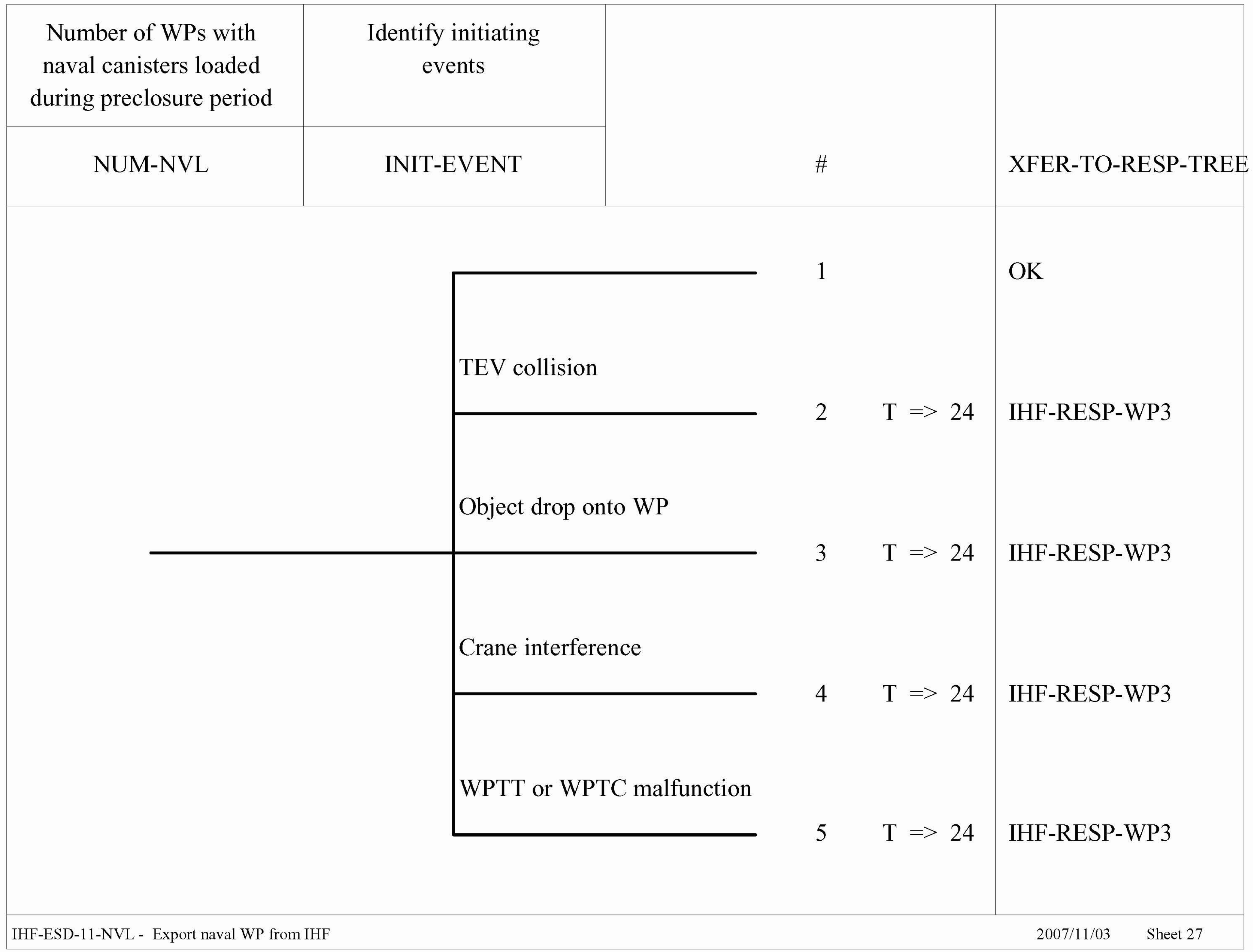
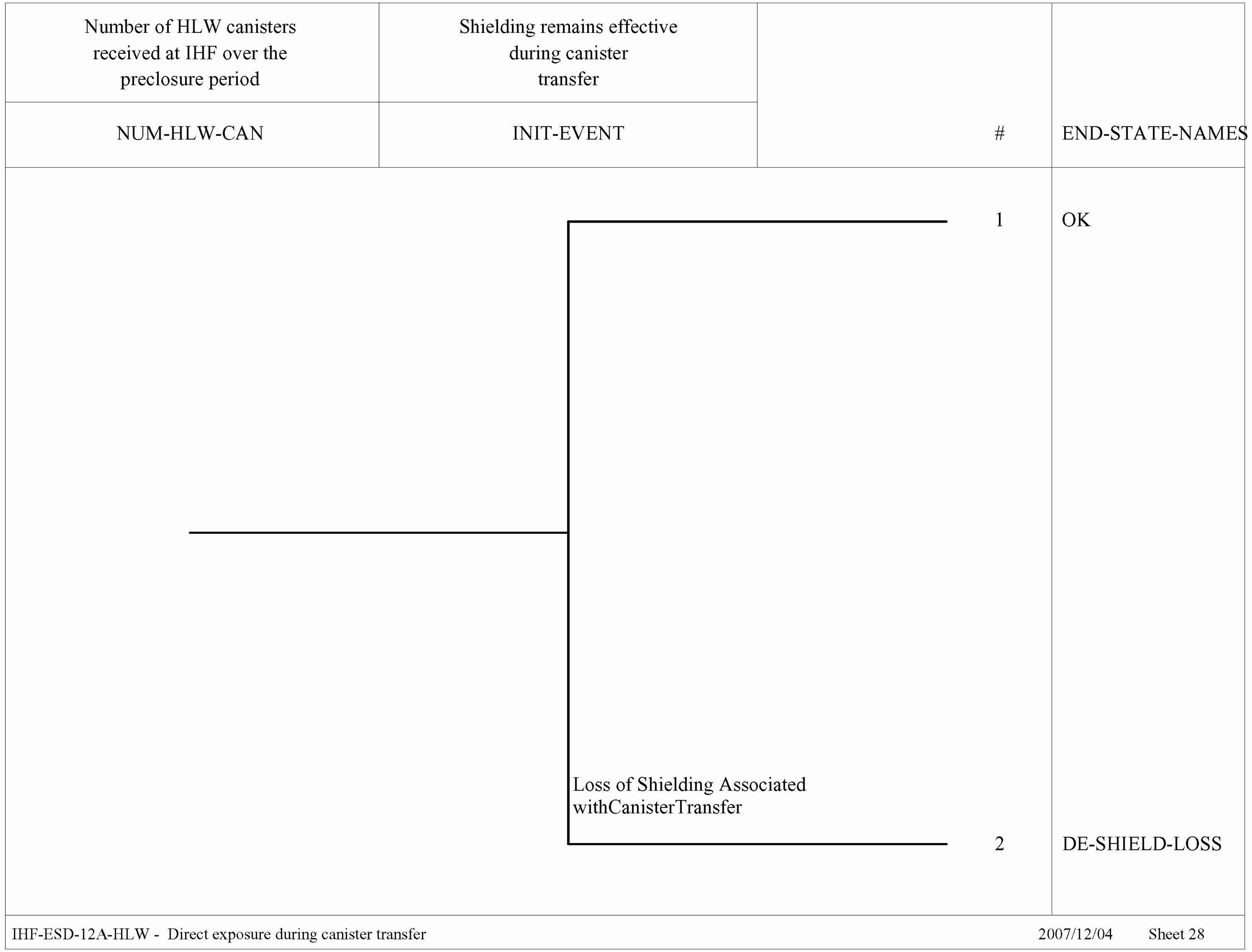


Source: Original

Figure A5-28. Event Tree IHF-ESD-11-NVL – Export Naval WP from IHF

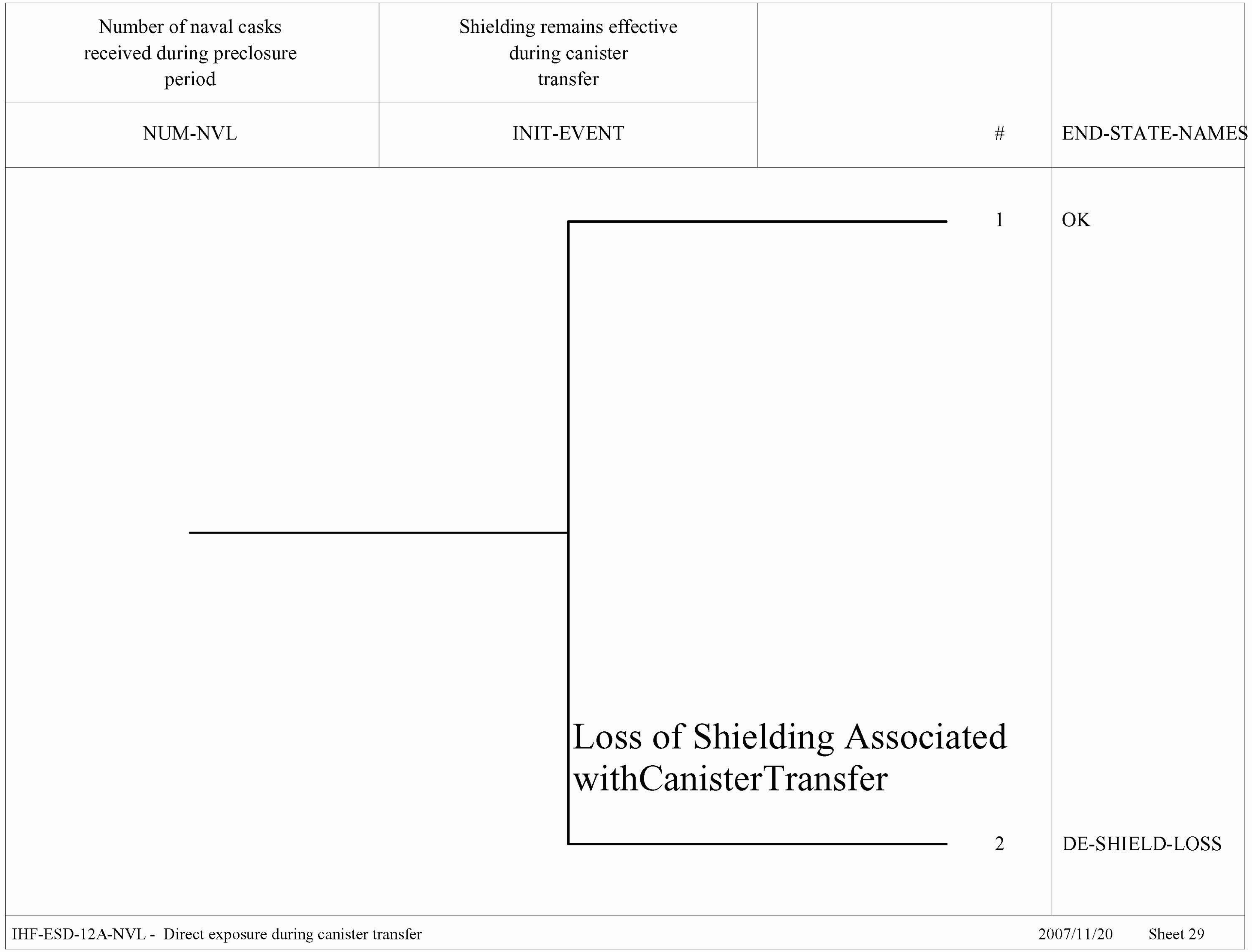
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-29. Event Tree IHF-ESD-12A-HLW – Direct Exposure during Canister Transfer

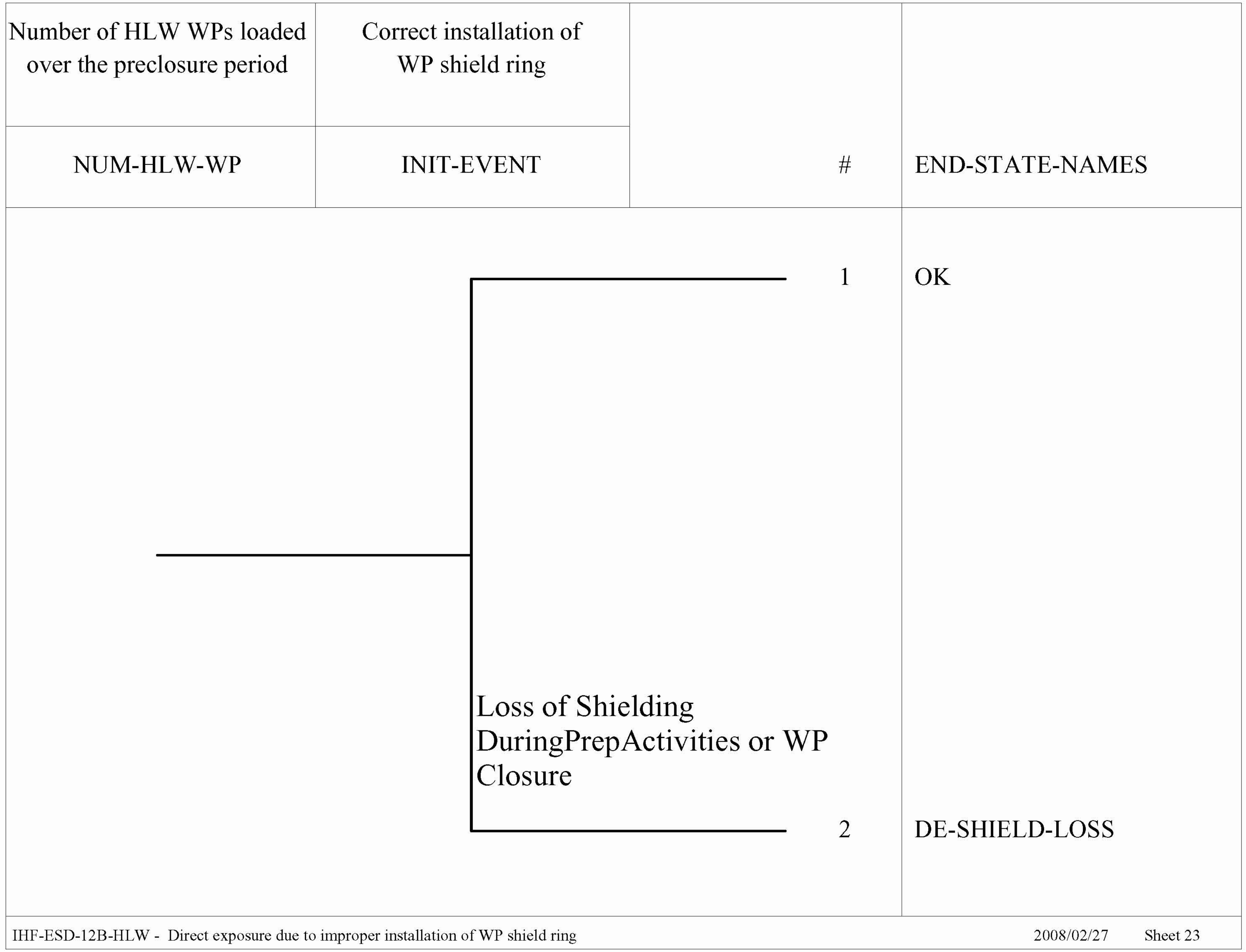
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-30. Event Tree IHF-ESD-12A-NVL – Direct Exposure during Canister Transfer

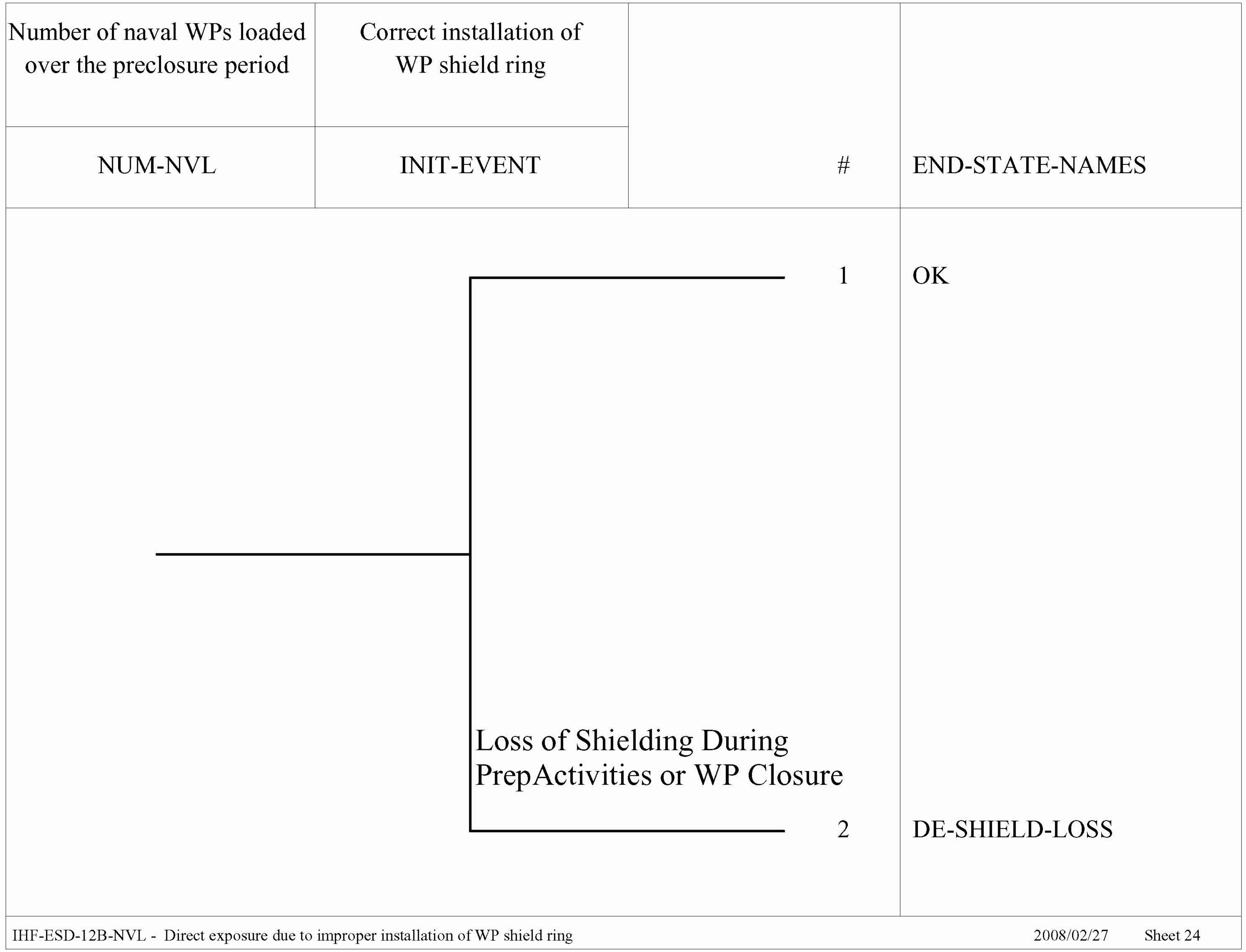
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-31. Event Tree IHF-ESD-12B-HLW – Direct Exposure due to Improper Installation of Shield Ring

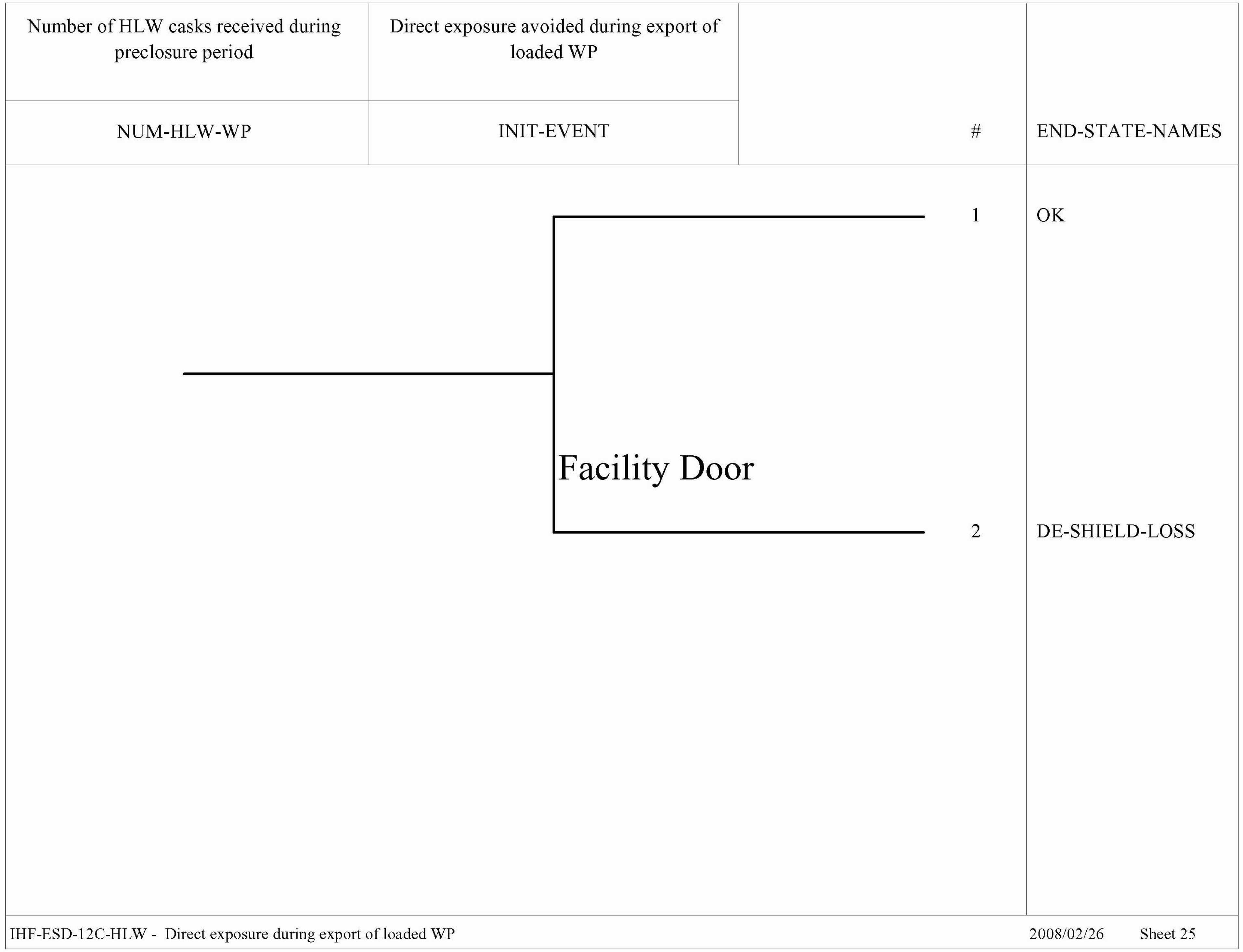
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-32. Event Tree IHF-ESD-12B-NVL – Direct Exposure due to Improper Installation of Shield Ring

INTENTIONALLY LEFT BLANK



Source: Original

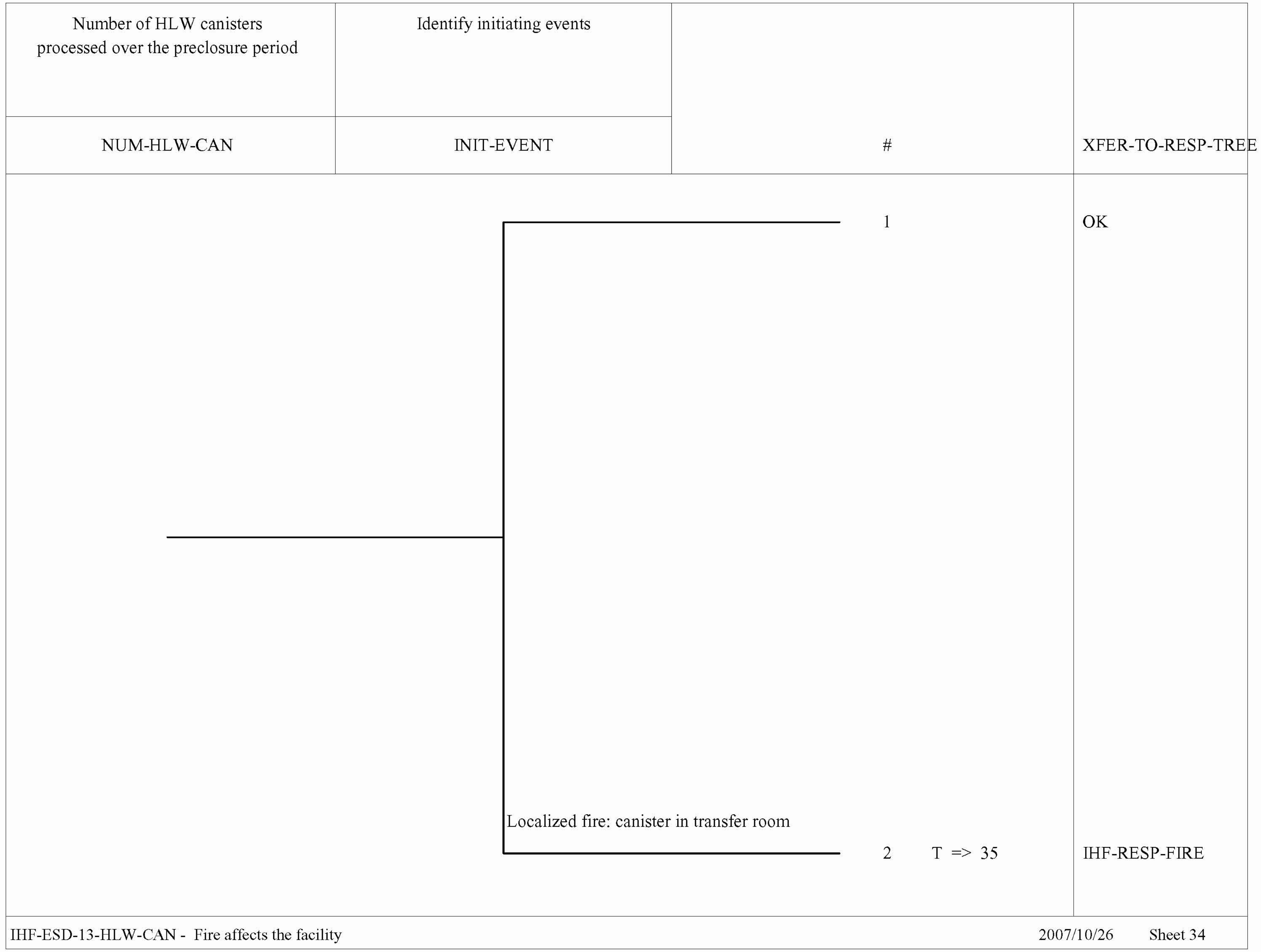
Figure A5-33. Event Tree IHF-ESD-12C-HLW – Direct Exposure during Export of Loaded WP

INTENTIONALLY LEFT BLANK

Source: Original

Figure A5-34. Event Tree IHF-ESD-12C-NVL – Direct Exposure during Export of Loaded WP

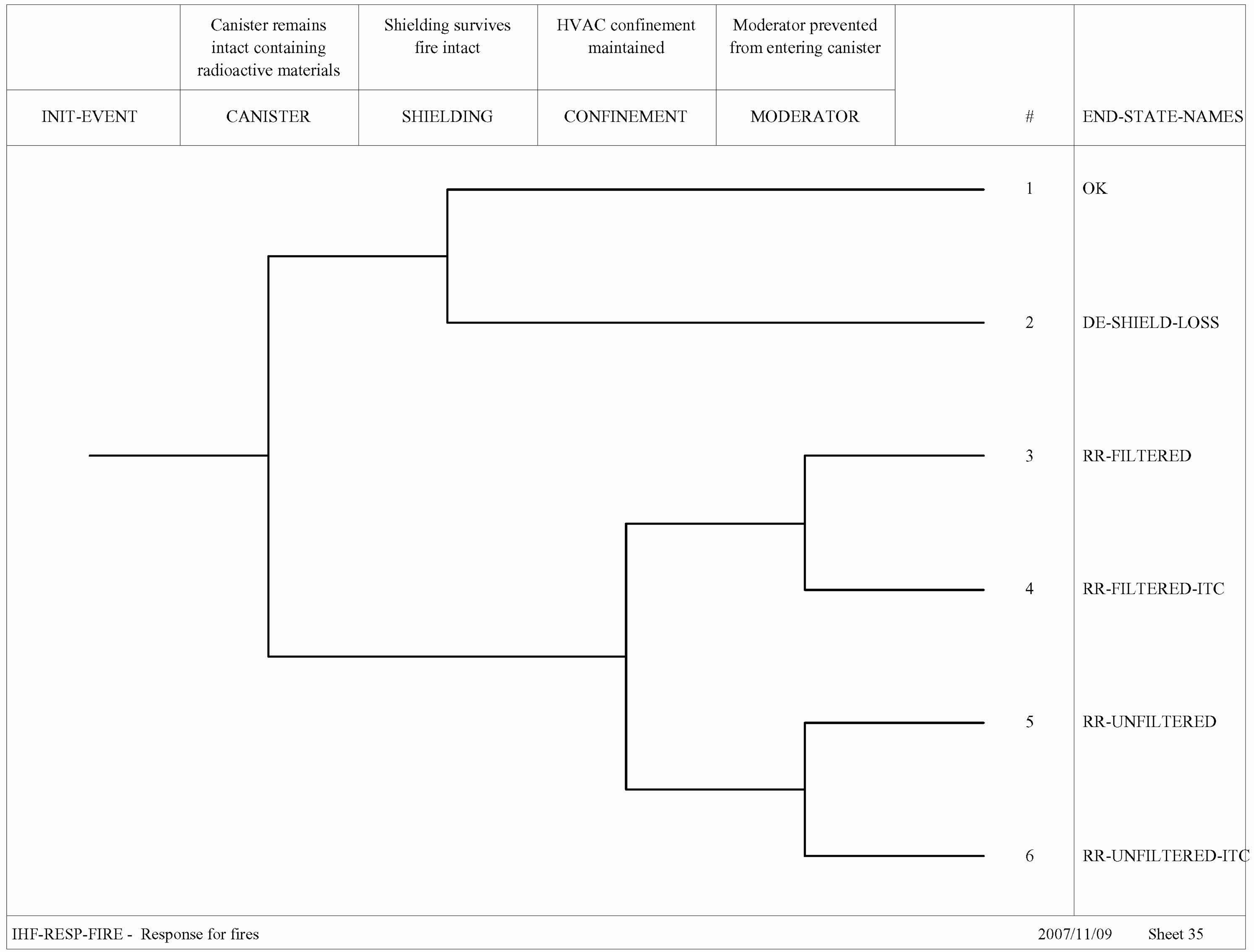
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-35. Event Tree IHF-ESD-13-HLW-CAN – Fire Affects the Facility

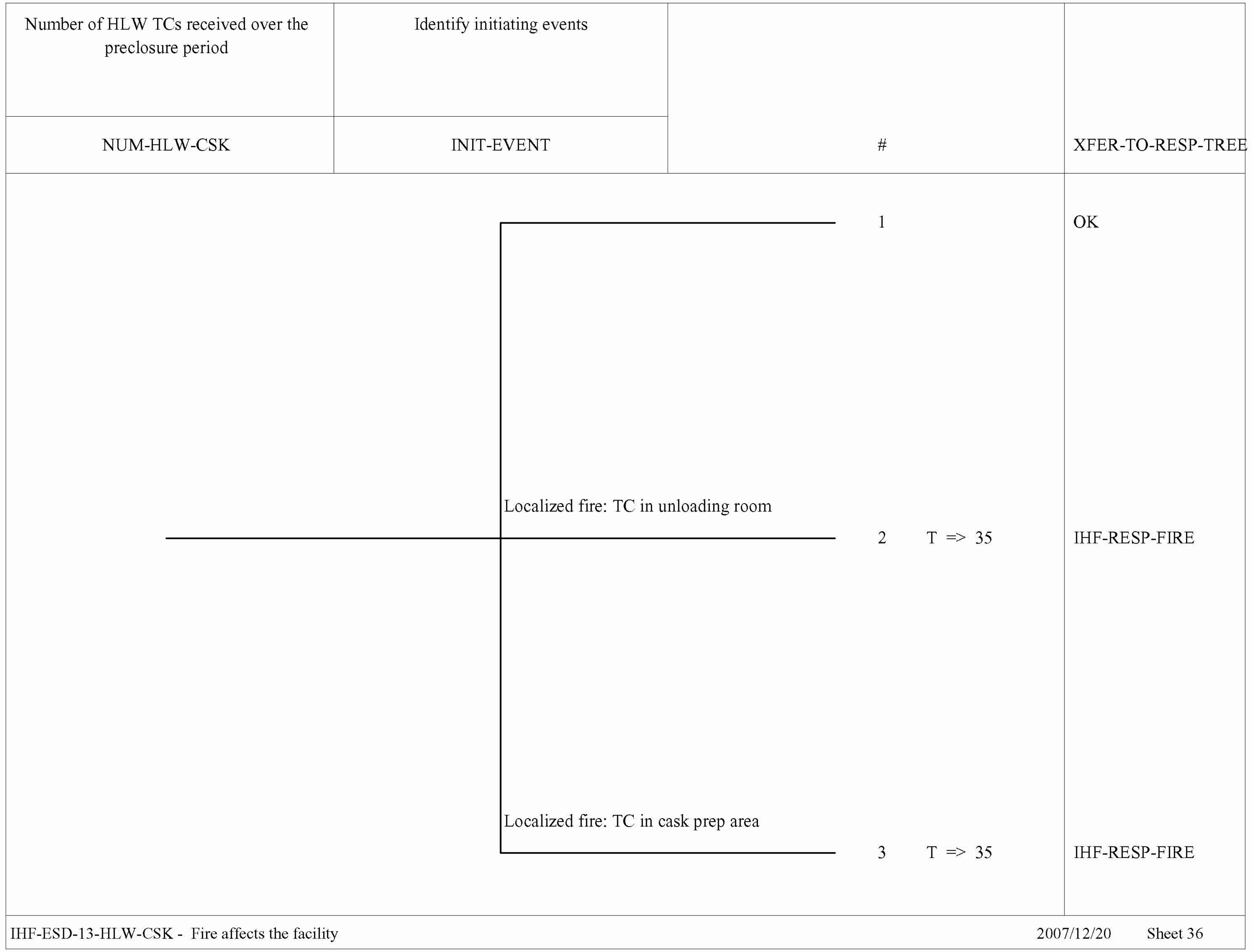
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-36. Event Tree IHF-RESP-FIRE – Response for Fires

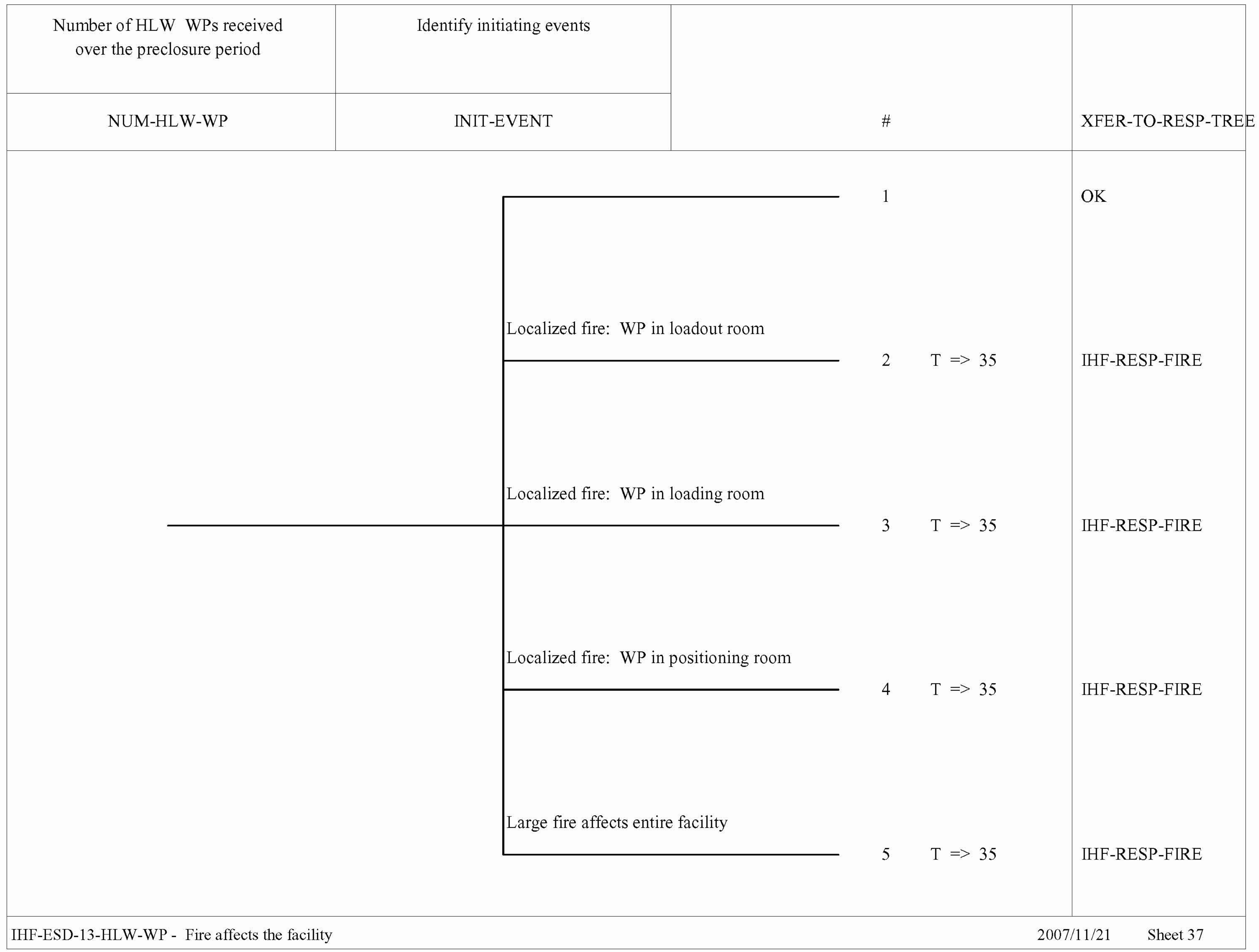
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-37. Event Tree IHF-ESD-13-HLW-CSK –Fire Affects the Facility

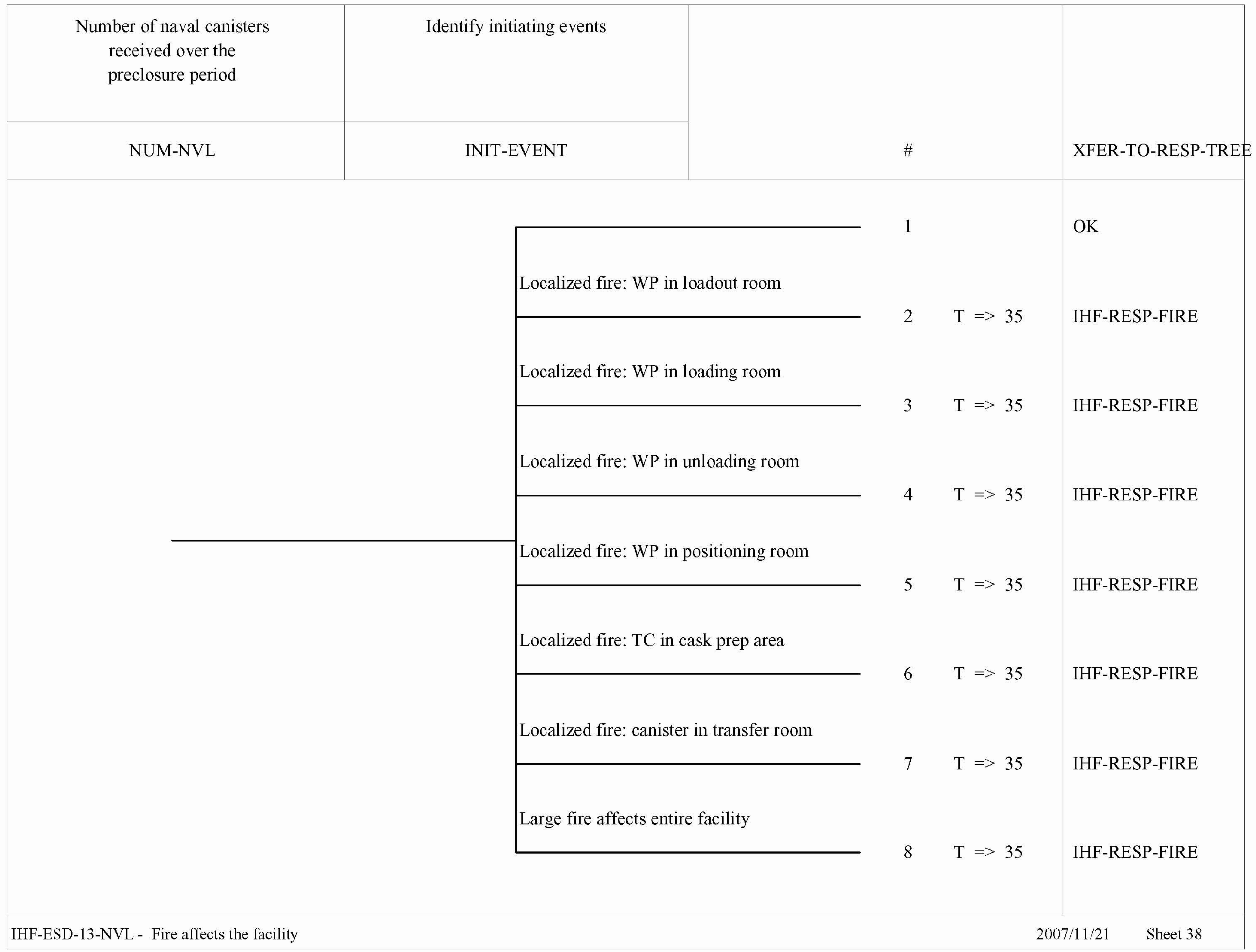
INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-38. Event Tree IHF-ESD-13-HLW-WP –Fire Affects the Facility

INTENTIONALLY LEFT BLANK



Source: Original

Figure A5-39. Event Tree IHF-ESD-13-NVL –
Fire Affects the Facility

INTENTIONALLY LEFT BLANK

ATTACHMENT B
SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

INTENTIONALLY LEFT BLANK

CONTENTS

Page

INTENTIONALLY LEFT BLANK

FIGURES

Page

FIGURES (Continued)

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

FIGURES (Continued)

Page

TABLES

TABLES (Continued)

TABLES (Continued)

Page

INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

Acronyms

AAR	Association of American Railroads
ASD	adjustable speed drive
CCF	common-cause failure
CRCF	Canister Receipt and Closure Facility
CTT	cask transfer trolley
CTM	canister transfer machine
ESD	event sequence diagram
FRA	Federal Railroad Administration
HLW	high-level radioactive waste
IHF	Initial Handling Facility
ITS	important to safety
NHTSA	National Highway Traffic Safety Administration
PLC	programmable logic controller
RF	Receipt Facility
RHS	remote handling system
SNF	spent nuclear fuel
SPM	site prime mover
SPMRC	site prime mover railcar
SPMTT	site prime mover truck trailer
TEV	transport and emplacement vehicle
WHF	Wet Handling Facility
WPTT	waste package transfer trolley

Abbreviations

AC	alternating current
DC	direct current
ft/min	feet per minute

INTENTIONALLY LEFT BLANK

SYSTEM/PIVOTAL EVENT ANALYSIS – FAULT TREES

This attachment presents system and pivotal event fault trees that are used in the event trees described in Attachment A. The system fault trees are presented and described in Sections B1 through B5, on a system basis. The pivotal event fault trees are presented in Section B6. For the most part, the pivotal events link to a basic event and these are presented in tables. In a few cases, the assignment is not straightforward and a supplemental fault tree provides a link to the system fault tree or basic event level. These supplemental fault trees are presented and described.

B1 SITE PRIME MOVER ANALYSIS – FAULT TREES

B1.1 REFERENCES

Design Inputs

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

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

B1.1.1 *AAR S-2043. 2003. *Performance Specification for Trains Used to Carry High-Level Radioactive Material.* Washington, D.C.: Association of American Railroads. TIC: 257585.

Design Constraints

B1.1.2 Motor Vehicle Safety. 49 U.S.C. 301.

B1.1.3 49 CFR 571. 2007. Transportation: Federal Motor Vehicle Safety Standards.

B1.2 SITE PRIME MOVER DESCRIPTION

B1.2.1 Overview

The site prime mover (SPM) is a diesel/electric self-propelled vehicle that is designed to move railcars or truck trailers loaded with transportation casks. The transport occurs both Intra-Site and within the Canister Receipt and Closure Facility (CRCF), Wet Handling Facility (WHF), Initial Handling Facility (IHF), and Receipt Facility (RF).

Movement of the site prime mover railcar (SPMRC) or site prime mover truck trailer (SPMTT) within the IHF is limited to the Cask Preparation Area (Room 1012).

Transportation casks arriving at the IHF on railcar or truck trailer can contain:

- High-level radioactive waste canisters
- Naval canisters.

B1.2.2 System Description

B1.2.2.1 Site Prime Mover

The SPM is a commercially available vehicle that has the capability of moving both railcars and truck trailers loaded with transportation casks. Retractable railroad wheels attached to the front and rear axles of the SPM are used for rail operations.

The driving and braking power comes directly from the road tires as they are in contact with the rails. Weight sharing between the flanged rail and regular road wheels is automatically varied to achieve the required power transmission needs. More weight can be distributed on the rail wheels when moving, or more on the road wheels when braking, accelerating, and negotiating inclines. The SPM has speed limiters that set the maximum speed of the vehicle to less than 9.0 miles per hour.

A diesel engine provides the energy to operate the SPM outside the facilities. Inside the IHF, the SPM is electrically driven via an umbilical cord (or remote control) from the facility main electrical supply.

The SPM is equipped with both an automatic wagon coupling system for railcars and a fifth wheel coupling device for truck trailers. In addition, the SPM is equipped with high-performance compressors, a priority filling system, and an electronic regulating valve with filling speed adjustments and a 100-gallon diesel fuel tank.

B1.2.2.2 Railcars

Railcars used for movement of transportation casks are designed in accordance with Federal Railroad Administration (FRA) requirements under authority delegated by the Secretary of Transportation. The FRA administers a safety program that oversees the movement of nuclear shipments throughout the national rail transportation system. Performance standards are addressed in the Association of American Railroads (AAR) Standard S-2043: *Performance Specification for Trains Used to Haul High Level Radioactive Material* (Ref. B1.1.1).

B1.2.2.3 Truck Trailers

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

Trailers used for the movement of transportation casks are designed in accordance with the National Highway Traffic Safety Administration (NHTSA) requirements as authorized by

Title 49. U.S.C. Part 301, Section 30111 (Ref. B1.1.2). The requirements are delineated in 49 CFR Part 571 (Ref. B1.1.3).

B1.2.2.4 Subsystems

The SPMRC and SPMTT systems are composed of four subsystems:

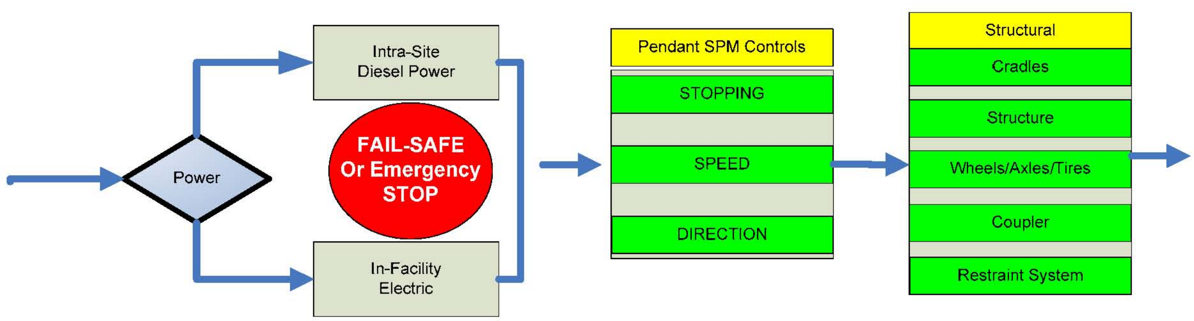
1. Power plant–A diesel engine, generator, and diesel fuel tank are enclosed in the SPM. The SPM utilizes a diesel engine for all Intra-Site Operations. For operations conducted inside facilities, the SPM is connected to the facility 480 V, 3-phase, 60-Hz power supply.

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

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

4. Brakes–For the railcar, brakes comply with FRA requirements; for the truck trailer; the braking system complies with 49 CFR Part 571, Transportation Federal Motor Vehicle Safety Systems (Ref. B1.1.3).

A simplified block diagram of the functional components on the SPMRC/SPMTT is shown in Figure B1.2-1.



Source: Original

Figure B1.2-1. Site Prime Mover Simplified Block Diagram Intra-Site and In-Facility

B1.2.3 Operations

B1.2.3.1 Normal Operations

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

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

B1.2.3.2 Site Prime Mover Off-Normal Operations

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

B1.2.3.3 Site Prime Mover Testing and Maintenance

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

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

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.

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

Table B1.3-1. Dependencies and Interactions Analysis

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

Source: Original

B1.4 SITE PRIME MOVER RELATED FAILURE SCENARIOS

There are four top events for the SPM operating inside the IHF:

1. SPMRC collides with IHF structures
2. SPMTT collides with IHF structures
3. SPMRC derailment
4. SPMTT rollover.

Table B1.4-1 provides a cross reference between the event sequence diagram (ESD) and the SPM fault trees that support them.

Table B1.4-1. ESD Cross Reference with SPMRC/SPMTT Fault Trees

IHF ESD Number	SPMRC Collision	SPMTT Collision	SPMRC Derailment	SPMTT Rollover
ESD-01-NVL	X	—	X	—
ESD-01-HLW	X	X	X	X

NOTE: ESD = event sequence diagram; HLW = high-level radioactive waste; IHF = Initial Handling Facility; NVL = naval; SPMRC = site prime mover railcar; SPMTT = site prime mover truck trailer.

Source: Original

B1.4.1 SPMRC Collides with IHF Structures

B1.4.1.1 Description

The two fault trees for SPMRC collision within the IHF are identical for each type of transportation cask. Collision can occur as a result of human error or mechanical failures. Mechanical failures leading to a collision consist of the SPM failure to stop when commanded, the SPM exceeding a safe speed, or the SPM moving in a wrong direction.

B1.4.1.2 Success Criteria

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

The SPM is designed to stop whenever commanded to stop or when there is a loss of power. The operator can stop the SPM by either commanding a "stop" from the start/stop button or by releasing the palm switch which initiates an emergency stop. At anytime there is a loss of power detected, the SPM performs a controlled stop. Once stopped, the SPM stops all movement or operations and enters into a "lock mode" safe state. The SPM remains in this locked mode until power is returned and the operator restarts the SPM.

Runaway situations on the SPM are prevented by hardware constraints. The maximum speed of the SPM is controlled by a speed limiter on the diesel engine for outside facility movement. The speed control on the SPM for in-facility operations is controlled by the physical limitations of the drive system. The SPM gearing prevents the SPM from exceeding 9.0 miles per hour. The power plant in the SPM has been sized to preclude simultaneous operations.

B1.4.1.3 Design Requirements and Features

Requirements

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

Design Features

The SPM has two off-equipment control devices that have complete control over the SPM. The Drive system limits the maximum speed of the SPM to 9.0 miles per hour.

System Configuration and Operating Conditions

Requirements

Two means of stopping the SPM are incorporated in the controllers. One is the normal stop button and the other consists of an emergency stop that is the equivalent of a "deadman switch." On the loss of AC power, the SPM performs a controlled stop. Once stopped, the SPM enters the lock mode state. The lock mode state is not reversible without specific operator action.

Design Features

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

Testing and Maintenance

Requirements

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

Design Features

None.

B1.4.1.4 Fault Tree Model

The fault tree model for "SPMRC Collides with IHF Structures" accounts for both human error and/or SPMRC mechanical problems that could result in a collision. Once the SPMRC has been properly positioned within the Cask Preparation Area, the SPM is decoupled from the railcar and the SPM moves out of the facility.

The fault tree for SPMRC and SPMTT are identical and a split fraction is used to account for the number/type of transportation casks that arrive at the IHF on either a railcar or truck trailer. The fault tree for the SPMTT is discussed in the next section.

The top event is a collision of the SPMRC in the IHF and is shown in Figure B1.4-3. This may occur due to human error coupled with failure of the speed control or interlocks, or failure of the mechanical and/or control system including failure to stop (Figure B1.4-4) or exceeding a safe speed (Figure B1.4-5). Failure to stop may occur due to mechanical failure of brakes, or failure of the control system. Exceeding a safe speed may also occur due to failure of the control system.

B1.4.1.5 Basic Event Data

Table B1.4-2 contains a list of basic events used in the SPMRC collision fault trees. The mission time is set at one hour which is conservative because it does not require more than one hour to disconnect the SPM from the railcar and remove it from the facility.

Table B1.4-2. Basic Event Probabilities for SPMRC Collision

Name	Calc. Type[a]	Calc. Prob.	Fail. Prob.	Lambda (hr^{-1})	Miss. Time (hr)[a]
51A-OPRCCOLLIDE1-HFI-NOD	1	3.000E-003	3.000E-003	—	—
51A-OPRCINTCOL01-HFI-NOD	1	1.000E+000	1.000E+000	—	—
51A-OPRCINTCOL02-HFI-NOD	1	1.000E+000	1.000E+000	—	—
51A-PWR-LOSS	1	4.100E-006	4.100E-006	—	—
51A-RC---BRP001--BRP-FOD	1	5.020E-005	5.020E-005	—	—
51A-SPMRC-BRK000-BRP-FOD	1	5.020E-005	5.020E-005	—	—
51A-SPMRC-BRP000-BRP-FOD	1	5.020E-005	5.020E-005	—	—
51A-SPMRC-CBP001-CBP-OPC	3	9.130E-008	—	9.130E-008	1
51A-SPMRC-CBP001-CBP-SHC	3	1.880E-008	—	1.880E-008	—
51A-SPMRC-CPL00-CPL-FOH	3	1.910E-006	—	1.910E-006	1
51A-SPMRC-CT000--CT--FOD	1	4.000E-006	4.000E-006	—	—
51A-SPMRC-CT001--CT-SPO	3	2.270E-005	—	2.270E-005	1
51A-SPMRC-CT001-CT-FOD	1	4.000E-006	4.000E-006	—	—
51A-SPMRC-CT002--CT--FOH	3	6.880E-005	—	6.880E-005	1
51A-SPMRC-G6500--G65-FOH	3	1.160E-005	—	1.160E-005	1
51A-SPMRC-HC001--HC--SPO	3	5.230E-007	—	5.230E-007	1
51A-SPMRC-HC001-HC--FOD	1	1.740E-003	1.740E-003	—	—
51A-SPMRC-IEL011-IEL-FOD	1	2.750E-005	2.750E-005	—	—
51A-SPMRC-MOE000-MOE-FSO	3	1.350E-008	—	1.350E-008	1
51A-SPMRC-SC021--SC--FOH	3	1.280E-004	—	1.280E-004	1
51A-SPMRC-SEL021-SEL-FOH	3	2.840E-006	—	2.840E-006	1
51A-SPMRC-STU01-STU--FOH	3	2.107E-004	—	4.810E-008	4380

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

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

Source: Original

B1.4.1.5.1 Human Failure Events

Three human errors have been identified for this fault tree. Both HFEs of operator initiates a runaway and operator causes a collision with mobile platform, are assigned a screening failure probability of 1.00E+00. A detailed analysis of operator causes collision is addressed in Section 6.4 and Attachment E.

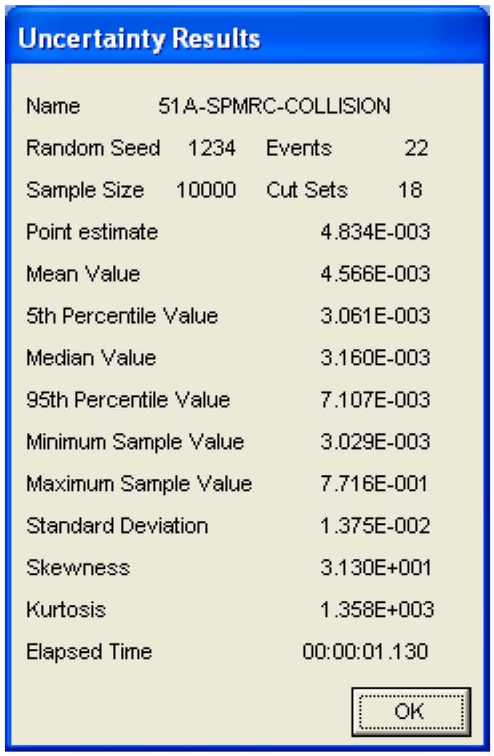
1. Operator causes a collision (51A-OPRCCOLLIDE1-HFI-NOD)
2. Operator initiates runaway (51A-OPRCINTCOL01-HFI-NOD)
3. Operator causes a collision with mobile platform (51A-OPRCINTCOL02-HFI-NOD).

B1.4.1.5.2 Common-Cause Failures

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

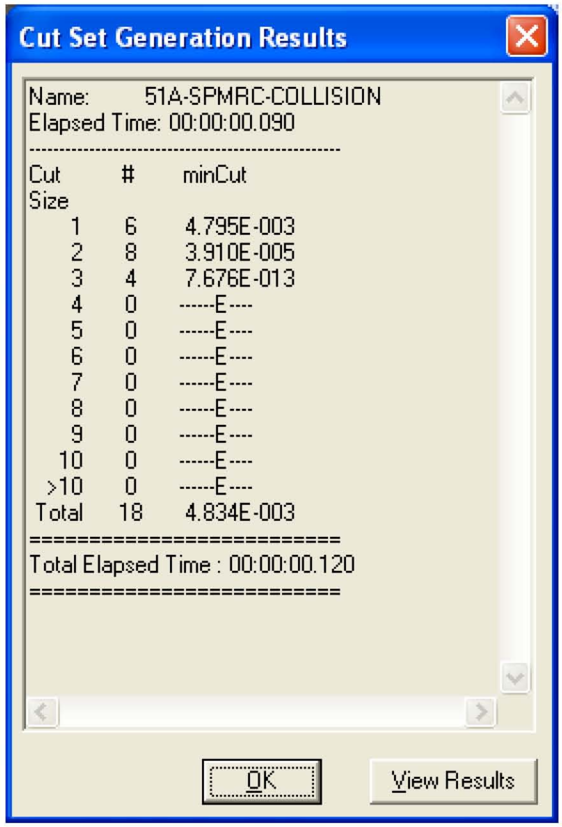
B1.4.1.6 Uncertainty and Cut Set Generation Results

Figure B1.4-1 contains the uncertainty results obtained from running the fault tree for "SPMRC Collides with IHF Structures." Figure B1.4-2 provides the cut set generation results for the "SPMRC Collides with IHF Structures" Fault Tree.



Source: Original

Figure B1.4-1. Uncertainty Results of the SPMRC Collides with IHF Structures Fault Tree



Source: Original

Figure B1.4-2. Cut Set Generation Results for the SPMRC Collides with IHF Structures Fault Tree

B1.4.1.7 Cut Sets

Table B1.4-3 contains the cut sets for “SPMRC Collides with IHF Structures”. The probability of failure is 4.83E-03.