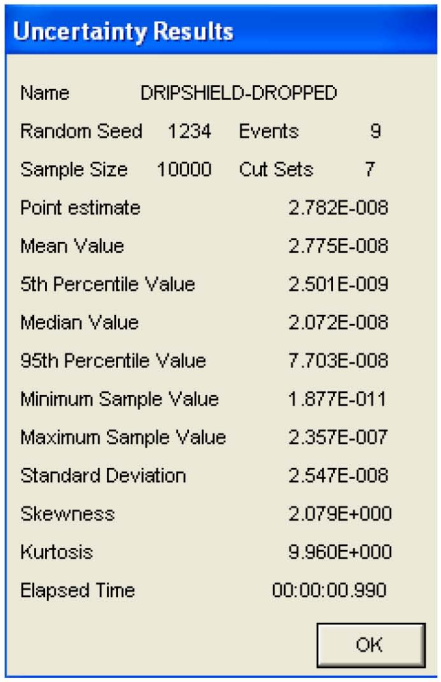
No basic event is identified as associated with human error for this model.

B4.4.1.5.2 Common-Cause Failures

One CCF failure is identified for this model: the CCF of at least two of four lifting rigs or hooks (800-HEE0-DSLIFTC-LRG-CCF).

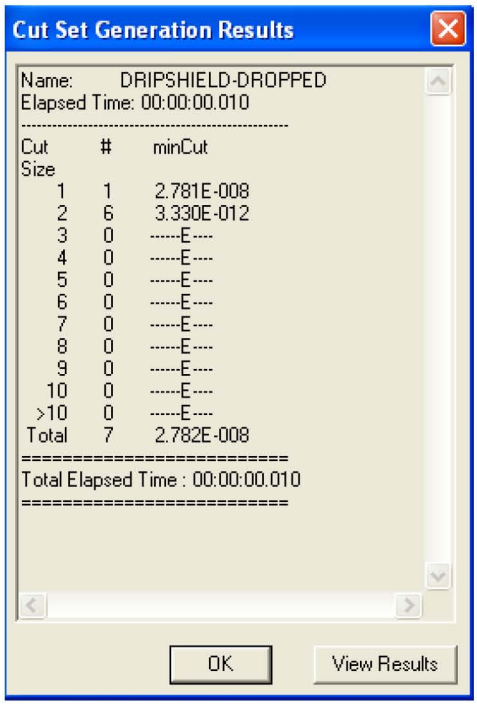
B4.4.1.6 Uncertainty and Cut set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree associated with the drop of the drip shield by the drip shield emplacement gantry, DRIPSHIELD-DROPPED, are presented in Figures B4.4-1 and B4.4-2.



Source: Original

Figure B4.4-1. Uncertainty Results for the DRIPSHIELD-DROPPED Fault Tree



Source: Original

Figure B4.4-2. Cut Set Generation Results for the DRIPSHIELD-DROPPED Fault Tree

B4.4.1.7 Cut Sets

Table B4.4-2 contains the cut sets for the DRIPSHIELD-DROPPED fault tree.

Table B4.4-2. DRIPSHIELD-DROPPED Cut Sets

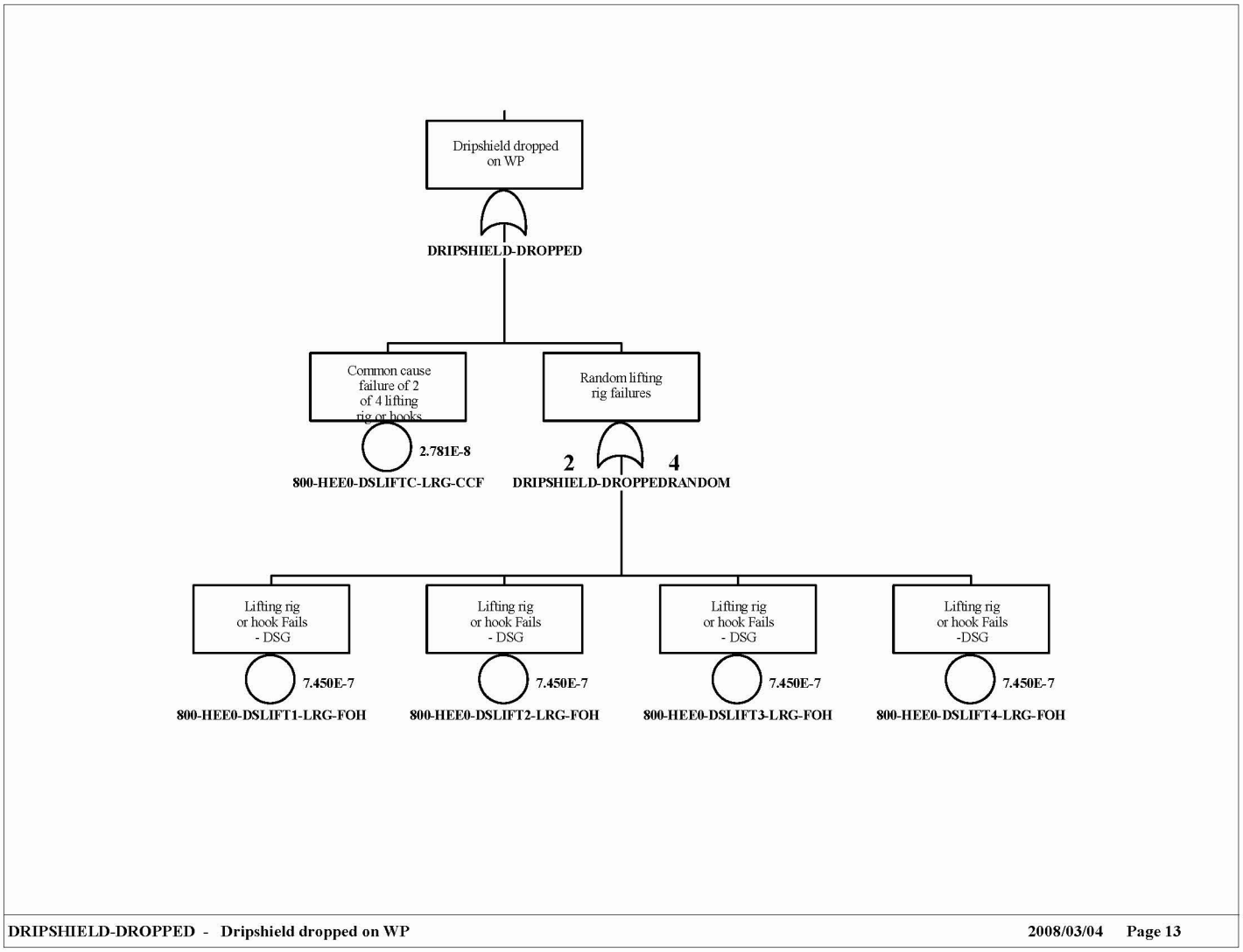
% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.99	99.99	2.781E-08	800-HEE0-DSLIFTC-LRG-CCF	Common cause failure of 2 of 4 lifting rig or hooks	2.781E-08
99.99	0.01	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
99.99	0.00	5.550E-13	800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
99.99	0.00	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
99.99	0.00	5.550E-13	800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook fails -drip shield emplacement gantry	7.450E-07
99.99	0.00	5.550E-13	800-HEE0-DSLIFT3-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT4-LRG-FOH	Lifting rig or hook fails -drip shield emplacement gantry	7.450E-07
99.99	0.00	5.550E-13	800-HEE0-DSLIFT1-LRG-FOH	Lifting rig or hook fails - drip shield emplacement gantry	7.450E-07
			800-HEE0-DSLIFT2-LRG-FOH	Lifting rig or hook fails -drip shield emplacement gantry	7.450E-07

NOTE: Prob. = probability.

Source: Original

B4.4.1.8 Fault Tree

The fault tree identified in Section B.4.3 associated with the drip shield emplacement gantry (DRIPSHIELD-DROPPED) is presented in Figure B4.4-3.



Source: Original

Figure B4.4-3. DRIPSHIELD-DROPPED - Fault Tree for Drop of Drip Shield onto a Waste Package

B5 SHIELD DOOR— FAULT TREE ANALYSIS

B5.1 REFERENCES

Design Inputs

The PCSA is a safety analysis based on a snapshot of the design. The reference design documents are appropriately documented as design input 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, paragraph 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

B5.1.1 BSC (Bechtel SAIC Company) 2007. *Nuclear Facilities Equipment Shield Door Process and Instrumentation Diagram*. 000-M60-H000-00101-000 REV 00D. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071220.0024.

B5.1.2 BSC 2008. *Canister Receipt and Closure Facility 1 General Arrangement Ground Floor Plan.* 060-P10-CR00-00102-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0013.

B5.1.3 BSC 2008. *Canister Receipt and Closure Facility 1 General Arrangement Second Floor Plan.* 060-P10-CR00-00103-000 REV 00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080122.0014.

B5.2 SHIELD DOOR SYSTEM DESCRIPTION

B5.2.1 Overview

Each of the CRCF Waste Package Positioning Rooms (room numbers 1018, 1019) has a shield door providing access to the Waste Package Loadout Room (room number 1015) (Ref. B5.1.2). The shield doors provide shielding during canister unloading and loading operations. The shield doors have been classified as ITS; they protect workers from the radiological exposure originating inside the Waste Package Loadout and Cask Unloading Rooms.

B5.2.2 Operations Description

Waste package loading operations in the Waste Package Positioning Rooms are analogous to cask unloading operations.

B5.2.3 Physical Description

The shield doors consist of pairs of large, heavy doors that are operated by individual motors with over-torque sensors to prevent crushing of an object. Each door has two position sensors to indicate either a closed or open door and an obstruction sensor prevents the doors from closing on an object. The obstruction sensor is also alarmed to provide operators indication when an object is between the shield doors. The shield doors and slide gate are interlocked to prevent one another from opening if the other is open. The shield doors are opened and closed via a hand

lever that must be enabled by an enable/disable switch. An emergency open switch exists enabling the doors to be opened in case of an emergency situation.

B5.2.4 Schematics

Schematics for the shield door are available separately for review (Ref. B5.1.1).

B5.3 DEPENDENCIES AND INTERACTIONS

Dependencies are broken down into five categories with respect to their interactions with structures, systems, and components (SSCs). 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 and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Door/gate motors	Over-torque sensors	—	—	Inadvertent operation	—

Source: Ref. B5.1.3

B5.4 SHIELD DOOR FAILURE SCENARIOS

The shield door system has one credible failure scenario for subsurface operations. This scenario involves the closure of the shield doors on a TEV carrying a sealed, filled waste package.

B5.4.1 Shield Door Closes on TEV

B5.4.1.1 Description

A radiological release may occur if the shield doors to the loading rooms are closed onto the TEV as the TEV carrying a waste package is transferred from the Waste Package Loadout Rooms. Engineered features, including motor over-torque sensors, ensure that this event does not occur.

B5.4.1.2 Success Criteria

The success criteria defined for this scenario requires that the shield doors do not cause a radiological release due to a closure of the doors on a conveyance. In the event that the shield doors do close on a conveyance, the motor over-torque sensors prevent excessive closure force ensuring no release.

B5.4.1.3 Design Features and Requirements

Motor over-torque sensors prevent shield doors from causing damage to casks or waste packages in the event of closure on a conveyance. Over-torque sensors are the only protective feature modeled in this fault tree. Other fault trees incorporate the modeling of an obstruction sensor that may also prevent collisions with any conveyance being used for transport.

B5.4.1.4 Fault Tree Model

The top event in this fault tree is "Facility Shield Door – Facility Door Closes on TEV." This event is defined as an inadvertent closure of the shield doors due to either operator action or component failure while the conveyance is in position to be hit by the doors. Faults considered in the evaluation of this top event include the failure of components in the control circuitry of the shield doors and human events that could contribute to the inadvertent shield door closing. The fault tree is shown in Figure B5.4-3.

B5.4.1.5 Basic Event Data

Eight basic events listed in Table B5.4-1 are used to model this failure scenario, including one human failure event.

Table B5.4-1. Basic Event Data

Name	Description	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time[a]
800-HEE0-FACMO01-MOE-SPO	Shield door motor #1 spurious operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
800-HEE0-FACMO02-MOE-SPO	Shield door motor #2 spurious operation	3	6.740E-07	0.000E+00	6.740E-07	1.000E+00
800-HEE0-FACTOR1-TL-FOH	Shield door motor #1 over-torque limiter failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
800-HEE0-FACTOR2-TL-FOH	Shield door motor #2 over-torque limiter failure	3	2.856E-02	0.000E+00	8.050E-05	3.600E+02
800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op - TEV doors	3	1.460E-06	0.000E+00	3.650E-07	4.000E+000
800-HEE0-WKRFACD-HFI-NOD	Operator closes facility door on TEV	1	2.000E-03	2.000E-03	0.000E+00	0.000E+00
800-SD---SRU001—SRU-FOH	Shield door ultrasonic obstruction sensor fails	3	9.620E-05	0.000E+00	9.620E-05	1.000E+00
800-SD---TL000-TL--CCF	Over-torque sensor CCF Failure	C	6.713E-04	—	—	—

NOTE: [a] For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time. See Table6.3-1 for definitions of calculation types.

Calc. = calculation; CCF = common-cause failure; Fail. = failure; Miss. = mission; PLC = programmable logic controller; Op = operation; Prob. = probability; TEV = transport and emplacement vehicle

Source: Original

B5.4.1.5.1 Human Failure Events

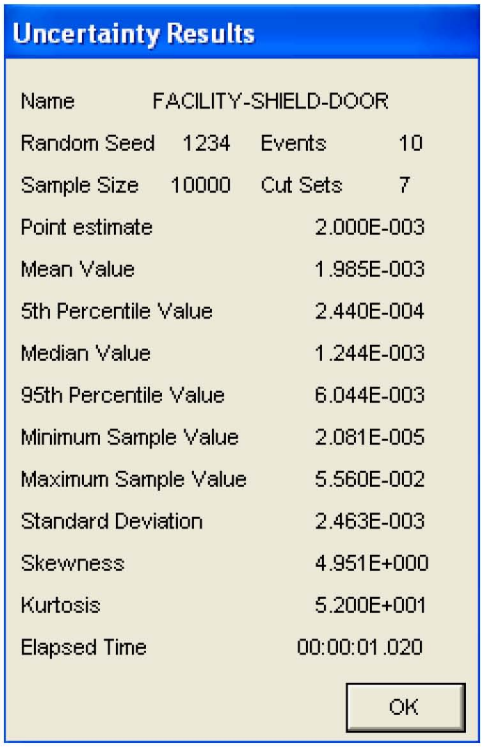
One human failure event, "800-HEE0-WKRFACD-HFI-NOD Operator closes facility door on TEV", is modeled in the fault tree as an operator attempting to close the shield doors while a conveyance is between the doors. The screening value used for this HFE has a probability of 2.0E-03.

B5.4.1.5.2 Common-Cause Failures

One CCF is considered in this fault tree, 800-SD---TL000-TL--CCF, the CCF of the shield door over-torque sensors.

B5.4.1.6 Uncertainty and Cut Set Generation

Figure B5.4-1 contains the uncertainty results obtaining from running the fault tree "Facility Shield Door – Facility Door Closes on TEV." Figure B5.4-2 provides the cut set generation results for the "Facility Shield Door – Facility Door Closes on TEV" fault tree.



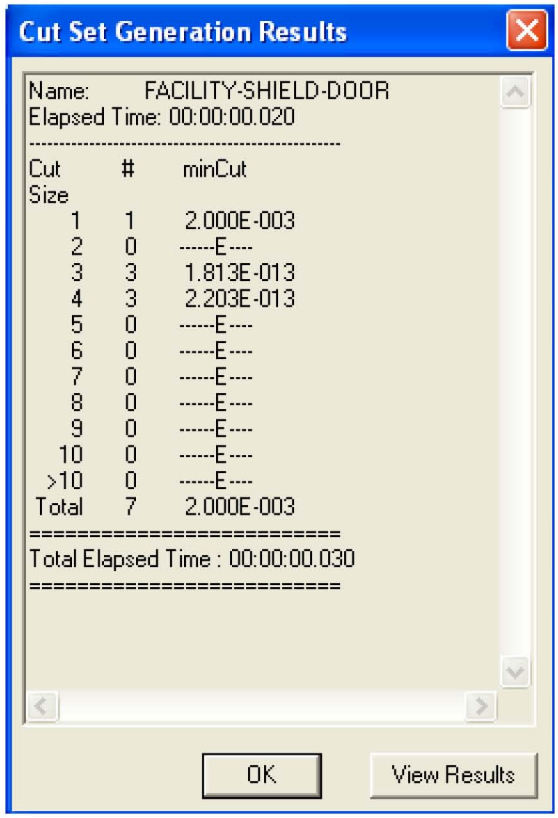
Uncertainty Results

Name	FACILITY-SHIELD-DOOR		
Random Seed	1234	Events	10
Sample Size	10000	Cut Sets	7
Point estimate			2.000E-003
Mean Value			1.985E-003
5th Percentile Value			2.440E-004
Median Value			1.244E-003
95th Percentile Value			6.044E-003
Minimum Sample Value			2.081E-005
Maximum Sample Value			5.560E-002
Standard Deviation			2.463E-003
Skewness			4.951E+000
Kurtosis			5.200E+001
Elapsed Time			00:00:01.020

OK

Source: Original

Figure B5.4-1. Uncertainty Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree



Source: Original

Figure B5.4-2. Cut Set Generation Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree

B5.4.1.7 Cut Sets

Table B.5.4-2 contains the cut sets for the "Facility Shield Door – Facility Door Closes on TEV" fault tree.

Table B5.4-2. Cut Sets for Facility Shield Door – Facility Door Closes on TEV

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	100.00	2.000E-03	800-HEE0-WKRFACD-HFI-NOD	Operator closes facility door on TEV	2.000E-03
100.00	0.00	1.146E-13	800-HEE0-FACTOR1-TL-FOH	Shield door motor #1 over-torque limiter failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield door motor #2 over-torque limiter failure	2.856E-02
			800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op - TEV doors	1.460E-06
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05

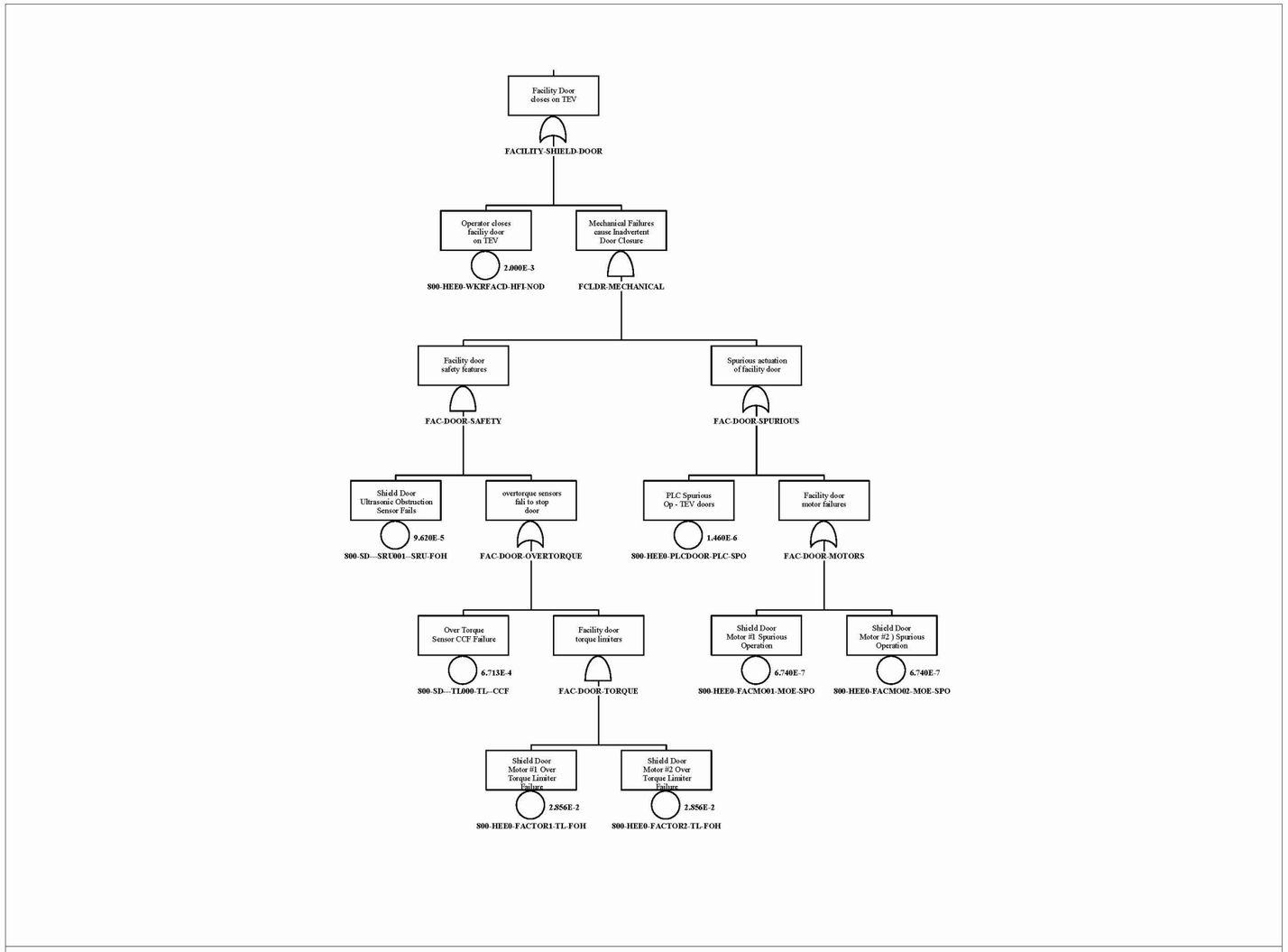
% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	0.00	9.427E-14	800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op - TEV doors	1.460E-06
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05
			800-SD---TL000-TL--CCF	Over-torque sensor CCF failure	6.713E-04
100.00	0.00	5.290E-14	800-HEE0-FACMO01-MOE-SPO	Shield door motor #1 spurious operation	6.740E-07
			800-HEE0-FACTOR1-TL-FOH	Shield door motor #1 over-torque limiter failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield door motor #2 over-torque limiter failure	2.856E-02
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05
100.00	0.00	5.290E-14	800-HEE0-FACMO02-MOE-SPO	Shield door motor #2 spurious operation	6.740E-07
			800-HEE0-FACTOR1-TL-FOH	Shield door motor #1 over-torque limiter failure	2.856E-02
			800-HEE0-FACTOR2-TL-FOH	Shield door motor #2 over-torque limiter failure	2.856E-02
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05
100.00	0.00	4.352E-14	800-HEE0-FACMO01-MOE-SPO	Shield door motor #1 spurious operation	6.740E-07
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05
			800-SD---TL000-TL--CCF	Over-torque sensor CCF failure	6.713E-04
100.00	0.00	4.352E-14	800-HEE0-FACMO02-MOE-SPO	Shield door motor #2 spurious operation	6.740E-07
			800-SD---SRU001--SRU-FOH	Shield door ultrasonic obstruction sensor fails	9.620E-05
			800-SD---TL000-TL--CCF	Over-torque sensor CCF failure	6.713E-04

NOTE: CCF = common-cause failure; Op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B5.4.1.8 Fault Tree

The fault tree associated with the facility shield doors is presented in Figure B5.4-3.



Source: Original

Figure B5.4-3. FACILITY-SHIELD-DOOR – Facility Door Closes on TEV Fault Tree Sheet

INTENTIONALLY LEFT BLANK

B6 EMPLACEMENT ACCESS DOOR ANALYSIS

B6.1 REFERENCES

Design Inputs

The PCSA is a safety analysis based on a snapshot of the design. The reference design documents are appropriately documented as design input 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, paragraph 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

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

B6.1.1 *BSC (Bechtel SAIC Company) 2007. *Emplacement Access Door & Turnout Bulkhead*. 800-S0C-SSD0-00600-000 Rev 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070326.0020.

B6.1.2 Not used.

B6.1.3 *BSC 2007. *Subsurface Emplacement Access Door and Bulkhead Arrangement for LA (Sheet 2 of 2)*. 800-KV0-VUE0-00402-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070813.0015.

B6.1.4 *BSC 2007. *Subsurface Emplacement Ventilation System Design Analysis*. 800-KVC-VUE0-00400-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071210.0009.

B6.1.5 *BSC 2008. *Subsurface Construction and Emplacement Ventilation*. 800-KVC-VU00-00900-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080124.0010.

B6.2 EMPLACEMENT ACCESS DOOR DESCRIPTION

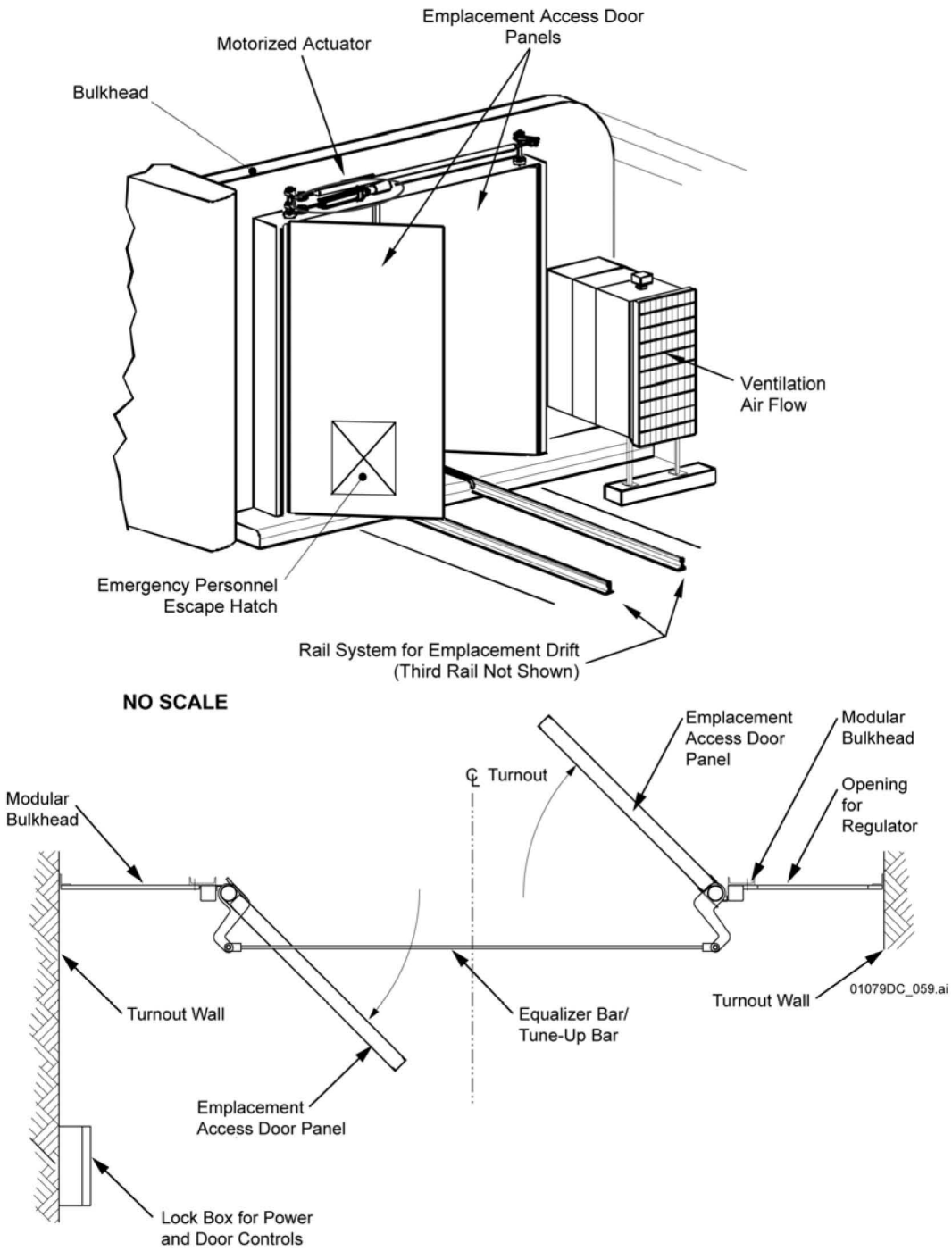
The emplacement access door is a counter-opening, two-panel design in which one panel opens inward and the other panel opens outward (Figure B6.2-1). The door is intended to control entry and is not to provide radiation shielding. The overall doorway has a clear opening of approximately 16.5 × 12.4 ft in width/height (Ref. B6.1.4, Figure 7) and the door is approximately 19.3 × 14.1 ft in overall dimension to accommodate door framing. The emplacement access door panel is constructed from 3/16 in. minimum thick steel plates that are separated and reinforced by steel spacers. The overall emplacement access door (both door panels) is estimated to weigh approximately 3.0 short tons (Ref. B6.1.1, Section 6.4.5).

The two door panels are linked together by an equalizer bar/tune-up bar that provides the linkage required for counter-opening the assembly (Figure B6.2-1). The linkage also contains an adjustment mechanism to provide fine-tuning of the door sealing. This design uses a single

actuator and linkage bar to open and close both doors, thereby reducing the maintenance cost when compared to dual actuators. The actuator provides the driving force necessary to open the emplacement access door. The capacity of the actuator is not defined.

B6.2.1 Operations

The emplacement access door is typically closed to maintain security and positive control of the emplacement drift. Normal door operation requires input from the CCCF to prevent inadvertent access to the high radiation areas (Ref. B6.1.4, Section 6.9). However, a manual override switch within a locked access box is provided to open the door locally (Ref. B6.1.3). The emplacement access door is remotely opened by the operator in the CCCF when a TEV is ready to proceed into an emplacement drift. The actuator drives the two door panels to swing in opposite directions to open, allowing the TEV to pass through the doorway. Upon visual confirmation that the TEV has passed through the threshold and has completely entered the turnout drift, the operator in the Central CCCF closes the door system. The process is reversed when the TEV is required to exit the emplacement drift. It is conservatively estimated that the emplacement access door for each drift will open and close approximately 470 times throughout the duration of emplacement operations. The emplacement access door instrumentation interfaces through the DCMIS to provide real-time status and supervisory control (Ref. B6.1.4, Section 6.9). When the emplacement access door is open, both audible and visual alarms notify workers and the CCCF of the change in position of the doors (Ref. B6.1.4, Section 6.8).



Source: Modified from (Ref. B6.1.5, Figure 20 and 21)

Figure B6.2-1. Illustration of an Emplacement Access Door

B6.3 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 B6.3-1 with the following dependencies:

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

Table B6.3-1. Dependencies and Interactions Analysis

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Electrical power	Provides power to door	—	—	—	—
Motorized actuator	Opens and closes the door panels	—	—	—	—
Bulkhead Structure	Constrains and supports door panels	Failure due to corrosion or poor maintenance	Keeps door panels in correct location	—	Seismic loading can cause impact
Central control switch	Controls operation	—	—	Premature activation	—
Manual switch	Controls operation	—	—	Premature activation	—

Source: Original

B6.4 EMPLACEMENT ACCESS DOOR RELATED FAILURE SCENARIO

The emplacement access door has one credible failure scenario for subsurface operations. This scenario involves the closure of the emplacement access door on a TEV carrying a sealed, filled waste package. The scenario and tree are described in the following subsection.

B6.4.1 Description

The identified scenario involves the closure or failure of the emplacement access door onto the TEV as the TEV passes through the door. The emplacement access door provides security to restrict the entrance of personnel into a high radiation area (i.e., the emplacement drift). However, the door does not provide any shielding protection. The door is actuated remotely to allow the TEV to pass in and out of the emplacement turnout drift as part of waste package emplacement operations. Door operation is not interlocked with TEV motion and no anti-collision safety features are identified for the door. Cameras on the TEV provide confirmation of door status.

B6.4.1.1 Success Criteria

The success criterion for the scenario requires that the emplacement access door operates without failure or spurious operations and that the operator does not close the door prematurely. The emplacement access door system should not close onto the TEV or collapse onto the TEV during normal operations.

B6.4.1.2 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The operational status of the door is clearly displayed on a visual monitor for the remote operations on the control panel, including operations such as opening and closing of the door.
- The TEV shielded enclosure is able to maintain the shielding function in case of closure of the emplacement access door on the TEV.
- Normal periodic maintenance and inspection are performed on the bulkhead and door mounting supports and door mechanism to allow for the safe operation of the door without collapsing the door panels onto the TEV.

B6.4.1.3 Fault Tree Model

The fault tree model for the sequence is labeled as AC-DRIMP-INIT. This fault tree has been discussed previously as part of the DRIFT-TEV-IMPACT fault tree presented in section B1. The top event is the initiating event involving the doors closing and impacting on the TEV. This top event is realized by either the occurrence of the door closure due to human error or by mechanical failure. Human error is represented by a basic event describing the operator failure by closing the emplacement access door prematurely and the door impacting the TEV, prior to the TEV complete passing into the turnout,. Mechanical failure occurs by the joint occurrence of a spurious signal to close the emplacement access door together with the failure of the door mechanism and safety features; the joint input is represented by an AND gate.

Regarding the failure of the door mechanism and safety features, a single input is identified involving the door actuator motor system. The door drive system is represented by a basic input event representing the failure of the motors driving the door system to stop.

The contributing factor that causes the mechanical door failure is the generation of a spurious signal that activates the door actuator to close. The spurious signal can be generated by either a fault in the programmable logic controller within the remote control and communication system or a failure in the actuator motor. The spurious signal generated by programmable logic controller is represented as a basic event, as is the failure of the actuator motor.

B6.4.1.4 Basic Event Data

Table B6.4-1 contains a list of basic events used in the fault tree, AC-DRIMP-INIT, which models the failures associated with the closure of the emplacement drift doors on a TEV.

Table B6.4-1. Basic Event Data for Closure of Drift Doors on TEV

Name	Description	Calc. Type[a]	Calculated Probability	Mean Failure Portability	Lambda	Mission Time[a]
800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	1	2.000E-03	2.000E-03	0.000E+00	0.000E+00
800-HEE0-AXSDR00-PLC-SPO	Programmable logic controller spurious operation	3	2.081E-09	0.000E+00	3.650E-07	5.700E-03
800-HEE0-AXSM001-MOE-FSO	Motor (electric) fails to shut off	3	7.695E-11	0.000E+00	1.350E-8	5.700E-03
800-HEE0-AXSM002-MOE-FSO	Motor (electric) fails to shut off	3	7.695E-11	0.000E+00	1.350E-8	5.700E-03
800-HEE0-ACTADR1-ATP-SPO	Actuator spurious op – emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03
800-HEE0-ACTADR2-ATP-SPO	Actuator spurious op – emplacement access door	3	7.638E-09	0.000E+00	1.340E-06	5.700E-03

NOTE: [a]For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; op = operation; TEV = transport and emplacement vehicle.

Source: Original

B6.4.1.4.1 Human Failure Events

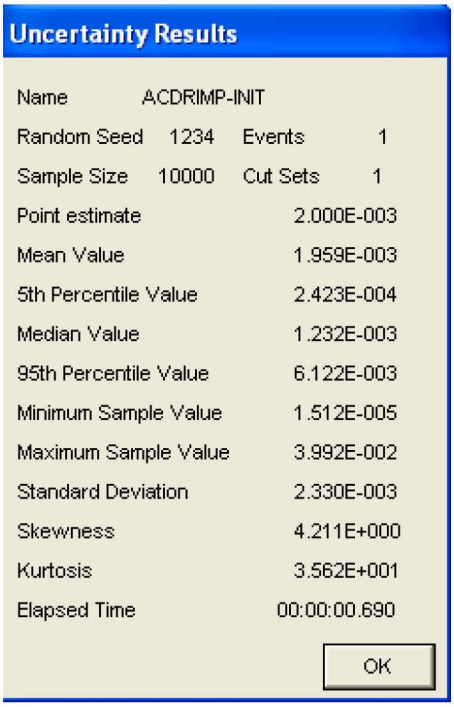
One basic event is identified as associated with human error involving the premature closure of the emplacement access door. The basic event, the operator closes the emplacement drift door on the TEV, is identified as 800-HEE0-AXSDR00-HFI-NOD.

B6.4.1.4.2 Common-Cause Failures

There are no CCFs identified for this model.

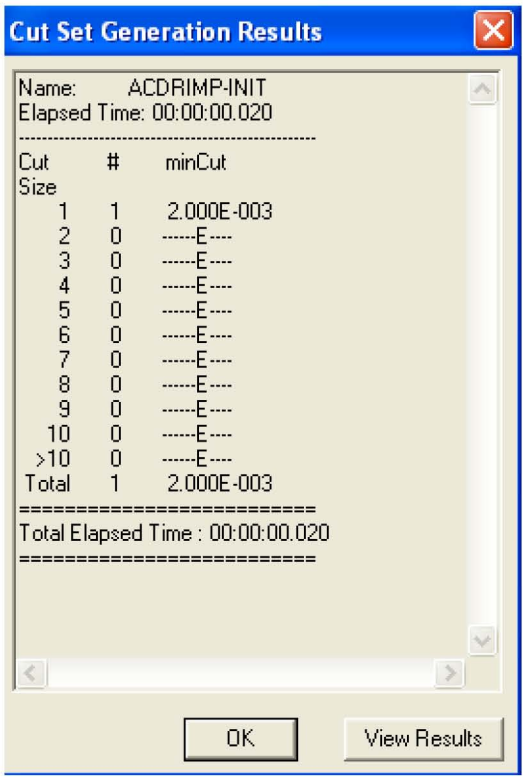
B6.4.1.5 Uncertainty and Cut Set Generation Results

Uncertainty and cut set quantification results from SAPHIRE for the fault tree associated with the emplacement access door, AC-DRIMP-INIT are presented in Figures B6.4-1 and B6.4-2.



Source: Original

Figure B6.4-1. Uncertainty Results for AC-DRIMP-INIT



Source: Original

Figure B6.4-2. Cut Set Generation Results for AC-DRIMP-INIT

B6.4.1.6 Cut Sets

Table B6.4-2 contains the cut sets for fault tree AC-DRIMP-INIT.

Table B6.4-2. AC-DRIMP-INIT Cut Sets

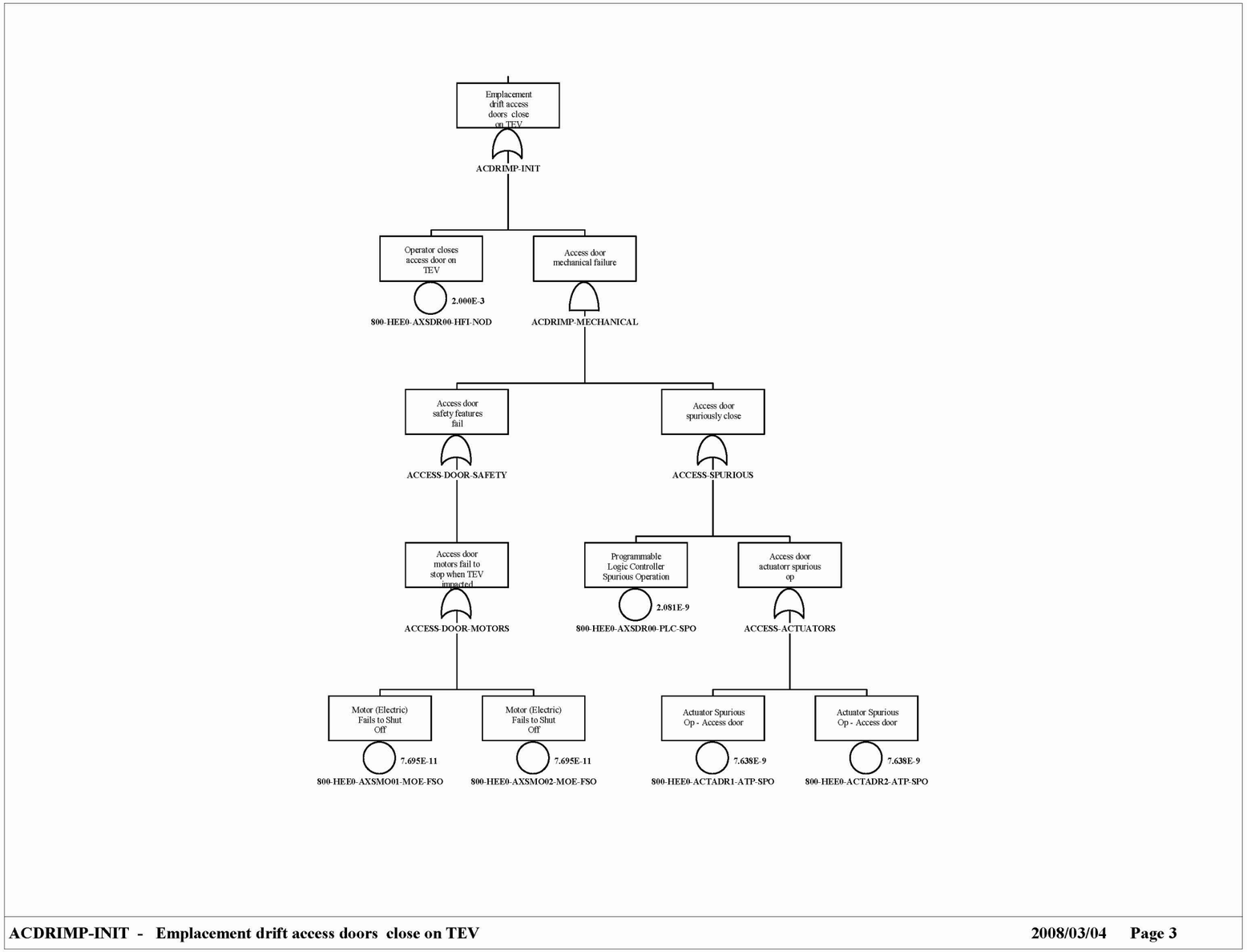
% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	100.00	2.000E-03	800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	2.000E-03
100.00	0.00	5.877E-19	800-HEE0-ACTADR1-ATP-SPO	Actuator spurious op - emplacement access door	7.638E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (electric) fails to shut off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR2-ATP-SPO	Actuator spurious op - emplacement access door	7.638E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (electric) fails to shut off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR1-ATP-SPO	Actuator spurious op - emplacement access door	7.638E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (electric) fails to shut off	7.695E-11
100.00	0.00	5.877E-19	800-HEE0-ACTADR2-ATP-SPO	Actuator spurious op - emplacement access door	7.638E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (electric) fails to shut off	7.695E-11
100.00	0.00	1.601E-19	800-HEE0-AXSDR00-PLC-SPO	Programmable logic controller spurious operation	2.080E-09
			800-HEE0-AXSMO01-MOE-FSO	Motor (electric) fails to shut off	7.695E-11
100.00	0.00	1.601E-19	800-HEE0-AXSDR00-PLC-SPO	Programmable logic controller spurious operation	2.080E-09
			800-HEE0-AXSMO02-MOE-FSO	Motor (electric) fails to shut off	7.695E-11

NOTE: op = operation; TEV = transport and emplacement vehicle.

Source: Original

B6.4.1.7 Fault Tree

The fault tree associated with the emplacement access doors (AC-DRIMP-INIT) is presented in Figure B6.4-3.



Source: Original

Figure B6.4-3. ACDRIMP-INIT - Fault Tree for Emplacement Access Door Closes on TEV

INTENTIONALLY LEFT BLANK