

FIGURES (Continued)

	Page
B2.2-1. Block Diagram of the CRCF HVAC System	B2-3
B2.2-2. General Location for the CRCF HVAC System.....	B2-4
B2.4-1. Uncertainty Results of the CRCF Failure to Maintain Delta Pressure Fault Tree	B2-19
B2.4-2. Cut Set Generation Results for the CRCF Failure to Maintain Delta Pressure Fault Tree.....	B2-20
B2.4-3. Delta Pressure not Maintained in CRCF Facility	B2-25
B2.4-4. Loss of HEPA Filtered Flow Due to Loss of Confinement Boundary or High Winds	B2-27
B2.4-5. Loss of HEPA Filtered Exhaust from Operating and Standby Trains	B2-29
B2.4-6. Loss of HEPA Filtered Flow from Standby Train (Train B).....	B2-31
B2.4-7. Loss of HEPA Flow from Train B after Manual Switchover	B2-33
B2.4-8. Loss of Flow through HEPA Filters Due to Open Doors	B2-35
B2.4-9. Train B Exhaust Fan Fails to Start Due to Mechanical or Electrical Failures.....	B2-37
B2.4-10. Supply Fans Fail to Supply Air.....	B2-39
B2.4-11. Switchover to Standby Train Fails to Occur.....	B2-41
B2.4-12. Flow to Train A Tornado Damper Fails	B2-43
B2.4-13. Flow from 1 of 3 Filter Plenums Fail when Supply Fans Operating.....	B2-45
B2.4-14. Flow through Train A Plenum 009 Fails	B2-47
B2.4-15. Flow through Train A Plenum 010 Fails	B2-49
B2.4-16. Flow through Train A Plenum 011 Fails	B2-51
B2.4-17. Flow from 2 of 3 Filter Plenums Fail.....	B2-53
B2.4-18. Flow to Train B Tornado Damper Fails.....	B2-55
B2.4-19. Flow to Train B Fan Discharge Backdraft Damper Fails	B2-57
B2.4-20. Flow from 1 of 3 Filter Plenums Fail when Supply Fans Operating.....	B2-59
B2.4-21. Flow through Train B Plenum 012 Fails.....	B2-61
B2.4-22. Flow through Train B Plenum 013 Fails.....	B2-63
B2.4-23. Flow from 2 of 3 Filter Plenums Fail.....	B2-65
B3.2-1. AC Power – Main Electrical Distribution.....	B3-4
B3.2-2. AC Power – 13.8 kV ITS Switchgear Train A	B3-5
B3.2-3. AC Power – 13.8 kV ITS Switchgear Train B.....	B3-6

FIGURES (Continued)

	Page
B3.2-4. Emergency Diesel Generator Facility – 480 V ITS Motor Control Center Train A	B3-7
B3.2-5. ITS 125 V DC System Train A	B3-8
B3.2-6. Emergency Diesel Generator facility – 480 V ITS Motor Control Center Train B	B3-9
B3.2-7. ITS 125 V DC System Train B	B3-10
B3.2-8. CRCF ITS Load Center Train A	B3-11
B3.2-9. CRCF ITS Load Center Train B	B3-12
B3.2-10. CRCF ITS MCC Train A	B3-13
B3.2-11. CRCF ITS MCC Train B	B3-14
B3.2-12. ITS Diesel Generator Fuel Oil System	B3-16
B3.2-13. Simplified Diagram of Representative Train of CRCF ITS Electrical and ITS Battery Rooms Ventilation System	B3-17
B3.4-1. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree	B3-29
B3.4-2. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train A	B3-30
B3.4-3. Uncertainty Results of the Loss of AC Power to CRCF ITS Load Center Train B Fault Tree	B3-42
B3.4-4. Cut Set Generation Results for Loss of AC Power to CRCF ITS Load Center Train B	B3-42
B3.4-5. Loss of Power to CRCF ITS Load Center Train A (1 of 12)	B3-47
B3.4-6. Loss of Power to CRCF ITS Load Center Train A (2 of 12)	B3-49
B3.4-7. Loss of Power to CRCF ITS Load Center Train A (3 of 12)	B3-51
B3.4-8. Loss of Power to CRCF ITS Load Center Train A (4 of 12)	B3-53
B3.4-9. Loss of Power to CRCF ITS Load Center Train A (5 of 12)	B3-55
B3.4-10. Loss of Power to CRCF ITS Load Center Train A (6 of 12)	B3-57
B3.4-11. Loss of Power to CRCF ITS Load Center Train A (7 of 12)	B3-59
B3.4-12. Loss of Power to CRCF ITS Load Center Train A (8 of 12)	B3-61
B3.4-13. Loss of Power to CRCF ITS Load Center Train A (9 of 12)	B3-63
B3.4-14. Loss of Power to CRCF ITS Load Center Train A (10 of 12)	B3-65
B3.4-15. Loss of Power to CRCF ITS Load Center Train A (11 of 12)	B3-67

FIGURES (Continued)

	Page
B3.4-16. Loss of Power to CRCF ITS Load Center Train A (12 of 12).....	B3-69
B3.4-17. Loss of Power to CRCF ITS Load Center Train B (1 of 12).....	B3-71
B3.4-18. Loss of Power to CRCF ITS Load Center Train B (2 of 12).....	B3-73
B3.4-19. Loss of Power to CRCF ITS Load Center Train B (3 of 12).....	B3-75
B3.4-20. Loss of Power to CRCF ITS Load Center Train B (4 of 12).....	B3-77
B3.4-21. Loss of AC Power to CRCF ITS Load Center Train B (5 of 12).....	B3-79
B3.4-22. Loss of AC Power to CRCF ITS Load Center Train B (6 of 12).....	B3-81
B3.4-23. Loss of AC Power to CRCF ITS Load Center Train B (7 of 12).....	B3-83
B3.4-24. Loss of AC Power to CRCF ITS Load Center Train B (8 of 12).....	B3-85
B3.4-25. Loss of AC Power to CRCF ITS Load Center Train B (9 of 12).....	B3-87
B3.4-26. Loss of AC Power to CRCF ITS Load Center Train B (10 of 12).....	B3-89
B3.4-27. Loss of AC Power to CRCF ITS Load Center Train B (11 of 12).....	B3-91
B3.4-28. Loss of AC Power to CRCF ITS Load Center Train B (12 of 12).....	B3-93
B4.2-1. Illustration of a Drip Shield	B4-2
B4.2-2. Illustration of the Drip Shield Emplacement Gantry	B4-3
B4.4-1. Uncertainty Results for the DRIPSHIELD-DROPPED Fault Tree.....	B4-8
B4.4-2. Cut Set Generation Results for the DRIPSHIELD-DROPPED Fault Tree.....	B4-8
B4.4-3. DRIPSHIELD-DROPPED - Fault Tree for Drop of Drip Shield onto a Waste Package	B4-10
B5.4-1. Uncertainty Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree	B5-14
B5.4-2. Cut Set Generation Results for the Facility Shield Door – Facility Door Closes on TEV Fault Tree	B5-15
B5.4-3. FACILITY-SHIELD-DOOR – Facility Door Closes on TEV Fault Tree Sheet...B5-17	
B6.2-1. Illustration of an Emplacement Access Door	B6-3
B6.4-1. Uncertainty Results for AC-DRIMP-INIT	B6-7
B6.4-2. Cut Set Generation Results for AC-DRIMP-INIT.....	B6-7
B6.4-3. ACDRIMP-INIT - Fault Tree for Emplacement Access Door Closes on TEV	B6-9
B7-1. Facility-Drop on Fault Tree	B7-4
B7-2. Transit-Derail Fault Tree	B7-5
B7-3. Transit-Drop on Fault Tree.....	B7-6

FIGURES (Continued)

	Page
B7-4. DRIFT-TEV-IMPACT Fault Tree.....	B7-7
B7-5. Drift-WP-Drop on Fault Tree.....	B7-8
B7-6. Drift-WP-Impact Fault Tree.....	B7-9
B7-7. DSGANT-INIT Fault Tree.....	B7-10
B7-8. SSO-CRCF-SD-IMPACT-HVAC Fault Tree.....	B7-11
B7-9. SSO-HVYLOAD-DROPON-HVAC Fault Tree.....	B7-12
B7-10. SSO-TEV-COLL-HVAC Fault Tree.....	B7-13
B7-11. SSO-WP-DROP-HVAC Fault Tree.....	B7-14
B7-12. SSO-WP-TEV-SD-HVAC Fault Tree.....	B7-15
B7-13. SHIELD-PROXIMITY Fault Tree.....	B7-16
B7-14. SHIELD-ENTRY Fault Tree.....	B7-17
B7-15. FIRE-DRIFT Fault Tree.....	B7-18
B7-16. FIRE-SUBSURFACE Fault Tree.....	B7-19
B7-17. FIRE-SURFACE Fault Tree.....	B7-20

TABLES

	Page
B1.2-1. TEV Shielding Configuration	B1-4
B1.3-1. Dependencies and Interactions Analysis	B1-10
B1.4-1. Basic Event Probabilities for Waste Package Impact from the TEV Front Shield Doors.....	B1-13
B1.4-2. DRIFT-DOOR-IMPACT Cut Sets	B1-15
B1.4-3. Basic Event Probabilities for TEV Collision within Facility.....	B1-16
B1.4-4. Facility-Collision Cut Sets	B1-18
B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit.....	B1-20
B1.4-6. DRIFT-TEV-IMPACT Cut Sets	B1-23
B1.4-7. Basic Event Probabilities for Impact to TEV during Transit.....	B1-26
B1.4-8. TRANSIT-IMPACT Cut Sets.....	B1-29
B1.4-9. Basic Event Probabilities for TEV Stops for Extended Time.....	B1-32
B1.4-10. SHIELD-STOP Cut Sets.....	B1-34
B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit.....	B1-35
B1.4-12. SHIELD-DOOR Cut Sets	B1-37
B1.4-13. Basic Event Probabilities for Waste Package Drop in Facility.....	B1-39
B1.4-14. FACILITY-DROP Cut Sets	B1-41
B1.4-15. Basic Event Probabilities for Waste Package Dropped during Transit	B1-44
B1.4-16. TRANSIT-DROP Cut Sets	B1-46
B1.4-17. Basic Event Probabilities for a Waste Package Drop or Dragging in an Emplacement Drift	B1-49
B1.4-18. DRIFT-DRAG Cut Sets	B1-52
B1.4-19. Basic Event Probabilities for TEV Collides with Emplaced Waste Package.....	B1-55
B1.4-20. TEV-IMPACTS-WP Cut Sets	B1-57
B2.2-1. HVAC Damper Failure Modes	B2-5
B2.2-2. HEPA Filter Plenum Failure Modes	B2-6
B2.2-3. CRCF Confinement and Shield Door Interlocks	B2-10
B2.3-1. Dependencies and Interactions Analysis	B2-12
B2.4-1. Basic Event Probability for the HVAC Failure to Maintain Delta Pressure in the CRCF	B2-15

TABLES (Continued)

	Page
B2.4-2. Human Failure Events.....	B2-19
B2.4-3. Dominant Cut Sets for the Failure to Maintain the Pressure Differential in the CRCF	B2-21
B3.3-1. Dependencies and Interactions Analysis	B3-20
B3.4-1. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train A Fault Tree	B3-23
B3.4-2. Human Failure Events.....	B3-27
B3.4-3. Common-Cause Basic Events.....	B3-28
B3.4-4. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train A.....	B3-30
B3.4-5. Basic Event Probability for the Loss of AC Power to CRCF ITS Load Center Train B Fault Trees	B3-36
B3.4-6. Human Failure Events.....	B3-40
B3.4-7. Common-Cause Basic Events.....	B3-41
B3.4-8. Dominant Cut Sets for the Loss of AC Power to CRCF ITS Load Center Train B	B3-43
B4.3-1. Dependencies and Interactions Analysis	B4-5
B4.4-1. Drip Shield Dropped on Waste package.....	B4-7
B4.4-2. DRIPSHIELD-DROPPED Cut Sets	B4-9
B5.3-1. Dependencies and Interactions Analysis	B5-12
B5.4-1. Basic Event Data.....	B5-13
B5.4-2. Cut Sets for Facility Shield Door – Facility Door Closes on TEV.....	B5-15
B6.3-1. Dependencies and Interactions Analysis	B6-4
B6.4-1. Basic Event Data for Closure of Drift Doors on TEV	B6-6
B6.4-2. AC-DRIMP-INIT Cut Sets	B6-8
B7-1. Top Level and Linking Fault Trees	B7-1
B7-2. Basic Events for Additional Fault Trees.....	B7-3

ACRONYMS AND ABBREVIATIONS

Acronyms

ASD	adjustable speed drive
AHU	air handling unit
CCCF	Central Control Center Facility
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
DCMIS	digital control and management information system
EDGF	Emergency Diesel Generator Facility
HEP	human error probability
HFE	human failure events
HEPA	high-efficiency particulate air
HVAC	heating, ventilation and air conditioning
ITS	important to safety
LOSP	loss of offsite power
MCC	motor control center
OOS	out of service
PLC	programmable logic controller
RF	Receipt Facility
SNF	spent nuclear fuel
SSCs	structures, systems, and components
TEV	transport and emplacement vehicle
UPS	uninterruptible power system
WHF	Wet Handling Facility

ACRONYMS AND ABBREVIATIONS (Continued)

Abbreviations

AC	alternating current
cfm	cubic foot per minute
DC	direct current
ft	foot/feet
hr	hour
hp	horsepower
in.	inch
km	kilometer
kV	kilovolt
kW	kilowatt
lb/lbs	pound/pounds
m	meter
min	minute
mph	miles per hour
mrem	millirem
rpm	revolutions per minute
V	volt

ATTACHMENT B SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

This attachment describes the fault trees developed for the subsurface operations. The fault trees are described in relation to each of the major systems or equipment involved in operations, with subsections providing a physical description and brief operational description of the system or equipment. In addition, the specific functions that the system performs to prevent or mitigate initiating events and the conditions required for that function to be successful are also described, together with the system dependencies and interactions. Fault trees and basic events are identified as well.

This attachment is not intended to be a stand-alone analysis. Inputs to the fault tree models are documented in different sections of the report. These include:

- Basic events related to active component failure, the data development is provided in Attachment C and Section 6.3-1.
- Human reliability assessment is documented in Attachment E and Section 6.4.

Fault trees results, including cut sets, mean probabilities and uncertainties, are outputs from SAPHIRE modeling.

B1 TRANSPORT AND EMPLACEMENT VEHICLE — FAULT TREES ANALYSIS

B1.1 REFERENCES

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 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.

B1.1.1 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.

B1.1.2 Not used.

B1.1.3 Not used.

B1.1.4 Not used.

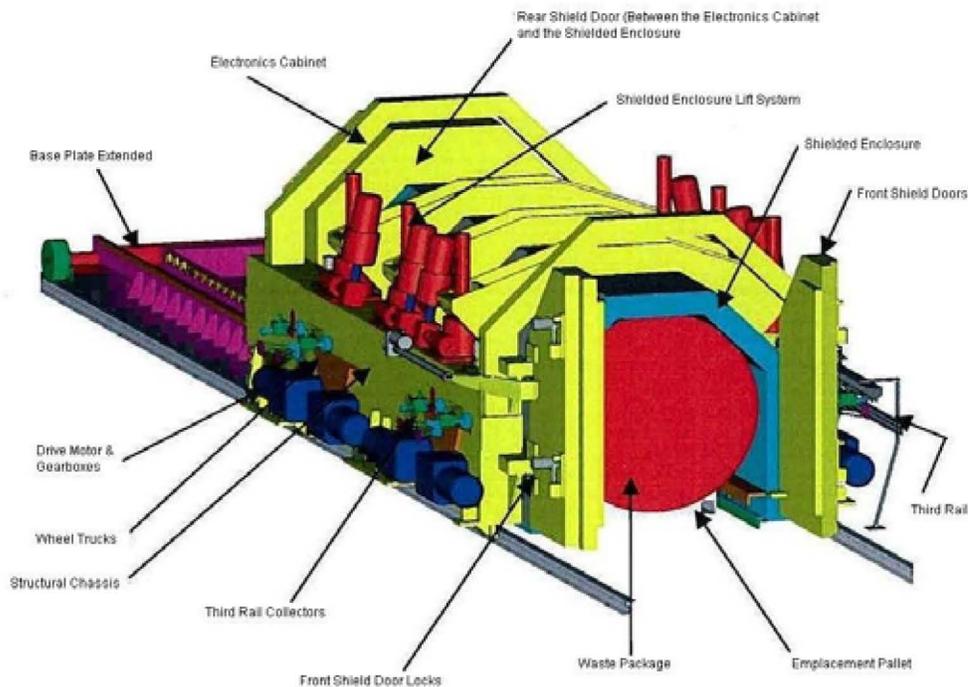
- B1.1.5 Not used.
- B1.1.6 BSC (Bechtel SAIC Company) 2007. *Emplacement and Retrieval Transport and Emplacement Vehicle Mechanical Equipment Envelope*. 800-MJ0-HE00-00101-000-REV B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070918.0041.
- B1.1.7 †BSC 2008. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle*. 000-30R-HE00-00200-000 REV 002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080307.0006.
- B1.1.8 Not used.
- B1.1.9 BSC 2007. *Waste Form Throughputs for Preclosure Safety Analysis*. 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.
- B1.1.10 BSC 2007. *Naval Waste Package Design Report*. 000-00C-DNF0-00800-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071030.0043.
- B1.1.11 BSC 2007. *Project Design Criteria Document*. 000-3DR-MGR0-00100-000-007. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071016.0005.
- B1.1.12 BSC 2007. *TAD Waste Package Configuration*. 000-MW0-DSC0-00101-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070301.0010.
- B1.1.13 †BSC 2007. *Transport and Emplacement Vehicle Envelope Calculation*. 800-MQC-HE00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20070830.0043.
- B1.1.14 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.
- B1.1.15 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 1 of 3)*. 800-M60-HE00-00101-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0041.
- B1.1.16 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 2)*. 800-M60-HE00-00102-000 REV 00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0042.
- B1.1.17 BSC 2007. *WP Transport & Emplacement Vehicle Process & Instrumentation Diagram (Sheet 3)*. 800-M60-HE00-00103-000 REV 00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071128.0043.
- B1.1.18 *CRWMS M&O 1998. *Evaluation of WP Transporter Neutron Shielding Materials*. BCAE00000-01717-0210-00002 REV 000. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990119.0320.

B1.1.19 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.

B1.2 TRANSPORT AND EMPLACEMENT VEHICLE DESCRIPTION

B1.2.1 Overview

The transport and emplacement vehicle (TEV) is an electrically powered, rail-based vehicle (Figure B1.2.-1) that is used to transport a waste package and an emplacement pallet from a surface nuclear facility into the subsurface repository for emplacement (Ref. B1.1.7). The equipment on the TEV is proven and commercially available technology. This technology is primarily from nuclear and heavy industrial crane applications. The TEV travels along a dedicated rail system. The TEV provides radiation shielding such that it is capable of safely transporting radioactive waste packages. The TEV contains multiple mechanical features for the handling of the waste packages. The TEV contains multiple mechanical features for handling of the waste packages. The TEV is remotely controlled and monitored by operators in the Central Control Center Facility (CCCF) using the digital control and management information system (DCMIS) interfacing to an onboard redundant programmable logic controller (PLC) (Ref. B1.1.7, Section 2.1). In most cases, operation of the TEV is under PLC control with only general oversight from the CCCF. However, in some cases, operations that are solely under manual control are performed as needed.



Source: Modified from Ref. B1.1.7

Figure B1.2-1. Illustration of the Transport and Emplacement Vehicle (TEV)

The maximum loaded TEV weighs approximately 300 short tons and has nominal height, width, and length of 11.1 × 15.4 × 29.8 ft respectively (Ref. B1.1.6). The instrumentation of the TEV is described in associated process and instrumentation diagrams ((Ref. B1.1.15), (Ref. B1.1.16), and (Ref. B1.1.17)).

Specific components of the TEV that are considered in fault trees are described in the following sections. The discussions are based on *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (Ref. B1.1.7).

B1.2.2 TEV Drive Wheels

The TEV has eight wheels (four on each side); each is driven by an electric motor. The wheels on one side of the vehicle are double-flanged (Ref. B1.1.7) to limit derailments. The wheels travel on 171 lbs crane rail with a gauge of 11 ft, installed in accordance with the requirements of ASME NOG-1 2004 (Ref. B1.1.1).

B1.2.3 TEV Electronics Cabinet

The PLCs and other TEV electronic controls are housed in a cabinet positioned externally at the rear of the TEV shielded enclosure. This compartment houses a number of sub-enclosures that contain the control and instrumentation components with duplicate equipment to provide defense-in-depth. Each sub-enclosure is totally enclosed to provide fire protection and to provide protection against internal explosions. The overall compartment also contains a heating, ventilation, and air conditioning (HVAC) unit to maintain the operating environment for the control instrumentation, as well as a fire detection system that activate the onboard fire suppression system should fire be detected within this compartment (Ref. B1.1.7).

B1.2.4 TEV Shielding

The TEV enclosure is shielded by approximately 10 in. of a layered metal/polymer composite (Table B1.2-1). The TEV shield enclosure is not airtight, but the shielding prevents a dose rate in excess of 100 mrem/hr at 11.81 in. from the external accessible surfaces, based on design requirements (Ref. B1.1.11, Table 4.10.1-1). The only non-metallic component, the synthetic polymer material NS-4-FR, is a fire-resistant neutron shielding material with a maximum continuous operating temperature limit of 150°C (300°F) (Ref. B1.1.18, Attachment II).

Table B1.2-1. TEV Shielding Configuration

Component	Material	Layer Thickness (inches)
Inner layer	Austenitic stainless steel, SS316L (UNS S31603)	1.5
Gamma shield	Depleted uranium	1.5
Structural steel	Austenitic stainless steel, SS316L (UNS S31603)	0.5
Neutron shield	Synthetic polymer material, NS-4-FR	6.0

Table B1.2-1. TEV Shielding Configuration (Continued)

Component	Material	Layer Thickness (inches)
Outer layer	Stainless steel, SS3316L	0.5
Total shielding thickness		-10.0

NOTE: Material layers start with inner material at the top of the list and progresses to the shielding outer layer at the base of the list.

Source: Modified from Ref. B1.1.18, Table 3

B1.2.5 TEV Lift System

The TEV engages the waste package by raising the entire shielded enclosure. Six screw jacks mounted on the TEV exterior frame lower and raise the enclosure. The front and rear jacks are used in normal operations; two central jacks act as backup units. The jacks for normal operations nominally have a capacity of 100 tons and have 20 in. of travel. The backup units have a nominal capacity of 150 tons. These jacks have the ability to self-lock in the event of drive failure (Ref. B1.1.13, Section 6.5).

B1.2.6 TEV Base Plate

The bottom of the TEV provides radiological shielding through the use of a moveable radiation shield called the base shielding plate (or simply the base plate). The base plate is extended and retracted from below the TEV by a simple gear motor driving a rack and pinion drive system mounted to the chassis on each side of the base plate. As the base plate is extended, the end of the plate is supported by a separate set of wheels at the rear of the TEV (Figure B1.2-1). The base plate is mechanically interlocked with the TEV front shield doors; this interlock prevents the extension of the base plate if the shield doors are closed. In addition, as the plate interfaces with the shielded enclosure, it prevents the enclosure from dropping (Ref. B.1.1.7).

B1.2.7 TEV Shield Doors

To allow the loading and emplacement of waste packages, the TEV has two hinged shield doors at the front of the TEV. Door movement is provided by electro-mechanical linear actuators. The door hinge system consists of four structural features at the front and on both sides of the main TEV chassis. This system provides a solid mounting for four hinge pins or vertical pivot shafts. Additionally, the four door hinge structures house radial and thrust bearings that allow easy and precise radial movement of the doors. The shield doors have the same shielding configuration as the shielded enclosure.

The door hinges are mounted to the structural chassis of the TEV, not to the shielded enclosure. These hinges provide a mechanical interlock that prevents the shielded enclosure from being lowered until the front shield doors are fully opened. In addition, to prevent the inadvertent opening of the shield doors during transit, the TEV incorporates an electro-mechanical interlock for the front shield doors. To allow the doors to open, a special switch is placed along the rail line next to waste handling facilities or in front to emplacement drift turnouts. The switch deactivates an interlock on the TEV upon entry into the emplacement drift or facility to allow the

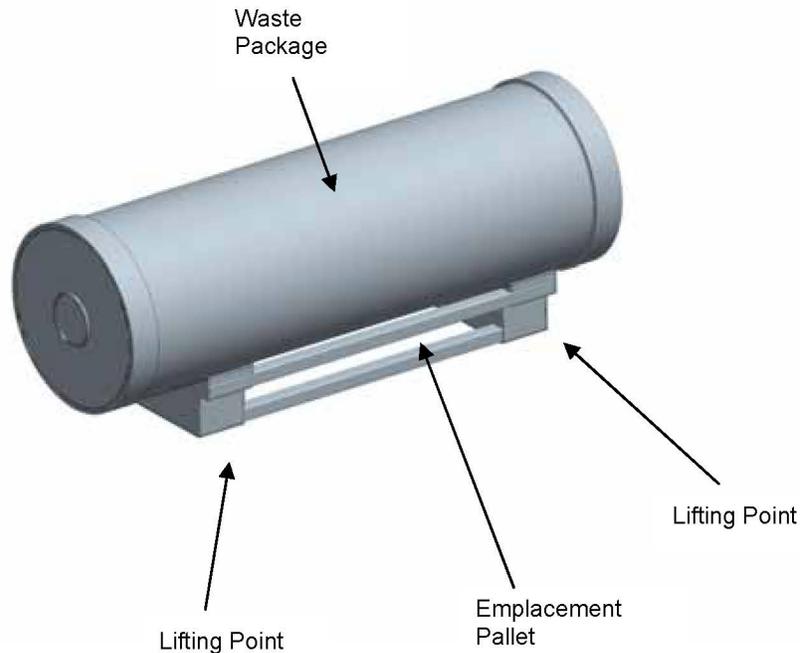
TEV shield doors to open. Conversely, the switch reactivates the interlock as the TEV exits either a facility or emplacement drift (Ref. B.1.1.7).

B1.2.8 TEV Linear Drive Gear Motors

Each of the eight TEV wheels are driven by a 20 hp (15 kW) AC, 480 V, 1,750 rpm motor, featuring integral disc brakes. Each motor is coupled to a flange mounting gear gearbox that has a nominal output speed of seventeen (17) rpm, a torque output of 72,200 lb-in., and a gearbox ratio of one hundred point seven five to one (100.75:1) (Ref.B1.1.7, Section 3.3.4).

B1.2.9 Waste Package

The waste packages emplaced in the subsurface facility each contain canisterized nuclear waste (Figure B1.2-2). A nuclear waste canister (or several canisters) is placed into a cylindrical waste package which is then welded closed within a surface handling facility prior to transport into the subsurface. The waste package provides containment to prevent, or limit, the introduction of a moderator into the disposed waste form and to prevent, or limit, the release of radionuclides into the environment (Ref. B1.1.12).



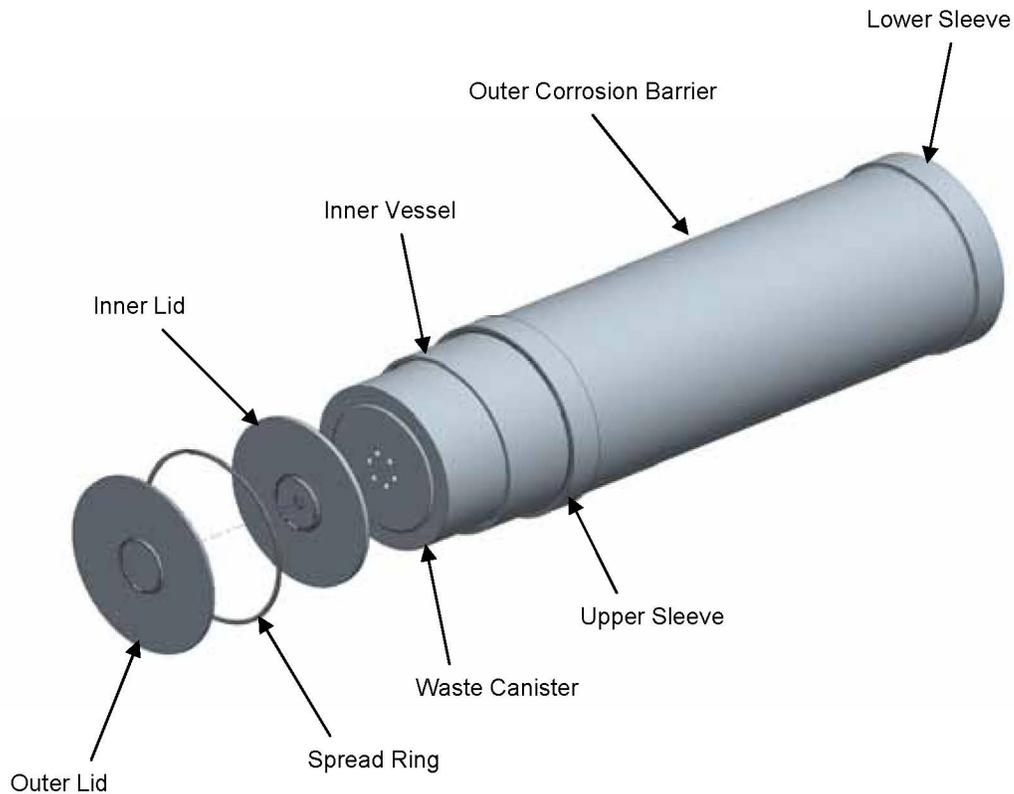
Source: Modified from Ref. B1.1.19, Figure 2

Figure B1.2-2. Illustration of the Waste Package on Pallet

The waste canisters within the waste package contain one of several waste forms, including: (1) commercial spent nuclear fuel (SNF) in a transportation, aging, and disposal canister;

(2) canistered U.S. Department of Energy SNF, including canistered naval SNF; and
(3) canistered high-level radioactive waste from prior commercial and defense fuel-reprocessing operations.

Approximately 12,000 waste packages of various sizes will be emplaced in the repository (Ref. B1.1.9). The general waste package design consists of two concentric cylinders in which the canisters are placed, as illustrated in Figure B1.2-3.



Source: Modified from Ref. B1.1.10, Figure 1

Figure B1.2-3. Illustration of the Waste Package Components

Each waste package rests upon a composite metal frame (pallet) that has been placed on the invert within the emplacement drift. The pallet consists of two V-shaped supports of Alloy 22 (UNS N06022) that are tied together by stainless steel tubes (UNS S31600). The waste package is handled solely using this pallet to prevent damage to the waste package, thereby ensuring that the handling equipment does not make direct contact with the waste package during normal subsurface operations.

B1.2.10 Operations

The TEV operations can be divided into three aspects:

1. Waste package and pallet receipt—the process of loading the waste package into the TEV and moving the TEV out of the facility.
2. Waste package and pallet transportation—the process of the TEV moving the waste package from the surface facility to the entrance of the emplacement drift in the subsurface.
3. Waste package and pallet emplacement—the process of the TEV moving the waste package, on the pallet, into the emplacement drift, placing the waste package and pallet on the invert, and then moving the empty TEV out of the drift.

Block diagrams on TEV operations are provided in *Waste Package Emplacement Mechanical Handling System Block Flow Diagram Level 3* (Ref. B1.1.14).

B1.2.11 Waste Package and Pallet Receipt

The TEV is designed to remotely receive a waste package and emplacement pallet in the Waste Package Loadout Rooms within either a Canister Receipt and Closure Facility (CRCF) or the Initial Handling Facility. A TEV enters the Waste Package Loadout Room in the appropriate facility prior to the staging of a waste package and emplacement pallet within the facility. The TEV passes over a stationary actuating bracket, which closes an important to safety (ITS) switch located on the TEV, thus allowing the TEV shielded enclosure to be opened. The facility shield doors and confinement doors are closed and secured after the TEV has entered the Waste Package Loadout Room.

After ensuring the facility doors are secured, the TEV front shield door locks are unlocked and the front shield doors are opened. The rear shield door is raised to the open position and the base plate is extended. The screw jacks are raised from a lowered, park position, to allow them to engage the lifting features and to support the weight of the shielded enclosure. When this action is completed, the transportation shot bolts are retracted into an unlocked position. The entire shielded enclosure is then lowered to allow for waste package and emplacement pallet receipt. After the shielded enclosure has been lowered, a waste package and emplacement pallet are loaded into the shielded enclosure such that the integral shielded enclosure lifting features are positioned under the emplacement pallet lifting points. Onboard cameras are used to verify the identity of the waste package. The shielded enclosure is then raised to the transport height and the transportation shot bolts are extended back into a locked position. This action allows the screw jacks to be driven back into a lowered park position. The base plate is retracted and the rear shield door is lowered, which mechanically prevents movement of the base plate. The front shield doors are then closed and locked. The facility doors are opened once this operation is complete and the TEV exits the facility Waste Package Loadout Room. Movement of the TEV out of this room (past the stationary actuating bracket) signals an ITS switch on the TEV, which prohibits the unlocking of the front shield doors and the raising of the rear shield door (Ref. B1.1.7).

B1.2.12 Waste Package and Pallet Transportation

The TEV then travels through a rail switch that allows access to the surface main TEV rail line that leads to the North Portal. Prior to arrival at the North Portal, the TEV passes through a series of switches to establish the correct direction of travel. Confirmation of the rail switch positions are verified by operators in the CCCF via the TEV front and rear cameras or by a signal from the DCMIS.

The TEV is stopped at the North Portal for an inspection and remote monitoring check of TEV systems by operators in the CCCF prior to the descent of the North Ramp. After the inspection and monitoring check, the TEV proceeds through the North Portal, down the North Ramp, through the curve at the ramp base, and then continues to the turnout of the selected emplacement drift.

Each emplacement drift turnout has an emplacement bulkhead with emplacement access doors. The configuration of each turnout is comprised of an initial curve, a straight segment, and a transition into an emplacement drift.

As the TEV nears the predetermined emplacement drift turnout rail switch, the operators in the CCCF confirm the correct position of the rail switch. The TEV motion ceases after it has proceeded through the rail switch to the emplacement access door. Onboard positional sensors (linear drive encoders) are then calibrated to confirm the vehicle location and establish a waste package positional datum point. The operators in the CCCF perform this calibration remotely. When calibration is complete, the emplacement access doors are opened, the TEV enters the drift, and the emplacement access doors are closed after the TEV has passed through. The stationary actuating bracket located on the TEV rails inside the emplacement access doors close the ITS switch on the TEV, unlocking the front shield doors and raising the rear shield door (Ref. B1.1.7).

B1.2.13 Waste Package and Pallet Emplacement

The TEV travels at a nominal design speed of 150 ft/min after entering the emplacement drift. The TEV stops at a predetermined position that is relative to a previously emplaced waste package. The locks on the front shield doors are unlocked and opened. The rear shield door is raised to the open position and the base plate is extended.

The TEV then moves forward at a crawl speed, nominally 15 ft/min, to a predetermined position that is relative to a previously emplaced waste package. At this stage the cameras and lights mounted on the top of the TEV are turned on. The forward range detection indicator is also closely monitored during this time; these instruments add confirmation during the positioning of the waste package as the TEV nears a previously emplaced waste package.

The speed of the TEV is then decreased to a slow crawl speed, nominally 1.5 ft/min, until the waste package emplacement position is reached. Onboard cameras and lights are used by operators in the CCCF to confirm the final emplacement position. When the waste package is confirmed to be correctly positioned, screw jacks are raised from a lowered, parked position, to engage the lifting features and support the weight of the shielded enclosure. Transportation shot bolts are retracted into the unlocked position. The shielded enclosure is lowered, placing the

waste package and pallet on the emplacement drift invert structure. Following emplacement, the weight indications for the screw jacks are monitored to confirm that the waste package and emplacement pallet are not being supported.

Once the waste package and emplacement pallet are in place, the TEV moves at a slow crawl speed away from the emplaced waste package and pallet to a predetermined distance. It ceases motion, thereby allowing for proper operation of the front shield doors. The shielded enclosure is raised to the travel height and the transportation shot bolts are extended into the locked position, allowing the screw jacks to be driven into a lowered parked position. The base plate is retracted and the rear shield door is lowered, mechanically preventing movement of the base plate. The front shield doors are closed and locked. When these actions are completed, the TEV returns through the emplacement drift and turnout to the emplacement access doors at the design nominal operating speed of 150 ft/min.

Movement of the TEV past the stationary actuating bracket inside the emplacement access doors signals the ITS switch on the TEV, which disables the unlocking mechanism for the front shield doors and raises the rear shield door. These actions ensure that the shielded enclosure cannot be opened inadvertently. The TEV returns to the surface by reversing the steps taken during travel from the surface to the emplacement location (Ref. B1.1.7).

B1.3 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 B1.3-1 with the following dependencies:

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

Table B1.3-1. 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	—	—	—	Seismic loading can fail third rail electrical power system
Programmable logic controllers	Provide local control of mechanical systems	Failure due to high temperature or radiation	—	—	—
Control enclosure HVAC system	Provides proper environment for logic controllers	Provides proper environment for control system	—	—	—

Table B1.3-1. Dependencies and Interactions Analysis (Continued)

Structures, Systems, and Components	Dependencies and Interactions				
	Functional	Environmental	Spatial	Human	External Events
Linear-drive gear motors for wheels	Provides motive force for vehicle	—	—	—	—
Rail system (including switches)	Constrains and supports vehicle movement	—	Controls vehicle path	—	Seismic loading can fail rail system
Motorized lifting screw jacks (lift system)	Lower and raise shielded enclosure	—	Constrains motion of shielded enclosure	—	—
Front shield doors	Provides shielding for waste package	—	Interlocks with base plate preventing movement while doors are closed	—	—
Base plate	Provides shielding for waste package	—	Interlocks with shield enclosure, preventing lowering of base plate when retracted	—	—
Shielded enclosure	Provides shielding for waste package	—	Engages pallet for waste package transport	—	—
Central control and communication system	Controls operation	—	—	Incorrect instruction	—

HVAC: heating, ventilation, and air conditioning.

Source: Original

B1.4 TRANSPORT AND EMPLACEMENT VEHICLE RELATED FAILURE SCENARIOS

There are 10 separate failure scenarios represented by fault trees associated with the TEV:

1. TEV front shield doors impact a waste package. Fault tree FACILITY-TEV-DOOR
2. TEV collision within facility. Fault tree FACILITY-COLLISION
3. TEV collides with object during emplacement in drift. Fault tree DRIFT-TEV-IMPACT
4. Impact to TEV during transit. Fault tree TRANSIT-IMPACT
5. TEV stops for extended time. Fault tree SHIELD-STOP
6. Inadvertent TEV door opening during transit. Fault tree SHIELD-DOOR

7. Waste package drop in facility. Fault tree FACILITY-DROP
8. Waste package dropped during transit. Fault tree TRANSIT-DROP
9. Waste package drop or dragging in an emplacement drift. Fault tree DRIFT-DRAG
10. TEV collides with emplaced waste package. Fault tree TEV-IMPACTS-WP.

B1.4.1 TEV Door Impacts a Waste Package

B1.4.1.1 Description

The scenario describes the closure of the TEV front shield doors onto, and impacting, a waste package during either loadout or emplacement operations. The occurrence can be realized during loadout operations when the TEV has moved to the loadout station and the waste package is being inserted into the TEV shielded enclosure (prior to the start of TEV operations to engage the waste package pallet). The occurrence can be realized during emplacement operations when the TEV has moved to the emplacement location within the drift and the waste package is being removed from the TEV for emplacement. If one or both of the TEV shield doors is activated during either of these periods, the door or doors will impact laterally on the waste package, pinching the waste package between the doors. Note that the TEV interlock for the shield doors is not activated at this stage to prevent the door operation.

B1.4.1.2 Success Criteria

The success criterion for the scenario is the operation of the TEV front shield doors without spurious movement. The shield door system is not to close onto the waste package during normal operation movement of the waste package under the TEV shielded enclosure.

B1.4.1.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The operational status of the TEV shield doors is clearly displayed for the remote operator on the control panel, including the opening and closing of the shield doors.
- The door actuators on the front shield door are sized so that the force of door closure on a waste package is minimized while assuring proper door operation.
- The waste package is designed to sustain the expected lateral force of door closure on a waste package without breach of the waste package containment.
- Normal periodic maintenance and inspection is performed on the TEV control system to minimize the generation of spurious signals.

B1.4.1.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-TEV-DOOR or DRIFT-DOOR-IMPACT. Identical fault trees are used for both occasions. The top event is the occurrence of the TEV front shield doors closing and impacting the waste package as the package is inserted into the TEV. This top event is realized by either the occurrence of the door closure due to a spurious signal from programmable logic controller or the spurious operation of the door actuators. The generation of the spurious signal from programmable logic controller is represented by a basic event. The spurious operation of a door actuator can be caused by either of the door actuators, as represented by two basic events connected through an OR gate. The fault tree is presented graphically in Figure B1.4-21. (DRIFT-DOOR-IMPACT is shown; FACILITY-TEV-DOOR is identical.)

B1.4.1.5 Basic Events Data

Table B1.4-1 contains a list of basic events used in the fault tree, DRIFT-DOOR-IMPACT, for a waste package impact from the TEV front shield doors.

Table B1.4-1. Basic Event Probabilities for Waste Package Impact from the TEV Front Shield Doors

Name	Description	Calc. Type ^a	Calculated Probability	Mean Failure Probability	Lambda ^a
800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op – TEV doors	3	1.460E-06	0.000E+00	3.650E-07
800-HEE0-ACTDR01-ATP-SPO	Actuator spurious op – TEV door	3	5.360E-06	0.000E+00	1.340E-06
800-HEE0-ACTDR02-ATP-SPO	Actuator spurious op – TEV door	3	5.360E-06	0.000E+00	1.340E-06

NOTE: ^aFor Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

B1.4.1.5.1 Human Failure Events

No basic event is identified as associated with human error involving the closure of the TEV doors.

B1.4.1.5.2 Common-Cause Failures

There are no common-cause failures (CCFs) identified for this model.

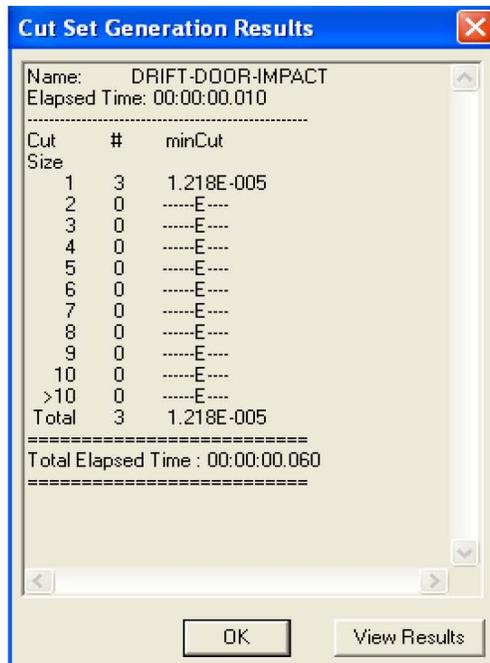
B1.4.1.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Door Impacts a Waste Package” are presented in Figures B1.4-1 and B1.4-2.



Source: Original

Figure B1.4-1. Uncertainty Results for the TEV Doors Impact Waste Package (FACILITY-TEV-DOOR and DRIFT-DOOR-IMPACT) Fault Tree



Source: Original

Figure B1.4-2. Cut Set Generation Results for the (FACILITY-TEV-DOOR and DRIFT-DOOR-IMPACT) Fault Tree

B1.4.1.7 Cut Sets

Table B1.4-2 contains the cut sets for the DRIFT-DOOR-IMPACT fault tree.

Table B1.4-2. DRIFT-DOOR-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
44.01	44.01	5.360E-06	800-HEE0-ACTDR01-ATP-SPO	Actuator spurious op - TEV door	5.360E-06
88.02	44.01	5.360E-06	800-HEE0-ACTDR02-ATP-SPO	Actuator spurious op - TEV door	5.360E-06
100.00	11.99	1.460E-06	800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op - TEV doors	1.460E-06

NOTE: op = operation; PLC = programmable logic control; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B1.4.2 TEV Collision within Facility

B1.4.2.1 Description

The scenario describes the collision of the TEV within the facility. After the TEV engages the waste package and pallet, and closes the shield doors, the TEV moves along the rail system to exit the facility. The scenario involves the collision of the TEV with a facility door or piece of equipment during uncontrolled movement of the TEV during the facility exit. If the facility shield door is impacted, the door system may fail, allowing the door to impact the TEV.

B1.4.2.2 Success Criteria

Success criteria for the scenario is that the TEV moves out of the facility without spurious operations, and when under manual control, that the TEV functions properly. During the normal operations, the TEV is to move in a predictable fashion from the loadout station to outdoors without collision.

B1.4.2.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The facility shield doors are be able to sustain the impact from the TEV such that after an impact from the TEV traveling at full operational speed, the facility shield door is retained in position and does not collapse onto the TEV.
- The operational status of the TEV is clearly displayed for the remote operator and cameras and other sensors are provided to monitor the TEV motion and avoid collision.

B1.4.2.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-COLLISION. Figure B1.4-22 presents the fault tree graphic for this model. The top event is the TEV collides with a structural component of a facility. This top event is realized by either the occurrence an improper command due to human error or by mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to TEV moving in an uncontrolled fashion, caused by either a spurious signal from programmable logic controller or the TEV activation to full operational speed by a switch failure when under manual control. The spurious signal generated by programmable logic controller is represented as a basic event. The switch failure requires the joint occurrence of the TEV being under manual control together with the switch failure when activated. These factors are each represented by as a basic event. The fault tree is presented graphically in Figure B1.4-22.

B1.4.2.5 Basic Events Data

Table B1.4-3 contains a list of basic events used in the fault tree, FACILITY-COLLISION, for a TEV collision within waste handling facility.

Table B1.4-3. Basic Event Probabilities for TEV Collision within Facility

Name	Description	Calc. Type	Calculated Probability	Mean Failure Probability	Lambda
800-HEE0-IMPACT-HFI-NOD	Operator causes uncontrolled movement of TEV	1	1.000E-03	1.000E-03	0.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC spurious op	3	1.460E-06	0.000E+00	3.650E-07
800-TEV1-HNSWCH-SEL-FOH	Speed selector fails – hand switch included	3	1.664E-05	0.000E+00	4.160E-06
TEV-CONTROL-MANUAL	TEV is operating in manual mode	1	1.000E-01	1.000E-01	0.000E+00

NOTE: Calc. = calculation; op= operation; PLC = programmable logic control; TEV = transport and emplacement vehicle.

Source: Original

B1.4.2.5.1 Human Failure Events

One basic event is identified as associated with human error involving the uncontrolled movement of the TEV. The basic event is identified as 800-HEE0-IMPACT-HFI-NOD.

B1.4.2.5.2 Common-Cause Failures

There are no CCFs identified for this model.

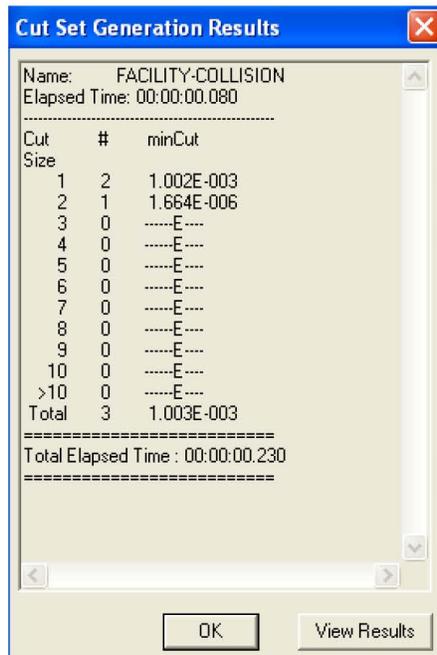
B1.4.2.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Collision within Facility” are presented in Figures B1.4-3 and B1.4-4.



Source: Original

Figure B1.4-3. Uncertainty Results for TEV Collides with Object in a Facility



Source: Original

Figure B1.4-4. Cut Set Results for TEV Collides with Object in a Facility

B1.4.2.7 Cut Sets

Table B1.4-4 contains the cut sets for the FACILITY-COLLISION fault tree.

Table B1.4-4. Facility-Collision Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.69	99.69	1.000E-03	800-HEE0-IMPACTF-HFI-NOD	Operator causes uncontrolled movement of TEV	1.000E-03
99.86	0.17	1.664E-06	800-TEV1-HNDSWCH-SEL-FOH	Speed selector fails – hand switch included	1.664E-05
			TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.000E-01
100.00	0.15	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious op	1.460E-06

NOTE: op = operation; PLC = programmable logic controller; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B1.4.3 TEV Collides With Object during Emplacement

B1.4.3.1 Description

The scenario describes the collision of the TEV entering into, or traveling within, an emplacement drift, as the TEV moves to emplace a waste package. The scenario involves three potential modes of collision: (1) the TEV impacting the emplacement access door when the door is closed or only partially open; (2) the derailment of the TEV leading to the impact with the tunnel wall; and (3) the impact of the TEV moving off the end-of-rail at the end of the emplacement drift.

As the TEV enters the turnout drift leading to an emplacement drift, the TEV must pass through emplacement access doors which restrict access into the emplacement area. The remote operator controls the operation of the emplacement access door and may fail to open the door or close the door before the TEV reaches the threshold, inducing the TEV to collide with either a closed or partially open emplacement access door. (This failure mode is described in more detail in Section B.6.)

The second collision mode can occur if the TEV derails due to mechanical failure of the TEV or of the rail system and collides with the tunnel wall.

The third collision mode can occur if the TEV passes the end-of-rail point. At the end of the turnout switch and at the end of the emplacement drift, the TEV rail terminates, and if the TEV inadvertently travels past this point, it can impact a bulkhead or tunnel wall. The TEV at this point may be under the local control or may be remotely operated. Position sensing of the TEV is based on rotary encoders located on each drive wheel.

B1.4.3.2 Success Criteria

The success criterion for the scenario are that the TEV and the emplacement access door operate without spurious operations, and that if a collision does occur, that the TEV can sustain the impact without damage to the waste package. During normal operations, the TEV moves the waste package into the emplacement drift without incident.

B1.4.3.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The TEV is able to sustain the impact from the emplacement access door such that after an impact from the TEV traveling at full operational speed, the shielding function of the TEV is preserved.
- The operational status of the TEV and the emplacement access door is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the TEV motion and avoid collision.

B1.4.3.4 Fault Tree Model

The fault tree model for the sequence is labeled as DRIFT-TEV-IMPACT. The top event is the occurrence of the TEV colliding with an object as the TEV enters the emplacement drift and as the TEV travels to emplace the waste package. This top event is realized by either the occurrence of three events: (1) the TEV impacts the emplacement access door; (2) the TEV derails; and (3) TEV is commanded to travel past the end of rail; the three events are connected by an OR gate. Figures B1.4-23 through B1.4-25 present the fault tree graphics for this model.

The TEV impacting the emplacement access door can be caused by the premature emplacement access door closure due to human error or mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to the failure of the emplacement access door safety features together with the spurious activation of the door to close, and is represented by an AND gate. The safety feature for the emplacement access door is identified as the actuator motor stopping and opening upon sensing an increased load, and is represented by a basic event. The spurious activation of the access door can be due to either a spurious signal from the programmable logic controller or the failure of the actuator; the frequency of both occurrences is represented basic events.

The logic for the derailment of the TEV is transferred to a subtree, DRIFT-DERAIL. This fault tree represents the frequency of derailment as the combination of two basic events: the frequency of derailment of the TEV per mile and the miles traveled by the TEV.

The TEV is commanded to travel beyond the end-of-rail by either human error or by mechanical failure. Human error is represented by a basic event describing the operator failure. The mechanical failure is attributed to the failure of the rotary encoders on the drive wheels of the TEV (which provide the location of the TEV to the control system) or the generation of a spurious signal to activate the motors when they not move. The failure of the rotary encoders is represented by both the failure of each of the eight encoders (as represented by eight basic events

joined under an AND gate) or the common-cause failure of all encoders. The spurious signal from programmable logic controller of the drive controller is represented as a single basic event. Although rail stops are installed at the end of the rail, they are not modeled in the fault tree because they only affect a couple of, but not all “failure to stop the TEV” scenarios. Not crediting rail stops in the model would yield a conservative result.

B1.4.3.5 Basic Event Data

Table B1.4-5 contains a list of basic events used in the fault tree, DRIFT-TEV-IMPACT, for a TEV colliding with object (e.g., a facility door, another vehicle) during transit.

Table B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit

Name	Description	Calculation Type ^a	Calculated Probability	Mean Failure Probability	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-AXSMO01-MOE-FSO	Motor (electric) fails to shut off	3	7.695E-11	0.000E+00	1.350E-08	5.700E-03
800-HEE0-AXSMO02-MOE-FSO	Motor (electric) fails to shut off	3	7.695E-11	0.000E+00	1.350E-08	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
800-HEE0-DETRAILS-TEV-DER	TEV derails – per mile	1	1.180E-05	1.180E-05	0.000E+00	0.000E+00
TEV-DETRAIL-MILES-DRIFT	Miles traveled by TEV in subsurface	V	4.000E+00	0.000E+00	0.000E+00	0.000E+00
OP-FAILS-ENDOFRAIL	Operator error causes TEV to run over end of rail	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00
800-HEE0-ROTARYC-ECP-CCF	Common cause failure of 8 rotary encoders	C	3.244E-08	1.000E+00	1.600E-08	4.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC spurious op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-ROTARY1-ECP-FOH	TEV position encoder failure -1	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY2-ECP-FOH	TEV position encoder failure -2	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00

Table B1.4-5. Basic Event Probabilities for TEV Collides with Object during Transit (Continued)

Name	Description	Calculation Type ^a	Calculated Probability	Mean Failure Probability	Lambda	Mission Time ^a
800-HEE0-ROTARY3-ECP-FOH	TEV position encoder failure -3	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY4-ECP-FOH	TEV position encoder failure -4	3	7.160E-06	0.0E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY5-ECP-FOH	TEV position encoder failure -5	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY6-ECP-FOH	TEV position encoder failure -6	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY7-ECP-FOH	TEV position encoder failure -7	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00
800-HEE0-ROTARY8-ECP-FOH	TEV position encoder failure -8	3	7.160E-06	0.000E+00	1.79E-06	4.000E+00

NOTE: ^aFor Calculation 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.
op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

B1.4.3.5.1 Human Failure Events

There are two basic events associated with human error: (1) the operator closes the emplacement access door prior to the TEV entering the emplacement drift, identified as 800-HEE0-AXSDR00-HFI-NOD; and (2) the operator error causes the TEV to continue past the end-of-rail, identified as OP-FAILS-ENDOFRAIL.

B1.4.3.5.2 Common-Cause Failures

One CCF is identified in the fault tree, associated with the CCF of the eight rotary encoders on the TEV wheels. The CCF is represented by a basic event and labeled as 800-HEE0-ROTARYC-ECP-FOH.

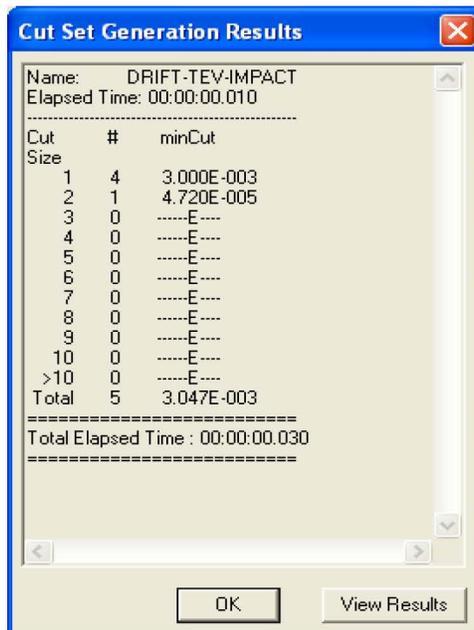
B1.4.3.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set results from SAPHIRE for the fault tree for “TEV Collides with Object during Transit” are presented in Figures B1.4-5 and B1.4-6.



Source: Original

Figure B1.4-5. Uncertainty Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT)



Source: Original

Figure B1.4-6. Cut Set Results for TEV Collides with Object during Transit (DRIFT-TEV-IMPACT)

B1.4.3.7 Cut Sets

Table B1.4-6 contains the cut sets for the DRIFT-TEV-IMPACT fault tree.

Table B1.4-6. DRIFT-TEV-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
65.65	65.65	2.000E-03	800-HEE0-AXSDR00-HFI-NOD	Operator closes emplacement access door on TEV	2.000E-03
98.47	32.82	1.000E-03	OP-FAILS-ENDOFRAIL	Operator error causes TEV to run over end of rail	1.000E-03
100.00	1.55	4.720E-05	800-HEE0-DERAILES-TEV-DER	TEV derails – per mile	1.180E-05
			TEV-DERAIL-MILES-DRIFT	Miles traveled by TEV in subsurface	4.000E+00
100.00	0.05	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller – PLC spurious op	1.460E-06
100.00	0.00	3.243E-08	800-HEE0-ROTARYC-ECP-CCF	Common-cause failure of eight rotary encoders	3.243E-08

NOTE: Op = operation; PLC = programmable logic control; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B1.4.4 Impact to TEV during Transit

B1.4.4.1 Description

The scenario describes the collision of the TEV during transit with an object or vehicle. The scenario involves three potential modes of collision: (1) a worker drives another vehicle into the TEV which is possible at a vehicular crossing on the TEV rail line; (2) the TEV accelerates uncontrolled down the North Ramp (a runaway) leading to the impact with the tunnel wall; and (3) the impact of the TEV with an object along the rail line such as a stalled vehicle at a crossing or another TEV also moving along the rail.

B1.4.4.2 Success Criteria

The success criteria for the scenario are that the TEV operates without spurious operations and avoid impacts. If a collision does occur, then the TEV can sustain the impact without damage to the waste package. During the normal operations, the TEV is to move the waste package along the rail without incident.

B1.4.4.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The TEV is able to sustain the side impact load from a service vehicle such that the TEV does not roll over.

- The operational status (including speed) of all TEV systems is clearly displayed to the remote operator.
- The TEV moving at full operational speed is able to sustain an impact with another TEV moving similarly without breach of the contained waste package.
- The operational status of all TEV rail crossings is clearly displayed to all vehicles. The crossings are closed prior to TEV transit and crossing barriers restrain vehicles from proceeding along the barrier to cross the rail.

B1.4.4.4 Fault Tree Model

The fault tree model for the sequence is labeled as TRANSIT-IMPACT. The top event is an impact to the TEV due to a collision during transit. This top event is realized by one of three possible causes: (1) a worker drives a vehicle into the side of a TEV; (2) a runaway of the TEV occurs on decline such as the North Ramp, leading to an acceleration and derailment of the TEV which results in an impact with a tunnel wall; and (3) a TEV collision with an object along the rail line. Figures B1.4-26 through B1.4-34 presents the fault tree graphics for this model.

The first potential cause of an impact, the collision of a vehicle into the TEV, is represented by a basic event describing the vehicle's operator failure to yield at a crossing, and hitting the TEV. The second potential cause of a runaway can be realized by either by mechanical failure of the drive wheel system by shearing or by failure of TEV subsystems. The mechanical failure by shearing requires the joint occurrence of the TEV traveling on a decline (downward slope) and the mechanical failure leading to the TEV exceeding the design speed (termed, "over speed"). The logic of the mechanical failure is transferred to a subtree, RUNAWAY-MECH, which described later. Similarly, the failure of the TEV subsystems is transferred to a subtree, TEV-NONSHEARING, which is also described later in this section.

The third potential cause of an impact, the collision of the TEV with an object, can be realized by the generation of a spurious signal instructing the onboard controllers to drive the TEV into an object, or by the mechanical failure of the manual control switch. The spurious signal generated within the programmable logic controller system is represented as a basic event. The realization of the mechanical failure of the manual control switch requires the combined occurrence that the TEV is operating in manual mode together with the failure of the speed control switch. The switch failure and the frequency of the TEV in manual mode are represented by basic events.

The fault tree model RUNAWAY-MECH is the subtree representing the mechanical failure of the wheel system due to shearing of the wheel system. Shearing of the wheel system can be caused by either the shearing of all eight of motor's splined shafts (represented by a basic event) or the shearing of the gear system of the motors. The logic of the gearbox failure can be represented by the individual shearing of the gear boxes (and transferred to a subtree, GEARBOX-IND-EVENT) or the common-cause failure of all gearboxes, represented by a basic event. The fault tree model GEARBOX-IND-EVENT is the subtree describing the combined failure of all gear boxes at one time, represented by an OR gate linking eight basic events, one for each motor gearbox.

The fault tree model TEV-NONSHEARING is the subtree that represents a system failure as the initiator of a runaway. The event can be realized by the combined occurrence of the TEV brake system failing to slow the TEV to within design parameters and the control system instructing the TEV motors to over speed. The control system condition can arise due to either of three causes: (1) a switch failure when in manual control; (2) a spurious signal in the programmable logic controllers instructs the TEV to over speed; or (3) a incorrect command instructs the TEV to over speed. The realization of the switch failure when in manual control requires the combined occurrence that the TEV is operating in manual mode together with the failure of the speed control switch. The switch failure and the frequency of the TEV in manual mode are both represented by basic events. A spurious signal in the programmable logic controllers can be induced in either the speed controller or the drive controller and again are both are represented by basic events. The logic for third possible cause is transferred to a subtree, RUNAWAY-SPURIOUS-SIGNAL. The event of the TEV brake system failing to slow the TEV is transferred to MOTOR-SEIZURE.

The fault tree model, RUNAWAY-SPURIOUS-SIGNAL, is the subtree representing the generation of spurious signal to cause the TEV to over speed. The event is represented by the joint occurrence (i.e., connected with an AND gate) of a spurious signal together with the failure of the operator to failure to halt the TEV as it starts to increase in speed. The source of the spurious signal is attributed to either the rotary position encoders or the speed indicators; the logic for these occurrences are transferred to subtree, SPUR-SIGN-ROTECODE and subtree, SPUR-SIGN-DRIVEIND, respectively.

MOTOR-SEIZURE is the subtree describing the failure of any of the eight motors to seize at one time, represented by an OR gate linking eight basic events, one for each motor.

SPUR-SIGN-ROTECODE is the subtree describing combined failure of all of the eight position encoders (i.e., one on each wheel) at one time, represented by an AND gate linking eight basic events, one for each position encored.

SPUR-SIGN-DRIVEIND is the subtree describing the failure of at least of two of the eight over speed sensors (i.e., one on each wheel), represented by a conditioned OR gate linking eight basic events, one for each sensor.

B1.4.4.5 Basic Event Data

Table B1.4-7 contains a list of basic events used in the fault tree, TRANSIT-IMPACT, for a TEV impact from another vehicle during transit.

Table B1.4-7. Basic Event Probabilities for Impact to TEV during Transit

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
800-HEE0-GEARBX1-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX2-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX3-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX4-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX5-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX6-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX7-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBX8-GRB-STH	Gear box stripped	3	3.144E-07	0.000E+00	7.860E-08	4.000E+00
800-HEE0-GEARBXC-GRB-STH	Common cause failure of TEV gearboxes	C	1.542E-08	—	—	—
800-HEE0-MOTOR01-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR02-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR03-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR04-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR05-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR06-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR07-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-MOTOR08-MOE-FSO	Motor (electric) fails to shut off	3	5.400E-08	0.000E+00	1.350E-08	4.000E+00
800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-SIDEIMP-HFI-NOW	Operator drives another vehicle into TEV side	1	3.000E-04	3.000E-04	0.000E+00	0.000E+00
800-HEE0-SPSHF1-AXL-FOH	TEV spline shaft 1 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF2-AXL-FOH	TEV spline shaft 2 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF3-AXL-FOH	TEV spline shaft 3 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF4-AXL-FOH	TEV spline shaft 4 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF51-AXL-FOH	TEV spline shaft 5 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF6-AXL-FOH	TEV spline shaft 6 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF7-AXL-FOH	TEV spline shaft 7 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00
800-HEE0-SPSHF8-AXL-FOH	TEV spline shaft 8 axle failure	3	6.400E-08	0.000E+00	1.600E-08	4.000E+00

Table B1.4-7. Basic Event Probabilities for Impact to TEV during Transit (Continued)

Name	Description	Calc. Type ^a	Calc. Prob.	Fail. Prob.	Lambda	Miss. Time ^a
800-HEE0-SPSHFC-AXL-CCF	Common-cause failure of spline shaft (8 of 8)	C	3.14E-09	—	—	—
800-TEV1-ECP0001-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0002-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0003-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0004-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0005-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0006-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0007-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-ECP0008-ECP-FOH	Position encoder failure	3	7.160E-06	0.000E+00	1.790E-06	4.000E+00
800-TEV1-HNDSWCH-SEL-FOH	Speed selector fails – hand switch included	3	1.664E-05	0.000E+00	4.160E-06	4.000E+00
800-TEV1-SRS0001-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0002-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0003-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0004-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0005-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0006-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0007-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0008-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00

NOTE: ^aFor 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.

PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

B1.4.4.5.1 Human Failure Events

There are two basic events associated with human error: (1) a worker drive another vehicle in the side of the TEV, identified as 800-HEE0-SIDEIMP-HFI-NOD; and (2) the operator failure to halt the TEV using the manual override during over speed, identified as HFE-RUNAWAY-RESPONSE.

B1.4.4.5.2 Common-Cause Failures

Two CCFs are identified in the fault tree. The first is associated with the CCF of the splined shafts of the eight TEV drive wheels. This CCF is represented by a basic event and labeled as 800-HEE0-SPSHFC-AXL-FOH. The second is associated with the CCF of the gearboxes of the eight TEV drive wheels. This CCF is represented by a basic event and labeled as 800-HEE0-GEARBXC-GRB-ST.

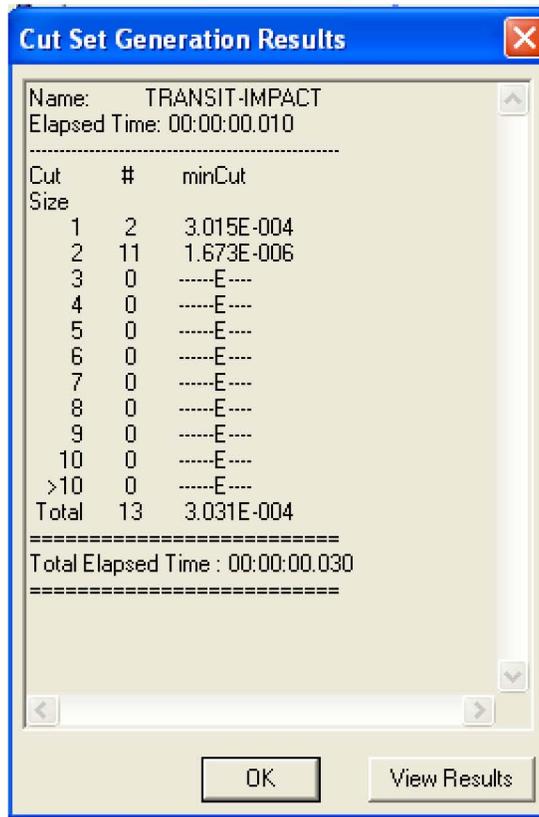
B1.4.4.6 Uncertainty and Cut Set Generation Results

Uncertainty results from SAPHIRE for the fault tree for “Impact to TEV during Transit” are presented in Figure B1.4-7 and the cut set generation results are shown in Figure B1.4-8.

Uncertainty Results			
Name	TRANSIT-IMPACT		
Random Seed	1234	Events	22
Sample Size	10000	Cut Sets	13
Point estimate	3.031E-004		
Mean Value	2.896E-004		
5th Percentile Value	1.380E-005		
Median Value	1.160E-004		
95th Percentile Value	1.067E-003		
Minimum Sample Value	2.338E-006		
Maximum Sample Value	2.669E-002		
Standard Deviation	6.420E-004		
Skewness	1.249E+001		
Kurtosis	3.447E+002		
Elapsed Time	00:00:01.360		
OK			

Source: Original

Figure B1.4-7. Uncertainty Results for Impact to TEV during Transit (TRANSIT-IMPACT)



Source: Original

Figure B1.4-8. Cut Set Generation Results for Impact to TEV during Transit (TRANSIT-IMPACT)

B1.4.4.7 Cut Sets

Table B1.4-8 contains the cut sets for the TRANSIT-IMPACT fault tree.

Table B1.4-8. TRANSIT-IMPACT Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.97	98.97	3.000E-04	800-HEE0-SIDEIMP-HFI-NOW	Operator drives another vehicle into TEV side	3.000E-04
99.52	0.55	1.664E-06	800-TEV1-HNSWCH-SEL-FOH	Speed selector fails – hand switch included	1.664E-05
			TEV-CONTROL-MANUAL	TEV is operating in manual mode	1.000E-01
100.00	0.48	1.460E-06	800-HEE0-PLCLDR1-PLC-SPO	Drive controller - PLC spurious op	1.460E-06
100.00	0.00	7.712E-09	800-HEE0-GEARBXC-GRB-STH	Common-cause failure of TEV gearboxes	1.542E-08
			TEV-DECLINE	TEV on decline	5.000E-01

Table B1.4-8. TRANSIT-IMPACT Cut Sets (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	0.00	1.570E-09	800-HEE0-SPSHFC-AXL-CCF	Common-cause failure of spline shaft (8 of 8)	3.140E-09
			TEV-DECLINE	TEV on decline	5.000E-01
100.00	0.00	7.884E-14	800-HEE0-MOTOR01-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR02-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR03-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR04-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR05-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR06-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR07-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.00	7.884E-14	800-HEE0-MOTOR08-MOE-FSO	Motor (electric) fails to shut off	5.400E-08
			800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06

NOTE: op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

B1.4.5 TEV Stops for an Extended Period of Time

B1.4.5.1 Description

The scenario describes the stopping of the TEV along the rail due to motive failure for an extended period time and the subsequent thermal heating and degradation of the TEV shielding. The scenario can be initiated by a loss of offsite power, a local failure of the third rail power system, the failure of the TEV onboard programmable controllers or the failure of the TEV motors speed sensors.

B1.4.5.2 Success Criteria

The success criterion for the scenario is that the TEV shielding can sustain its shielding function over a prolonged period without operational support.

B1.4.5.3 Design Requirements and Features

The following requirement is identified with respect to this scenario: The TEV shielding is able to sustain the thermal loading for all waste package loadings over an extended period of time without significant degradation of the shielding function.

B1.4.5.4 Fault Tree Model

The fault tree model for the sequence is labeled as SHIELD-STOP. The top event is the occurrence that the TEV is stopped for an extended period of time along the rail without active ventilation of the shielded enclosure. This top event is realized by lack of power and control to the drive motors together with the failure of the TEV fan, which provides air circulation for the shielded enclosure. The fan failure is represented by a basic event. The lack of power and control to the drive motors can be caused by either of four occurrences: (1) failure of the third rail system which powers the TEV; (2) the failure of the programmable logic controllers for the speed control of the TEV motors; (3) the loss of offsite power at the repository; and (4) failure of one of the eight the speed sensors which causes the TEV to stop and shutdown. The first three possible causes are represented by basic events. The fourth cause is represented by an OR gate linking eight basic events, one for the speed sensor on each motor. Figure B1.4-35 presents the fault tree graphic for this model.

B1.4.5.5 Basic Event Data

Table B1.4-9 contains a list of basic events used in the fault tree, SHIELD-STOP, for a TEV stopped for extended time.

Table B1.4-9. Basic Event Probabilities for TEV Stops for Extended Time

Name	Description	Calc. Type ^a	Calculated Probability	Mean Failure Probability	Lambda	Mission Time ^a
800-HEE0-3RDRAIL-THR-BRK	Third rail breaks	3	8.080E-08	0.000E+00	1.101E-08	8.000E+00
800-HEE0-PLCSPD1-PLC-SPO	Speed controller – PLC spurious op	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
LOSP-THERMAL	Loss of offsite power for thermal condition	1	7.940E-06	7.940E-06	0.000E+00	0.000E+00
800-TEV1-SRS0001-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0002-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0003-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0004-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0005-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0006-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0007-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00
800-TEV1-SRS0008-SRS-FOH	Over speed sensor fails	3	8.560E-05	0.000E+00	2.140E-05	4.000E+00

NOTE: ^a For Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; PLC = programmable logic controller.

Source: Original

B1.4.5.5.1 Human Failure Events

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

B1.4.5.5.2 Common-Cause Failures

There are no CCFs identified for this model.

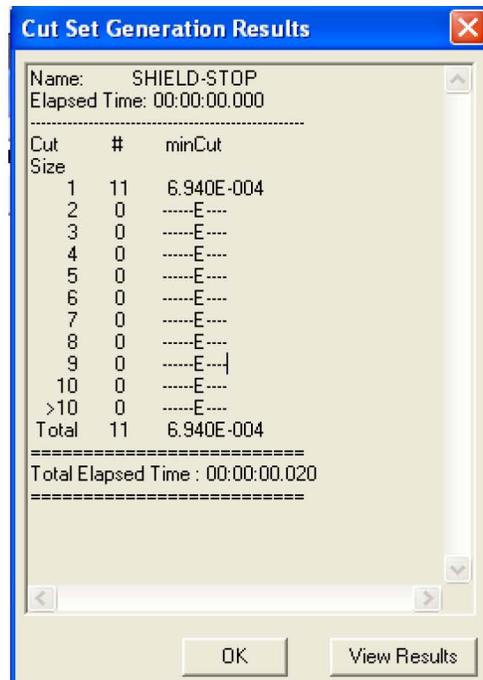
B1.4.5.6 Uncertainty and Cut Set Results

Uncertainty results from SAPHIRE for the fault tree for “TEV Stops for an Extended Period of Time” are presented in Figure B1.4-9 and the cut set generations results are shown in Figure B1.4.10.



Source: Original

Figure B1.4-9. Uncertainty Results for TEV Stops for Extended Time (SHIELD-STOP)



Source: Original

Figure B1.4-10. Cut Set Generation Results for TEV Stops for Extended Time (SHIELD-STOP)

B1.4.5.7 Cut Sets

Table B1.4-10 contains the cut sets for the SHIELD-STOP fault tree.

Table B1.4-10. SHIELD-STOP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
12.33	12.33	8.560E-05	800-TEV1-SRS0002-SRS-FOH	Over speed sensor fails	8.560E-05
24.66	12.33	8.560E-05	800-TEV1-SRS0003-SRS-FOH	Over speed sensor fails	8.560E-05
36.99	12.33	8.560E-05	800-TEV1-SRS0004-SRS-FOH	Over speed sensor fails	8.560E-05
49.32	12.33	8.560E-05	800-TEV1-SRS0005-SRS-FOH	Over speed sensor fails	8.560E-05
61.65	12.33	8.560E-05	800-TEV1-SRS0001-SRS-FOH	Over speed sensor fails	8.560E-05
73.98	12.33	8.560E-05	800-TEV1-SRS0006-SRS-FOH	Over speed sensor fails	8.560E-05
86.31	12.33	8.560E-05	800-TEV1-SRS0007-SRS-FOH	Over speed sensor fails	8.560E-05
98.64	12.33	8.560E-05	800-TEV1-SRS0008-SRS-FOH	Over speed sensor fails	8.560E-05
99.78	1.14	7.940E-06	LOSP-THERMAL	Loss of offsite power for thermal condition	7.940E-06
99.99	0.21	1.460E-06	800-HEE0-PLCSPD1-PLC-SPO	Speed controller - PLC spurious op	1.460E-06
100.00	0.01	8.080E-08	800-HEE0-3RDRAIL-THR-BRK	Third rail breaks	8.080E-08

NOTE: Op = operation; PLC = programmable logic controller; Prob. = probability.

Source: Original

B1.4.6 Inadvertent TEV Door Opening during Transit

B1.4.6.1 Description

The scenario describes the opening of the TEV front shield doors as the TEV exits a waste handling facility. The scenario can be initiated by a spurious signal or by a failure of the front shield door actuators. The interlock to prevent these shield doors has not been activated at this stage.

B1.4.6.2 Success Criteria

The success criterion for the scenario is that the TEV operates without spurious operations and subsystem failures.

B1.4.6.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- Operational requirements require workers to be at a distance from the facility shield doors as a loaded TEV exits a facility.
- Both visual and audio alarms are used to alert workers of the movement of the TEV along the rail line as the TEV exits a facility.

B1.4.6.4 Fault Tree Model

The fault tree model for the sequence is labeled as SHIELD-DOOR. The top event is the occurrence of the TEV shield doors opening during transit. The top event is realized by either (1) an interlock failure together with human error, or (2) a mechanical-based failure of the system. For the human-error initiated event, the opening of the door initiated erroneously by an operator command must be accompanied by the failure of the TEV interlock system (which is to prevent the front shield doors opening in transit) to be realized. This logic is represented by two basic events (representing the operator command and the interlock failure) joined by an AND gate. The mechanical-based failure also incorporates the failure of the interlock system (again represented by a basic event) together with the opening of the door initiated by a spurious signal or by spurious movement of the TEV front shield door actuators. The spurious signal is (represented by basic event) joined by an OR gate to the spurious movement of the door actuators, which is represented as an OR joining basic failure events for each actuator. Figure B1.4-36 presents the fault tree graphic for this model.

B1.4.6.5 Basic Event Data

Table B1.4-11 contains a list of basic events used in the fault tree, SHIELD-DOOR, for the inadvertent TEV door opening during transit.

Table B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit

Name	Description	Calc. Type ^a	Calculated Probability	Mean Failure Probability	Lambda	Mission Time ^a
800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op _ TEV doors	3	1.460E-06	0.000E+00	3.650E-07	4.000E+00
800-HEE0-ACTDR01-ATP-SPO	Actuator spurious op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-ACTDR02-ATP-SPO	Actuator spurious op – TEV door	3	5.360E-06	0.000E+00	1.340E-06	4.000E+00
800-HEE0-INTRLCK-IEL-FOH	Interlock failure-TEV door interlock	3	1.372E-04	0.000E+00	3.430E-05	4.000E+00

Table B1.4-11. Basic Event Probabilities for Inadvertent TEV Door Opening during Transit (Continued)

Name	Description	Calc. Type ^a	Calculated Probability	Mean Failure Probability	Lambda	Mission Time ^a
800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1	1.000E-03	1.000E-03	0.000E+00	0.000E+00

NOTE: ^aFor Calc. Type 3 with a mission time of 0, SAPHIRE performs the quantification using the system mission time.
Calc. = calculation; op = operation; PLC = programmable logic controller; TEV = transport and emplacement vehicle.

Source: Original

B1.4.6.5.1 Human Failure Events

One basic event is identified as associated with human error of the operator opening the TEV shield doors. The basic event is identified as 800-HEE0-TEVDOOR-HFI-NOD.

B1.4.6.5.2 Common-Cause Failures

There are no CCFs identified for this model.

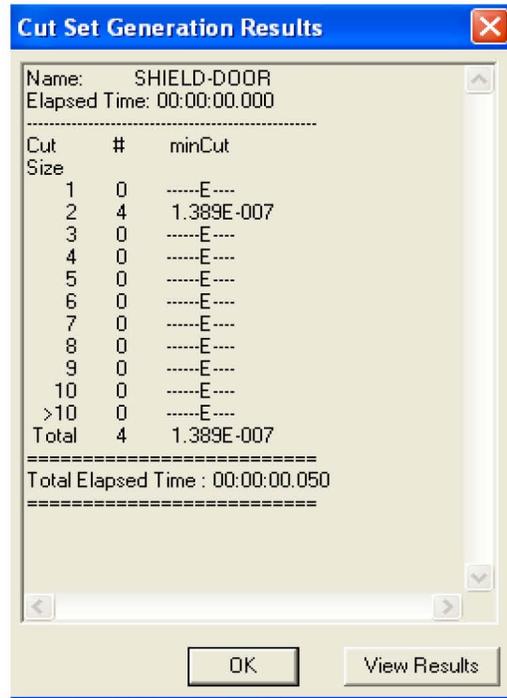
B1.4.6.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for an “Inadvertent TEV Door Opening during Transit” are presented in Figures B1.4-11 and B1.4-12.



Source: Original

Figure B1.4-11. Uncertainty Results for TEV Exits Facility with Open Shield Doors (SHIELD DOOR)



Source: Original

Figure B1.4-12. Cut Sets for TEV Exits Facility with Open Shield Doors (SHIELD DOOR)

B1.4.6.7 Cut Sets

Table B1.4-12 contains the cut sets for the SHIELD-DOOR fault tree.

Table B1.4-12. SHIELD-DOOR Cut Sets

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
98.80	98.80	1.372E-07	800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
			800-HEE0-TEVDOOR-HFI-NOD	Operator attempts to open door erroneously	1.000E-03
99.33	0.53	7.353E-10	800-HEE0-ACTDR01-ATP-SPO	Actuator spurious op - TEV door	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04
99.86	0.53	7.353E-10	800-HEE0-ACTDR02-ATP-SPO	Actuator spurious op - TEV door	5.360E-06
			800-HEE0-INTRLCK-IEL-FOH	Interlock Failure - TEV door interlock	1.372E-04

Table B1.4-12. SHIELD-DOOR Cut Sets (Continued)

% Total	% Cut set	Prob./ Frequency	Basic Event	Description	Event Prob.
100.00	0.14	2.003E-10	800-HEE0-INTRLCK-IEL-FOH	Interlock failure - TEV door interlock	1.372E-04
			800-HEE0-PLCDOOR-PLC-SPO	PLC spurious op - TEV doors	1.460E-06

NOTE: op = operation; PLC = programmable logic controllers; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B1.4.7 Waste Package Drop in Facility

B1.4.7.1 Description

The scenario describes the drop of a waste package within a facility during the loadout operation. After the waste package has been placed under the TEV at the loadout dock, the TEV shielded enclosure raises the waste package to allow the retraction of the base plate. At this point, the lift system of screw jacks or the lifting features on the shielded enclosure can fail, allowing the drop of the waste package to the dock.

B1.4.7.2 Success Criteria

The success criteria for the scenario are that the TEV operates without spurious operations and without structural or system failures.

B1.4.7.3 Design Requirements and Features

The following requirement is identified with respect to this scenario: The operational status of the TEV is clearly displayed for the remote operator and cameras as well as other sensors are provided to monitor the status of the TEV and the waste package.

B1.4.7.4 Fault Tree Model

The fault tree model for the sequence is labeled as FACILITY-DROP. The top event is the drop of a waste package by the TEV during the loadout operations within a waste handling facility. This top event is realized by either the failure of the lift system (jack failure) or the mechanical failure of the lift features holding the pallet and waste package configuration. Figure B1.4-37 presents the fault tree graphic for this model.

The lift system can fail if two of the primary jacks fail as represented by the failure of the individual jacks joined by a conditional OR gate. For the waste package to be dropped, a minimum of two of the primary jacks must fail (at either end of the TEV).

The lift features can also fail, allowing the waste package to drop. Again, for the waste package to be dropped, a minimum of two of the four lift features must fail. The failure of the lift features is represented by the failure of the lift features joined by a conditional OR gate requiring the failure of two of the four features for realization.

B1.4.7.5 Basic Event Data

Table B1.4-13 contains a list of basic events used in the fault tree, FACILITY-DROP, for the drop of a waste package in a waste handling facility.

Table B1.4-13. Basic Event Probabilities for Waste Package Drop in Facility

Name	Description	Calc. Type ^a	Calculated Probability	Mean Failure Probability	Lambda	Mission Time ^a
800-HEE0-JACK000-SJK-CCF	Screw jack CCF failure	C	1.216E-06	—	—	—
800-HEE0-JACK001-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK002-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK003-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-JACK004-JCK-FOH	TEV screw jack failure	3	3.256E-05	0.000E+00	8.100E-06	4.000E+00
800-HEE0-LIFT000-LRG-CCF	CCF failure of at least two lifting rig/hooks	C	1.113E-07	—	—	—
800-HEE0-LIFT001-LRG-FOH	Lifting rig or hook failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT002-LRG-FOH	Lifting rig or hook failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT003-LRG-FOH	Lifting rig or hook failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00
800-HEE0-LIFT004-LRG-FOH	Lifting rig or hook failure	3	2.980E-06	0.000E+00	7.450E-07	4.000E+00

NOTE: ^aFor 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.
CCF = common-cause failure; TEV = transport and emplacement vehicle.

Source: Original

B1.4.7.5.1 Human Failure Events

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

B1.4.7.5.2 Common-Cause Failures

There are two CCFs identified for this model. One (800-HEE0-JACK000-SJK-CCF) is the CCF of the TEV screw jacks to hold the load during transit and the second (800-HEE0-LIFT001-LRG-FOH) is the failure of at least two lifting rig/hooks. Both CCFs use the operational alpha factors as described in Attachment C Section C3 for a two of four CCF events.

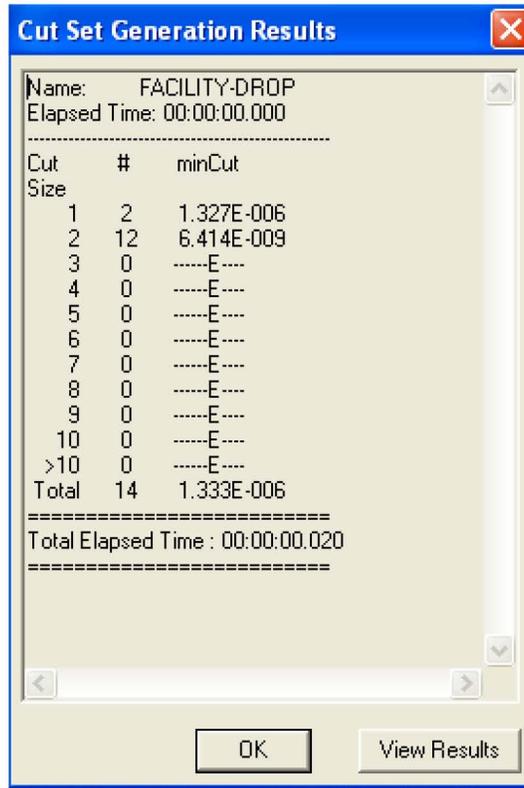
B1.4.7.6 Uncertainty and Cut Set Generation Results

Uncertainty and cut set generation results from SAPHIRE for the fault tree for “Waste Package Drop in Facility” are presented in Figures B1.4-13 and B1.4-14.

Uncertainty Results			
Name	FACILITY-DROP		
Random Seed	1234	Events	14
Sample Size	10000	Cut Sets	14
Point estimate	1.333E-006		
Mean Value	1.339E-006		
5th Percentile Value	3.033E-008		
Median Value	4.358E-007		
95th Percentile Value	5.677E-006		
Minimum Sample Value	1.056E-009		
Maximum Sample Value	4.889E-005		
Standard Deviation	2.552E-006		
Skewness	5.435E+000		
Kurtosis	5.195E+001		
Elapsed Time	00:00:01.220		
<input type="button" value="OK"/>			

Source: Original

Figure B1.4-13. Uncertainty Results for Package Drop During Loading in Facility (FACILITY-DROP)



Source: Original

Figure B1.4-14. Cut Set Generation Results for Package Drop during Loading in Facility (FACILITY-DROP)

B1.4.7.7 Cut Sets

Table B1.4-14 contains the cut sets for the FACILITY-DROP fault tree.

Table B1.4-14. FACILITY-DROP Cut Sets

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
91.17	91.17	1.216E-06	800-HEE0-JACK000-SJK-CCF	Screw jack CCF failure	1.216E-06
99.51	8.34	1.113E-07	800-HEE0-LIFT000-LRG-CCF	CCF failure of at least two lifting rig/hooks	1.113E-07
99.59	0.08	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
99.67	0.08	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
99.75	0.08	1.060E-09	800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
99.83	0.08	1.060E-09	800-HEE0-JACK001-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05
99.91	0.08	1.060E-09	800-HEE0-JACK002-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05

Table B1.4-14. FACILITY-DROP Cut Sets (Continued)

% Total	% Cut Set	Prob./ Frequency	Basic Event	Description	Event Prob.
99.99	0.08	1.060E-09	800-HEE0-JACK003-SJK-FOH	TEV screw jack failure	3.256E-05
			800-HEE0-JACK004-SJK-FOH	TEV screw jack failure	3.256E-05
99.99	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT002-LRG-FOH	Lifting rig or hook failure	2.980E-06
99.99	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting rig or hook failure	2.980E-06
99.99	0.00	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT003-LRG-FOH	Lifting rig or hook failure	2.980E-06
99.99	0.00	8.880E-12	800-HEE0-LIFT001-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting rig or hook failure	2.980E-06
99.99	0.00	8.880E-12	800-HEE0-LIFT002-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting rig or hook failure	2.980E-06
99.99	0.00	8.880E-12	800-HEE0-LIFT003-LRG-FOH	Lifting rig or hook failure	2.980E-06
			800-HEE0-LIFT004-LRG-FOH	Lifting rig or hook failure	2.980E-06

NOTE: CCF = common-cause failure; Prob. = probability; TEV = transport and emplacement vehicle.

Source: Original

B1.4.8 Waste Package Drop during Transit

B1.4.8.1 Description

The scenario describes the drop of a waste package by the TEV during transit. To allow for a fall of the waste package to the invert during transit, the TEV base plate must be first extended from underneath the TEV. To allow this extension, the TEV front shield doors must open to disengage the mechanical interlock on base plate movement. However for the TEV shield doors to open, the electro-mechanical interlock on the shield doors must fail as well. [Note: as the TEV exits a facility, an interlock is activated to restrict the opening of the front shield doors.] After the base plate is extended, the lift system of screw jacks or the lifting features on the shielded enclosure fail, allowing the drop of the waste package to the dock.

B1.4.8.2 Success Criteria

The success criterion for the scenario is that the TEV operates without structural or system failures.

B1.4.8.3 Design Requirements and Features

The following requirements are identified with respect to this scenario:

- The TEV has an electro-mechanical interlock to prevent the front shield doors to open when the TEV is in transit outside of a facility or an emplacement drift.