SANDIA REPORT
SAND2019-1827
Unlimited Release
Printed February 2019

Preclosure Risk Assessment for Deep Borehole Disposal

Ernest L. Hardin, Andrew Clark, Jiann Su
Sandia National Laboratories

Fred Peretz
Oak Ridge National Laboratory

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2019-1827
Unlimited Release
Printed February 2019

Preclosure Risk Assessment for Deep Borehole Disposal

Ernest L. Hardin, Andrew Clark, and Jiann Su
Sandia National Laboratories,
P.O. Box 5800, Albuquerque, New Mexico 87185-0747

Fred Peretz
Oak Ridge National Laboratory
1 Bethel Valley Rd, Oak Ridge, Tennessee 37830

Abstract

This report presents a preclosure radiological safety assessment for deep borehole disposal (DBD) of nuclear wastes. The primary purpose of the safety assessment is to identify risk factors for disposal operations, to aid in design for an engineering demonstration of technology for DBD. The assessment is based on a conceptual design for disposal packages and borehole systems that was developed previously. It considers operational steps that could be used for actual DBD, with internal and external initiating off-normal events, to develop insights that can be applied to an engineering demonstration that would be performed without using any form of nuclear waste.

This research was performed as part of the deep borehole field test (DBFT). Based on revised U.S. Department of Energy (DOE) priorities in mid-2017, the DBFT and other research related to a DBD option was discontinued; ongoing work and documentation were closed out by the end of fiscal year (FY) 2017. This report was initiated as part of the DBFT and documented as an incomplete draft at the end of FY 2017. The report was finalized by Sandia National Laboratories in FY2018 without DOE funding, subsequent to the termination of the DBFT, and published in FY2019.

Acknowledgments

Author	Contribution
Ernest Hardin/SNL Project Lead	Sections 1 through 10, 12, 13, 14
Fred Peretz/ORNL (now retired)	Sections 1 through 10, 13, 14, and Appendices B, C and D
Andrew Clark/SNL	Section 11
Jiann Su/SNL	Appendix A

Reviewer	Contribution
Laura Price/SNL	Technical Reviewer – All sections

The authors also acknowledge feedback and suggestions received from Bill Spezialetti/DOE SFWD, and Geoff Freeze and Bob MacKinnon of Sandia.

Contents

Figures

Tables

Nomenclature

ALARA	As-low-as-reasonably-achievable
BOP	Blowout preventer
BSC	Bechtel-SAIC Co.
CFR	Code of Federal regulations
DBD	Deep borehole disposal
DBGM	Design basis ground motion
DBFT	Deep Borehole Field Test
DOE	U.S. Department of Energy
ET	Event tree
EZ	Emplacement zone
FMEA	Failure Modes and Effects Analysis
FT	Fault tree
FY	Fiscal year
GROA	Geologic repository operations area
HAZOP	Hazard and Operability Analysis
HEP	Human error probability
HLW	High-level waste
HRA	Human reliability analysis
HVAC	Heating, ventilation and air conditioning
ITS	Important to safety
MLD	Master logic diagram
MT	Metric ton
NRC	U.S. Nuclear Regulatory Commission
PCSA	Preclosure safety analysis
PFD	Process flow diagram
PRA	Probabilistic risk assessment
RF	Receipt Facility (Yucca Mountain License Application)
SAR	Safety Analysis Report
SNL	Sandia National Laboratories
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SSC	System, structure or component
TBD	To-be-determined
WP	Waste package

1 PURPOSE AND SCOPE

The primary purpose of the preclosure radiological safety assessment presented here is to identify risk factors for disposal operations, to aid in design for an engineering demonstration of technology for deep borehole disposal of nuclear wastes. The assessment considers operations that could be used for actual deep borehole disposal (DBD), to develop insights that can be applied to an engineering demonstration that would be performed without using any form of nuclear waste. The safety assessment seeks to improve the conceptual design for DBD operations, and for an engineering demonstration, by considering risks associated with waste handling and emplacement operations. It is expected that by describing and analyzing disposal operations in more detail, from waste package receipt to borehole closure, that additional active and passive safety functions and operational controls can be identified and incorporated in the design.

This research was performed as part of the deep borehole field test (DBFT). Based on revised U.S. Department of Energy (DOE) priorities in mid-2017, the DBFT and other research related to a DBD option was discontinued; ongoing work and documentation were closed out by the end of fiscal year (FY) 2017. Further DBFT work, for example, implementation of an engineering demonstration (SNL 2016), would require resumption of DBD research and development at some future time.

This report describes a probabilistic risk assessment (PRA) methodology that is similar to the approach required by 10 CFR 63, and generally consistent with the preclosure safety analysis (PCSA) for a Yucca Mountain repository (BSC 2008a,b). The PRA approach is also similar to that required for 10 CFR 60, although it does not include dose calculations for comparison to regulatory objectives.

The full extent of preclosure safety analysis for deep geologic disposal of nuclear waste following 10CFR63.112 (and related parts, and a review plan such as NUREG-1804), is not practical or necessary for developing a generic conceptual design for the DBFT. This analysis is intended to identify risk mitigation measures for incorporation in the design, and to characterize but not necessarily quantify the various risks from disposal operations. This important distinction limits the scope of events that must be considered in this analysis, and the effort needed to quantify probabilities and analyze fragility for affected systems, structures and components (SSCs).

Performance standards and requirements for consideration in a preclosure safety assessment for DBD were summarized by Freeze et al. (2016). Key items identified (from 10 CFR 63.112) include:

- A description of the design, both surface and subsurface, of the geologic repository operations area (GROA) including design requirements and criteria specified in the preclosure performance objectives, and the design bases.
- Identification and analysis of naturally occurring and human-induced hazards at the GROA, including potential initiating event sequences.
- The technical basis for including or excluding naturally occurring and human-induced hazards in the safety analysis.

- Identify items in the DBD concept that could become SSCs important to safety in a future, regulatory PCSA.

This safety assessment addresses the regulatory preclosure performance objectives in the manner summarized in Table 1-1 and Table 1-2. Importantly, dose levels are not quantified because only high-level conceptual design information is available, and no site is selected.

Detailed description of the concept of operations was given previously (SNL 2016) and a summary is provided in Section 2.

Methodology considerations leading to selection of fault tree/event tree implementation of PRA are discussed in Section 3.

Assumptions that support the safety assessment, such as the number of waste packages in a disposal campaign, or which naturally occurring and human-induced hazards are included, are described in Section 4.

Description of waste handling and emplacement process flow, and description of the overall process using activity sequences, are provided in Sections 5 and 6 respectively. The process is compartmentalized using activity sequences that run sequentially.

In Section 7 the hazards associated with waste handling and emplacement are identified, and a set of off-normal initiating events is proposed for failed states that originate from causes internal to the engineered systems for waste handling and emplacement (internal events).

A master logic diagram (MLD) for the safety assessment, modeled on the approach used for the Yucca Mountain PCSA, is developed in Section 8. The MLD summarizes radiological consequences and how they relate to process activities and initiating events. Based on the MLD and the process activities sequences and steps (from Sections 5 and 6), a set of event trees is used to describe normal and off-normal operation (Section 9). The activity sequences are sequential

Using the PRA approach, fault trees are developed in Section 10 to quantify probabilities for "top events" on the event trees. The PRA safety assessment model thus consists of fault trees, event trees, and probability estimates. Calculation results, and the sensitivity of results to key input probability values, are presented in Section 11.

External initiating events consist of seismic ground motion, or other events originating outside of the engineered systems (external events). Various types of external events were considered (see assumptions in Section 4) and seismic ground motion was identified as the most significant. A scoping analysis of external seismic events is presented in Section 12, identifying the types of constraints that seismic performance could impose on DBD equipment selection and design.

Finally, design insights developed from the safety assessment are summarized in Section 13. Additional aspects of performance that cannot be readily determined from available information, are tabulated in a list of to-be-determined (TBD) items that was published previously (SNL 2016).

Table 1-1. Regulatory requirements pertaining to PCSA.

Hazard or Performance Objective	Regulatory Reference	Requirement	Treatment in This Study
On-Site Worker Dose	10 CFR 60.111(a) 10 CFR 63.111(a)(1) 10 CFR 20.1201(a)	The geologic repository operations area (GROA) must be designed so that, for normal operations and Category 1 event sequences through permanent closure, the aggregate radiation exposures and the aggregate radiation levels in both restricted and unrestricted areas, and the aggregate releases of radioactive materials to unrestricted areas, will limit doses to: • The more limiting of (i) an annual dose* ≤ 5 rem/yr, or (ii) the sum of the deep-dose equivalent and the committed dose equivalent to any individual organ or tissue other than the lens of the eye ≤ 50 rem/yr, and • Lens dose equivalent ≤ 15 rem/yr, and • Shallow-dose equivalent to the skin ≤ 50 rem/yr.	Qualitative, judgment-based as-low-as-reasonably-achievable (ALARA) treatment for normal and off-normal operations.
Off-Site Dose to Members of the Public	10 CFR 63.111(a)(2) 10 CFR 63.202 10 CFR 63.204 40 CFR 191.2 40 CFR 191.3(a) 40 CFR 197.4	Aggregated annual dose to an individual during normal operations including storage, and Category 1 event sequences, is limited to ≤ 15 mrem/yr.	• Off-site dose (caused by release of radioactive material) is not considered credible for normal and off-normal DBD operations (unless one or more waste packages is breached downhole, for which recovery operations could result in releases, but which is beyond the scope of this assessment). • Storage of waste on-site is not planned for DBD (see Section 4).
	10 CFR 60.111(a) 40 CFR 191.03(a)	Annual dose to any member of the public in the general environment limited to: • ≤ 25 mrem/yr to the whole body, and • ≤ 75 mrem/yr to the thyroid, and • ≤ 25 mrem/yr to any other critical organ.	
Preclosure Design Objectives	10 CFR 63.111(b)(2)	Taking into consideration a single Category 2 event sequence (i.e., at least one chance in 10,000 of occurring before permanent closure) off-site dose (on or beyond the site boundary) is as specified above for on-site worker dose.	Partly addressed by the conceptual design and potential design improvements described in this assessment.
Preclosure Performance Objectives for the GROA	10 CFR 63.111 10 CFR 63.112 10 CFR 63.204	• Design of, and operations in the GROA must meet 10 CFR 20. • Preclosure safety analysis. A preclosure safety analysis of the GROA that meets the requirements specified at	• Treatment of radiological hazards is limited to qualitative consideration of radiation exposure, as identified above.

Hazard or Performance Objective	Regulatory Reference	Requirement	Treatment in This Study
		63.112 must be performed. • Performance confirmation requirements from Part 63, Subpart F. • Waste retrievability requirements from 63.111(e)(1).	• PCSA requirements are partly addressed in this report (which is not intended as a regulatory safety assessment). • Performance confirmation is beyond the scope of this study. • Application of retrievability requirements to DBD and the DBFT is to-be-determined (SNL 2016, TBD-39).
Standards	40 CFR 191.03	Management and storage of spent nuclear fuel or high-level or transuranic radioactive wastes at all facilities regulated by the Commission or by Agreement States shall be conducted ... to provide reasonable assurance that the combined annual dose equivalent to any member of the public in the general environment resulting from: (1) discharges of radioactive material and direct radiation from such management and storage and (2) all operations covered by Part 190; shall not exceed 25 mrem to the whole body, 75 mrem to the thyroid, and 25 mrem to any other critical organ.	• The requirement stated to the left is that which would apply if the U.S. Nuclear Regulatory Commission regulated DBD. The applicability of regulatory requirements for DBD (and the DBFT) is to-be-determined (SNL 2016, TBD-01). • Off-site dose (caused by release of radioactive material) is not considered credible for normal and off-normal DBD operations, as identified above.
* TEDE = Total effective dose equivalent (the sum of the effective dose equivalent, for external exposures, and the committed effective dose equivalent, for internal exposures). ALARA = As low as reasonably achievable (10 CFR 20.1003).			

Table 1-2. GROA design criteria from repository regulations.

Design Criteria	Treatment in This Study
10 CFR 60.131 – General design criteria for the geologic repository operations area.	
(a) *Radiological protection*. The GROA shall be designed to maintain radiation doses, levels, and concentrations of radioactive material in air in restricted areas within the limits specified in part 20 of this chapter. Design shall include: (1) Means to limit concentrations of radioactive material in air; (2) Means to limit the time required to perform work in the vicinity of radioactive materials, including, as appropriate, designing equipment for ease of repair and replacement and providing adequate space for ease of operation; (3) Suitable shielding; (4) Means to monitor and control the dispersal of radioactive contamination; (5) Means to control access to high radiation areas or airborne radioactivity areas; and (6) A radiation alarm system to warn of significant increases in radiation levels, concentrations of radioactive material in air, and of increased radioactivity released in effluents. The alarm system shall be designed with provisions for calibration and for testing its operability.	Qualitative, judgment-based ALARA treatment for normal and off-normal operations. Review will identify, where appropriate, design features and procedural steps to limit worker exposure. Shielding is included in the conceptual design, and may be supplemented (SNL 2016; TBD-37). Access control and monitoring of radiation in work areas, and monitoring for radioactive contamination, with alarms, are assumed (see Section 4). Measures to control dispersal of radioactive contamination, should it occur, will be considered.
(b) *Protection against design basis events*. The structures, systems, and components important to safety shall be designed so that they will perform their necessary safety functions, assuming occurrence of design basis events.	Design basis earthquake ground motion will be assumed (see Sections 4 and 12) and incorporated in the safety assessment. Extreme weather (wind, lightning) will be considered; procedural controls and design features will be considered for mitigation.
(c) *Protection against dynamic effects of equipment failure and similar events*. The structures, systems, and components important to safety shall be designed to withstand dynamic effects such as missile impacts, that could result from equipment failure, and similar events and conditions that could lead to loss of their safety functions.	Any use of equipment with stored energy sufficient to cause damage that could potentially lead to radiological consequences (aside from local fire) will be identified and evaluated.

Design Criteria	Treatment in This Study
(d) *Protection against fires and explosions*. (1) The structures, systems, and components important to safety shall be designed to perform their safety functions during and after credible fires or explosions in the geologic repository operations area. (2) To the extent practicable, the GROA shall be designed to incorporate the use of noncombustible and heat resistant materials. (3) The GROA shall be designed to include explosion and fire detection alarm systems and appropriate suppression systems with sufficient capacity and capability to reduce the adverse effects of fires and explosions on structures, systems, and components important to safety. (4) The GROA shall be designed to include means to protect systems, structures, and components important to safety against the adverse effects of either the operation or failure of the fire suppression systems.	The potential for explosions will be evaluated. Casks will be designed to maintain shielding functions in the event of credible fires in the GROA. Materials used in the GROA will be noncombustible except as identified and evaluated in this study. Explosion and/or fire alarms will be included in the conceptual design. Fire suppression systems will be included, and evaluated for impact in the event of operation or failure to operate.
(e) *Emergency capability*. (1) The structures, systems, and components important to safety shall be designed to maintain control of radioactive waste and radioactive effluents, and permit prompt termination of operations and evacuation of personnel during an emergency. (2) The GROA shall be designed to include onsite facilities and services that ensure a safe and timely response to emergency conditions and that facilitate the use of available offsite services (such as fire, police, medical, and ambulance service) that may aid in recovery from emergencies.	Responses to emergencies will be evaluated, including types of credible events (fire, weather, accident), and measures to ensure that operations can be safely terminated and personnel evacuated.
(f) *Utility services*. (1) Each utility service system that is important to safety shall be designed so that essential safety functions can be performed, assuming occurrence of the design basis events. (2) The utility services important to safety shall include redundant systems to the extent necessary to maintain, with adequate capacity, the ability to perform their safety functions. (3) Provisions shall be made so that, if there is a loss of the primary electric power source or circuit, reliable and timely emergency power can be provided to instruments, utility service systems, and operating systems, including alarm systems, important to safety.	Safety functions of utility systems such as electrical power will be identified and evaluated, including the need for redundant systems. Recovery from loss of electrical power will be described and any associated safety equipment identified.
(g) *Inspection, testing, and maintenance*. The structures, systems, and components important to safety shall be designed to permit periodic inspection, testing, and	Inspection and maintenance of all equipment, especially that which functions in radiation areas, will be specified.

Design Criteria	Treatment in This Study
maintenance, as necessary, to ensure their continued functioning and readiness.	
(h) *Criticality control*. All systems for processing, transporting, handling, storage, retrieval, emplacement, and isolation of radioactive waste shall be designed to ensure that nuclear criticality is not possible unless at least two unlikely, independent, and concurrent or sequential changes have occurred in the conditions essential to nuclear criticality safety. Each system must be designed for criticality safety assuming occurrence of design basis events. The calculated effective multiplication factor (keff) must be sufficiently below unity to show at least a 5 percent margin, after allowance for the bias in the method of calculation and the uncertainty in the experiments used to validate the method of calculation.	Waste types considered in this analysis do not include fissile materials in sufficient quantities for criticality to be credible (SNL 2016; TBD-23).
(i) *Instrumentation and control systems*. The design shall include provisions for instrumentation and control systems to monitor and control the behavior of systems important to safety, assuming occurrence of design basis events.	The system for handling, transferring and emplacing waste packages in a deep borehole will include functional safety (interlock) components. The need for interlocks will be developed in the fault tree analysis (where human error is explicitly considered).
(j) *Compliance with mining regulations*. To the extent that DOE is not subject to the Federal Mine Safety and Health Act of 1977, as to the construction and operation of the GROA, the design of the GROA shall nevertheless include provisions for worker protection necessary to provide reasonable assurance that all structures, systems, and components important to safety can perform their intended functions. Any deviation from relevant design requirements in 30 CFR, chapter I, subchapters D, E, and N will give rise to a rebuttable presumption that this requirement has not been met.	Mining regulations do not apply to deep borehole operations.
(k) *Shaft conveyances used in radioactive waste handling*. (1) Hoists important to safety shall be designed to preclude cage free fall. (2) Hoists important to safety shall be designed with a reliable cage location system. (3) Loading and unloading systems for hoists important to safety shall be designed with a reliable system of interlocks that will fail safely upon malfunction. (4) Hoists important to safety shall be designed to include two independent indicators to indicate when waste packages are in place and ready for transfer.	Shaft conveyances will not be used in DBD operations. Standard wireline hoists will be used, with tool configurations to provide indications (SNL 2016; TBD-21). Inherent safety features of the DBD emplacement system will limit radiological consequences in the event of hoist failure (analysis of dropped packages in SNL 2016).

Design Criteria	Treatment in This Study
10 CFR 60.132 – Additional design criteria for surface facilities in the geologic repository operations area.	
(a) *Facilities for receipt and retrieval of waste*. Surface facilities in the GROA shall be designed to allow safe handling and storage of wastes at the geologic repository operations area, whether these wastes are on the surface before emplacement or as a result of retrieval from the underground facility.	This requirement is directly addressed in the conceptual design.
(b) *Surface facility ventilation*. Surface facility ventilation systems supporting waste transfer, inspection, decontamination, processing, or packaging shall be designed to provide protection against radiation exposures and offsite releases as provided in 60.111(a).	Surface facilities of types requiring ventilation are not included in the conceptual design.
(c) *Radiation control and monitoring*: (1) Effluent control. The surface facilities shall be designed to control the release of radioactive materials in effluents during Category 1 design basis events so as to meet the performance objectives of 60.111(a). (2) Effluent monitoring. The effluent monitoring systems shall be designed to measure the amount and concentration of radionuclides in any effluent with sufficient precision to determine whether releases conform to the design requirement for effluent control. The monitoring systems shall be designed to include alarms that can be periodically tested.	Effluents (other than internal combustion exhaust) will not be generated by DBD normal operations, and Category 1 events (that do not include release of radioactive material).
(d) *Waste treatment*. Radioactive waste treatment facilities shall be designed to process any radioactive wastes generated at the GROA into a form suitable to permit safe disposal at the GROA or to permit safe transportation and conversion to a form suitable for disposal at an alternative site in accordance with any regulations that are applicable.	Radioactive waste will not be generated by DBD normal operations or Category 1 events.
(e) *Consideration of decommissioning*. The surface facility shall be designed to facilitate decontamination or dismantlement to the same extent as would be required, under other parts of this chapter, with respect to equivalent activities licensed thereunder.	Consideration of final decommissioning of disposal boreholes, and surface operations, is part of the DBD concept.
10 CFR 60.133 – Additional design criteria for the underground facility [only parts most relevant to DBD are listed].	
(a) *General criteria for the underground facility*. (1) The orientation, geometry, layout, and depth of the underground facility, and the design of any engineered barriers that are part of the underground facility shall contribute to the containment and isolation of radionuclides. (2) The underground facility shall be designed so that the effects of credible disruptive events during the period of operations, such as flooding, fires and	Borehole verticality and dogleg severity are addressed in the conceptual design (SNL 2016; TBD-10 and -11). Consequences of radioactive material release in the borehole (waste package breach) are addressed. Effects from disruptive events on disposal boreholes are limited, as discussed in the analysis.

Design Criteria	Treatment in This Study
explosions, will not spread through the facility.	
(c) *Retrieval of waste*. The underground facility shall be designed to permit retrieval of waste in accordance with the performance objectives of 60.111.	Retrieval requirements for borehole disposal are to-be-determined (SNL 2016; TBD-39).
(h) *Engineered barriers*. Engineered barriers shall be designed to assist the geologic setting in meeting the performance objectives for the period following permanent closure.	Engineered barriers consisting of borehole plugs and seals are included in the conceptual design, but specifics are to-be-determined (SNL 2016; TBD-46).
(i) Thermal loads. The underground facility shall be designed so that the performance objectives will be met taking into account the predicted thermal and thermomechanical response of the host rock, and surrounding strata, groundwater system.	Thermal analysis supports the conceptual design (SNL 2015, 2016), and the downhole structures and waste packaging will function within specified temperature limits.
10 CFR 60.134 – Design of seals for shafts and boreholes.	
(a) *General design criterion*. Seals for shafts and boreholes shall be designed so that following permanent closure they do not become pathways that compromise the geologic repository's ability to meet the performance objectives or the period following permanent closure.	Borehole plugs and seals are included in the conceptual design, but specifics are to-be-determined (SNL 2016; TBD-46).
(b) *Selection of materials and placement methods*. Materials and placement methods for seals shall be selected to reduce, to the extent practicable: (1) The potential for creating a preferential pathway for groundwater to contact the waste packages or (2) For radionuclide migration through existing pathways.	These criteria have been used for conceptual design of borehole plugs and seals (e.g., see Arnold et al. 2011).
10 CFR 60.135 – Criteria for the waste package and its components (only parts most relevant to DBD are listed).	
(a) *High-level-waste package design in general*. (1) Packages for HLW shall be designed so that the in-situ chemical, physical, and nuclear properties of the waste package and its interactions with the emplacement environment do not compromise the function of the waste packages or the performance of the underground facility or the geologic setting. (2) The design shall include but not be limited to consideration of the following factors: solubility, oxidation/reduction reactions, corrosion, hydriding, gas generation, thermal effects, mechanical strength, mechanical stress, radiolysis, radiation damage, radionuclide retardation, leaching, fire and explosion hazards, thermal loads, and synergistic interactions.	Waste packages will be designed to provide containment in the borehole environment, with margin for unexpected conditions. Requirements include weight of stacked packages, hydrostatic pressure, downhole temperature, and containment longevity to corrosion (including radiolysis). Specifics of design features are to-be-determined (SNL 2016; TBD-12, -13, -14, -15, -17, -18, -19, -27, -32, -40, 41, and -48). Gas generation by corroding ferrous materials is addressed in the conceptual design but aspects such as final material selection for DBD are to-be-determined (SNL 2016; TBD-43). Fire and explosion hazards in the borehole environment are not credible.

Design Criteria	Treatment in This Study
10 CFR 60.136 – Preclosure controlled area.	
(a) A preclosure controlled area must be established for the GROA.	A controlled area boundary is assumed (see Section 4) but is not critical to the analysis because it is generic (non-site specific), and because release and dispersal of radioactive material are unlikely, and possibly not credible, because of robust waste packages.
(b) The GROA shall be designed so that, for Category 2 design basis events, no individual located on or beyond any point on the boundary of the preclosure controlled area will receive the more limiting of a total effective dose equivalent of 0.05 Sv (5 rem), or the sum of the deep-dose equivalent and the committed dose equivalent to any individual organ or tissue (other than the lens of the eye) of 0.5 Sv (50 rem). The eye dose equivalent shall not exceed 0.15 Sv (15 rem), and the shallow dose equivalent to skin shall not exceed 0.5 Sv (50 rem). The minimum distance from the surface facilities in the GROA to the boundary of the preclosure controlled area must be at least 100 meters.	This requirement is important to DBD only if the design basis Category 2 event causes waste package breach at the surface, and release of radioactive material. The likelihood of that outcome may be insignificant because of the robustness of DBD waste packages. The finite element drop analysis provided in Appendix A shows (for a vertical drop onto compacted gravel) that vertical stresses are mitigated by the integral impact limiter. Most lifts would be essentially vertical and the site surface is assumed to be gravel. However, other such analyses are needed, such as drops onto equipment that could produce transverse stresses that are not mitigated by the impact limiter.
(c) The preclosure controlled area may be traversed by a highway, railroad, or waterway, so long as appropriate and effective arrangements are made to control traffic and to protect public health and safety.	Protection of the public using highways, etc., is addressed by assumption (see Section 4) but is not critical to the analysis because it is generic (non-site specific).

2 OVERVIEW OF DBD CONCEPT OF OPERATIONS

The following information is excerpted from SNL (2016), the current source for conceptual design of DBD packaging and emplacement systems.

Waste forms to be considered for disposal are granular high-level waste (HLW) materials, including those in sealed capsules. Packages will be heavy-walled metal vessels having fill ports with redundant closures, designed to resist the external fluid pressure at the bottom of a 5-km disposal borehole. Suitable materials, connections, closures, impact limiters, and fabrication services are available from vendors to the oil-and-gas industry. The heavy construction of waste packages (WPs) will give them significant resistance to damage from accidental drops during surface handling (Appendix A). Packages will be filled with waste and sealed before transport to the borehole disposal site. They will weigh up to approximately 2.1 MT depending on the borehole size (up to 17-inch diameter) and the waste form contained.

Borehole drilling and construction will be based on currently available technology. The goal will be to achieve total depth with the maximum diameter that can be completed with reasonable certainty in the emplacement zone (EZ) at depths up to approximately 5 km. The final stage in borehole construction will be to hang a guidance casing of constant diameter, over the full length of the borehole, in two pieces. The lower piece will permanently line the EZ, while the upper piece (tieback) will be removable for final plugging/sealing. Wireline emplacement will be used for WPs based on consideration of safety and cost (SNL 2016). Wireline emplacement is made more attractive by the availability of modern wireline cable and equipment, and the use of impact limiters at the bottom of each waste package.

The disposal system will include surface equipment to receive one WP at a time in a truck-transportation cask, transfer the WP to a double-ended transfer cask, position the transfer cask over a disposal borehole, and lower the WP on a wireline, emplacing it at depth. The concept was developed assuming availability of the NAC LWT® Type B transportation cask, or equivalent (SNL 2016). The purpose-built transfer cask must be double-ended (operable openings at both ends) in order to lower packages into the borehole. As a safety measure, the transfer cask, wellhead (at the top of the borehole), and associated components are required to serve together as a pressure envelope for well control, i.e., to contain an unlikely pressure "kick" during operations. To this end, the concept meets the engineering challenge of removing a shield plug at the bottom of the transfer cask and then attaching the open cask to the wellhead with a pressure-tight connection, using remotely operated equipment.

The operational sequence will begin with placing the transportation cask containing a WP into a cradle at ground level. The transfer cask will be placed in another cradle, with the cradles arranged end-to-end. A sliding plate shield between them will allow for removal or replacement of shield plugs from the cask ends, and for pulling or pushing a waste package from one cask to the other.

At this stage of WP handling and emplacement operations, a special suite of wireline logs will be run to qualify the borehole (e.g., an acoustic casing-caliper, radiation detector, and a gauge ring with a junk basket).

The transfer cask containing the WP, with the lower shield plug installed, will be hoisted into a vertical position over the borehole and lowered onto the top surface of a shielded enclosure around the wellhead. The top of the enclosure will consist of a shield plate, with a large (e.g., 3 m diameter) circular plate or "carousel" that turns to locate the cask over tool stations below, or directly over the wellhead (see SNL 2016, Section 3 for illustrations).

Below the carousel, the shielded "pit" will contain: 1) the wellhead (with remotely operated valves, fittings for fluid control, annular blowout preventer, and a flange for attaching the transfer cask); 2) remotely operated equipment to remove or replace the lower shield plug from the transfer cask; 3) a remotely operated actuator to make/unmake the wellhead flange connection; and 4) a sump for collecting spilled borehole fluid and draining washdown water. Once the transfer cask is fixed to the wellhead flange, the cask and associated hardware will be part of the pressure envelope for well control, so that any unexpected pressure transients encountered during emplacement operations would not necessarily require actuation of the blowout preventer. Details of the shield plate, carousel, pit, transfer cask attachment, the wireline interface at the top of the transfer cask, and provisions to access the borehole for plugging, sealing, and WP fishing, are provided by SNL (2016).

The WP will be supported by side latches in the transfer cask at all times when it is mounted on the carousel or attached to the wellhead, before a secure wireline connection has been established. This is designed as a backup so that a single component failure or human error cannot cause a WP to drop into the wellhead or borehole.

The wireline system will include a headframe (approximately 20 m tall) with sheaves, wireline cable on a spool, and a truck-mounted wireline winch. The downhole tool string will consist of a cable head, an electromechanical release section, and logging tools for location, tool weight, and other downhole monitoring functions. The release mechanism will be designed with the capability to re-latch a WP if downhole retrieval is required.

For emplacement, the WP will be supported by the wireline, the borehole valve opened, and the side latches released so the package can be lowered into the borehole. The electromechanical release will be actuated once the WP is landed on the bottom. Each WP will have an impact limiter attached at the bottom to prevent damage if the package is accidentally dropped in the borehole. A latch and fishing neck will be attached at the top. Wireline retrieval of individual WPs could be done by reversing the steps and hoisting the WP back into the transfer cask.

The WP descent rate during wireline emplacement will be about 0.15 m/sec for the first kilometer, to control load transients that could break the wireline, then 0.6 m/sec thereafter (SNL 2016, Section 2.9.3). After releasing the WP, the wireline and tool string will be hoisted out of the borehole with an ascent rate of approximately 1 m/sec. Once the tool string is back in the transfer cask, the wellhead valve will be closed, and the transfer cask and tool string will be moved to a wash-down area for cleaning, inspection, and preparation for the next use.

Waste packages will be emplaced individually and stacked one on top of the other. They will be designed to provide containment throughout the emplacement phase and plugging/sealing of the borehole, to prevent radioactive contamination of borehole fluid during operations.

The reference disposal concept calls for 10-m cement plugs within the guidance casing, spaced about 200 m apart in the EZ (SNL 2016, Section 3.1). Cement plug installation is therefore part of emplacement operations, and will be done using wireline tools and coiled-tubing. A squeeze cement method with casing perforations is recommended (SNL 2016, Option 2) for bonding the guidance casing to the host rock, to stabilize the guidance casing and support the weight of stacked WPs. Once all WPs are emplaced, a drilling or workover rig will be moved in for final plugging/sealing of the borehole.

This study assesses radiological risk for all activities associated with WP receipt, handling, emplacement, and setting of cement plugs. Final plugging/sealing activities under normal conditions will not involve radioactive materials or the potential for radiation exposures, and are therefore beyond the scope of the study.

Off-normal events may either directly lead to radiological exposures, or may lead to response activities that carry risk of subsequent events that lead to radiological exposures. Earlier analysis led to identification of five off-normal events associated with downhole operations:

- Waste package becomes stuck and breached above the emplacement zone;
- One or more waste packages are breached in the emplacement zone;
- A waste package is dropped and comes to rest intact within the emplacement zone;
- An intact (unbreached) waste package becomes stuck in the emplacement zone; and
- An intact (unbreached) waste package becomes stuck above the emplacement zone.

Off-normal events during surface operations can also occur, with the potential for loss of shielding and radioactive material release. In the event of such an occurrence a recovery plan would be developed and implemented before operations would be allowed to continue. For example, a waste package that was damaged because of a cask drop would be assessed, recovered, and dispositioned which might involve re-attempting emplacement or sending it back to the point of origin for re-packaging and re-qualification. This assessment acknowledges the need for such recovery operations but does not simulate them explicitly. The potential for radiological consequences during recovery operations is addressed in the description of off-normal outcomes of different severity (Section 9).

3 SELECTION OF PROBABILISTIC RISK ASSESSMENT

Quantitative PRA is regarded among the most suitable methods for developing full understanding of process risks and appropriate measures to prevent or mitigate them (Milstein 2001). The fault tree/event tree implementation of PRA is also considered to be one of the best methods for analyzing multiple-failure sequences. Other documented methodologies that are comparable include:

- Hazard and Operability Analysis (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Human Reliability Analysis (HRA)

HAZOP and FMEA tend to be more structured in their implementation than other alternatives. HAZOP is well suited for identification of failure modes and initiating events, while FMEA is typically used for system-level treatment that begins with failure modes. HAZOP focuses on "process upset conditions," while FMEA focuses on "failure of equipment and components" (Milstein 2001). The structure built into these methodologies is challenging to implement for conceptual design, given limited detail (without explicit specifications, engineering drawings, procedures, etc.).

The methodology for examining DBD concept performance should be modeled on 10 CFR 63, because that rule (and 10 CFR 60) is a modern approach deemed appropriate by the U.S. Nuclear Regulatory Commission (NRC) for licensing nuclear waste disposal. These regulations do not actually prescribe a methodology, but they specify event probability levels of significance, which requires a PRA approach. The only real-world application of these regulations for preclosure operational safety is found in the Yucca Mountain Safety Analysis Report (SAR; DOE 2008), and the complementary Safety Evaluation Report (NRC 2015). This analysis follows the approach used in the Yucca Mountain SAR for scoping and design, but is simplified in the formulation and presentation of event trees and fault trees because the scale of this assessment is so much smaller than the PCSAs for Yucca Mountain facilities.

The fault tree/event tree PRA approach can be implemented at a general level while still providing useful design insights (e.g., SNL 2016, Appendix A). For the present study, unlike previous work on DBD (SNL 2016), radiological consequences are considered while cost is not. Also, additional hazards are considered to evaluate how they affect radiological risk, such as flammable materials, toxic materials, potentially hazardous process conditions, and external hazards. The assessment (Section 4, and Sections 7 through 10 of this report) relies on engineering judgment to determine whether an initiating event, or subsequent events in a sequence, will lead to consequences of concern (Milstein 2001).

Where compartmentalization of systems (into subsystems) is used to simplify the analysis of risk, the effect of a particular hazard should be followed by consideration of the resulting effects on or contributions from other subsystems (Ma et al. 1992). For example, off-normal events during emplacement of waste packages could potentially degrade processes used to retrieve them. In addition, each hazard should be correlated to other hazards to evaluate the likelihood, and if appropriate, the consequences of joint occurrence (see Section 3.2). Finally, the interfaces between subsystems require clearly defined boundaries and similar levels of descriptive detail ("level of resolution") so that inconsistencies can be recognized (Vesely et al. 1981).

The Receipt Facility (RF) described for the Yucca Mountain License Application Design is perhaps the simplest waste handling facility in that design, in terms of function and physical layout. The RF safety analysis (BSC 2008a, 2008b) demonstrates facility compliance with criteria such as those at 10 CFR Parts 63.131, 63.132, and 63.136, and is a starting point for features to consider in developing an analysis methodology for DBD operations.

Using the event categorization approach of BSC (2008a) but without facility ventilation (no HVAC confinement for DBD operations) or the possibility of criticality (because DBD as analyzed is not intended for fissiles), four end states of system response are defined for DBD operations:

1. **OK** (normal operations; corresponds to endpoint A in Table 9-1)
2. **Degraded shielding, direct exposure** – Applies to event sequences where shielding is not breached, but its shielding function is jeopardized. An example is a lead-shielded transportation cask that is dropped from a height great enough for the lead to slump toward the bottom of the cask at impact, leaving a partially shielded path for radiation to stream. This end state does not include radionuclide release. Corresponds to endpoints B and C in Table 9-1.
3. **Loss of shielding, direct exposure** – Applies to event sequences where a component providing shielding fails or is improperly installed, leaving a direct path for radiation to stream. For example, a breached cask with the intact waste canister inside, still maintaining its containment function. Excludes radionuclide release. Corresponds to endpoints D and E Table 9-1, without waste package breach.
4. **Radionuclide release** – Indicates an unfiltered release of radioactive material from its confinement, to the environment. Corresponds to endpoints E, F and G from Table 9-1, with waste package breach and radionuclide release.

The present study is intended to provide insights that improve the conceptual design for DBD, and not to estimate radiological exposure or dose for comparison to regulatory limits (Table 1-1). Accordingly, consequence analysis is abstracted for this study (see Section 9) in a way that assigns end states that are defined qualitatively, without quantification, in terms of relative levels of possible exposure or dose (e.g., as consequence categories A, B, etc.).

Initiating events considered include internal events that are initiated within the WP receipt/handling/ emplacement system, and external events (seismic, extreme weather, external fire). Selection of internal and external events is addressed further in the following sections.

Initiating events that are associated with conditions introduced in SSCs before they reach the site (e.g., drops of casks) or during cask or canister manufacture, are not within scope of the analysis.

The probability for each independent, internal initiating event is quantified using a fault tree. Fault trees are structured as having a top event (stated as a positive outcome) that is made up of causal events and basic events (negatives such as equipment malfunction, human error, etc.). Fault trees use Boolean logic and basic event probabilities to estimate the top event probability.

Safety Functions of Support Equipment – The treatment given to failed states and initiating events in this preliminary assessment has not explicitly included the reliability of some key components of supporting equipment such as the crane, headframe, hoist, generator, and wireline equipment (SNL 2016). Assumptions on reliability of supporting equipment should be carried forward as design criteria, and they may be incorporated explicitly in future risk assessments especially if design and available equipment are not likely to provide the desired reliability.

Fragility Analysis – The level of detail in system response modeling depends on fragility analysis. For example, the analysis in Appendix A addresses the likelihood of WP breach in the event of a vertical drop, whether or not cask containment (and by inference, cask shielding integrity) is maintained. This is the only instance of quantitative fragility analysis produced in this study. Fragility analysis is not the focus of this assessment because of the generic, conceptual nature of the design concept. Rather, this study is expected to provide design and performance insights than can be used in follow-on design activities.

4 ASSUMPTIONS FOR RISK ANALYSIS

The following assumptions are proposed to allow a generic (non-site specific) analysis of worker radiological safety, and to simplify the analysis. Sources for information that may be needed for risk assessment of the type described in this report, include guidelines from siting regulations (10CFR960), and regulator reviews of Safety Analysis Reports (NUREG-1949 Volume 2; NRC 2015).

4.1 Scope of Waste Disposal Activities

1. ***No waste storage*** – Waste will not be stored at the disposal site, so a license under 10 CFR 72 is not required, and storage or aging will not be part of a license under a disposal regulation such as 10 CFR 63. For implementation of DBD this means that waste shipments will be received just-in-time, and that lag storage to accommodate schedule disruptions, emplacement stoppages due to weather, etc., will be performed elsewhere. We note that transportation rules for particular projects may allow for a few days of temporary storage where waste transportation vehicles can be parked safely and securely.

2. ***No waste re-packaging*** – Waste packages suspected of leakage and/or contamination, prior to emplacement in a deep borehole, will be returned to the point of origin for further inspection, decontamination, and rework if necessary. Transportation and transfer casks, and the wellhead station, will be routinely surveyed for radioactive contamination.

3. ***Waste types for disposal*** – DBD would be used for high-level waste (HLW) streams of limited scope (see assumptions from SNL 2016). For purposes of analysis these wastes are assumed to be solid (possibly particulate), and gamma emitting such that shielding is required for waste handling operations, but not fissile, and not neutron-emitting so that neutron shielding is not required. Neutron shielding would not pose a serious challenge to the conceptual design, and could take the form of an added layer of solid or liquid hydrogenous material on the outside of the casks (e.g., as described by NAC International 2008).

4. ***Single borehole campaign*** – A single-borehole campaign is assumed as one case for analysis, such as that which could be used to dispose of the full inventory of sealed capsules containing Cs and Sr from irradiated fuel processing at Hanford. The duration of this campaign (SNL 2016) is assumed to be approximately two years for drilling, construction, emplacement (one WP per day during emplacement operations), sealing, and plugging.

5. ***Multiple borehole campaign*** – A multi-borehole campaign is assumed as a separate case for analysis. The number of boreholes for the multi-borehole case is assumed to be 100, without specifying the waste form beyond the characteristics assumed in this report. The duration for the multi-borehole campaign is assumed to be 50 years. Each borehole would take 2 years as noted above, with emplacement activity for approximately 1 year of that. The schedule of activities may not be important to the risk assessment, but if necessary may be assumed:

# Boreholes Active at a Time	Duration of Phase (yr)	Total # Boreholes in Phase
1	6	3
3	10	15
5	32	80
2	2	2

6. ***Use of a purpose-built transfer cask*** – As stated in Section 2 and by SNL (2016), a double-ended cask such that WPs can be loaded or unloaded at either end, is needed for DBD emplacement and retrieval. The capability may also be important for recovery from off-normal downhole conditions. On the other hand, existing licensed transportation casks of the size needed are single-ended, being loaded and unloaded from the same end. For the conceptual design (SNL 2016) a purpose-built double-ended transfer cask was adopted for use with a currently existing transportation cask (NAC International 2008). This assumed selection impacts risk assessment for surface operations because it requires transfer to another cask, but it does not require successful licensing of a double-ended transportation cask with additional features for coupling to a borehole.

7. ***Site area*** – The site area is assumed to be sufficient to accommodate drilling and workover activities, construction of surface facilities, surface waste handling, downhole emplacement operations, transport vehicles, and other site operations needs.

4.2 Compliance with Other Regulations

8. ***No interference between occupational and radiological safety measures*** – The same measures to avoid cask drops, collisions, unplanned movement, etc. will support both occupational and radiological safety. Where additional measures are used for occupational safety, they do not increase radiological risk.

9. ***Regulations and permitting*** – For purpose of analysis it is assumed that legal and regulatory requirements associated with permitting and preclosure operations (i.e., drilling, construction of surface facilities, and waste handling and emplacement) are achievable using the conceptual approach to DBD operations (summarized in Section 2, based on SNL 2016). The regulatory environment varies from state to state and for government-owned versus private land. Potential requirements include use of a blowout preventer, and incorporating the transfer cask and associated components into the wellbore pressure control envelope, both of which are incorporated in the current conceptual design (SNL 2016).

4.3 Limited Use of Hazardous Materials

10. ***No hazardous materials*** – During normal waste handling and emplacement operations hazardous materials will not be used except fuels and lubricants, sealed-source geophysical tools, and cements and other materials that are commonplace in oil-and-gas borehole operations. Use of such hazardous materials will not increase radiological risk except for internal fire and certain external events addressed in this analysis. (Note that borehole cuttings and wasted borehole fluids, without radioactive contamination, may be designated as hazardous wastes by local regulations.)

4.4 Ease and Cost of Siting, Construction, Operation, and Closure

11. ***Suitable landform surface characteristics*** – Favorable surface characteristics for DBD surface operations can be assumed for this analysis, including stable surface geology and uniform (flat) topography (surface hydrology is discussed below). Such characteristics are assumed to be suitable for reasonable construction of graveled roads in remote locations, with the configuration and load-bearing capacity for safe and secure transport of waste.

12. ***Suitable subsurface rock characteristics*** – The scope of guidelines in 10 CFR 960.5 includes rock characteristics pertaining to ease of constructing and operating a mined geologic repository. Such characteristics may also affect construction and operation of boreholes for DBD. For purposes of analysis, suitable rock characteristics can be assumed that allow for safe DBD construction and operation.

13. ***Suitable surface hydrologic characteristics*** – DBD disposal surface facilities will not be located in wetland areas or watershed settings where there is the potential for direct, adverse environmental impacts. The site for DBD would be engineered to sustain heavy precipitation without detrimental effects, and the intensity considered in that analysis would be at least that corresponding to Category 1 event. A predictive-engineering approach might not be sufficient to describe a more intense event because of limited observational data for extreme weather over very long time frames. However, a different approach in analysis and controls on DBD operations is assumed for mitigation of the effects of extreme precipitation. For example, constructed boreholes have casing cemented to great depth, and are fluid-filled during operations, so they could not be compromised by surface erosion resulting from a beyond-Category 1 precipitation event. Further, that heavy precipitation can be modeled and occurs over durations of many hours so that DBD operations would be suspended and demobilized before waste packages could be compromised.

14. ***Suitable subsurface hydrologic characteristics*** – Subsurface hydrology is considered in site characterization and site suitability determination for DBD, which will be verified during construction of each borehole. Such determination is assumed to assure that subsurface hydrologic characteristics have no significant effect on radiological safety of DBD operations.

4.5 Site Remoteness and Control

15. ***Population density and distribution*** – DBD is assumed to be sited in a remote region with appropriate separation from centers of population (e.g., tens of kilometers), and further, to be remote from permanent habitations (e.g., distance of at least 10 km).

16. ***Site ownership and control*** – The implementing agency for DBD is assumed to have full site ownership and control, of an area containing the controlled area and including additional area as appropriate.

17. ***Offsite installations and operations*** – DBD operations are assumed to be conducted in remote settings separated from offsite installations and operations, especially ones involving radioactive materials, by sufficient distance that they present no significant additional radiological hazard to DBD workers or members of the public. Such remote locations are assumed to be accessed by improved, graveled roads with appropriate controls on public access.

4.6 Environment, Socioeconomics, and Transportation

18. ***Environmental quality*** – The DBD operation is assumed to contribute no significant potential for environmental impacts (such as wetland impacts discussed above) that should be taken into account in the design of DBD equipment and operations, apart from the fate of radioactive waste, and the proper and compliant use of hazardous materials discussed above (fuels and lubricants, sealed-source geophysical tools, cements, and possibly borehole fluids and cuttings).

19. ***Socioeconomic impacts*** – The potential for socioeconomic impacts is assumed to have no bearing on the design of DBD equipment and operations.

20. ***Transportation*** – The manner and routing of safe and compliant waste transportation to the remote DBD site is assumed to have no impact on DBD equipment and operations, except for the choice of transportation cask and truck transport. For this analysis, it is assumed that WPs are delivered to the DBD site one at a time, on a just-in-time basis, in a single-package cask such as the existing LWT® cask from NAC International. The choice of a single-package transport cask is consistent with delivery of packages by legal-weight truck over improved gravel roads. Use of a cask that contains multiple WPs is possible, but involves heavier loads, better roads, and the potential complication of onsite storage.

4.7 Loss of Cask Shielding Function

21. ***Cask containment and loss of shielding*** – Loss of containment may occur when a shielded plug is dislodged by impact (Sprung et al. 2000). A plug needs be dislodged only a few millimeters to break its seal, and such damage is relatively straightforward to simulate. The resulting loss of shielding is more difficult to model, and gamma scattering occurs anyway, so loss of shielding is typically associated with loss of containment, and is assumed in this analysis.

22. ***Cask deformation and loss of shielding*** – Loss of shielding (possibly without loss of containment) can occur with lead shielded casks, by slump of the lead caused by impact. The accelerations calculated in Appendix A are assumed to be insufficient to cause significant slumping of the shield layers in the transportation and transfer casks.

4.8 Assumptions Affecting Treatment of Internal Initiating Events

23. ***Potential internal initiating events*** – A survey of potential internal initiating events, using the events identified BSC (2008a, Table 10) with the addition of events and categories specific to DBD, is shown in Table 4-1. As noted in the table some of the events are not credible for DBD.

24. ***Safety functions of supporting equipment*** – The DBD system for receipt, handling, and emplacement of waste packages includes major components such as the crane for unloading transportation casks, headframe, hoist for moving the transfer cask, wireline hoist, and wireline logging equipment. In the discussion of initiating events, the reliability of certain aspects of the performance of these components has been implicitly assumed. For example, the crane, headframe, and hoist for cask handling and movement are assumed to be reliable except for the possibility of drops or collisions.

25. ***Internal flooding*** – DBD operations are assumed to be performed in the open, on an engineered pad with drainage features, so that flooding from internal causes is not credible. No fissile materials will be handled so the potential for flooding is much less important.

26. ***Fire suppression*** – Availability of a robust fire suppression system is assumed, with redundant capabilities (e.g., water and foam), pre-arranged for access to all vehicles, casks, generators, and other equipment on the pad. Note the assumption above on waste types (non-fissile).

27. ***Safe shutdown*** – The waste handling and emplacement system is assumed to have internal, intrinsic capability for safe shutdown if one of a list of off-normal events occurs. For example, cranes and hoists are assumed to arrest all load movement if power failure occurs. Where safe shutdown must occur across different self-contained subsystems, it may be directed by an integrated functional safety system. This assumption is used in consideration of single failures, while multiple simultaneous failures are addressed below for external initiating events (Section 4.9).

28. ***Maximum cask drop height*** – The maximum drop is assumed to be 3 m, corresponding to the lift height (from bottom of cask) to clear the transport vehicle, and to clear equipment at the transfer station and the wellhead station.

29. ***Pad for surface DBD operations*** – Waste receipt, handling, and emplacement operations will take place on a pad (which may be the former drill pad), constructed from at least 60 cm of compacted gravel with appropriate grade and drainage features. The subgrade material is assumed to be stable and compliant. The size of the pad will be at least 100 m square, sufficient to set up the operations area around the borehole, surrounded by access, parking, supporting equipment, and facilities for waste fluid management (normal operating conditions). It is expected that the former drill pad will be 2.5 to 5 acres, and thus provide the room needed for DBD operations (although rework of the pad base may be required).

30. ***Recovery from off-normal event sequences*** – For event sequences resulting in system damage, recovery operations are beyond the scope of this study. Thus, the refinement of conceptual design for WP handling and emplacement, may not consider recovery from WPs becoming stuck or breached downhole. However, some consideration may be given to features of surface equipment that could facilitate recovery from drops, equipment malfunction, etc.

Table 4-1. Survey of internal initiating events.

Potential Internal Initiating Event	Comment
General:	
Flooding from pipe failure	Not credible for operation of portable equipment in open (not confined) spaces.
Flooding from actuation of fire suppression	
Large fire, internally caused	Not credible with limited amounts of combustible materials, and fire suppression.
Electrical fire	Mitigate by safe shutdown features, electrical shutoffs, and fire suppression.
Localized fire with fuel present	Vehicle fires mitigated by safe shutdown and fire suppression.
Excessive temperature (excluding fire)	Mitigate by procedural controls, where necessary.
Loss of generator power	Mitigate by safe shutdown features.
Transportation cask movement:	
Transport cask vehicle collision (onsite)	
Crane drops object (e.g., impact limiter) onto cask	
Crane drops transportation cask onto ground surface	Assume maximum drop height of 3 m, established by crane setup and procedural controls.
Crane drops transportation cask onto equipment (e.g., cradle)	
Unplanned crane or transportation vehicle movement	Mitigate using the functional safety system, as appropriate.
Incorrect position or movement of cradle for cask	
Loaded cask collides with object/equipment during move	
Shield plug dislodges from cask	
Work platform falls or collapses onto cask	
Cask-to-cask transfer:	
Cask-cask misalignment	
Failure of shield plate actuation (e.g., becomes stuck)	
Cask shield plug becomes stuck	
Waste package stuck in transportation cask	
Shield plug bolts fail or become stuck	
Transfer cask movement:	
Hoist drops transfer cask onto ground surface	Assume maximum drop height of 3 m, established by crane setup and procedural controls.
Hoist drops object (e.g., impact limiter) onto cask	
Hoist drops cask onto equipment (e.g., wellhead station)	
Unplanned hoist movement	Mitigate using the functional safety system, as appropriate.
Incorrect position or movement of cradle for cask	
Loaded cask collides with object/equipment during move	
Shield plug dislodges from transfer cask	
Side-latches fail to grip transfer cask	
Shield plug flange mechanism fails or becomes stuck	

Potential Internal Initiating Event	Comment
Wellhead setup:	
Misplacement of transfer cask	
Failure of carousel actuation	Access for repair in unshielded work environment.
Failure of kneeling jacks	
Unplanned carousel movement	
Toppling of transfer cask on wellhead station	
Failure of remotely operated shield plug removal mechanism	Mitigated by repair capabilities.
Flange actuation fails	
Wellhead equipment (valve, blowout preventer) actuation fails	
Pressure "kick" with valve open	Mitigated by well pressure control envelope.
Wireline emplacement operations:	
Misassembly of latch or cable head	Addressed by previous risk analysis for emplacement mode selection (see SNL 2016, Appendix A).
Electromechanical latch not secure	
Waste package falls a short distance while attached to wireline	
Wireline hoist failure	
Wireline instrumentation failure (e.g., loss of power)	
Cable damage (leads to break if undetected)	
Gauge ring fails to remove debris (package can get stuck)	
"Other" debris in borehole	
Casing collapse	
Waste package becomes stuck above emplacement zone	
Waste package becomes stuck in emplacement zone	
Waste package drops from surface	
Waste package drops during trip in	
Latch fails to release	
Wireline drops on trip out	
Recovery from off-normal downhole conditions:	
Inadequate shielding at the surface during package recovery	Planning and risk analysis for recovery operations would be performed (and reviewed) on an as-needed basis and are beyond the scope of this study.
Failure of remotely operated equipment (e.g., casing cutting, decontamination)	
Radionuclide release and radiation exposure from contaminated borehole fluid	
Release and exposure from contaminated solids (e.g., drill pipe and casing)	
Failure of washdown system for contaminated components	

4.9 Assumptions Affecting Treatment of External Initiating Events

31. ***Potential external initiating ev*ents** – A survey of categories of potentially significant external initiating events is shown in Table 4-2. As noted in the table some of the events are not credible for DBD.

32. ***Safety functions of supporting equipment*** – As stated above for internal events, the DBD system for WP receipt/handling/emplacement includes major components such as the crane, headframe, hoist, and wireline equipment. The capability of these components to perform their safety functions needs to be supported by assessment of responses to design basis external events (e.g., seismic ground motion, extreme weather, external fire). The response to Category 2 ground motion and faulting also needs to be assessed to determine whether worker exposure limits could be exceeded (Section 12).

33. ***Tectonic characteristics (seismicity)*** – Tectonic activity results in faulting and ground motion hazards to DBD operations. Ground motion is identified as an external initiating event (Section 3). As a design basis, events with less than 2% probability within 50 years (2,500-year recurrence) of peak ground acceleration greater than 0.16 g, is assumed to be sustained during DBD surface operations without damage or radiological incident. This magnitude is generally indicative of an area of tectonic stability. Such an event (0.16 g) is less frequent, and therefore more intense than a Category 1 event, supporting a conservative design approach. For Category 2 events (500,000-year recurrence) a peak ground acceleration of 0.5 g is assumed. This is a somewhat ad hoc selection for risk analysis, that is intended to guide selection of reasonable (and not excessive) DBD design features.

34. ***Extreme ground motion*** –Peak ground acceleration greater than 0.5 g may be possible at the Category 2 level depending on site conditions, and may result in waste package breach with release of radioactive material. It can be assumed that procedural controls will be developed for DBD operations, that would be invoked after any off-normal event that could cause breach, for detecting and mitigating releases. Protocols would be implemented to stabilize released material from atmospheric dispersion (e.g., immediate application of adhesive chemical foam), and hydrologic transport (e.g., erection of a temporary structure). Additional planning, design, and review activities would precede further mitigation activities.

35. ***Tectonic characteristics (faulting)*** – Fault offset would have minimal impact on a constructed borehole, because the surface casing is robust and cemented to great depth. However, an offset could disrupt surface operations by toppling casks, equipment, etc. For this reason it is assumed that boreholes will be located with appropriate standoff from indications of past fault offsets in near-surface sediments. This approach is assumed to mitigate the faulting hazard for Category 1 events because the associated seismic magnitude is limited, and slip on any new (unmapped) fault through a DBD operational area would be too small to result in radiological consequences. For Category 2 events it is assumed that only capable faults (evidence of past events indicating sufficient likelihood) would be included in the assessment, so that the likelihood of unknown, capable faults is insignificant, and impact is limited to ground motion.

36. ***Limits on non-seismic geologic events*** – The possibility of non-seismic events such as landslides, karst collapse, or volcanism is assumed to be very remote, and will be addressed

during characterization for DBD. The DBD system for WP receipt/handling/emplacement would not reasonably be designed to withstand such events.

37. ***Limits on extreme weather*** – Extreme weather (high winds, tornadoes, hurricanes, lightning) is assumed to have no significant effect on radiological safety of operations, because: 1) procedural controls will suspend operations such as cask lifts when appropriate to do so; 2) all SSCs will be electrically grounded in a manner known to limit lightning damage; 3) cask handling equipment (cradles, headframe, wellhead station) will be well anchored and designed to survive design-basis wind loading (in addition to seismic ground motion); 4) supporting equipment will also be well-anchored and designed to survive design-basis wind loading; and 5) DBD boreholes are intrinsically resistant to damage from extreme weather because of multiple, heavy, cemented casings and wellhead equipment. The intensity of design-basis wind loading will be greater than Category 1, and consistent with the probability level of the seismic design basis (2,500-year recurrence). Management of the hazard from extreme weather will be similar to managing operations on a large drilling rig (offshore or land-based). The hazard from extreme weather is site-dependent and the approach represented by this assumption will be reviewed if and when site-specific information becomes available.

38. ***Limits on external flooding*** – Flooding may occur from extreme precipitation, but impact to DBD operations will be limited by: 1) mitigating flood control excavation at DBD sites; 2) procedural controls that suspend operations, particularly when extreme precipitation is imminent; and 3) intrinsic resistance of DBD boreholes to damage from flooding, as noted above for extreme weather.

39. ***Limit on loss of power or cooling*** – DBD operations will not use offsite power, and will not rely on central cooling. For onsite power the system for WP receipt/handling/emplacement, including support equipment, will tolerate loss of power without initiating failed states that cause radiological consequences.

40. ***Limits on aircraft crash hazard*** – The DBD site is assumed to be sufficiently remote from airports with commercial or heavy military traffic, and not situated in mountainous terrain, so that the aircraft crash hazard probability is comparable to the smallest found anywhere in the conterminous U.S. The likelihood of an aircraft crashing directly into a waste cask is assumed to be beyond Category 2 based on the incidence of crashes over remote regions, and an assumed footprint for DBD operations.

41. ***Limits on nearby industrial/military accidents (incl. transportation)*** – Sites for DBD are assumed to be sufficiently remote from industrial or military facilities (e.g., at least 10 km) that impacts from those facilities on DBD operations, and radiological doses from those facilities at points of compliance for DBD operations, are insignificant.

42. ***Limits on onsite hazardous materials release*** – Hazardous materials will not be used for DBD operations (with the exception of fuel and radioactive waste). Fuel release is treated by considering internal fire to be the most severe potential impact on operations, and hazards from radioactive waste is the focus of the assessment.

43. ***Limits on external fire*** – We assume that the DBD campaign will be conducted in sparsely vegetated terrain, and that vegetation will be removed to a safe distance so that a large fire

cannot damage the operations area. Also, that procedural controls will cause operations to be safely suspended in the event of a fire with potential to become a large fire in the vicinity.

44. ***Limits on extraterrestrial activity (meteorites, falling satellites)*** – These hazards are assumed to be excluded from assessment on the basis that they are beyond Category 2.

Table 4-2. Categories of potential external initiating events

Potential External Initiating Event Category	Treatment
Tectonic events (seismic ground motion and faulting)	Inclusion (see text)
Non-seismic geologic events (incl. volcanic activity)	Exclusion (see text) either because they are not workable for a generic analysis of DBD or they are sufficiently unlikely that they do not serve as reasonable bases for design.
Extreme weather (high winds, tornadoes, hurricanes, lightning)	
External floods	
Loss of power	
Loss of cooling capability	
Aircraft crash	
Nearby industrial/military accidents (incl. transportation)	
Onsite hazardous materials release	
External fire	
Extraterrestrial activity (meteorites, falling satellites)	

5 PROCESS FLOW DIAGRAM

The process for receiving, handling, and emplacing waste packages, and completing the disposal borehole, was diagrammed as a series of activity sequences and nodes (Figure 5-1). Node A represents the starting point; Sequence 1 (borehole qualification) must be completed prior to moving the loaded transfer cask into position over the wellhead station. Sequences 2 through 8 proceed in linear fashion. As seen in Section 3.8, Sequence 8 is split into four subsets, with some flexibility for overlap with prior or subsequent sequences. A decision point is shown after Sequence 8. If a string of about 40 packages has been placed, Sequences 9 and 10 are used to place an interval plug. Otherwise, the process flow returns to Node A and emplacement activities for the next waste package begin. A second decision point follows setting of the interval plug; if space remains in the borehole emplacement zone the flow again returns to Node A. If the emplacement zone has been filled, the borehole is closed under Sequence 11. The same process may then be used to fill another borehole.

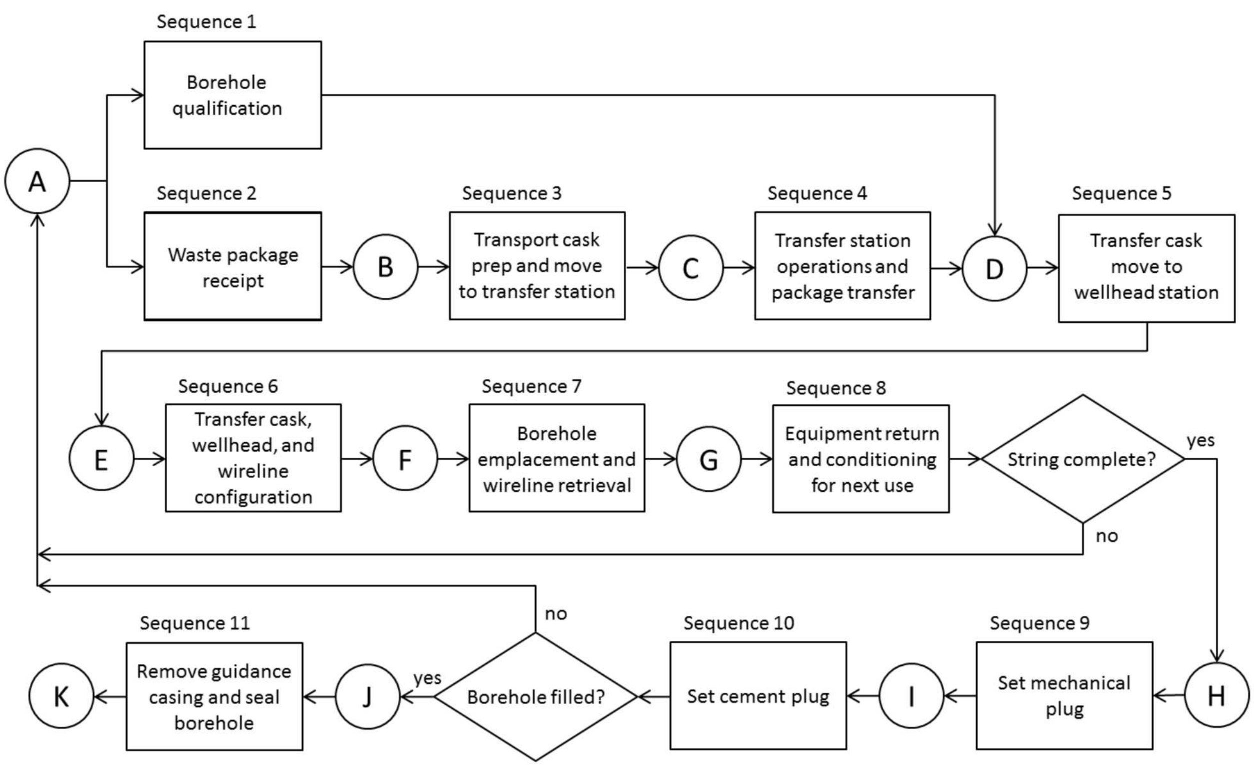


Figure 5-1. Simplified process flow diagram.

The activity sequences identified in Figure 5-1 are connected at the nodes. Each node correlates to a fixed set of conditions, as described in Table 5-1 below. The overall sequence begins at Node A, *ready to initiate next emplacement sequence*, and the logic flow returns to Node A for each subsequent package placement. Emplacement and closure of an individual borehole terminates at Node K, *borehole sealed and equipment moved off borehole*.

Individual steps associated with the activity sequences are identified in the next section.

Table 5-1. Status at each process flow diagram node.

Node	Status
A	Ready to initiate next emplacement sequence.
B	Sealed transportation cask trailer properly placed on borehole site.
C	Transportation cask and waste package on cradle #1, ready to transfer package.
D	Transfer cask and waste package ready to be moved to wellhead station.
E	Transfer cask and waste package ready for wellhead and wireline configuration.
F	Waste package and wellhead ready for package emplacement in borehole.
G	Waste package emplaced in borehole, wireline retrieved, and wellhead closed.
H	Package string emplacement complete, ready to set interval plug.
I	Mechanical plug set, ready to set cement plug.
J	Borehole filled, ready for borehole closure.
K	Borehole sealed and equipment moved off borehole.

6 ACTIVITY SEQUENCES FOR WASTE PACKAGE RECEIPT, HANDLING AND EMPLACEMENT – NORMAL OPERATIONS

Outlines of the individual steps needed to perform each of the activity sequences shown in the process flow diagram, transitioning from one nodal state to the next, were initially described by Peretz and Hardin (2017). This section repeats the summary tables for each sequence; the overall sequences are the same as documented in the prior report with the exception of two cases in which pull tests or leak tests were added.

Activity sequence steps consist of both verification steps, such as steps that ensure initial conditions are met at the beginning of a sequence or that the site status is as intended at the end of a sequence, along with the actual action steps needed to accomplish the intended objectives. Additional detail on the processes, equipment used, and general risks encountered in each step can be found in the relevant sections of Peretz and Hardin (2017).

6.1 Borehole Qualification

Activity steps for the first activity sequence are listed in Table 6-1. This sequence confirms that the borehole is open and ready for placement of a waste package, and is performed just prior to initiating each emplacement sequence. Action steps include preparing, running, and removing the qualification tool string. Verification steps are provided to ensure the wellhead is ready prior to attaching equipment, verifying that no uncontained radiological material is present in the borehole (as an indicator of damage to a package in the borehole), and inspection of material collected in the junk basket.

Table 6-1. Activity steps for borehole qualification.

Step	Description
1.1	As necessary, disconnect the package placement tool string from the wireline.
1.2	Assemble the qualification tool, string consisting of a gauge ring, junk basket and other tools such as a casing collar locator, onto the wireline, along with an appropriate fluid seal system.
1.3	Attach lubricator (riser) to the wellhead flange, ready to accept the qualification tool string and grease seal, and verify that the lower gate valve is closed.
1.4	Insert the tool string and connect the grease seal to the lubricator.
1.5	Open the lower gate valve and allow the borehole fluid to achieve a steady elevation/pressure.
1.6	Run the gauge ring and junk basket down and up borehole.
1.7	Pull the qualification tool string into the fluid seal system, close the gate valve, and drain excess borehole fluid from the wellhead components.
1.8	Verify no radiological contamination is present on the wireline or tool string as it is withdrawn from the borehole.
1.9	Remove and dismantle the qualification tool string and fluid seal from the wellhead and the wireline.
1.10	Inspect the junk basket for retrieved material, and evaluate gauge ring data to show the borehole is ready for package emplacement.

At the end of this operating sequence, if no problems are detected then the wellhead equipment will be left ready to establish a connection with the transfer cask. If either the data collected by the gauge ring or material identified in the junk basket indicates a need for remedial action, such action will be planned and executed as a separate activity. Once completed, the borehole qualification activity sequence should be repeated to demonstrate that the borehole is ready to accept a waste package.

This activity sequence utilizes the wellhead, and must be completed prior to achieving Node D conditions, *transfer cask and waste package ready to be moved to wellhead station*. It can be completed in parallel with any of the other activity sequences leading up to Node D.

6.2 Waste Package Receipt

The simple waste package receipt activity sequence (Table 6-2) addresses arrival and positioning of the trailer containing the transportation cask at its intended location on site. The process flow diagram depicts this sequence beginning when Node A conditions are achieved, but it could be performed at any time that the site is ready to accept a loaded cask and trailer system. The trailer is not opened, and no cask dismantling activities such as removal of impact limiters are performed in this sequence. Although the cask contains a radioactive waste package, it remains in its certified shipping status.

Completion of this sequence achieves Node B conditions, *sealed transportation cask trailer properly placed on borehole site*.

Table 6-2. Activity steps for waste package receipt.

Step	Description
2.1	Drive tractor-trailer with loaded transportation cask onto site.
2.2	Position and park trailer, and disconnect and move tractor to designated area.
2.3	Ensure trailer is secure.
2.4	Confirm waste package data package and trailer tamper seals.

6.3 Transportation Cask Preparation and Move to Transfer Station

Activity Sequence 3 begins with the transportation cask on its properly parked trailer, corresponding to Node B conditions. Prior to initiating the sequence, the empty transfer cask is verified to be in place on cradle #2 (this ensures that mishandling of the transfer cask cannot lead to loss of waste package shielding in the transportation cask or interface assembly). The transportation cask is prepared and moved in accordance with common procedures used to handle the cask, and the steps are inverted to place the cask on cradle #1. As cask surfaces are accessed, radiological conditions are verified to ensure contamination from the loading site is not spread at the borehole site. After handling equipment is removed from the transportation cask, cradle #1 is rolled into position against the transfer shield. Action steps are described in Table 6-3.

Table 6-3. Activity steps to prepare and move transportation cask to cradle #1.

Step	Description
3.1	Ensure cradle #1 is in position to receive the transportation cask (withdrawn from the shield).
3.2	Ensure an empty transfer cask has been placed in cradle #2 (withdrawn from the interface shield).
3.3	Remove the trailer cover and doors and set into a laydown area, using a crane.
3.4	Remove the impact limiters from the transportation cask while it is secured to the trailer, using a crane, and set them in a laydown area.
3.5	Verify there is no radioactive contamination on the exterior surfaces of the transportation cask.
3.6	Remove the fixtures securing the cask to the trailer, and attach a crane-supported yoke to the cask trunnions.
3.7	Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.
3.8	Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.
3.9	Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.
3.10	Ensure the shield plug is in position for removal of the transportation cask shield plug.
3.11	Prepare the end plug for removal, and roll cradle #1 into position against the transfer shield.

At the end of this sequence, the transportation cask with the waste package is on cradle #1 at the interface shield, ready for removal of the end shield plug. Completion of this sequence achieves Node C conditions, *transportation cask and waste package on cradle #1, ready to transfer package*.

6.4 Transfer Station Operations and Cask-to-Cask Transfer

Activity Sequence 4 begins with Node C conditions. Sequence steps begin with confirmation that the transportation and transfer casks are on their respective cradles, in proper position, and that the lower shield plug for the transfer cask is pre-positioned in the interface shield slide. Working through the interface shield, the transportation cask shield is detached and pulled into the shield slide. As the plug is handled, contamination and radiation surveys are used to ensure safe conditions.

Cradle #2 is moved in position against the interface shield, the slide is moved to the open position, and again radiation conditions are verified. The latch mechanism is configured, moved through the transfer cask and interface shield to engage with the waste package, and the waste package is pulled through the interface shield into the transfer cask. The latch system is configured as a component of the transfer cask upper shield plug, with the waste package remaining engaged. Side latches on the transfer cask are engaged with the waste package, providing redundant approaches to securing the package in place, and a pull test is performed to demonstrate secure attachment of both the top and side latches.

Table 6-4. Activity steps to transfer waste package to transfer cask.

Step	Description
4.1	Ensure the transportation cask is on cradle #1, in its shielded position against the interface shield assembly.
4.2	Ensure the transfer cask is on cradle #2, withdrawn from the interface shield.
4.3	Ensure the lower shield plug for the transfer cask has been pre-positioned in the transfer shield.
4.4	Position the sliding shield plate in its first position, ready to receive transportation cask end shield plug.
4.5	Detach and pull the end shield from the transportation cask into the sliding shield, using appropriate tooling to align, pull, and secure the plug in the sliding shield.
4.6	Verify there is no radioactive contamination on accessible surfaces of the shield plug and that dose rates are acceptable.
4.7	Roll cradle #2 (with the transfer cask) into its shielded position against the interface shield assembly.
4.8	Position the sliding shield plate in its second position, providing an open path between the two casks.
4.9	Verify the radiation exposure dose rates around the shield are acceptable.
4.10	Release the flange from the package latch subassembly on the transfer cask top plug, and attach the extension shaft to the transfer latch subassembly.
4.11	Push the package latch subassembly through the interface shield assembly until it makes contact with the waste package in the transportation cask.
4.12	Confirm latch engagement on the waste package.
4.13	Pull the waste package through the interface shield assembly until it is in position in the transfer cask, and the extension shaft connection is clear of the transfer cask upper plug. Monitor radiation exposure dose rates throughout this operation.
4.14	Verify there is no radioactive contamination on the extension shaft, and remove the extension shaft.
4.15	Engage the side latches, securing the package in position in the transfer cask. Perform a pull test to verify engagement of the latches.
4.16	Attach the flange to the package latch subassembly, and attach the flange to the transfer cask top shield plug. Leave the latch subassembly attached to the waste package.
4.17	Verify the radiation exposure dose rates at the transfer cask are acceptable.
4.18	Position the sliding shield plate in its third position, with the transfer cask lower shield plug in the slide shield ready for insertion.
4.19	Roll cradle #1 away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved
4.20	Verify there is no radioactive contamination in the open end of the transportation cask or on the interface shield assembly, and that radiation exposure dose rates at the interface shield assembly are acceptable
4.21	Push the transfer cask lower shield plug into position in the transfer cask, using appropriate tooling.
4.22	Engage the Grayloc® clamp on the bottom of the transfer cask to the lower shield plug, and verify engagement.
4.23	Roll cradle #2 with the loaded transfer cask away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved.
4.24	Verify the radiation exposure dose rates at all locations around the transfer cask are acceptable.

The slide is moved to the third position and the lower transfer cask shield plug is positioned in the cask and secured. In all cases, radiological surveys accompany any change in shield configuration or waste package location. Finally, with the lower shield plug inserted, the transfer cask on cradle #2 is rolled away from the interface shield and a final radiological survey is performed. The activity steps are listed in Table 6-4.

At the end of this sequence, the waste package is in the transfer cask, shield plugs at both ends of the transfer cask are secured in place, the waste package is secured by the transfer latch and the side latches (as well as the plugs at either end of the cask), and the transfer cask has been surveyed and is ready to move to the wellhead.

This sequence, along with the borehole qualification sequences, completes the actions needed to achieve Node D conditions, *transfer cask and waste package ready to be moved to wellhead station*.

6.5 Transfer Cask Move to Wellhead Station

Activity Sequence 5 begins with Node D conditions. Initial verification steps ensure the transfer cask is rolled away from the interface shield, and that the waste package and shield plugs are secure; and that the pit shield carousel is in its intended position, ready to receive the transfer cask. The transfer cask is rotated into a vertical orientation and picked off the cradle #2 in a manner similar to that used for the transportation cask; the key difference is that a gantry crane is used rather than a mobile crane. The cask is then moved and lowered into the designated opening in the shield carousel, and the tie-downs are secured. A final verification step confirms that radiation dose exposure levels remain low (no disruption to the shield plugs) and that no contamination is present. Activity steps are shown in Table 6-5.

Table 6-5. Activity steps to move loaded transfer cask to wellhead station.

Step	Description
5.1	Confirm that the transfer cask, with waste package, is ready to move to the wellhead.
5.2	Confirm the wellhead pit shield carousel is in position over the lower plug removal station, and is ready to accept the transfer cask.
5.3	Remove the fixtures securing the cask to cradle #2, and attach a crane-supported yoke to the cask trunnions (this might be a field crane, or might be a hoist on a headframe assembly).
5.4	Rotate the cask into a vertical position with pins set on cradle #2, and lift the cask just above the cradle and wellhead structures.
5.5	Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.
5.6	Secure the transfer cask to the shield carousel, using TBD features to prevent the cask from tipping or being dislodged (features such as guy wires must allow carousel rotation and kneeling jack actuation).
5.7	Verify that radiation exposure dose rates are acceptable, and no radioactive contamination is present.

At the end of this sequence, the transfer cask with the waste package is in position over the lower plug removal station. The waste package remains secured by both the central upper latch assembly and the side latches, and is further secured by the lower shield plug. This sequence completes the actions needed to achieve Node E conditions, *transfer cask and waste package ready for wellhead and wireline configuration*.

6.6 Transfer Cask, Waste Package, Wellhead and Wireline Configuration

Activity Sequence 6 begins at Node E conditions. An initial set of verification steps ensure the transfer cask is secured in place, the wellhead and plug removal stations are ready, the wireline, tool string, lubricator, and fluid seal are ready, the waste package is secure in the transfer cask, and radiological conditions are as expected. Work platforms are set up around the top of the transfer cask, with jigs and additional personnel shielding to allow removal of the upper latch assembly. While the package is held by the side latches and still captured by the lower shield plug, the upper latch is pulled out of the upper shield (with personnel working from the side, avoiding streaming radiation up through the open hole) and the wireline tool string is lowered through the opening in the shield plug. The remote disconnect at the bottom of the tool string latches onto the top pintle on the waste package, and after confirming a secure connection, the lubricator and fluid seal are mounted onto the transfer cask.

The lower shield plug handling mechanism is raised up to accept the lower transfer cask shield plug, the remotely operated flange clamp is released, and the mechanism and plug are lowered again. The waste package remains secured by the side latches, and is suspended from the slightly slack wireline. Radiological conditions are confirmed, slack in the wireline is confirmed, and the shield carousel is rotated to position the lower flange on the transfer cask directly over the wellhead flange. A slight sliding motion is available in addition to rotation to ensure the necessary degrees of freedom for alignment.

When alignment is confirmed (using remote monitoring equipment in the pit), the kneeling jacks are used to gently set the cask on the borehole flange. Position verification continues as the cask is lowered. Once in place, the remote flange clamp is activated to secure the connection between transfer cask and wellhead. A pressure test is performed to ensure successful makeup of the flanged connection. Cask tie-down hardware is verified, radiological conditions are confirmed, and wireline slack is taken up.

Activity steps for this sequence are listed in Table 6-6.

At the end of this sequence, the transfer cask is secured to the wellhead, and the wireline is attached to the waste package. The wellhead gate valve remains closed. The waste package is secured by both the side latches and the wireline. This sequence completes the actions needed to achieve Node F conditions, *waste package and wellhead ready for package emplacement in borehole*.

Table 6-6. Activity steps to configure waste package, wellhead and wireline for emplacement.

Step	Description
6.1	Ensure the transfer cask is in place on the shield plate carousel, properly secured and positioned over the lower plug handling mechanism.
6.2	Ensure the wellhead flange is ready to accept the transfer cask, with a new flange seal in place.
6.3	Verify the radiation exposure dose rates at the transfer cask are acceptable.
6.4	Verify the side latches are engaged with the waste package.
6.5	Ensure the tool string is attached to the wireline, and the lubricator and fluid seal are ready for use.
6.6	Position personnel access hardware adjacent to the transfer cask, and install temporary shielding as required for removal of the latch assembly and installation of the tool string.
6.7	Disconnect the top latch assembly from the upper shield plug, activate the latch rod to release the assembly from the waste package, and remove the latch assembly from the upper shield plug.
6.8	Verify the radiation exposure dose rates at the transfer cask are acceptable, and adjust temporary shielding as appropriate.
6.9	Lower the tool string and wireline assembly, temporarily support the lubricator and seal above the transfer cask, and insert the tool string into the top shield plug until it latches onto the waste package.
6.10	Verify that the tool string is securely latched onto the waste package.
6.11	Verify the radiation exposure dose rates at the transfer cask are acceptable.
6.12	Lower the lubricator and grease seal section to the top of the transfer cask, and attach the lubricator flange to the transfer cask.
6.13	Attach the fluid seal to the top of the lubricator (if not pre-attached).
6.14	Take up wireline slack to the extent possible movement of the package is minimized but cask movements remain possible.
6.15	Raise the lower shield plug handling mechanism until it engages with the shield plug.
6.16	Activate the Grayloc® clamp on the bottom of the transfer cask to release the lower shield plug.
6.17	Lower the shield plug handling mechanism so the shield plug is clear of the bottom flange of the transfer cask.
6.18	Verify the radiation exposure dose rates at the wellhead pit shield are acceptable.
6.19	Ensure the wireline is sufficiently slack to accommodate cask movement, but not excessively slack as to break if the package is inadvertently released.
6.20	Rotate, and if necessary slide, the carousel to position the cask over the wellhead.
6.21	Confirm cask position over the wellhead flange, and adjust position as necessary.
6.22	Use the kneeling jacks to gently lower the cask onto the wellhead flange, while monitoring alignment of the bottom cask flange with the wellhead flange. Adjust the position of the carousel as necessary to maintain alignment as the cask is lowered.
6.23	With the cask in contact with the wellhead flange, activate the Grayloc®clamp on the bottom of the transfer cask to complete the flange connection between the transfer cask and the wellhead. Perform a pressure leak test to ensure the flange connection has been properly made up and is leak tight.
6.24	Ensure the cask is secured against movement in the vertical or horizontal (tipping) directions.
6.25	Verify the radiation exposure dose rates at the wellhead pit shield are acceptable.
6.26	Take up tension in the wireline.

6.7 Borehole Emplacement, Release, and Wireline Retrieval

Activity Sequence 7 begins at Node F conditions with a series of verification steps to ensure the transfer cask is properly set up, the wireline and tool string are properly installed and tensioned, the lubricator and fluid seal system are in place and operational, and the blowout preventer (BOP) is open and ready for operation. Radiation exposure dose rates are verified, as are the position of the side latches still supporting the package, and the closed status of the borehole gate valve. To minimize risk and consequences of a package drop as the waste package is initially suspended only on the wireline, the side latches are released prior to opening the gate valve, and the waste package is lowered a short distance until it is just above the gate valve. The valve is then opened, and the package is lowered down into the emplacement zone. When the position of the waste package is verified, an electric current is sent to activate the remote disconnect and the wireline and tool string are retrieved. With the package remaining in the borehole and the tool string in the lubricator, the gate valve is closed and the wellhead is drained of fluid. Activity steps are listed in Table 6-7.

Table 6-7. Activity steps for waste package emplacement, release, and wireline retrieval.

Step	Description
7.1	Ensure the transfer cask is in place on the shield plate carousel, attached to the wellhead flange, and secured against inadvertent movement.
7.2	Ensure the wireline tool string is connected waste package, and is properly tensioned.
7.3	Ensure the lubricator and wireline fluid seal are in place.
7.4	Ensure the BOP is ready for operation and in open position.
7.5	Verify the radiation exposure dose rates at the transfer cask are acceptable.
7.6	Verify the side latches are engaged with the waste package.
7.7	Verify the wellhead gate valve is closed.
7.8	Fill the guidance casing up to the gate valve, with borehole fluid.
7.9	Release the side latches, allowing the waste package to be supported by the wireline.
7.10	Lower the package through the wellhead components, to just above the closed gate valve, while monitoring radiation dose exposure rates at the wellhead shield.
7.11	Open the wellhead gate valve and verify the fluid level in the guidance casing.
7.12	Continue to lower the waste package to the emplacement zone, monitoring depth of the package using the tool string locator, wireline runout, and wireline tension.
7.13	Stop the wireline when the package rests on the previous package or borehole plug (or, in the case of the initial package, the bottom of the borehole).
7.14	Verify the package is at its intended location in the borehole.
7.15	Send a signal to release the package from the wireline tool string.
7.16	Confirm package release by signal and/or tension on the wireline.
7.17	Retrieve the wireline, monitoring depth of the tool string, until the tool string is returned to the transfer cask lubricator.
7.18	Verify the tool string in the lubricator, clear of the wellhead components.
7.19	Close the gate valve.
7.20	Verify that radiation exposure dose rates are minimal, and no radioactive contamination is present.

At the end of this sequence, the waste package remains in the emplacement zone, the wireline tool string has been withdrawn into the lubricator, the gate valve in the wellhead has been closed, and the fluid has been drained from wellhead components above the gate valve. This sequence completes the actions needed to achieve Node G conditions, *waste package emplaced in borehole, wireline retrieved, and wellhead closed*.

6.8 Condition Equipment for Next Use

Activity Sequence 8, condition equipment for next package emplacement sequence, is described as four sub-sequences addressing reconfiguration of the wireline system, the transfer cask and interface shield, the wellhead, and return of the empty transportation cask. This sequence begins after waste package emplacement is complete, with Node G conditions, *waste package emplaced in borehole, wireline retrieved, and wellhead closed*.

Under normal operating conditions, none of these sequences involve the handling of radioactive material, or include activities that could have an immediate impact on previously emplaced waste packages.

In Sequence 8a the lubricator, wireline seal, and tool string are removed from the transfer cask, surveyed and inspected, and reconditioned for use with the next waste package. Individual steps are described in Table 6-8.

Table 6-8. Activity steps to prepare the wireline for the next operating sequence.

Step	Description
8a.1	Ensure the transfer cask is in place on the shield plate carousel, securely fixed, with no waste package present, the wellhead gate valve closed, and drained of borehole fluid.
8a.2	Ensure that radiation and contamination surveys indicate no radioactive material is present.
8a.3	Ensure the wireline tool string is in the lubricator.
8a.4	Provide sufficient slack in the wireline to disconnect the fluid seal and lubricator from the transfer cask, and possibly from each other.
8a.5	Using the wireline, carefully withdraw the tool string out of the transfer cask.
8a.6	Verify no radioactive contamination is present on the tool string as it is withdrawn.
8a.7	Using the wireline crane or headframe, move the wireline, lubricator, and tool string to a laydown and wash area.
8a.8	Separate the tool string, lubricator, and fluid seal and wash borehole fluid residue off the components.
8a.9	Inspect the wireline termination and rebuild if necessary.
8a.10	If the next wireline application is other than waste package emplacement, disconnect the package placement tool string and prepare the wireline for an alternate tool string.
8a.11	If the next wireline application is emplacement of another waste package, rebuild or reset the remote disconnect for the next use.

In Sequence 8b, the transfer cask is removed from the wellhead, moved back to cradle #2 (positioned in the washdown area), washed and reconditioned, and positioned near the interface shield to prepare for the next package transfer sequence. The lower shield plug is removed from the wellhead pit, washed and reconditioned as required, and pre-positioned in the interface shield assembly. Steps for this sequence are described in Table 6-9.

In Sequence 8c (Table 6-10) the wellhead equipment is surveyed and cleaned as required, and prepared for the next operating sequence.

In Sequence 8d (Table 6-11) the empty transportation cask is surveyed and cleaned as necessary, the shield plug is reinserted, the cask is moved back onto the transportation trailer, the transportation system is reassembled, and the cask is shipped back to the waste package loading facility.

Completion of all four sub-sequences achieves either Node A conditions, *ready to initiate next emplacement sequence* (if the emplaced package string is not complete), or Node H conditions, *package string emplacement complete, ready to set interval plug* (if the package string is complete).

Table 6-9. Activity steps to prepare the transfer cask for the next operating sequence.

Step	Description
8b.1	Ensure the transfer cask is in place on the shield plate carousel, securely attached and empty.
8b.2	Ensure the wireline tool string has been removed from the transfer cask.
8b.3	Ensure that radiation and contamination surveys have been completed, and no radioactive material is present in the wellhead pit or the transfer cask.
8b.4	Move empty cradle #2 into the washdown area, within reach of the headframe gantry crane, and secure it to prevent motion.
8b.5	Ensure there is no load on the transfer cask lower flange assembly (e.g., ensure the kneeling jacks are raised).
8b.6	Connect the handling yoke to the trunnions of the transfer cask using the headframe gantry crane.
8b.7	Release the Grayloc® flange clamp assembly to disconnect the transfer cask from the wellhead.
8b.8	Disconnect features used to prevent vertical and horizontal movement of the transfer cask.
8b.9	Use the kneeling jacks to separate the transfer cask from the wellhead flange.
8b.10	Verify the transfer cask is free of attachments to the wellhead or the wellhead shield or carousel assemblies, and lift the transfer cask from the wellhead shield.
8b.11	Move the transfer cask to cradle #2, and lower the cask so the cradle rotation pins fit into pockets on the cask.
8b.12	Lower and rotate the cask until it rests on cradle #2 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.
8b.13	Remove the top shield plug, and wash borehole fluid residues from the interior of the transfer cask.
8b.14	Inspect, clean and refurbish as necessary, and replace the top shield plug and transfer latch assembly onto the top of the transfer cask.
8b.15	Inspect, clean and refurbish as necessary the lower Grayloc® flange and actuating mechanism.
8b.16	Move cradle #2, with the transfer cask, into position near (but not against) the interface shield, and secure it to prevent motion.
8b.16	Attach the handling yoke to the cask trunnions, and raise it off the washdown cradle into a vertical orientation.
8b.17	Confirm that all components are present and the transfer cask is ready to accept the next waste package.
8b.18	Using the crane and an appropriate open access port in the wellhead shield carousel, attach a lift fixture to the transfer cask lower shield plug and lift it off the shield plug handling fixture and out of the wellhead pit.
8b.19	Move the lower shield plug to the washdown area, and inspect and clean the shield plug.
8b.20	Verify the condition of the interface shield assembly, and pre-position the transfer cask lower shield plug in the sliding shield, using appropriate tooling.

Table 6-10. Activity steps to prepare the wellhead for the next operating sequence.

Step	Description
8c.1	Ensure the transfer cask has been removed, the wellhead gate valve is closed, and all wellhead equipment is in a stable condition.
8c.2	Verify that radiation exposure dose rates are minimal, and no radioactive contamination is present.
8c.3	Wash borehole fluid residues and other material off the borehole equipment as appropriate, and drain the pit using the pit sump pump.
8c.4	Ensure the lower transfer cask shield plug has been removed from the shield plug handling mechanism, and confirm proper operation of the mechanism.
8c.5	Test operation of the BOP, as appropriate.
8c.6	Inspect the wellhead flange, recondition the flange as appropriate, and place a new gasket on the wellhead flange.
8c.7	Confirm operation of the wellhead pit shield assembly, including the carousel and transfer cask kneeling jacks, and position for the next operating sequence.

Table 6-11. Activity steps to prepare to ship the empty transportation cask off site.

Step	Description
8d.1	Ensure cradle #2 has been rolled away from the interface shield assembly.
8d.2	Confirm the condition of the transportation cask shield plug, and position new gaskets as appropriate.
8d.3	Roll cradle #1, with the empty transportation cask, into position against the interface shield assembly.
8d.4	Position the sliding shield plate in its first position, with the transportation shield plug in position for insertion into the transportation cask.
8d.5	Push the transportation cask shield plug into position in the cask, using appropriate tooling.
8d.6	Detach handling tooling and insert bolts attaching shield plug to transportation cask.
8d.7	Roll cradle #1 away from the interface shield assembly, and torque bolts attaching shield plug to cask.
8d.8	Ensure transportation cask is ready for return to waste package loading facility.
8d.9	Remove the fixtures securing the cask to cradle #1, and attach a crane-supported yoke to the cask trunnions.
8d.10	Rotate the cask into a vertical position with pins set on cradle #1, and lift the cask just above the cradle and trailer structures.
8d.11	Move the cask over the transportation trailer, and lower the cask so the trailer cradle rotation pins fit into pockets on the cask.
8d.12	Lower and rotate the cask until it rests on the transportation trailer cradle in a horizontal position, remove the handling yoke, and secure the cask to the cradle.
8d.13	Using a crane, retrieve the impact limiters from the laydown area and attach them to either end of the transportation cask.
8d.14	Re-assemble the trailer components and verify the transportation cask is ready to move off the borehole site.

6.9 Setting an Interval Plug

As waste packages are stacked on each other, mechanical loading on the bottom package increases. At intervals of approximately 40 waste packages, an interval plug is set to transfer load through the casing to the host rock, establishing a new load path for the next stack of packages. Initial conditions for these activity sequences correspond to Node H, *package string emplacement complete, ready to set interval plug*. Emplacement of a package string is complete, the transfer cask has been removed from the wellhead area, and the wellhead has been reconditioned for its next use.

Setting an interval plug is described as two separate activity sequences. In the first, coiled tubing is used to set a mechanical bridge plug above the top package. A riser (reaching over the pit shield assembly) is used over the wellhead to aid insertion of the coiled tubing, and to protect the flange surface used to mount the transfer cask on the wellhead. In the second sequence, a squeeze packer is set 10 meters above the bridge plug, and cement is injected under pressure through the packer. Casing perforations in the interval between the bridge plug and the packer allow cement to flow into the annulus and upward, following the path of displaced annulus fluid. After injection of the fluids, the packer is released and the coiled tubing is withdrawn to the surface and cleaned. The wellhead is then prepared for the next waste package emplacement Sequence.

Steps for Activity Sequence 9, setting a mechanical interval plug, are shown in Table 6-12.

Table 6-12. Activity steps for setting a mechanical interval plug.

Step	Description
9.1	Obtain and confirm operability of pressure-operated coiled tubing bridge plug.
9.2	Install riser on wellhead, including injector head if borehole is flowing.
9.3	Assemble bridge plug and squeeze packer on coiled tubing.
9.4	Set up coiled tubing injection system on wellhead.
9.5	Open gate valve and establish fluid control.
9.6	Run coiled tubing with bridge plug into position over the last waste package.
9.7	Activate bridge plug and confirm set.
9.8	Release coiled tubing from bridge plug, and confirm release.

Individual steps for setting a cement interval plug are given in Table 6-13. This analysis presumes that proper setting of a mechanical interval plug provides adequate protection for previously emplaced waste packages, and this activity sequence is not addressed in detail in this analysis. The events and fault trees developed here consider the performance of the interval plug in an integral fashion.

At the completion of both these sequences, mechanical and cement plugs establish a load path between the plug and the host rock, and no further mechanical load is placed on the previously emplaced waste package string.

If the interval plug is set after the final waste package string has been placed in the borehole, the end state corresponds to Node J, *borehole filled, ready for borehole closure*. If another waste package string is to be placed, completion of this task along with completion of Sequence 8 achieves conditions for Node A, *ready to initiate next emplacement sequence*.

Table 6-13. Activity steps for setting a cement interval plug.

Step	Description
10.1	Set squeeze packer 10 meters above mechanical bridge plug.
10.2	Obtain and mix cement for plug.
10.3	Inject cement and spacer fluids in coiled tubing.
10.4	Release packer and raise coiled tubing (rinse tubing at the surface).
10.5	Verify no radiological contamination on coiled tubing as it is pulled up
10.6	Remove and clean coiled tubing system for next use.
10.7	Close gate valve and remove riser and injector head.
10.8	Recondition the wellhead to prepare for the next emplacement sequence.

6.10 Borehole Closure

Once an interval plug is placed over the final waste package string in a borehole, the borehole is closed. The coiled tubing is removed, and the wireline system, the headframe, and other equipment used for package placement are dismantled and moved to the next borehole. Shielding and wellhead components are also removed from the borehole pit.

The filled borehole is then sealed and closed. A workover drill rig is erected over the borehole, and the tieback guidance casing is pulled out and dismantled. The upper crystalline basement liner is then cut near the bottom using a specialized cutting tool, removed from the borehole, and dismantled. This leaves about 1 km (or more) of open borehole above the waste emplacement zone, with no casing present.

Details of sealing and plugging depend on conditions at an actual site, including regulatory requirements applicable to that site. In general, the workover rig with a string of drill pipe, and appropriate wireline tools, are used to place a series of cement and clay (bentonite) plugs in the uncased seal zone, interspersed with lifts of sand, cemented ballast (crushed rock), and other materials.

The final interval plug provides protection for the emplaced waste packages during borehole closure activities, and no radioactive material is handled. Borehole closure is not within the scope of the analysis presented in this report.

7 HAZARD REVIEW AND ANALYSIS

7.1 General Approach and Preliminary Screening by Activity Sequence

A hazard analysis for radiological risk was prepared earlier to identify potential initiating and contributory events for use in development of this PRA model. Although the events modeled in this PRA differ from the specific events in the hazard analysis, the hazard analysis served as a primary basis for identifying events used in this model. It also serves as the structure for the external event analysis presented in Section 12.

The approach used for the hazard analysis began by defining the process flow diagram and the activity sequence steps shown in the previous sections. A standardized set of hazards were identified, and each activity step was screened against these hazards. An equipment list was prepared, and the equipment used in the performance of each sequence was identified and considered in identifying hazards and potential events. These were checked against other resources, including earlier evaluations of borehole technology and earlier work prepared by BSC for the Yucca Mountain repository to prepare a master list of potential initiating and contributory events. Finally, a select set of events were described in event sequence diagrams.

The master logic diagram shown in the next section is based on the events selected during the hazard analysis exercise. The event sequence diagrams are not repeated in this document, but are included in a previous report (Peretz and Hardin 2017). The events in the hazard analysis are reflected in the PRA model, but are further condensed to facilitate completion of a PRA model compatible with the level of design and operation definition available at this stage of borehole disposal development.

7.2 Hazard Screening by Activity Sequence

The matrix used to screen activity steps against hazard categories is attached to this report as Appendix B. The activity sequence steps are as shown in Section 6. Each step is assessed against seven hazard categories; two additional categories are used to provide documentation for steps that are not carried forward in the analysis. The seven action categories are as follows:

- *Lift*, generally referring to a lift of a cask containing a waste package or a lift of other objects with the potential for dropping that object on a cask containing a waste package.
- *Cradle roll*, in which a cask containing a waste package is moved horizontally on a track-mounted cradle.
- *Shield plug* manipulation, in which changes are made to shield configurations at the end of a cask containing a waste package.
- *Shield slide* manipulation, in which the sliding portion of the interface shield is moved, potentially changing the shield interface between cask and interface shield or the passage from cask to cask.
- *Package latch* mechanism manipulation or package *movement*, in which a non-wireline latch mechanism is attached to, removed from, or used to move a waste package.
- *Wellhead system* operation, referring to activities that orient a transfer cask over a wellhead station (either the wellhead flange or the lower plug removal station), that

connect the transfer cask to the wellhead flange, or that connect the package in the cask or other downhole equipment to the wireline.

- *Wireline* operation, addressing sequences in which the waste package is lowered into an open borehole, the wireline and tool string are retrieved from an open borehole, or qualification or other equipment is run down and up a borehole over an uncovered emplaced waste package.

The two categories used to document why steps are not considered further are:

- *Verification* action only, addressing steps that confirm the status of the system prior to performing the next action step (no direct action, and thus no physical hazard, is covered by these steps).
- *Not selected* for radiological hazard evaluation because the activity described either does not involve handling of radioactive materials, or is a simple activity that poses no credible radiological risk.

The matrix shown in Appendix B documents the screening of each activity step against these seven categories. In most cases, a single category is associated with the step. A few steps involve multiple hazards; some include both a confirmation and a potential response action with possible risk.

7.3 Equipment used in each Activity Sequence

A similar matrix was used to assess which activity sequences use which equipment items. The matrix, included as Appendix C, lists equipment by system and provides columns for Activity Sequences 1 through 10 (final borehole closure is not included, as radiological risk is not anticipated under normal operations).

Some equipment items are used in only one activity sequence; many items are used in multiple sequences. Most items are handled in Activity Sequence 8, under which equipment is reconditioned as needed and prepared for the next operating sequence. However, under normal operation, no radioactive material is handled during reconditioning and thus no immediate radiological risk is incurred.

This matrix is used as a check against the screening of hazards by action step. For example, if the screening for a specific sequence did not identify lift hazards, but a crane was used to perform the sequence, the screening would be reviewed to check if a hazard was not properly identified.

Hazard and Operations Analysis

Based on the screening of activity steps against the hazard categories, and referencing the equipment used in each sequence, lists of potential initiating and contributory events were prepared. First, a master list of all events associated with the identified hazards was prepared. Other resources including earlier borehole studies and the Yucca Mountain repository safety analysis report and supporting documents were reviewed for other events that might be relevant to the hazard analysis. This master list was then used as a reference to prepare specific event tables for each activity sequence (Peretz and Hardin 2017, Section 5).

A small number of events from each table were highlighted, as indicated in the tables. These events, still grouped by hazard category, were then used to draw a series of event sequence diagrams. There are a total of 22 event sequence diagrams (Peretz and Hardin 2017, Section 7).

Each diagram identifies initiating events around a central event, and tracks the potential consequences associated with the events. The most common consequence is worker exposure, but in some cases the event sequence may result in other consequences such as a release of radioactive material.

The Yucca Mountain license application was based on similar evaluations, including a structured HAZOP identification process. The methodology used in the borehole hazard analysis is based on the same type of evaluations as were used by BSC to prepare the HAZOP forms, but the borehole analysis did not actually produce the HAZOP tables themselves. A few examples, such as shown in Appendix D, were used to demonstrate that the two analyses were equivalent.

The event tables were also used to prepare a master logic diagram, as shown in the following section. This diagram contains all of the individual events identified by hazard category. The highest-level master logic diagram shown in Figure 8-1 identifies the event table from Peretz and Hardin (2017) that is applicable to each sequence and hazard category.

8 MASTER LOGIC DIAGRAM

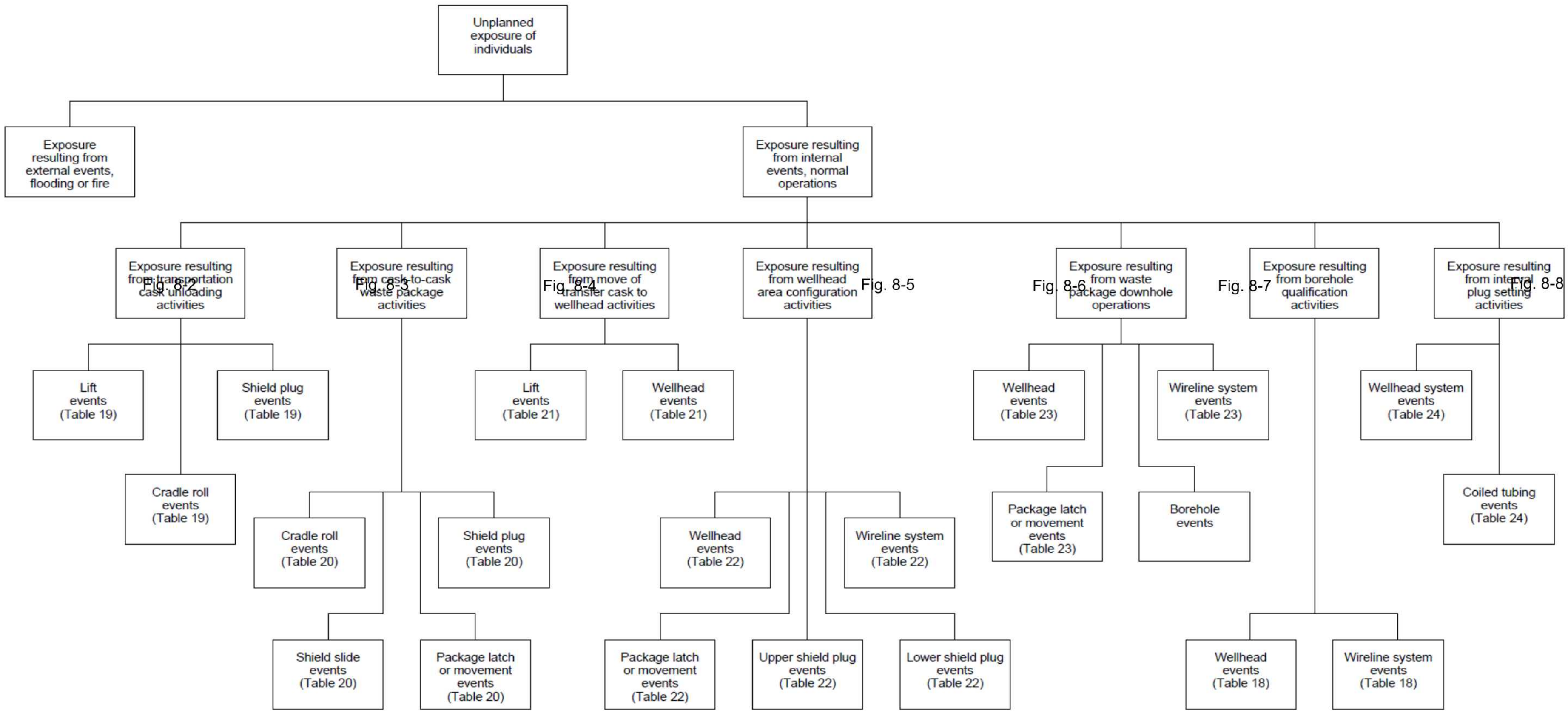
The master logic diagram (MLD) is a tool that captures the hazards, locations, activities, and initiating events associated with a process. The MLD discussed here (Figures 8-1 through 8-8) uses the PFD for the activity sequence structure (Figure 5-1), and is based on the activity sequences described in Section 6. The MLD identifies selected initiating events for each activity sequence, by hazard category (Peretz and Hardin 2017). The MLD presented here is an earlier step in the evolution of the DBD operational risk model. In subsequent sections of this report, the events from all hazard categories are merged, and in some cases further down-selected, to prepare the event and fault trees shown in Sections 9 and 10. In other words, the fault tree and event tree analyses relate to somewhat simplified MLDs, and some off-normal events are neglected because they are considered to be very unlikely or to have insignificant consequences.

The MLD uses a layered structure, with an entry point that describes the undesired condition for the borehole disposal facility. Because this analysis addresses radiological risk, the entry point (Level 0) is the undesired condition of unplanned exposure of individuals to radiation. The descending layers of the MLD describe events, pathways, and activity boundaries as described in Table 8-1.

Table 8-1. Master logic diagram level descriptions (based on BSC 2008a).

Level 0	The entry point into the MLD is an expression of the undesired condition for a given facility. Level 0 is the highest-level of the MLD. This includes direct exposure to radiation sources, or exposure as result of release of airborne radioactive material or conditions that could lead to a criticality. The basic question answered by the MLD through the decomposition is “How can the highest-level event occur?”
Level 1	This level differentiates between internal events and external events. The external event development at this level would be for initiating events that affect the entire facility (e.g., seismic ground motion). Common cause initiating events that affect less than the entire facility are incorporated at the appropriate level in the MLD.
Level 2	This level identifies the operational area where the initiating events can occur.
Level 3	This level identifies the exposure pathways of concern for the operational areas identified in Level 2.
Level 4	This level identifies the specific operational activities to be evaluated.
Level 5	This level specifies the initiating event that can result in the failure in the specified operational activity (i.e., the actual deviations from successful operation that could lead to the exposure type). Level 5 is considered the appropriate grouping of initiating events for purposes of subsequent fault tree analysis.
Level 6	This level provides a short list of examples (one or two) to help elucidate the interpretation of the Level 5 initiating event group. Each Level 5 initiating event is modeled in detail by a combination of fault trees and/or direct use of empirical information. Level 6 entries, therefore, are found as failure modes in fault trees.

The highest-level master MLD is shown in Figure 8-1. Under the highest-level event box (Level 0) the diagram branches into internal and external events. As presented, the MLD provides details for internal events that are deviations from normal operations. In the master diagram, operational areas (activity sequences) and pathways are combined into single boxes showing combined Levels 2 and 3. These levels are separated in the MLD detail figures that follow (Figures 8-2 through 8-8). Events are collected by operational activity in Level 4. Initiating events for each of these Level 4 activities are described in the MLD detail figures. The MLD only shows events associated with activity sequences that can lead directly to the highest-level condition, unplanned exposure of personnel to radiation (see Table 12-2 for a summary of initiating events). Sequences for delivery of the cask by truck, reconditioning of equipment for the next operating sequence, and setting cement interval plugs have not been associated with events that directly lead to radiation exposure under normal operating conditions, and are thus not included in Figures 8-1 through 8-8.



Note: Figure numbers refer to this report, while table numbers refer to Peretz and Hardin (2017).

Figure 8-1. Highest-level master logic diagram.

Figure 8-2 shows the MLD details for transportation cask preparation and movement from the trailer to cradle #1. The MLD acknowledges the possibility of structural damage to both cask and waste package, leading to direct exposure of on-site workers to radiation and release of radioactive material (on a scale that impacts on-site workers only, or a larger scale that could have off-site impacts). However, such releases are considered to be not credible for risk analysis, because of the assumed remote location and the robust waste packages. Events are correlated with lift activities, horizontal movements (cradle roll), and activities that could impact the cask end shield plug. There are nine initiating events in three hazard categories shown in Figure 8-2; these are merged and down-selected to six "top events" in the corresponding event tree shown in Section 9.

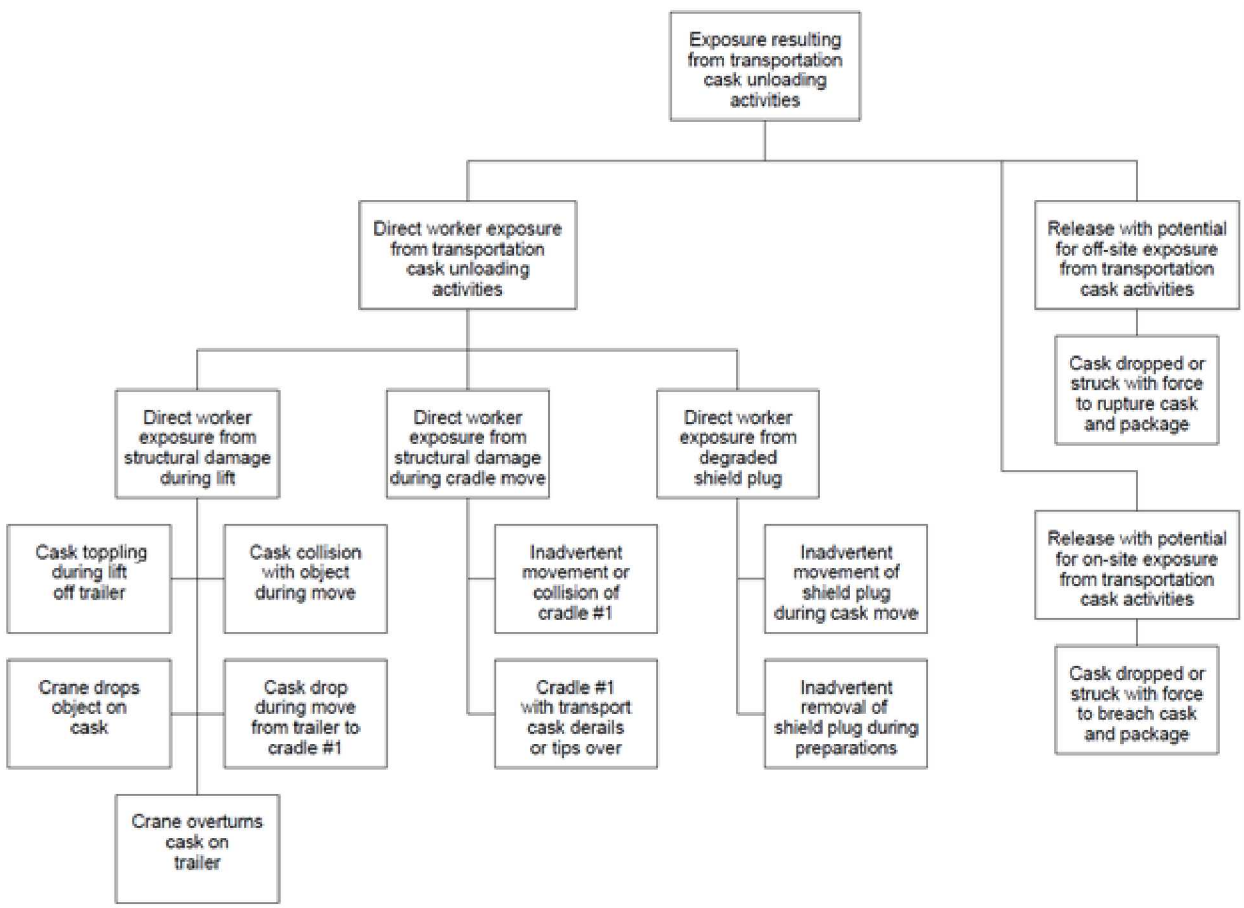


Figure 8-2. MLD detail for transportation cask unloading events.

MLD details for transferring the waste package from the transportation cask to the transfer cask are shown in Figure 8-3. Casks are raised from a horizontal to vertical position, lifted, moved horizontally to the transfer station, and laid down in a cradle. The primary hazard is the potential for direct worker exposure during various changes in shielding configuration as the transportation cask is opened, the interface shield is repositioned, the waste package is pulled from the transportation cask to the transfer cask, and the transfer cask shield plug is inserted and clamped. Drops during lifting operations are included in the analysis, but releases are not included for the reasons given previously. The MLD shows events for off-normal horizontal cask movement (cradle roll), shield plug manipulations, sliding interface shield manipulations, and package latch and movement activities. Once at the transfer station, physical damage to the waste package could conceivably occur as it transits the interface shield (e.g., shearing the package with the slide mechanism).

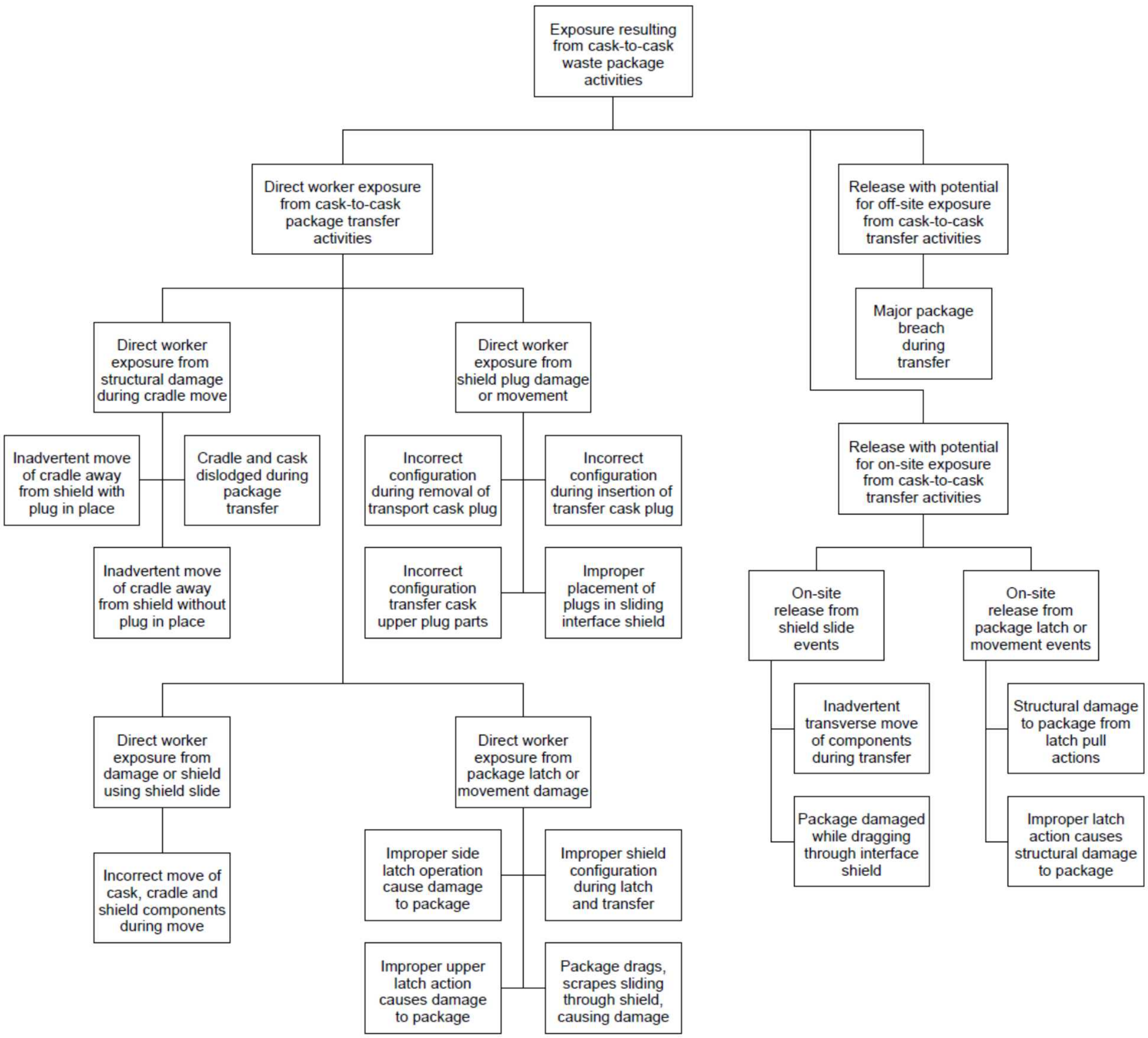


Figure 8-3. MLD detail for waste package transport cask to transfer cask move events.

Figure 8-3 shows 12 initiating events under four hazard categories for worker direct exposure. The events associated with on-site or off-site releases are not included in the risk analysis because of the assumed remote location away from population, and robust waste packages. These 12 are condensed and down-selected into ten “top events” in Section 9.

The MLD detail for movement of the loaded transfer cask from cradle #2 to the wellhead (Figure 8-4) reflects most of the pathways, activities, and initiating events for the movement of the transportation cask to cradle #1, as well as activities and initiating events related to the operation of the wellhead pit shield components. As with transportation cask lift and movement, damage to both cask and waste package is considered. Mechanical failure as the cask is inserted into the pit shield carousel is also included.

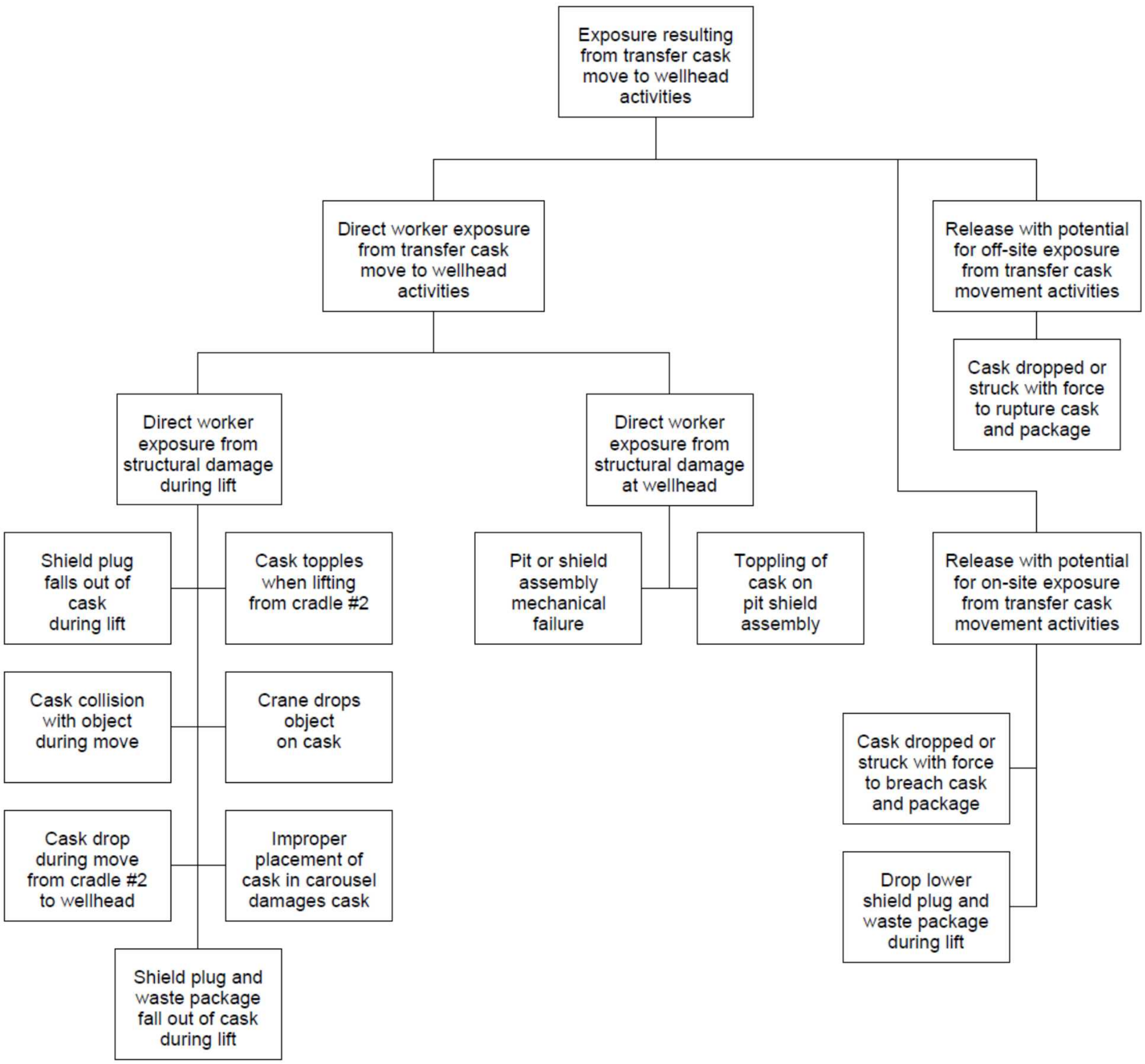


Figure 8-4. MLD detail for transfer cask move to the wellhead events.

The waste package remains in the cask throughout this sequence, and no intentional movement of either the cask upper shield plug or lower shield plug is planned (Figure 8-4). Nine initiating events under two hazard categories are shown (not including those associated with releases) and these are condensed into eight "top events" in Section 9.

Wellhead configuration is one of the more detailed operating sequences in the PFD, using a range of components. Exposure pathways include damage to cask and waste package, with the potential for structural or operational failure of the pit shield system including function of the central carousel and kneeling jacks (Figure 8-5).

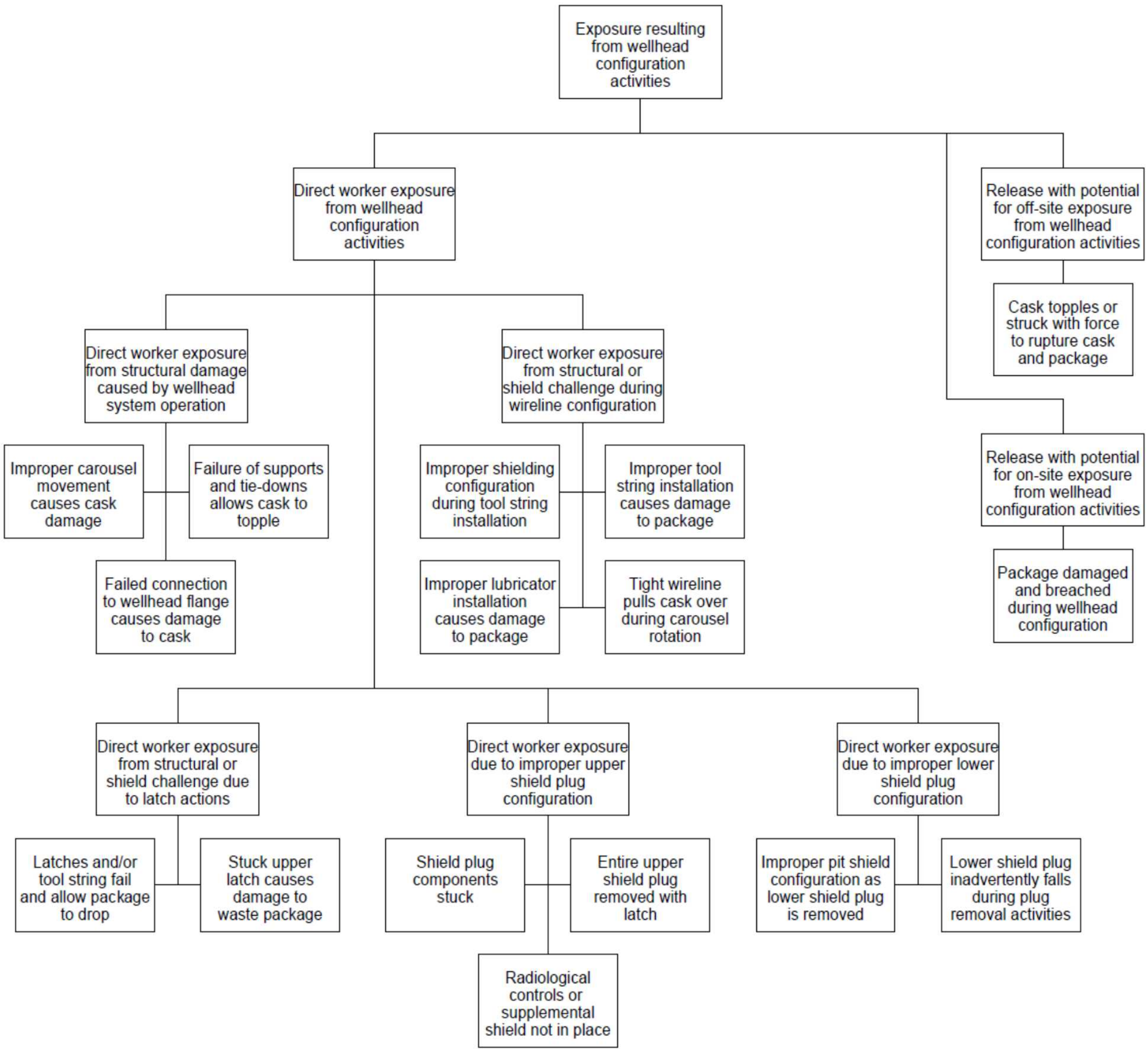


Figure 8-5. MLD detail for wellhead configuration events.

Potential for worker exposure exists with actions affecting configuration of the transfer cask upper shield plug, actuation of the top and side latches holding the waste package in place, connection of the wireline tool string to the waste package and connection of the lubricator and grease injector section to the top of the transfer cask. Although the pit shield should protect against exposure, removal of the transfer cask lower shield plug and connection of the transfer cask lower flange to the wellhead flange may also lead to exposure events, particularly if coupled with side latch or wireline latch failures. Loss of electrical power, loss of data or functional safety systems, or flooding of the wellhead pit may also contribute to radiological exposures.

Aside from rotation of the carousel, the physical position and orientation of the transfer cask remains static, and the position of the waste package in the transfer cask does not change (the side latches are to remain engaged at all times, and at least two failures are required to drop a waste package out of the cask). The MLD detail for wellhead configuration is depicted in Figure 8-5. For worker exposure, 14 initiating events under five hazard categories are shown (hazards with the top and bottom shield plugs are treated separately). These are condensed into six “top events” in Section 9.

The MLD for downhole wireline emplacement of waste packages has a somewhat different structure than the earlier sequences (Figure 8-6). Initial surface events that might lead to direct radiological exposure include latch or wellhead operational events. Package structural integrity could be challenged by actuation of the BOP or gate valve as the waste package transits the wellhead components, leading to a release of radioactive material downhole, but near the surface.

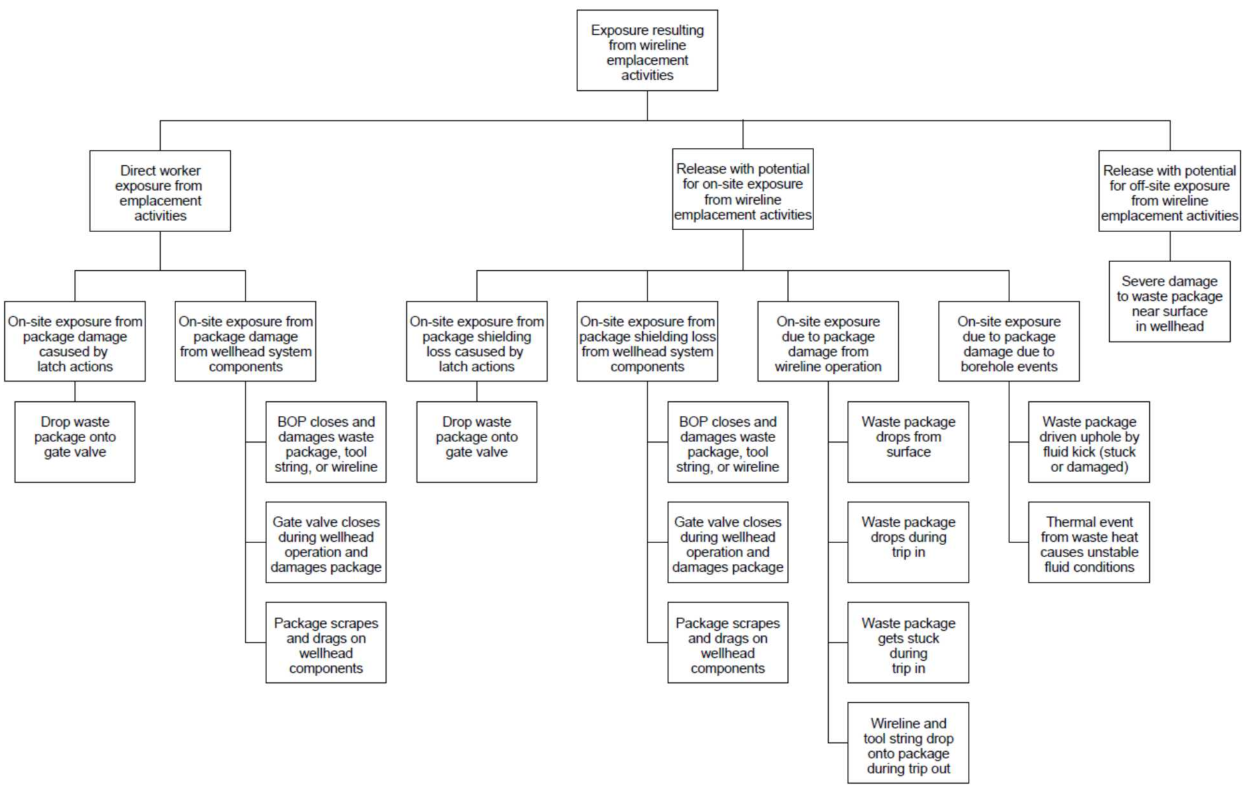


Figure 8-6. MLD detail for downhole wireline waste package emplacement events.

Once emplacement is underway, the waste package is immersed in borehole fluid and radiation from unshielded packages no longer reaches the surface. At this point the most likely hazards shift from direct exposure to radioactive material releases downhole.

Emplacement hazards include packages being damaged or stuck during the trip in, either within or above the emplacement zone. Breached waste packages could release radioactive material into the borehole fluid, which is not a direct radiological hazard to the emplacement operation. Once waste package breach was detected by radiation monitoring of the borehole fluid, further fluid circulation would be deferred to a recovery program that is beyond the scope of this assessment (onsite and off-site releases would be addressed by recovery planning). Wireline emplacement risk has been evaluated in earlier studies (SNL 2016) and events consistent with those analyses are included in this diagram, and included in the risk analysis.

Once waste package emplacement is complete, the radiological risk is limited to the potential of further actions causing damage to emplaced packages. An example is a drop of the tool string during trip out. The MLD detail for the wireline emplacement sequence is shown in Figure 8-6. For the downhole branch, ten initiating events are shown; four of these are also shown in the worker exposure branch. In Section 9, these are condensed into six "top events."

MLD details for borehole qualification using a wireline tool string and for setting of an interval plug using coiled tubing are generally similar. No radioactive material is intentionally handled during either operation; radiological risk is posed only by the potential for downhole damage to previously emplaced waste packages. For normal operations there is no credible risk for direct radiation exposure to workers, and any detected radioactive material release into the borehole would result in suspension of operations.

Initiating events impact wellhead operations (such as activation of the gate valve or BOP causing a drop of a tool string onto emplaced waste packages) or wireline or coiled tubing system failures. The MLD detail for borehole qualification activities is shown in Figure 8-7, and the equivalent detail for setting the mechanical bridge plug is shown in Figure 8-8. Three initiating events are shown for each; these are carried forward into Section 9 as "top events." One additional event is added to the interval plug event tree in Section 9.

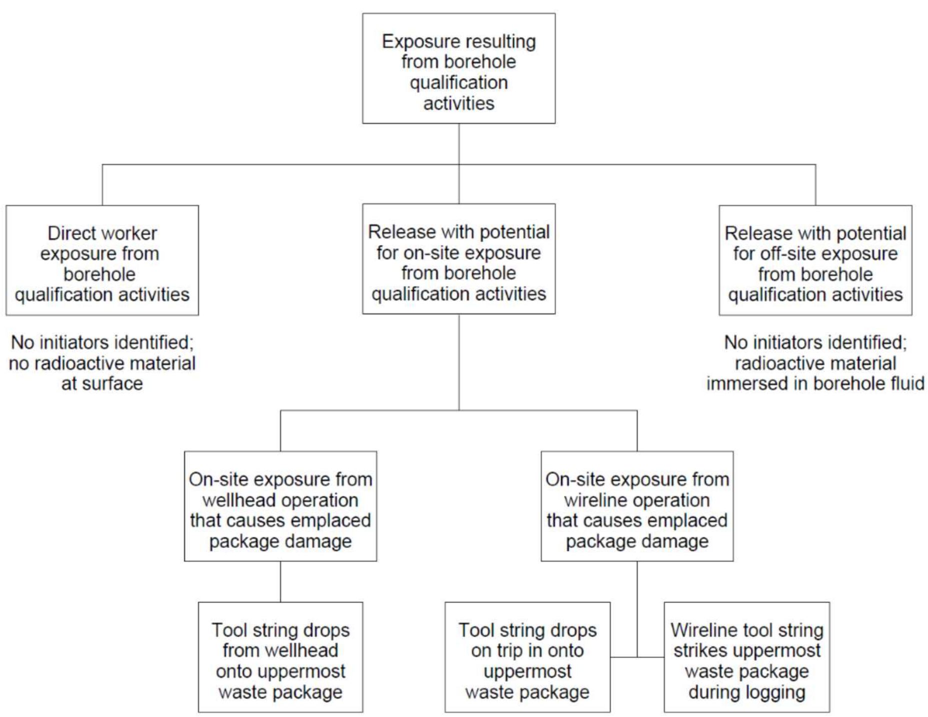


Figure 8-7. MLD detail for borehole qualification events.

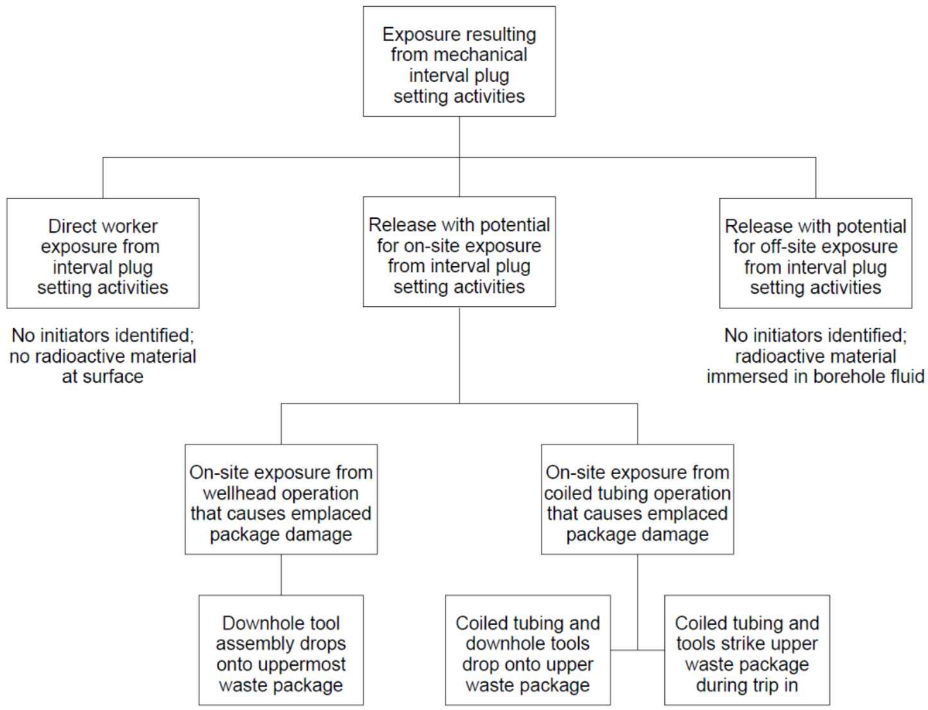


Figure 8-8. MLD detail for mechanical bridge plug setting events.

9 EVENT TREE DEVELOPMENT FOR ACTIVITY SEQUENCES

This section describes the event trees for each activity sequence with the potential for worker exposures or release of radioactive material. It describes the "top events," and the end states associated with success or failure of the top events. Top events are defined as the important success-oriented, positively stated, independent events in an event tree for which the uppermost path is success. At this stage of the design, numerical quantification of dose or radiological release consequences is not attempted. Instead, the radiological consequence associated with each end state is binned into general categories as shown in Table 9-1.

Table 9-1. Consequence categories.

Category A	**Success**
Category B	Loss of shielding and <u>minor</u> worker exposure
Category C	Loss of shielding and <u>moderate</u> worker exposure
Category D	Loss of shielding with potential damage or displacement of waste package, but low potential for release of radioactive material
Category E	Loss of shielding with potential damage or displacement of waste package, and credible, significant potential for release of radioactive material
Category F	Downhole waste package impact with <u>low</u> likelihood of package breach
Category G	Downhole waste package impact with quantified probability of package breach

Category A is the successful completion of the activity sequence. Categories B and C describe end states with the potential for low to moderate worker exposure to penetrating radiation, without release of radioactive material. The lower Category B would likely lead to exposures within occupational limits; Category C could involve exposures beyond those expected in normal operations and exceeding occupational limits.

Categories D and E address surface handling events in which a waste package may be damaged or displaced outside of its intended shielding. Category D is used for end states in which damage or displacement may occur but the potential for release of radioactive material is considered low. Category E addresses end states, such as dropping a waste package out of a shield cask, where dose rates encountered in the event or later recovery operations may be significant and where a package breach and release of radioactive material is credible.

Categories F and G are used for downhole events. Category F is used for end states in which control of the waste package is lost but package breach does not occur. Category G is used for end states in which a downhole beach of a waste package does occur, with a release of radioactive material into the borehole and spread of contamination via circulation of borehole fluid.

Worker exposures may occur immediately upon an event failure, or may be incurred during recovery operations. For surface handling events, most event failure scenarios that could lead to immediate worker exposures would also likely have the potential for further exposures during recovery operations. In the case of a downhole event, end states other than those with gross contamination of borehole fluids would likely not result in an immediate worker exposure. For downhole events, however, recovery operations could be extensive and would likely incur the potential for worker exposures during recovery.

The likelihood for immediate dispersal of radioactive material beyond the site boundary is low, because of the robustness of waste packages and the low likelihood of events at the surface that could compromise containment. For downhole events involving the release of radioactive material, the release pathway would be via borehole fluid, and shut-in of the borehole and proper management of borehole fluid at the surface would be used to prevent off-site consequences. Most surface events are associated with improper operation or damage to shielding; these do not involve the release of radioactive material. A small set of very unlikely outcomes involve the potential release of radioactive material in air at the surface.

9.1 Borehole Qualification

The event tree for Activity Sequence 1, borehole qualification using wireline tools, is shown in Figure 9-1. Activity steps associated with these events were given as Table 6-1.

Conceptualization in the form of a MLD is provided in Figure 8-7. This is a simple event tree with three top events and no conditional events. The success sequence begins with insertion of the qualification tool string and wireline into the borehole. The tool string is run down the borehole over its intended interval, and retrieved from the borehole, without causing the tool string or wireline to crash into the last previously emplaced waste package.

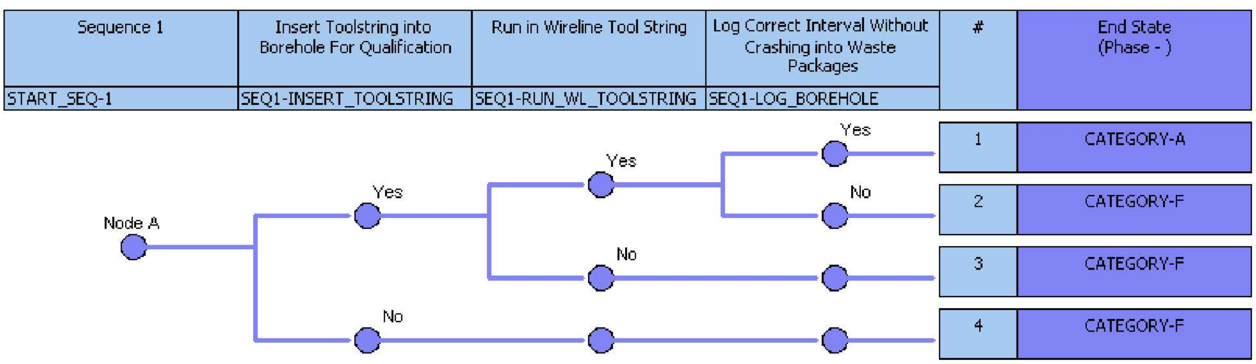


Figure 9-1. Event tree for Sequence 1, borehole qualification.

The four possible end states and the consequence categories applicable to each end state are shown below:

1. Success
2. Tool string crashes into waste packages; Category F.
3. Tool string dropped onto waste packages during run in; Category F.
4. Tool string dropped onto waste packages during insertion; Category F.

Two types of adverse occurrences are encountered; the tool string may be dropped onto a previously emplaced package or the wireline may not be stopped before the tool string crashes into the top package. The qualification tool string is not especially heavy, and borehole fluid limits the speed of a potential impact from a dropped package. Impact energy imparted onto the top waste package would likely be insufficient to cause package breach, and the downhole end states other than success are classified as Category F. The possibility for further damage during recovery operations is unlikely; without release of material there would be no worker exposure during recovery.

Fault trees and basic event probabilities for the three events shown in Figure 9-1 are discussed in Section 10.1.

9.2 Waste Package Receipt

Delivery of the waste package in a licensed transportation cask is described as Activity Sequence 2 in Table 6-2. These activity steps are limited to the arrival and positioning of the trailer containing the transportation cask at its intended location on site. The trailer is not opened, and no cask dismantling activities such as removal of impact limiters are performed in this sequence. Although the cask contains a radioactive waste package, it remains in its certified shipping status. Radiological safety of handling radioactive material in a qualified transportation system is not within the scope of this study, and no event tree is prepared for this activity sequence.

Transportation Cask Unloading and Move

The event tree for preparing and moving the transportation cask from its shipping trailer to cradle #1 is described as Activity Sequence 3 and individual steps were listed in Table 6-3. Conceptualization in the form of a MLD is provided in Figure 8-2. The event tree is shown in Figure 9-2. The tree has six basic events; there are no conditional events in this tree. The first event in the success path is lifting the transportation cask off the trailer cradle without tipping. The cask is then lifted above the cradle without dropping. Movement events include move without collision and move without dropping. Once moved over cradle #1, the cask is set onto the cradle and secured. The final event is to roll cradle #1, with the transportation cask, into position against the interface shield.

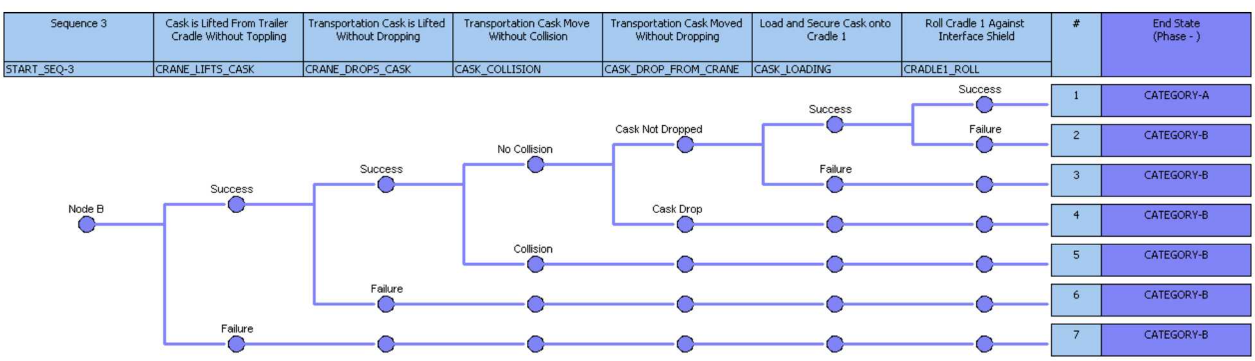


Figure 9-2. Event tree for Sequence 3, prepare and move transportation cask to cradle #1.

Possible end states and the consequence categories applicable to each end state are shown below:

1. Success
2. Cask collision during cradle roll causes cask damage, Category B.
3. Cask damage while lowering and securing in cradle #1, Category B.

4. Cask dropped while moving with mobile crane, Category B.
5. Cask collides with object during move, Category B.
6. Cask lifted without dropping (initial crane or rigging failure), Category B.
7. Cask topples while lifting off transportation trailer cradle, Category B.

The transportation cask is designed for road accidents, and has only one plug (at the top). Although the cask is being handled without its impact limiters in place, the lift heights are minimal and the possibility for serious damage is not significant. Appendix A provides a preliminary fragility analysis for a 3-meter cask drop in air onto a compacted gravel base, and shows that the resulting waste package stresses are not likely to cause damage. The shield plug is not removed during this sequence, and the cask design does not place the plug in a vulnerable configuration. The most likely consequence of a cask drop or collision would be cask deformation such that it no longer completely accomplishes its shielding function, possibly leading to a brief exposure of personnel to penetrating radiation. The event would be easily recognized, and personnel would move away immediately. Thus, all end states other than the success path are shown as Category B. Additional radiological dose could be incurred during recovery operations.

Fault trees and basic event probabilities for the six events shown in Figure 9-2 are discussed in Section 10.3.

9.3 Cask-to-Cask Waste Package Transfer

The event tree for Activity Sequence 4, transferring the waste package from the transportation cask to the transfer cask, is shown in Figure 9-3. Activity steps for this sequence were shown in Table 6-4. Conceptualization in the form of a MLD is provided in Figure 8-3. A broader range of radiological hazards are encountered in this sequence compared to the previous set. The event tree has ten top events and several conditional events.

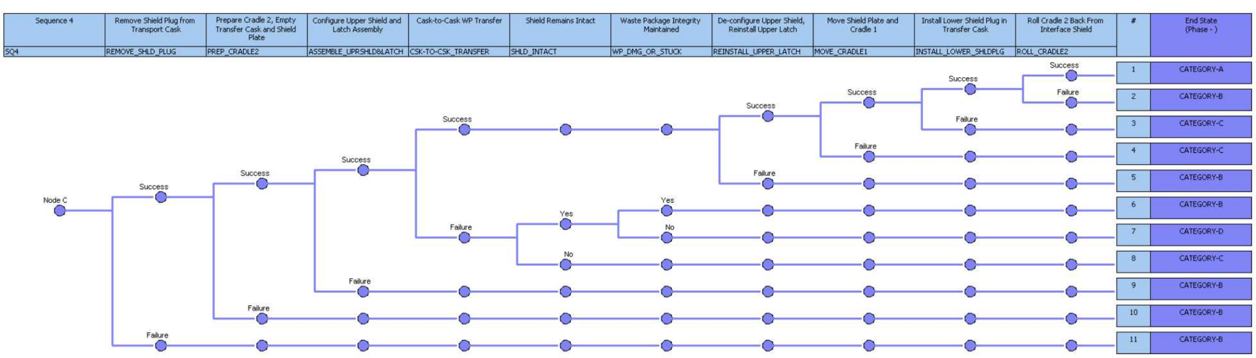


Figure 9-3. Event tree for Sequence 4, transfer waste package to transfer cask.

This activity sequence is based on sequential operations involving the transportation cask, the transfer cask and its latch mechanisms and end shields, the interface shield (especially the slide shield), and the cradles supporting the two casks. The first event in the success path is to pull the shield plug off the transportation cask into the shield slide. The second event is to roll cradle #2 up to the interface shield and reposition the slide. Next, the upper transfer cask shield components are reconfigured to prepare for latching onto the waste package. In the fourth event, the latch is engaged with the waste package and the package is pulled from the transportation cask into the transfer cask. Two conditional events follow; one accounts for possible failures in the overall shield configuration during the transfer, and the second accounts for the possibility of physical damage to the waste package as it is dragged through the interface shield into the transfer cask.

Assuming success in the transfer, the next event on the success path is to de-configure the transfer cask upper shield plug components, including the use of a pull test to demonstrate that both the side latches and the central latch effectively grasp the waste package. Next, the shield slide is moved to its third position to allow insertion of the lower shield plug and the transportation cask on cradle #1 is rolled away to provide access for the insertion process. The shield plug is then installed and clamped in place. The final event is to roll the transfer cask, on cradle #2, away from the interface shield into a position where it can be picked up with the gantry crane.

The possible end states and associated consequence categories are described below:

1. Success
2. Transfer cask collision damage during cradle #2 roll, Category B.
3. Failure to properly install lower shield plug in transfer cask, Category C.
4. Improper movement of shield plate or cradle #1 causing loss of shielding, Category C.
5. Improper configuration of transfer cask upper shield and latch after move, Category B.
6. Waste package transfer mishap without damage to waste package, Category B.
7. Waste package transfer mishap with unspecified damage to waste package, Category D.
8. Improper movements cause loss of shielding during transfer, Category C.
9. Improper configuration of transfer cask upper shield and latch prior to move, Category B.
10. Improper movements of shield plate or empty transfer cask cause loss of shielding, Category B.
11. Improper removal of transport cask shield plug, Category B.

Consequence categories vary throughout this event sequence. Failures involving manipulations of the transportation cask shield plug or the top shield plug assembly on the transfer cask have the potential for a relatively small worker dose, especially with an integral shield in the top of the waste package. Thus, end states 11, 10, 9, and 5 are correlated with Category B consequences. Similarly, workers would not likely receive a significant dose in the event of a failure to complete the package transfer but without damage to the package (end state 6). The kinetic energy of a cradle roll event (end state 2) would be low. These two end states thus are also correlated with Category B consequences.

Event failures while working near the transfer cask lower plug, with a waste package present, have the potential for somewhat higher worker doses. Thus, end states 3 and 4 are assigned consequence Category C. Similarly, loss of shielding during transfer (such as a cradle and cask pulling away from the interface shield) would create the possibility of a more direct exposure to radiation from the waste package, and thus end state 8 is assigned consequence Category C.

Finally, end state 7 represents an event in which a waste package is physically damaged and radioactive material may be released. Because of limited force expected to be applied to the waste package, such damage would be limited and the end state is assigned consequence Category D.

Most of these events also carry the potential for worker exposures during recovery operations. This may especially apply to events in which the waste package transfer itself cannot be completed.

Fault trees and basic event probabilities for the ten events shown in Figure 9-3 are discussed in Section 10.4.

9.4 Transfer Cask Move to the Wellhead

The event tree for Activity Sequence 5, moving the loaded transfer cask off cradle #2 and securing it in the wellhead shield assembly, is shown in Figure 9-4. Activity steps for this sequence were shown in Table 6-5. Conceptualization in the form of a MLD is provided in Figure 8-4. Radiological hazards are encountered should a variety of lift or toppling events occur. Since the transfer cask has a somewhat exposed lower shield plug, there is a remote possibility that a sequence of failures can lead to an air drop of a waste package. The event tree, shown in Figure 9-4, has eight top events, including conditional events.

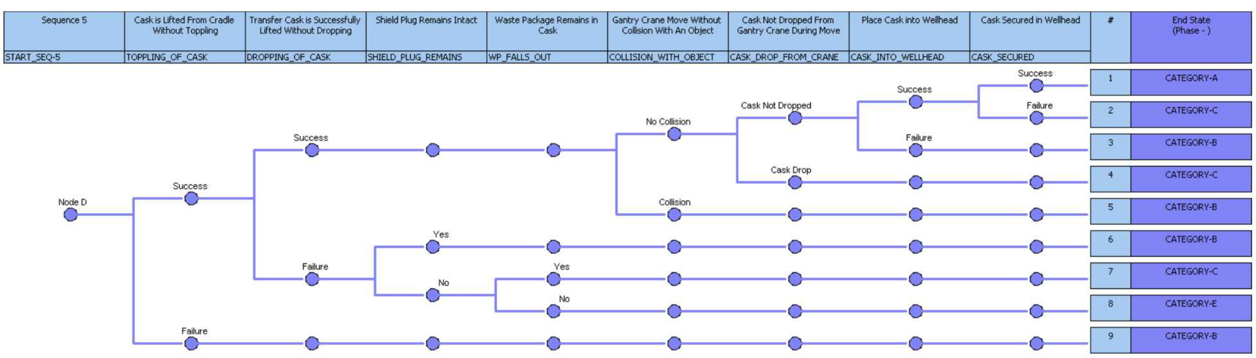


Figure 9-4. Event tree for sequence 5, move loaded transfer cask to wellhead station.

The first event is to lift the transfer cask off cradle #2 without toppling, followed by continuing to a full lift without dropping. Should the lift fail, two conditional events are considered. The first is whether the lift failure (drop) results in the lower shield plug being dislodged. Should the plug be dislodged, the second conditional event considers whether the waste package remains captured by the top latch and side latches in the cask. Failure of both conditional events could lead to an air drop of the unshielded waste package out of the transfer cask.

Assuming the transfer cask is successfully lifted away from cradle #2, the event sequence continues with movement without collision (relatively likely, since a controlled gantry crane is being used), movement without dropping, and successful placement into the opening in the wellhead shield. The final event is to secure the transfer cask in a vertical orientation on the lifting jack system, positioned over the lower shield plug removal station.

The possible end states and associated consequence categories are as follows:

1. Success
2. Cask topples while being secured in wellhead causing cask and shield damage; Category C
3. Cask lower components or wellhead shield damaged as cask is lowered; Category B
4. Cask dropped onto lower components during move with gantry crane, Category C
5. Cask collides with object during move by gantry crane, Category B
6. Cask dropped when lifted causing potential loss of shielding, but shield plug and waste package remain intact, Category B
7. Cask dropped when lifted and shield plug dislodges, but waste package remains captured, Category C
8. Cask dropped when lifted, shield plug dislodges, and waste package is dropped from cask, Category E
9. Cask topples while being lifted out of cradle #2 causing damage to cask, Category B

In order to enable a pressure-tight connection to the wellhead, the lower cask components extend below the main cask body. This leaves the lower flange and shield plug exposed, and thus damage to these components is associated with a greater personnel exposure risk (Category C consequence). In the case of damage while lowered into the wellhead shield, shielding in the pit mitigates the consequences and thus end state 3 remains Category B. Similarly, the additional control on movements associated with repetitive use of a gantry crane keeps end state 5 at Category B.

End states 6, 7, and 8 are associated with a drop of the transfer cask containing a waste package. End state 6 assumes the shield plug remains in place, limiting the consequence to Category B. End state 7 assumes the lower shield plug is displaced but the waste package remains in place, resulting in the higher Category C exposure. End state 8 assumes the shield plug is lost and the waste package falls out of the transfer cask, resulting in consequence Category E.

It is assumed that the energy available to cause damage during the initial lift while the cask is still partially engaged with the cradle is limited, so toppling associated with end state 9 results only in a Category B exposure.

Fault trees and basic event probabilities for the eight events shown in Figure 9-4 are discussed in Section 10.5.

9.5 Wellhead Area Configuration

Figure 9-5 depicts the event tree for Activity Sequence 6, configuration of the waste package, wellhead and wireline systems in preparation for downhole waste package emplacement. Activity steps for this sequence were presented as Table 6-6. Conceptualization in the form of a MLD is provided in Figure 8-5. The event tree shows six top events, performed sequentially. No conditional events are identified. The initial event is preparation of the upper latch and shield assembly for insertion of the wireline tool string, followed by the connection of the tool string to the waste package. The success path for the first event is that upper cask manipulations are performed without unplanned exposure of workers to penetrating radiation; the second addresses successful connection of the tool string without dislodging the waste package.

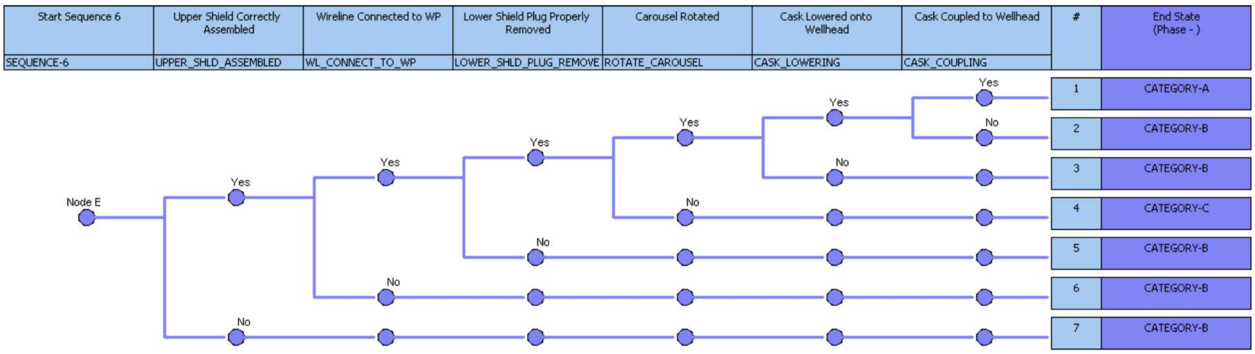


Figure 9-5. Event tree for Sequence 6, configure waste package, wellhead and wireline for emplacement.

The third event covers successful removal of the lower shield plug, using the remotely operated flange clamp and the plug handling station in the borehole pit. In the fourth event, the wellhead shield carousel, with the transfer cask, is rotated to move the cask from the shield plug handling station to its proper location over the wellhead. The final two events are to use the kneeling jack system to lower the transfer cask onto the wellhead, and to complete the flange connection between transfer cask and wellhead using the remotely-operated clamp. A pressure test is used in the last event to confirm an effective seal between cask and wellhead.

Potential end states and consequence categories are as follows:

1. Success
2. Damage or misalignment of the cask/wellhead system as the cask is coupled to the wellhead, Category B.
3. Damage occurs as the transfer cask is lowered onto the wellhead, Category B.
4. Cask topples as a result of improper rotation of carousel (collision or tie-downs) with no lower shield plug in place, Category C.
5. Failure to properly remove lower shield plug while cask is properly placed in wellhead shield, Category B.
6. Package drop during attachment of wireline tool string with no breach, Category B.
7. Loss of shielding during manipulation of upper shield components while attaching wireline tool string, Category B.

Many of these failures would occur with the transfer cask installed in the wellhead shield, and thus immediate dose consequences are minor (and may be mostly associated with recovery operations). In the case of end state 4, the cask containing a waste package topples after the lower shield plug has been removed, leading to Category C potential exposure levels. For end state 6, the package may be dropped within the established shield infrastructure, but package damage is not considered credible. Immediate dose consequences for this occurrence would be minor; additional dose may be incurred during recovery operations.

End state 2 describes a failure to properly make up the flanged connection between the transfer cask and wellhead. At the time the event occurs, consequences would be minor (retraction of the waste package and repair of the flange) and is shown as Category B. If not recognized, consequences may occur during Activity Sequence 7. If the alignment is close and there is no fluid excursion in the borehole, there may be no consequence or slow leakage of borehole fluid into the wellhead pit. If significant misalignment occurs, there is a possibility that the waste package cannot transit the wellhead, or becomes stuck in the wellhead. These impacts are addressed in the Activity Sequence 7 evaluation.

Fault trees and basic event probabilities for the eight events shown in Figure 9-5 are discussed in Section 10.6.

9.6 Wireline Emplacement of the Waste Package

The event tree for Activity Sequence 7, wireline emplacement of the waste package, is shown in Figure 9-6. Conceptualization in the form of a MLD is provided in Figure 8-6. This event tree combines the current activity sequences with analyses performed earlier and documented in the DBD conceptual design report (CDR; SNL 2016) with certain deviations that are explained in Section 10.7 (so that the assessment described in this report does not explicitly model recovery operations). The activity sequence steps for this sequence are documented in Table 6-7. The success sequence begins with release of the side latches and transition to supporting the waste package by wireline alone, with the gate valve closed. The gate valve is then opened, and the package is lowered into position, first without dropping, then with delivery to its intended location in the emplacement zone. The tool string is then released and retrieved along with the wireline.

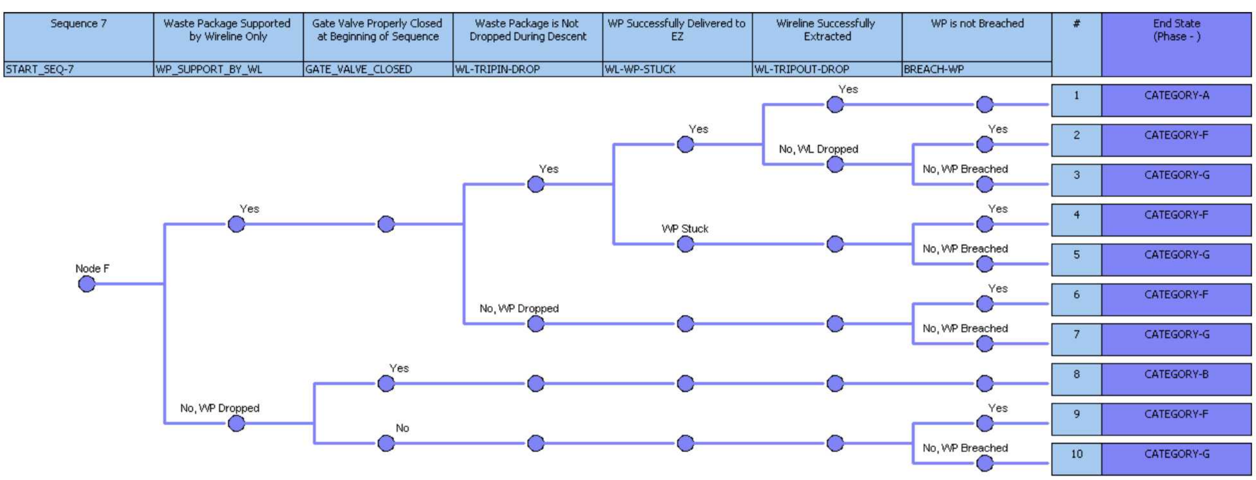


Figure 9-6. Event tree for Sequence 7, waste package emplacement, release, and wireline retrieval.

Two conditional events are added to the event tree. At the time the side latches are released, the gate valve is to be closed so a failure would result only in a short drop of the package onto the gate valve. If the gate valve is improperly open, the package may drop into the borehole. For all drops and impacts, a second conditional event addresses the integrity of the waste package; if integrity is maintained consequences are minimal (Category F) but if integrity is lost contamination of the borehole occurs (Category G). This conditional event is seen on four branches to the right on Figure 9-6.

End states and consequence categories shown in the event tree are described as follows:

1. Success
2. Wireline tool string drops on emplaced package during trip out (package not breached), Category F.
3. Wireline tool string drops on emplaced package during trip out (package breached), Category G.
4. Waste package not delivered to intended location in emplacement zone (package not breached), Category F.
5. Waste package not delivered to intended location in emplacement zone (package breached), Category G.
6. Waste package dropped during descent (package not breached), Category F.
7. Waste package dropped during descent (package breached), Category G.
8. Waste package drops from wireline at surface (gate valve closed), Category B.
9. Waste package drops from wireline at surface (gate valve not closed, package not breached), Category F.
10. Waste package drops from wireline at surface (gate valve not closed, package breached), Category G.

In the case of a package drop onto the gate valve, minimal if any damage should occur. It is likely that there is no immediate dose impact on workers; damage may be limited to deformation of the impact limiter. Small (Category B) dose impacts may result from recovery operations. Certain initiating events identified in Figure 8-6, including the BOP closing on a waste package, pressure "kicks" in the borehole, and thermal effects from packages on the borehole fluid, are not significant (thermal effects) or can be mitigated (using an annular BOP and a functional safety system to detect borehole anomalies).

Events during trip in, or should an initial drop occur with the gate valve open, may lead to a package that becomes stuck above its intended location (either in or above the emplacement zone) or is damaged or damages a previously emplaced package as it comes to a stop at the bottom. Possible recovery actions for a stuck package are addressed in the appendices to the CDR, and are not the subject of this report. For end states that do not involve a breached package, costly recovery operation may be called for but a contaminated borehole may be avoided and operator dose during recovery operations may be kept to a minimum (Category F). For end states with a breached package, recovery or premature borehole closure activities would likely be extensive, and borehole fluid may spread contamination and result in worker exposures (Category G).

Fault trees and basic event probabilities associated with the six top events associated with this event tree are described in Section 10.7

9.7 Conditioning of Equipment for Next Use

Preparation of the wireline system, the transfer cask and interface shield, and the wellhead, along with return of the transportation cask to the package loading site are treated as four sub-sequences, Table 6-8 through Table 6-11. Under normal operations, none of these sequences directly handle radioactive material or place waste packages at immediate risk. Thus, no event tree is developed for Activity Sequence 8.

Incorrect performance of actions included in Activity Sequence 8 may lead to failures that have radiological consequences but occur during the execution of other activity sequences. An example would be incorrect assembly of the wireline disconnect leading to a waste package drop in Activity Sequence 7. These events are treated under the activity sequence in which they occur.

9.8 Placement of Mechanical Interval Plug

Activity Sequence 9, placement of a mechanical bridge plug over an interval of 40 waste packages, resembles the activity sequence for borehole qualification. No radioactive materials are handled, and risk is limited to causing damage to previously emplaced packages. Key differences are that a coiled tubing system is used rather than a wireline, and the activity is performed only at completion of a package string rather than with every package. Action steps for this sequence were described in Table 6-12. Conceptualization in the form of a MLD is provided in Figure 8-8. The event tree consists of four top events as shown in Figure 9-7.

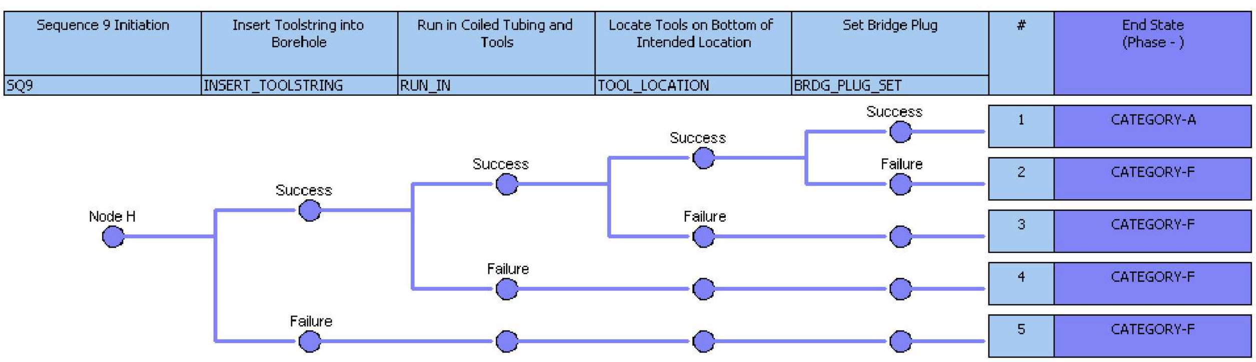


Figure 9-7. Event tree for Sequence 9, set a mechanical interval plug.

The first event shown is successful insertion of the tool string, on the coiled tubing system, into an interface mounted onto the wellhead in a manner similar to that used for the transfer cask. The coiled tubing with the tools is then run into the borehole without damage or dropping. The intended plug location is properly determined, and the coiled tubing is stopped without running into the previously emplaced package string. Finally, the mechanical bridge plug is activated and properly engaged in its intended location.

Setting of the mechanical bridge plug is followed by placing a cement plug in the borehole, including the annulus between the guidance casing and the rock structure. Since a properly set mechanical bridge plug would provide protection for the package string during the cementing process, no separate event sequence is provided for cementing (Activity Sequence 11, Table 6-11).

The event tree end states are correlated with consequence categories as follows:

1. Success
2. Bridge plug fails to set, leading to excess loading and damage to previously emplaced waste packages, Category F.
3. Bridge plug tool string on coiled tubing not properly stopped prior to impacting previously emplaced waste packages, Category F.
4. Coiled tubing breaks during run in, dropping tubing and bridge plug tool string on previously emplaced waste packages, Category F.
5. Tool string drops from surface during initial insertion activities, impacting previously emplaced waste packages, Category F.

By definition, this activity sequence is only performed for waste packages that are already emplaced in their proper location in the emplacement zone. The collective action of the impact limiters throughout the tool string provides the capability to absorb energy, and reduce the potential impact of a coiled tubing drop. Thus, all end states are limited to Category F. Because of the kinetic energy of a falling string and coiled tubing segment that might weigh several thousand pounds, the consequence of end states 4 and 5 could be more severe than end state 3.

Fault trees and basic event probabilities associated with the six top events associated with this event tree are described in Section 10.9.

10 FAULT TREES FOR TOP EVENTS

This section presents fault trees for the "top events" shown in the event trees in the previous section. It also shows the failure probabilities used as input for the risk model, on fault tree graphics generated using SAPHIRE (Smith et al. 2012). Failure probabilities given here are typical for equipment performance and human performance with similar processes. When practical, equipment and human performance is coupled to functional safety system features such as interlocks, or other mitigating factors such as supervision and procedures, to reduce failure rates for top events. Ultimately, event failure values have been adjusted to balance risk across the system. At this preliminary stage of design, many of the input values represent design goals rather than a specific performance analysis for an as-designed system.

Throughout this section, failure probability is presented with the sequence in which the failure occurs. In some cases, this means a failure represented in one sequence is the result of a failure to properly complete a step performed in an earlier activity sequence.

All failure probabilities are for a single emplacement sequence. Later sections will assess likelihood of success for a borehole or repository scale operation. In the case of Activity Sequence 9, placement of the mechanical interval bridge plug, the values are given for a single performance of that sequence. It should be noted that the interval plug sequence is performed at a different rate than the package emplacement sequence; if there are 40 packages between interval plugs, the interval plug sequence is performed once after every 40 emplacement sequences.

10.1 Borehole Qualification

Fault trees have been prepared to assess probability of failure to accomplish three top events:

1. Insert tool string into borehole.
2. Run in wireline tool string.
3. Log correct interval without crashing into packages.

Radiological risk in the qualification operation essentially results from events associated with improper insertion of the tool string into the wellhead causing a drop onto the previously emplaced waste packages, a drop of the tool string during run-in, or a tool string that impacts the emplaced waste packages due to a failure to stop prior to crashing into the waste packages. The steps for this activity sequence are given in Table 6-1. The event tree is presented in Figure 9-1. Fault trees are shown in Figure 10-1 through Figure 10-3.

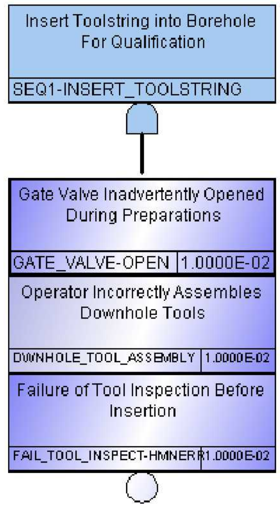


Figure 10-1. Fault tree 1.1, insert tool string into borehole.

Values used in Figure 10-1 are typical for human performance activities. The functional safety system may further mitigate against the gate valve being inadvertently opened during this activity. Further consideration of these operations can be found in the earlier analysis documented in Figure B-1 of the CDR (SNL 2016).

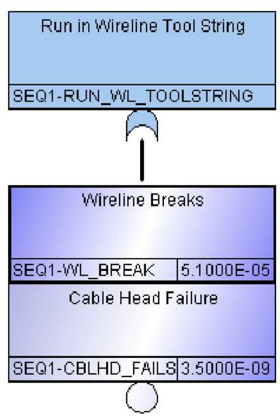


Figure 10-2. Fault tree 1.2, run in wireline tool string.

Input values for wireline breaks and cable head failure were taken from the earlier analysis of wireline operations, documented in Figure B-2 of the CDR (SNL 2016).

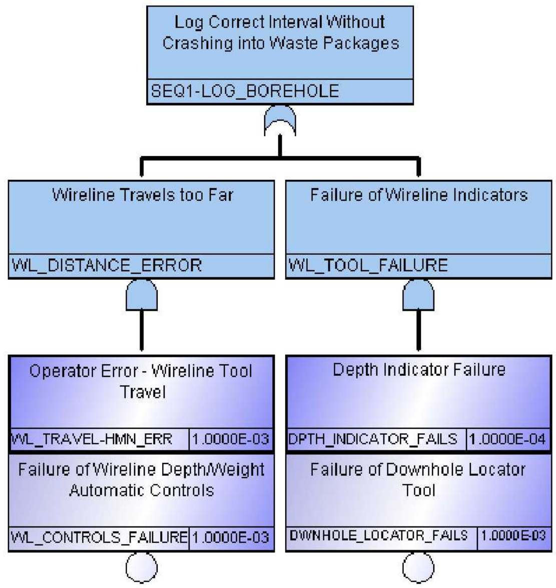


Figure 10-3. Fault tree 1.3, log correct interval without crashing into waste packages.

This fault tree also reflects the CDR effort (SNL 2016). Multiple approaches toward monitoring tool string depth, along with functional safety controls, minimize the failure rate for this activity.

The resulting failure probabilities for these three top events are:

Failure during insertion	1×10^{-6}
Drop during run in	5.1×10^{-5}
Impact with waste packages	1.1×10^{-6}

The overall risk for Activity Sequence 1 is dominated by a tool string drop during run in.

The failure consequence for impacts of the borehole qualification tool string on previously emplaced waste packages is categorized as Category F. The tool string is not especially heavy, and the impact limiters on the waste packages would absorb much of the mechanical energy. Damage to a previously emplaced waste package would have minimal impact on surface operations (other than contamination appearing in the borehole fluid management system) but would result in a contaminated borehole with potential for worker exposure and spread of contamination during recovery operations.

10.2 Waste Package Receipt

As noted in Section 9.2, Activity Sequence 2 is limited to the arrival and positioning of the trailer containing the transportation cask at its intended location on site. The trailer is not opened, and no cask dismantling activities such as removal of impact limiters are performed in this sequence. Although the cask contains a radioactive waste package, it remains in its certified shipping status. No event tree has been drawn for this activity sequence, and there are no fault trees to present.

10.3 Transportation Cask Unloading and Move

Fault trees have been prepared to assess probability of failure to accomplish six top events:

1. Lift transportation cask off trailer cradle without toppling.
2. Lift transportation cask off trailer cradle without dropping.
3. Move transportation cask to cradle #1 without collision.
4. Move transportation cask to cradle #1 without dropping.
5. Set and secure transportation cask on cradle #1 without mishap.
6. Roll cradle #1, with transportation cask, into position against interface shield without collision.

Radiological risk during transportation cask unloading and movement to cradle #1 is associated with drop, collision, and toppling events.

The initial event is lifting the transportation cask off its trailer cradle without toppling. The fault tree is shown in Figure 10-4. The associated event tree is Figure 9-2. Failures considered are not removing the restraints (leading to an overload), a mechanical failure in the trailer cradle, a rigging failure, and a crane failure. Probabilities that these faults occur with sufficient severity to cause toppling are presumed low; these serve as goals for future design.

Figure 10-4. Fault tree 3.1, cask is lifted from trailer cradle without toppling.

The second event is lifting the transportation cask away from the trailer without dropping. Two branches are shown in Figure 10-5; one branch addresses either rigging or crane failure, and the other addresses crane operations. Because rigging performance has been demonstrated in the prior event, the probability of rigging failure is reduced. A crane failure includes human error (improper operation of the crane) mitigated by crane safety features, including pre-programmed limits on speed and position.

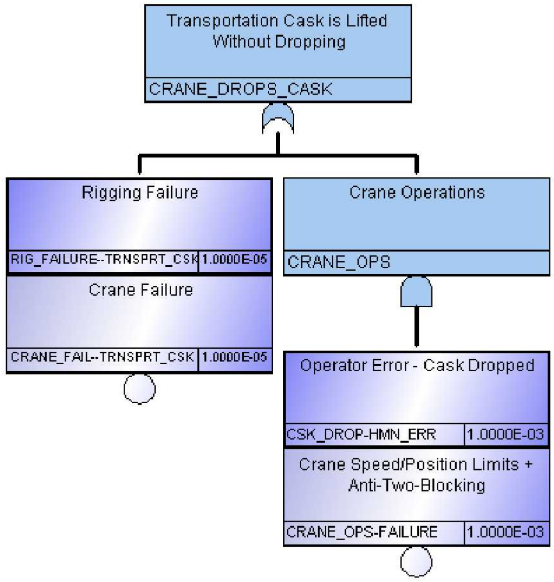


Figure 10-5. Fault tree 3.2, transportation cask is lifted without dropping.

The next event is movement of the transportation cask without collision. One branch of Figure 10-6 shows improper operation mitigated by crane safety features, similar to the previous fault tree. The other depicts crane mechanical failure. Again, crane performance has been demonstrated in the prior steps and the assigned failure probability is low.

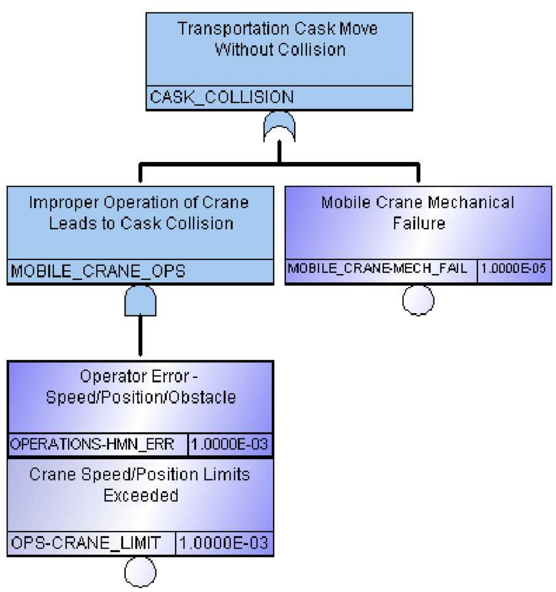


Figure 10-6. Fault tree 3.3, transportation cask does not collide with an object during move.

The fault tree for movement of the transportation cask without a drop, shown in Figure 10-7, is similar. The operator error branch remains the same; the other branch includes either crane failure or rigging failure. Both crane and rigging have been successfully used in prior steps, and failure probabilities assigned to each are the same values.

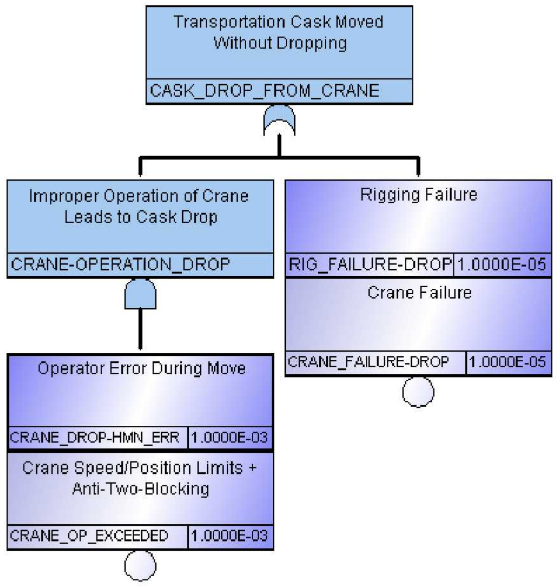


Figure 10-7. Fault tree 3.4, transportation cask is not dropped from mobile crane.

Figure 10-8 depicts the fault tree for setting the transportation cask on cradle #1 and securing the cask to the cradle. The fault tree has three branches. The operator error branch considers misalignment while setting the cask such that the pockets properly engage with the pegs on the cradle, and is lowered in the proper orientation. The initial probability for this task is relatively low; this will be a design goal for the control system (including administrative). Misalignment is mitigated with a diagnosis step. As a procedurally-controlled step, the failure probability is relatively high.

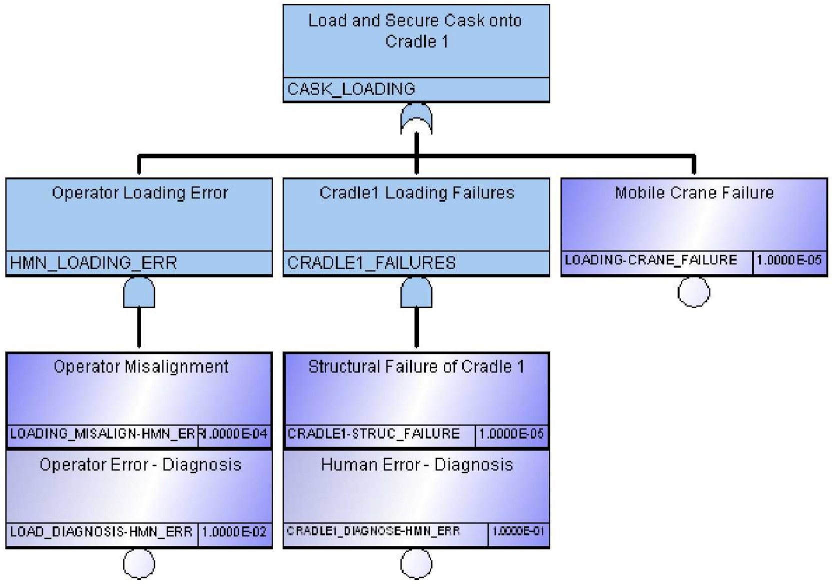


Figure 10-8. Fault tree 3.5, load and secure cask onto cradle #1.

The cradle #1 failure branch is based on a structural failure of cradle #1 as the cask is set on the cradle. A relatively low failure probability is given; this becomes a goal for the design, inspection, and quality assurance for the cradle. A diagnostic task is used to mitigate risk, and a relatively high failure probability is assigned.

The crane failure branch carries with the same probability of failure as in the previous steps.

The final event in this activity sequence is to roll cradle #1, with the transportation cask secured to the cradle, up against the interface shield assembly (Figure 10-9). This will be carried out using programmed equipment at low speed. Thus, the probability of events such as collision or derailment is low. A functional safety system will be provided, incorporating features such as limit switches and obstacle avoidance monitors. This further reduces the probability of failure in the cradle roll event.

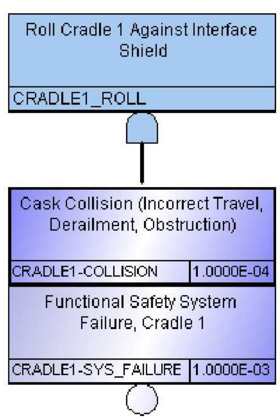


Figure 10-9. Fault tree 3.6, roll cradle #1 against interface shield.

Based on the inputs shown in the figures, the failure probabilities for each of the top events are:

Toppling while lifting off cradle	2.3×10^{-5}
Transportation cask drop while lifting	2.1×10^{-5}
Transportation cask collision while moving	1.1×10^{-5}
Transportation cask drop while moving	2.1×10^{-5}
Transportation cask mishap setting in cradle #1	1.2×10^{-5}
Transportation cask collision during cradle roll	1×10^{-7}

The probability of damage caused by improper cradle roll is negligible. Failure probabilities for each of the other events are comparable to each other; risk is spread evenly throughout this sequence.

The consequence category for each of the event failures in this activity sequence is Category B. The radiological risk associated with any of these failures would involve damage to the transportation cask. Foreseeable damage could cause deformation and possible loss of shielding, but actually dislodging the end plug is not credible for these events. Exposure rates would be minor, and personnel would be trained to move away promptly. Potential dose exposures during recovery operations could be managed at negligible levels.

10.4 Cask-to-cask Waste Package Transfer

Fault trees have been prepared to assess probability of failure to accomplish ten top events:

1. Remove shield plug from transportation cask.
2. Prepare cradle #2, empty transfer cask, and interface shield.
3. Configure upper transfer cask shield and latch assembly.
4. Move waste package from transportation cask to transfer cask.
5. Maintain shielding during waste package transfer.
6. Maintain waste package integrity during waste package transfer.
7. De-configure upper transfer cask shield and reinstall upper latch [add test to actions].
8. Move interface shield slide and cradle #1.
9. Insert lower shield plug into transfer cask.
10. Roll cradle #2 away from interface shield, into position for pickup by gantry crane.

Radiological risk factors associated with the waste package transfer sequence are more varied than those encountered in the borehole qualification or initial cask move sequences. The associated event tree is Figure 9-3.

The fault tree for transportation cask shield plug removal (Figure 10-10) is given two branches, one addressing the external shield configuration, and the other addressing the actual plug removal.

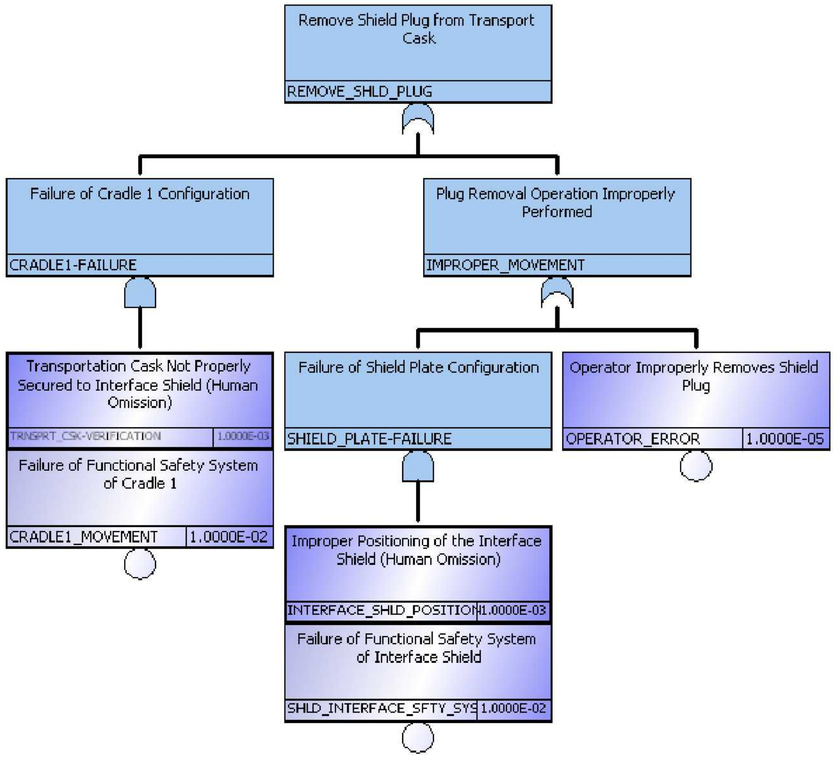


Figure 10-10. Fault tree 4.1, remove shield plug from transportation cask.

If the cradle is not properly positioned against the interface shield, the shielding configuration may not be effective. The fault tree describes the proper positioning and securing of the cask/cradle against the interface shield, mitigated by a functional safety system (interlocks and radiation monitoring) that does not allow progress without this operation being properly completed. Because this activity is easily monitored, relatively low failure probabilities are used.

Shield plug handling is modeled in two branches; one addresses a direct operator error handling the plug (such as cocking or complete removal of the plug from the shield); the other addresses a failure of the interface shield slide configuration (such as moving to the open position prior to positioning cradle #2 over the opening). Improper positioning of the interface shield can be indicated by interlocks, and thus a properly-operating functional safety system would not permit further actions. Operator action is controlled by procedures and supervision, but is shown as a single event.

Risk is balanced across the various branches of this fault tree. Although significant dose exposure rates might be encountered should the plug drop out, pre-positioned alarms would alert operators and the exposure duration would be brief. The failure consequence assigned to this fault is Category B.

The next fault tree covers preparations for waste package transfer, including setup of the empty transfer cask, positioning cradle #2 (containing the empty cask), and moving the interface shield to its middle position, open for package transfer. The fault tree (Figure 10-11) depicts three branches; failure of the interface shield, failure in positioning cradle #2, and a collision of cradle #2 with the interface shield as it is moved into position.

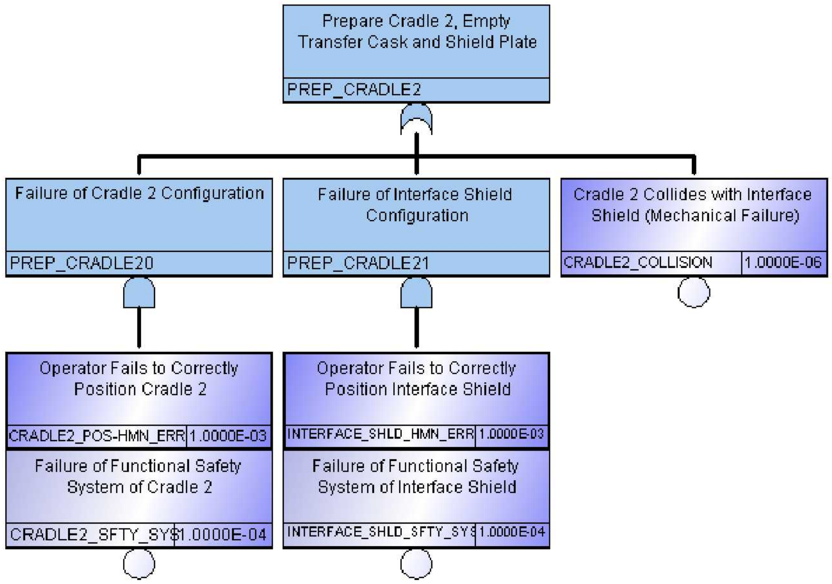


Figure 10-11. Fault tree 4.2, prepare cradle #2, empty transfer cask, and shield plate.

Failure to achieve the proper position of the interface shield slide, at the appropriate time (with both cradles in place) is modeled as a reliable operator action mitigated by the functional safety system. Failure to correctly position cradle #2 against the interface shield is similarly modeled as a reliable operator action mitigated by the functional safety system. Mechanical failure as a result of a collision between cradle #2 and the empty transfer cask with the interface shield is shown as a single, unlikely event. As with the previous event, consequences are limited to a minor worker dose, and are assigned Category B.

Figure 10-12 depicts a simple fault tree for the assembly of the transfer cask shield and latch components, in preparation for waste package transfer. Worker exposures can result from improperly handling these components during transition from a fixed latch assembly (for holding the package in place) to a moveable latch assembly (for cask-to-cask transfer). Operations are simple, and design features such as requiring different tools to manipulate different parts in the upper shield and latch assembly can further reduce the probabilities of meaningful event failures. Relatively low failure probabilities are assigned to the two events. Consequences of failure are again a limited worker dose (especially with a shield section built into the top of each waste package), and assigned to consequence Category B.

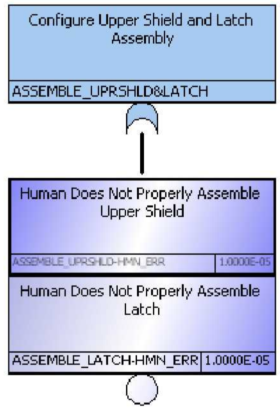


Figure 10-12. Fault tree 4.3, configure upper shield and latch assembly.

The actual cask-to-cask transfer of the waste package is modeled in Figure 10-13. The event tree considers the actual transfer first; subsequent conditional events consider whether a failure of the transfer is accompanied by a loss of proper shielding configuration, and then whether the integrity of the waste package is maintained or compromised. For the transfer failure alone (no loss of shielding or package integrity), consequence Category B is assigned primarily on the presumption that some minor worker exposure would occur during recovery operations.

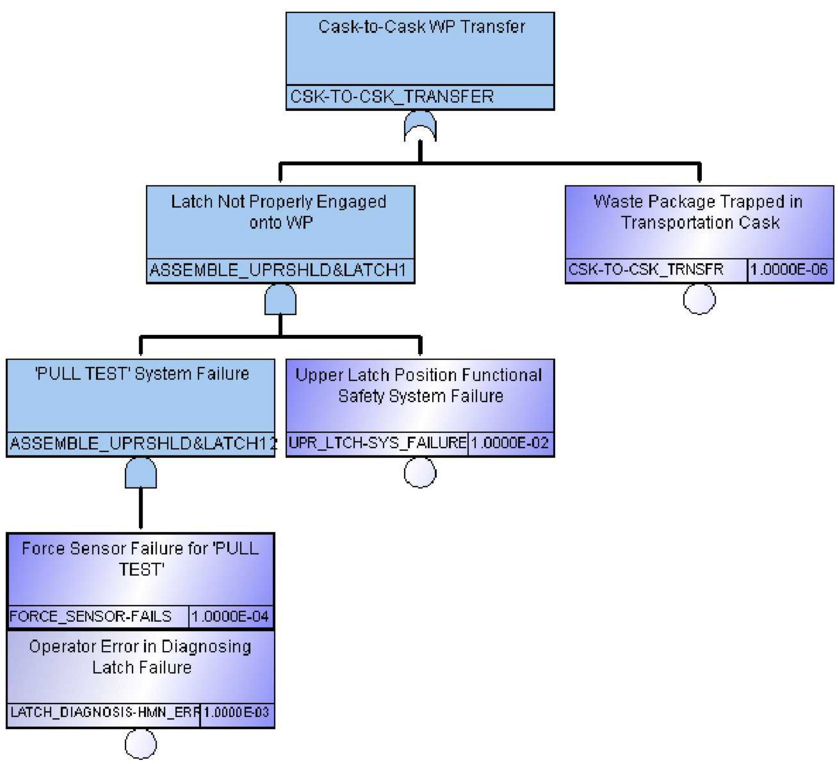


Figure 10-13. Fault tree 4.4, cask-to-cask waste package transfer.

Failure to transfer the waste package is modeled in two branches. The first represents an unrecognized latch failure. Anticipated design features include a signal that the latch is engaged; a failure of this functional safety feature is represented on the right-hand side of the branch with a relatively high failure probability (subject to refinement in design). An initial pull test is also used to determine that the load on the latch corresponds to the expected load for pulling a package. On this branch are force sensor failure, and failure of the operator to notice there is insufficient load on the latch pull assembly. Because these are simple and readily corrected events, lower failure probabilities are assigned.

The second branch to the cask-to-cask transfer tree considers the possibility that the waste package is somehow trapped in the transportation cask, and cannot be pulled out with reasonable force. This is assigned a low probability.

Figure 10-14 depicts a conditional event associated with a failure to accomplish the waste package transfer. It addresses the potential loss of shielding due to either relative movement between one of the cradles and the interface shield, or loss of upper shield configuration during the transfer. The former is modeled as an improper operator action to move a cradle away (mitigated by the functional safety system features on the cradle), along with a mechanical failure that allows inadvertent cradle movement (such as pulling cradle #2 away from the interface shield rather than pulling the waste package into the transfer cask).

The right side of the figure depicts a failure in the upper shield configuration during the transfer, such as might occur should the pull rod separate from the actual latch assembly resulting in an open hole in the upper shield. The model combines failures in the shield or latch/pull components with a functional safety system failure.

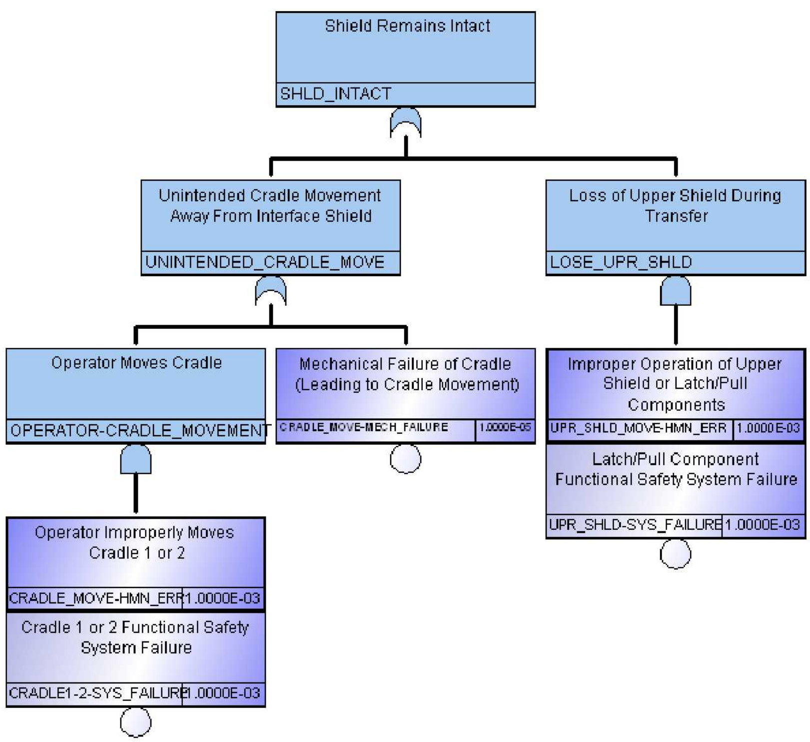


Figure 10-14. Fault tree 4.5, shield remains intact.

Dose rates that might be encountered should the shield configuration be lost during a package transfer may be greater than in previous events, so they are assigned consequence Category C.

The second conditional event associated with waste package transfer (assuming work was not halted due to a shield configuration error) is physical damage to the waste package. This event is modeled in Figure 10-15.

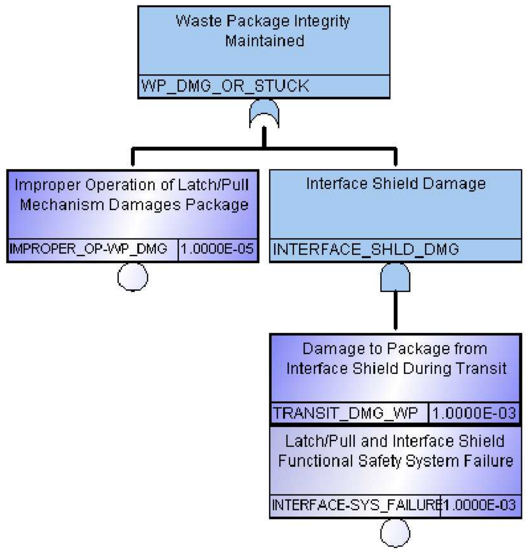


Figure 10-15. Fault tree 4.6, waste package integrity maintained.

Two branches are shown: the first addresses physical damage during transfer as a result of dragging or misalignment of components. The design will incorporate load limits; thus this event can only occur as a result of improper operation of the latch/pull mechanism. A relatively low probability is assigned to this single event.

The other possibility is that the interface shield causes damage, such as movement transverse to the waste package during the transfer operation. This event is again mitigated by the functional safety system. Relatively conservative failure probabilities are assigned to the two elements under interface shield damage.

Loss of waste package integrity can lead to a release of radioactive material and worker exposures. Because the energy available for damage remains limited and the casks would tend to constrain the spread of releases, the consequences of this fault tree are classified as Category D.

Figure 10-16 depicts a relatively simple fault tree for the de-configuration and reinstallation of the upper shield and latch assembly following completion of the waste package transfer. Failure probabilities used are typical of similar operations, and administrative controls are assumed to further reduce the probability of failure.

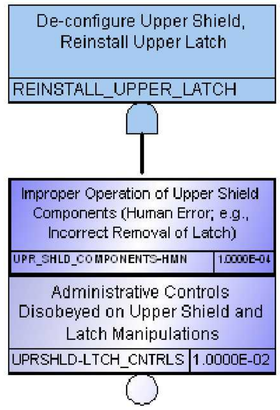


Figure 10-16. Fault tree 4.7, de-configure upper shield and reinstall upper latch.

Consequences associated with the upper shield and latch de-configuration event are limited to operator exposure, and are classified as Category B. Further consequences may include failure to properly capture the waste package when latch manipulations are complete; these events are considered in the sequence in which the consequence occurs (as a potential waste package drop).

After the waste package and the upper shield and latch assemblies are de-configured, the shield plate is repositioned and the empty cradle #1 is moved away to gain access for lower shield plug installation. The fault tree for this event is shown in Figure 10-17. Separate branches are provided for interface shield and cradle operation. Typical failure probabilities are used; each mitigated by the functional safety system. In the case of the interface shield, failure to properly pre-position the lower shield plug in the interface shield slide is also included.

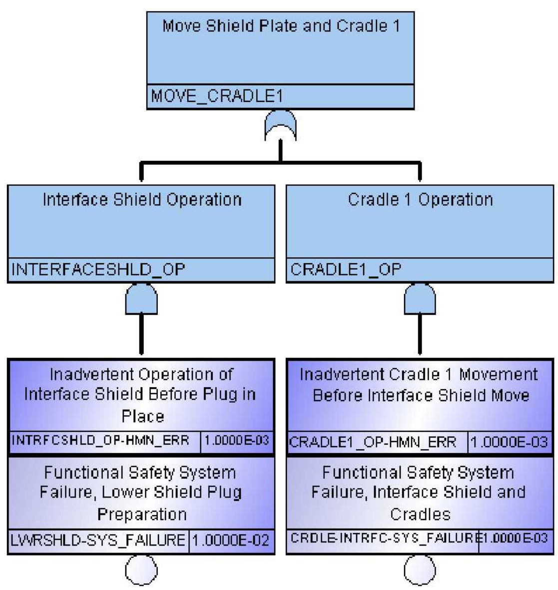


Figure 10-17. Fault tree 4.8, move shield plate and cradle #1.

Failures associated with this fault tree tend to leave a meaningful shield gap near the unshielded, lower portion of the waste package, which is assigned consequence Category C.

Figure 10-18 depicts the installation of the lower shield plug into the transfer cask containing a waste package. The branch to the left addresses possible loss of shield configuration due to improper movement of cradle #2 away from the interface shield. This fault requires both an improper operator action and a failure in the functional safety system.

The main branch of this fault tree considers improper installation of the shield plug itself. One branch considers human error during the insertion process; since fixturing and other controls will aid in the insertion a relatively low probability is assigned. The other branch considers a failure to secure the plug using the remotely-operated flange clamp. A moderate failure probability is assigned to clamp operation, mitigated by an inspection step.

As with the previous sequence, failures could expose the operator to a relatively large shield opening near the lower portion of the waste package, and are assigned to consequence Category C.

Improper installation of the shield clamp can result in a drop of the shield plug in later sequences. The consequence of this event is considered under the activity sequence in which the drop occurs.

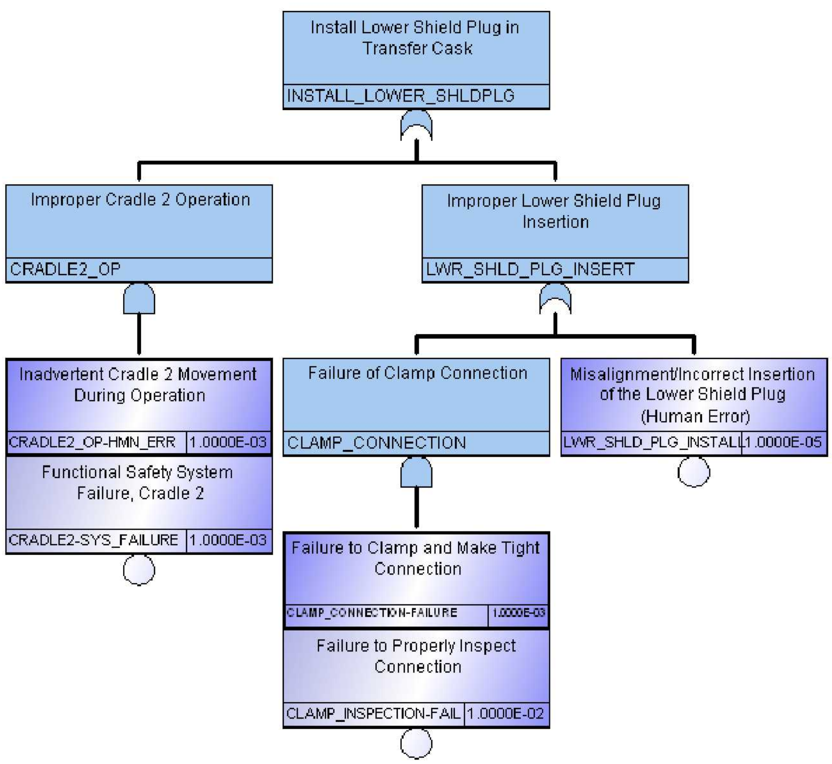


Figure 10-18. Fault tree 4.9, insert lower shield plug in transfer cask.

Figure 10-19 depicts a simple fault tree for movement of the closed transfer cask away from the interface shield, where it can be picked up by the gantry crane and moved to the wellhead. This fault tree is similar to the earlier cradle roll addressed in Figure 10-9. Event failure requires both improper cradle roll operation, and a failure of the functional safety system. The result of such failure would likely be limited to modest damage to shielding, and consequence Category B is assigned.

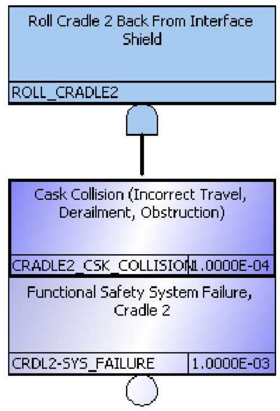


Figure 10-19. Fault tree 4.10, roll cradle #2.

Based on the inputs shown in the figures, the failure probabilities for each of the top events are:

Exposure while removing shield plug from transportation cask	3×10^{-5}
Exposure or damage preparing transfer cask and interface shield for transfer	1.2×10^{-6}
Exposure while configuring upper shield and latch assembly	2×10^{-5}
Failure to properly complete cask-to-cask transfer	1×10^{-6}
Exposure during cask-to-cask transfer	1.2×10^{-5}
Physical damage to waste package during cask-to-cask transfer	1.1×10^{-5}
Exposure or improper operation while reconfiguring upper shield and securing latch	1×10^{-6}
Exposure during interface shield and cradle #1positioning	1.1×10^{-5}
Exposure or improper manipulation during lower shield plug installation	2.1×10^{-5}
Exposure or cask damage rolling cradle #2 away from interface shield	1×10^{-7}

Overall risk for worker exposure in this sequence is spread between potential exposure while removing the shield plug from the transportation cask, exposure while configuring the upper shield and latch assembly, exposure or physical damage during cask-to-cask transfer, exposure during repositioning the interface shield and rolling away cradle #1 after the transfer, and exposure or improper manipulation of the lower shield plug. As indicated with the individual fault tree discussions, most worker exposure event consequences are Category B but a few are Category C.

Event failure risk for exposure or physical damage during cask-to-cask transfer is also significant, but the events are conditional on failure to complete cask-to-cask transfer. Physical damage to the waste package can result in release of radioactive material, as well as increased potential for exposure to personnel and spread of contamination during recovery operations. Although the sequenced probability for this event is low, the greater consequence indicates it merits attention.

10.5 Transfer Cask Move to the Wellhead

Movement of the transfer cask from cradle #2 to the wellhead is in many ways similar to movement of the transportation cask from the trailer cradle to cradle #1, with added steps and risks associated with placing and securing the transfer cask in the wellhead shield assembly. Because of the presence of a lower shield plug in a protruding lower flange and shield plug assembly, the potential consequences of collisions or drops also increase. Conversely, collisions are less likely because of the physical movement constraints imparted through the use of a gantry crane as opposed to a mobile crane.

Fault trees have been prepared to assess probability of failure to accomplish eight top events:

Lift transfer cask off cradle #2 without toppling.

1. Lift transfer cask off cradle #2 without dropping.
2. Maintain secure lower shield plug during the transfer cask move.
3. Maintain grasp of waste package in the event the lower shield plug is lost.
4. Move transfer cask to wellhead without collision.
5. Move transfer cask to wellhead without dropping.
6. Set transfer cask into wellhead without mishap.
7. Secure transfer cask onto wellhead without mishap.

The associated event tree is Figure 9-4.

Radiological risk during the move of the transfer cask from cradle #2 to the wellhead includes drop, collision, and toppling events. It also includes the possibility the lower shield plug drops out when translated into vertical orientation. If the package top and side latches also fail, risk includes the possibility that the waste package drops out of the cask.

Figure 10-20 shows the fault tree for lifting the transfer cask out of cradle #2 without toppling. This fault tree is similar to the one prepared earlier for lifting the transportation cask off the trailer cradle (Figure 10-4). Failures considered are not removing the restraints (leading to an overload), a mechanical failure in the trailer cradle, a rigging failure, and a crane failure. Cradle and crane failure probabilities are considered low. Rigging failures are slightly more likely, although a single-purpose rigging design would tend to reduce risk. The consequence would most likely be modest damage to the transfer cask shielding, which is assigned consequence Category B.

Similarly, the fault tree for a successful lift of the transfer cask without dropping is similar to the tree for lifting the transportation cask (given earlier as Figure 10-5). Two conditional events follow this event; shield plug remains intact and waste package remains in cask. This evaluation is for the drop event alone, without loss of shield plug or waste package.

Figure 10-20. Fault tree 5.1, cask is lifted from cradle without toppling.

Two branches are shown in Figure 10-21; one branch addresses either rigging or crane failure, and the other addresses crane operations. Because rigging performance has been demonstrated in the prior event, the probability of rigging failure is low. Unlike the transportation cask move, this sequence involves the use of a pre-programmed, limited motion gantry crane, and crane failure probability is low. Similarly, the possibility for operator error is relatively low, and is further mitigated by crane safety features, including pre-programmed limits on speed and position and other safety features such as anti-two-blocking devices.

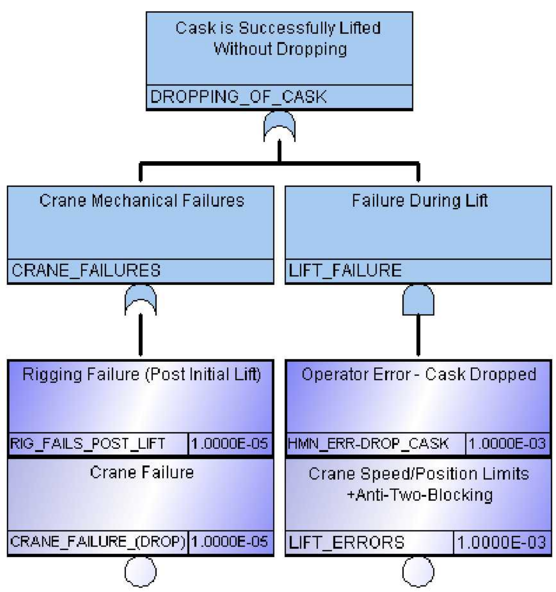


Figure 10-21. Fault tree 5.2, cask is successfully lifted without dropping.

The consequence of a simple drop of the cask, without further loss of shield plug or waste package control, would likely remain Category B.

The first of the two conditional events in the case of a cask drop when lifted considers the probability that the shield plug remains intact. The transfer cask has a pressure boundary tube that extends below the cask body, allowing for coupling to the wellhead. In the case of a drop, the integrity of the clamping mechanism holding the shield plug in place is questioned. The fault tree for this event is presented as Figure 10-22. The fault tree shows two branches. To the left is clamp failure due to operator actions, including improper assembly as part of an earlier activity sequence. The right branch covers clamp failure as a result of accumulated effects from prior operations. Inspection activities serve to reduce the risk of failure in either of these events.

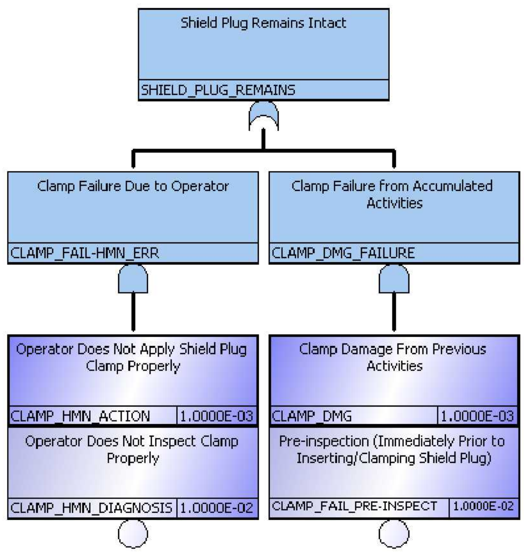


Figure 10-22. Fault tree 5.3, shield plug remains intact.

Loss of the lower shield plug can lead to significant worker exposures, and a Category C consequence is assigned.

The second conditional event, presuming a drop and loss of the lower shield plug, addresses the probability that the waste package remains secured in the transfer cask. The waste package should be held by three features during this move. One, the lower shield plug, is assumed to fail by the structure of the event tree. The other two are the upper latch and the side latches. The fault tree for this conditional event thus has two branches, as shown in Figure 10-23. Each branch shows a moderate probability for a failure event, mitigated by a diagnostic activity. The pull test performed when the latch was de-configured after the waste package transfer is applied directly to the upper latch, with the probability that the operator fails to read the test properly. A similar mitigating event addresses the failure of the operator to assess the position of the side latch system.

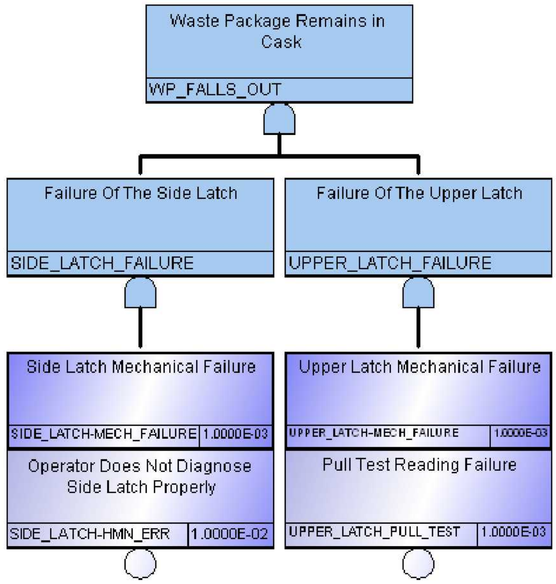


Figure 10-23. Fault tree 5.4, waste package remains in cask.

Dropping the waste package out of the transfer cask is the most serious end state considered during operation of the surface handling systems. The waste package would be partially or completely unshielded, with the potential for a significant worker dose and further dose during recovery operations. It also involves the potential for a waste package breach with release of radioactive material.

The probability for independent failures of the two latch systems shown in the fault tree, with their mitigating test and inspection actions, is 1 x 10^{-11}. The probability of the overall sequence of events is lower still. Thus, although this event is assigned consequence Category E, its probability of occurrence is extremely low.

The next two events considered are collision and drop during the move of the cask, and are similar to the transportation cask move events depicted earlier as Figures 10-6 and 10-7. Although the use of a programmed gantry crane system likely increases the probability of success compared to the use of a mobile crane, the same probabilities are used. The fault tree for a move of the transfer cask without collision is shown in Figure 10-24, and the fault tree for a move of the transfer cask without a drop is shown in Figure 10-25.

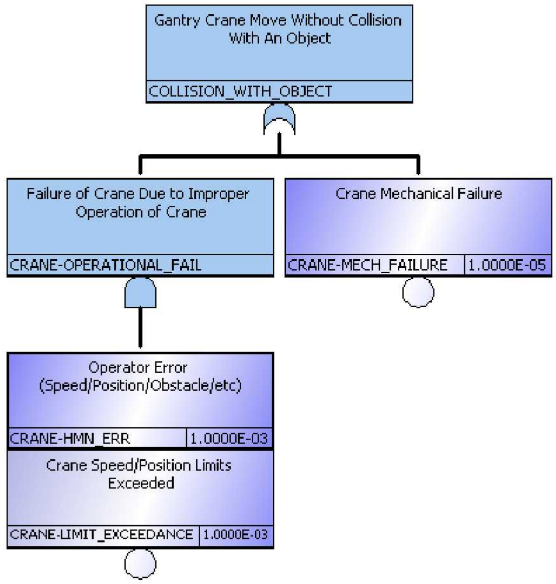


Figure 10-24. Fault tree 5.5, cask does not collide with an object.

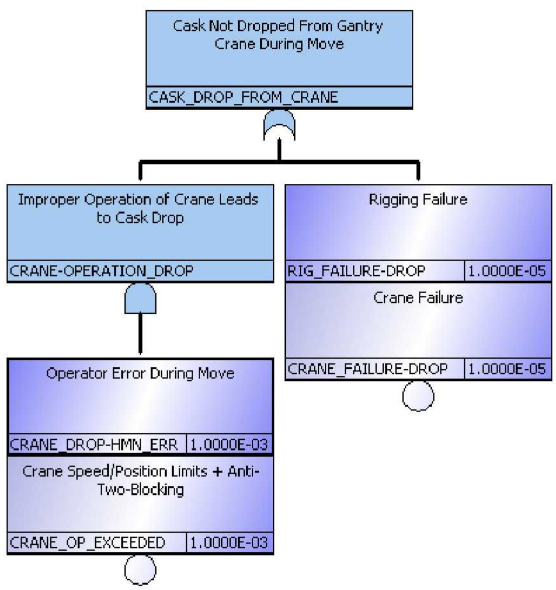


Figure 10-25. Fault tree 5.6, cask is not dropped from crane.

Especially considering the control features anticipated for the gantry crane, the consequences of a collision during this move are classified as Category B. Because of the vulnerability of the lower section, the possibility exists that a drop leads to a more significant shield configuration failure, and the drop is assigned consequence Category C.

The last two events in this activity sequence address actions that take place at the wellhead. These differ from the earlier transportation cask move, where the cask was placed in another cradle. The first of these two events involve placing the cask into the appropriate penetration and kneeling jack features in the wellhead shield structure. The second addresses securing the cask in place, preventing toppling of the transfer cask.

The fault tree for placement of the transfer cask into the wellhead shield assembly is given as Figure 10-26. Three branches describe a crane failure, an alignment failure, and a structural failure of the wellhead shield components into which the transfer cask is being placed. In this model, crane failure stands alone as a relatively unlikely event. A failure to align the cask with the wellhead openings is assigned a moderate probability, but is mitigated by a diagnostic (monitoring and supervision) task. Structural failure of the wellhead is a low probability; the observation task to assess incipient failure is given a more moderate probability.

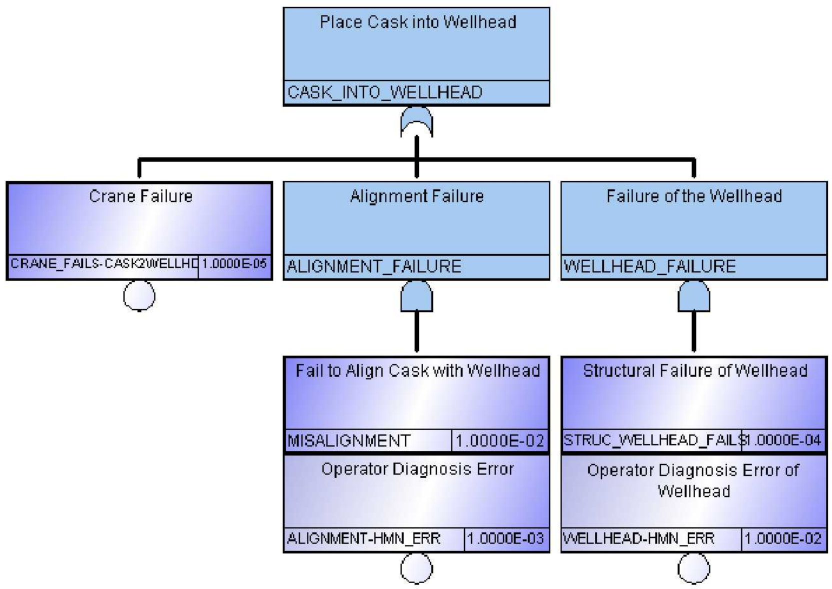


Figure 10-26. Fault tree 5.7, place cask into wellhead.

Alignment or crane failure during this task would not likely cause sufficient damage to the transfer cask that a major compromise of shielding would result. In the case of a structural failure, the cask would still be suspended by the crane. The shield failure would likely occur within the shielding envelope provided by the wellhead system. Thus, the consequence assigned to this event is Category B.

The fault tree shown in Figure 10-27 considers the possibility that improper installation of equipment used to secure the cask in the wellhead leads to toppling of the transfer cask. The fault tree has two branches; initial events address either improper installation or mechanical failure of the tiedowns. Each event is mitigated by an inspection and diagnostic program, with moderate probabilities for success. Toppling could lead to cask damage, including damage to the bottom shield system. In the case of a toppled cask, the damage would end outside of the wellhead shield assembly. Thus, this event is assigned consequence Category C.

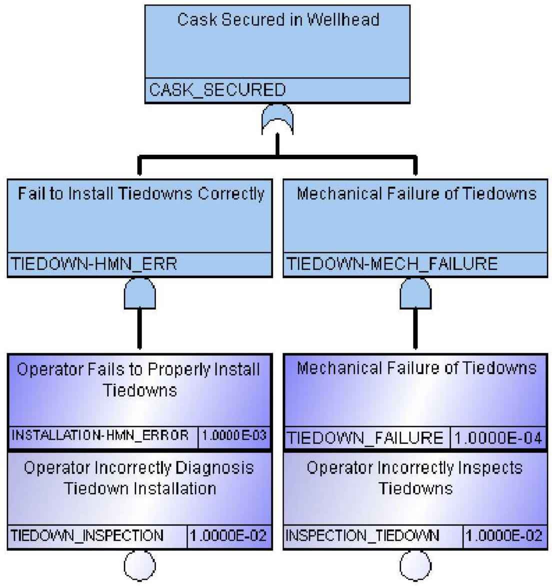


Figure 10-27. Fault tree 5.8, cask secured in wellhead.

Based on the inputs and logic shown in the figures, the failure probabilities for each of the top events are:

Transfer cask toppling while lifting off cradle	1.4×10^{-5}
Transfer cask drop while lifting	2.1×10^{-5}
Lower shield plug fails to remain intact	2×10^{-5}
Waste package drops from cask (after shield plug failure)	1×10^{-11}
Transfer cask collision while moving	1.1×10^{-5}
Transfer cask drop while moving	2.1×10^{-5}
Transfer cask mishap while placing cask into wellhead shield assembly	2.1×10^{-5}
Transfer cask toppling resulting from failure to secure in wellhead shield assembly	1.1×10^{-5}

With the exception of the waste package dropping from the cask, risk is spread fairly evenly through the events comprising this activity sequence. It should be kept in mind that with the current structure of the event tree, loss of the lower shield plug is contingent on a cask drop while lifting, and a drop of the waste package is contingent on both those events.

Consequences range from Category B (moderate damage to a shield plug) to Category E (major dose exposure potential with possible release of radioactive material). However, the Category E consequence is extremely unlikely; it is conditional on a sequence of three events, and multiple failures requirements give a low probability for the drop even should the precursor events occur.

10.6 Wellhead Area Configuration

Wellhead area configuration activities include the sequential operation of systems involving the top and bottom of the transfer cask, the wireline system, a carousel rotation, and coupling of the transfer cask to the wellhead. Fault trees have been prepared to assess probability of failure to accomplish six top events:

1. Transfer cask upper shield components correctly assembled.
2. Wireline properly connected to the waste package.
3. Transfer cask lower shield plug properly removed.
4. Carousel with transfer cask properly rotated from plug removal station to wellhead.
5. Transfer cask properly lowered and mated with the wellhead flange.
6. Transfer cask remote clamp successfully couples cask to wellhead.

The associated event tree is Figure 9-5.

As this sequence begins, the transfer cask is secured in the wellhead shield and the waste package is captured by the upper latch, the side latches, and the lower shield plug. At least two independent features for capturing the waste package remain in place at all times. The upper latch is removed and the wireline attached in the first two events, with side latches and lower shield plug intact. Later, the lower shield plug is removed with the wireline and side latches securing the package.

The first event in this sequence is proper assembly of upper shield components, in preparation for attachment of the wireline tool string to the waste package. The fault tree shown in Figure 10-28 has similar components to the configuration of the upper shield in preparation for cask-to-cask transfer (shown earlier in Figure 10-12). In this case, there is a brief period where a small-diameter open hole allows radiation to stream upward; as a result, special radiological controls are implemented. These controls are shown in the box to the left. The box to the right accounts for improper operator assembly; it can result from either mishandling of the upper shield and latch components or improper handling of the lubricator and seal sections being installed. Moderate failure probabilities are assigned to these tasks.

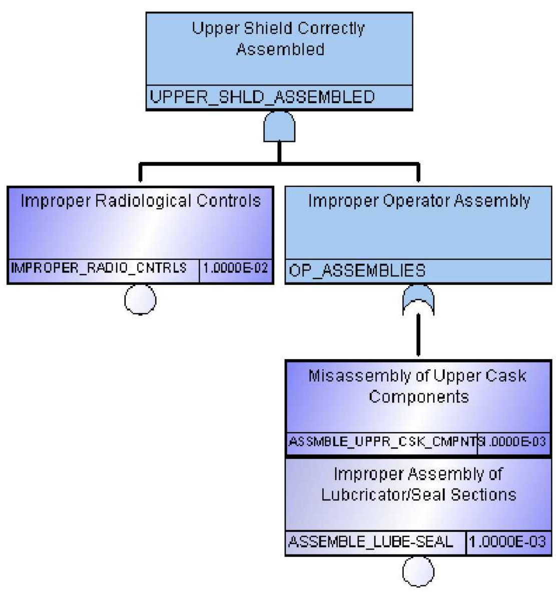


Figure 10-28. Fault tree 6.1, upper shield correctly assembled.

Although a small diameter open hole briefly exists in this event sequence, the additional radiological controls and the presence of a shield in the upper section of the waste package limit potential dose exposures. The consequence category for this fault tree is Category B.

The next event is connection of the wireline tool string, including final assembly of lubricator as appropriate. The failures addressed in Figure 10-29 refer specifically to the latch manipulation; upper shield faults are covered in Figure 10-28. A package drop onto the lower shield plug could occur if both the wireline latch operation fails and the side latches fail. An earlier pull test was used to determine that the side latch is secure; both the initial failure and failure to diagnose the fault in the pull test are shown on the left. Similarly, once the wireline tool string latch is attached, a pull test is performed. Similar logic with a failure of the latch and failure to diagnose a fault with the pull test are shown to the left. Moderate failure probabilities are applied to all faults; with and gates throughout the overall probability for this event is very low.

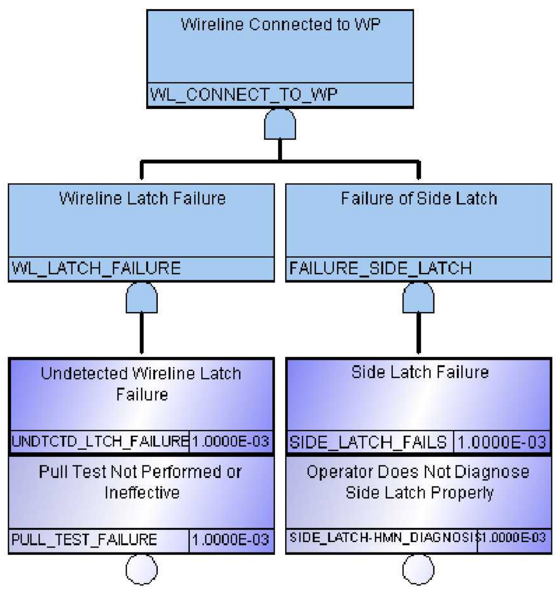


Figure 10-29. Fault tree 6.2, wireline connected to waste package.

At this point in the activity sequence, the consequence of failure would be a drop internal to the transfer cask. This is assigned consequence Category B, with worker exposure most likely during recovery operations. The consequence of a drop of an improperly secured waste package into the borehole is addressed in the waste emplacement activity sequence.

Figure 10-30 provides the fault tree for removal of the lower shield plug. Failure results from either equipment failures in the plug handling mechanisms, or failure to execute the activity as a result of using the wrong sequence of steps or a failure of the interlock system. Moderate failure probabilities are used throughout.

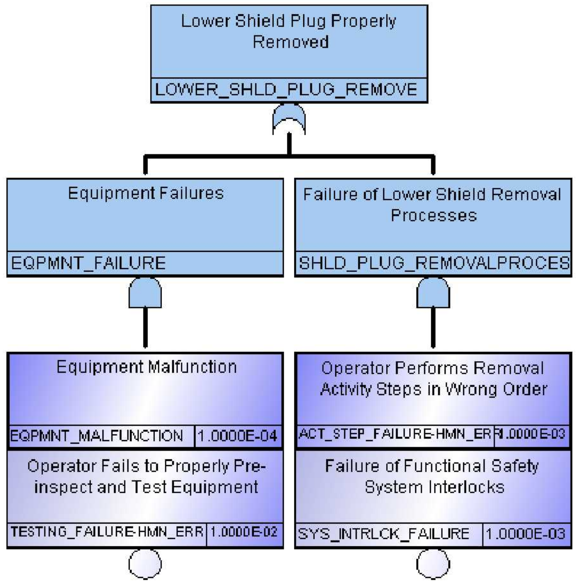


Figure 10-30. Fault tree 6.3, lower shield plug properly removed.

The result of a failure to properly perform the lower shield plug removal operation would be an open transfer cask shield configuration at the bottom of the transfer cask. Entering this sequence under normal operations, however, requires the transfer cask to be properly emplaced in the wellhead shield. The shield is designed to provide adequate protection for workers with an opening at the cask bottom. This fault is assigned consequence Category B, with worker dose most likely during recovery operations.

With the shield plug removed, the next event in this activity sequence is to rotate the carousel to reposition the transfer cask from the lower shield plug removal station into position over the wellhead. Figure 10-31 depicts a number of faults that might occur during this operation. Mechanical failure of the carousel is a direct fault that would prevent successful completion of this event. The rotation equipment is simple, and relatively high reliability is presumed.

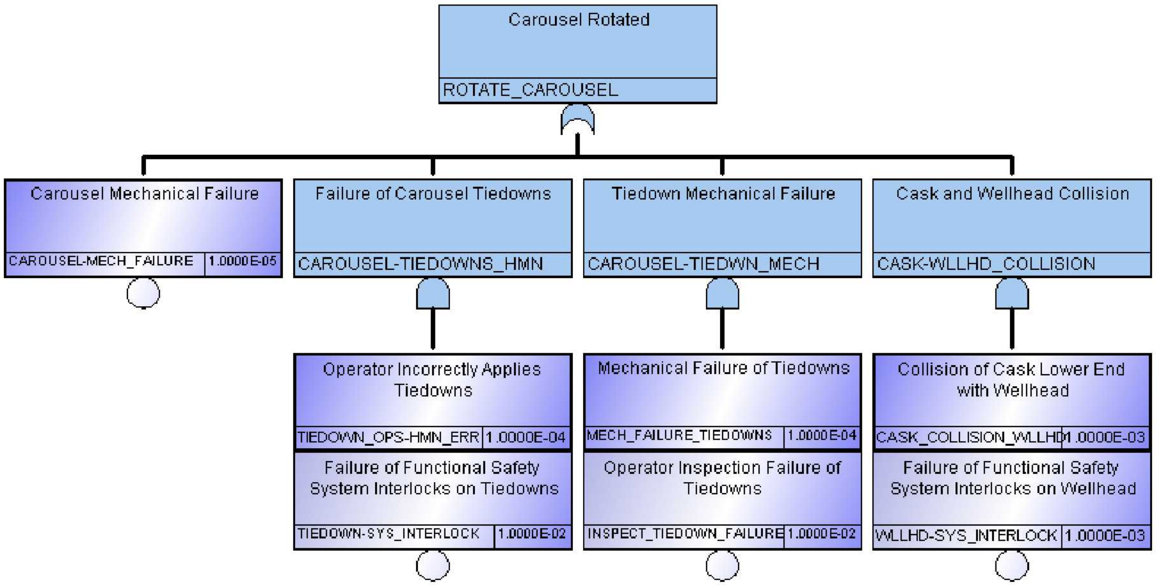


Figure 10-31. Fault tree 6.4, carousel rotated.

The next two faults considered are associated with the transfer cask and carousel system tiedowns. Tiedowns are used to prevent transfer cask toppling while installed in the wellhead shield. Although the tiedown system has not been fully described, it likely attaches to the upper portion of the transfer cask and spans beyond the carousel section. Thus, rotation of the carousel is likely to require manipulation of the tiedowns; improper manipulation or failure to remove tiedowns could lead to cask toppling. Two fault sequences are shown; one considers improper operation of tiedowns (such as failure to remove a component that prevents successful rotation) and the other addresses a mechanical failure of the tiedown hardware (such that it does not support the cask when required). Each of these faults is mitigated; operator action by the functional safety systems and tiedown mechanical integrity by an inspection program. Relatively high reliability is presumed for the operation and hardware, modest reliability is used for the mitigating features.

The fourth fault considered is a collision between the lower portion of the transfer cask and the wellhead flange. This might occur if the kneeling jacks are not in their raised position during rotation. Moderate reliability is assigned to both successful elevation during rotation and the function of interlocks to prevent rotation without proper elevation.

The most serious consequence of the faults described in Figure 10-31 would be toppling of the transfer cask. In this case, toppling would occur after the lower shield plug has been removed, and shielding at the lower end of the transfer cask would be compromised. The fault is assigned consequence Category C.

Lowering of the transfer cask onto the wellhead, so the two halves of the flange connection meet, is addressed in Figure 10-32. The single fault considered is a collision between the lower transfer cask flange and the wellhead flange, with failure of the functional safety system designed to prevent excess downward motion from the kneeling jack system. Again, the event occurs under the wellhead shield, and toppling is not considered likely. The consequence assigned to this fault is Category B, with worker dose exposure again most likely during recovery operations.

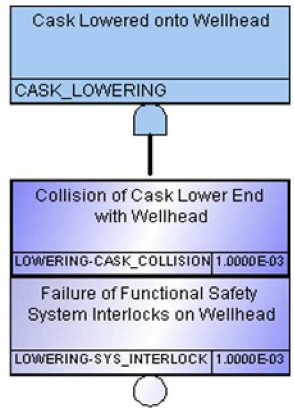


Figure 10-32. Fault tree 6.5, cask lowered onto wellhead.

The final event in this activity sequence is completing the flange connection between the transfer cask and the wellhead. This system is intended to provide a pressure-resistant, leak-tight connection. The fault tree shown in Figure 10-33 depicts a flange, gasket, or flange clamp failure, along with a pressure test used to confirm successful completion of the connection.

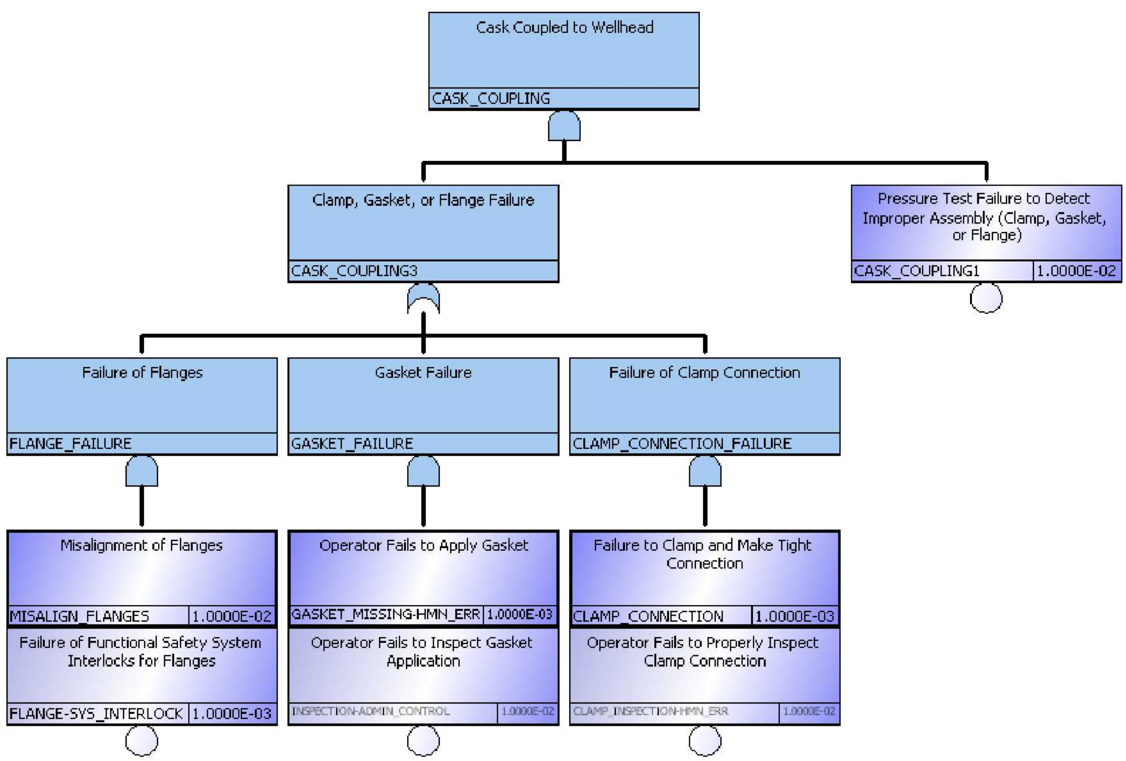


Figure 10-33. Fault tree 6.6, cask coupled to wellhead.

The most likely failure to mate the flanges would be misalignment. The fault tree shows a relatively low reliability for initial alignment, but a higher reliability for identification of misalignment by the functional safety system. The most likely failure associated with the gasket would be failure to place a new gasket in the wellhead flange prior to operation. An inspection step is included to reduce the probability of this fault (either as failure to insert a gasket, or to observe potential misalignment or damage to the gasket). The final fault would be unsuccessful operation of the remote flange clamp assembly. The clamp is inspected prior to initiating the overall waste emplacement sequence, and its operation is monitored in all activity sequences in which the clamp is used.

An inadequate flange connection may have a range of consequences, or if alignment is close and no pressure surge occurs during borehole emplacement, may have no consequence at all. Failure to properly place a waste package is treated in the next activity sequence. For this sequence, a Category B consequence is applied to reflect potential worker dose during recovery operations.

Based on the inputs and logic shown in the figures, the failure probabilities for each of the top events are:

Worker exposure as a result of incorrect upper shield component configuration	2×10^{-5}
Wireline not properly connected to waste package	1×10^{-12}
Lower shield plug not properly removed	2×10^{-6}
Failure or toppling of transfer cask during carousel rotation	1.3×10^{-5}
Collision as transfer cask is lowered onto wellhead	1×10^{-6}
Failure to properly couple cask flange to wellhead flange	3×10^{-5}

Events with the highest probability of failure are worker exposure as a result of improper upper shield configuration, failure or toppling of transfer cask during carousel rotation, and failure to properly complete the flange connection to the wellhead. Of these, toppling of the transfer cask would have the greatest consequence. Intuitively, worker dose to extremities during upper shield and wireline tool string manipulations would most readily occur and must be prevented with effective radiological controls (including tooling that prevents the worker from entering the higher dose area) and supervision.

10.7 Wireline Emplacement of the Waste Package

This section draws heavily on work performed earlier to compare risk and cost for wireline and drill-string waste package emplacement methods. That study, documented as an appendix to the CDR (SNL 2016), is used here with updates to reflect interfaces with the current surface handling concepts.

Fault trees have been prepared to assess probability of failure to accomplish six top events:

1. Waste package successfully transitioned to support by wireline alone.
2. Gate valve properly closed at beginning of sequence (available to catch waste package in the event of a drop when transitioning to wireline support).
3. Waste package remains connected to wireline during trip in.
4. Waste package successfully delivered to emplacement zone.
5. Wireline and tool string successfully extracted after waste package emplacement.

6. Waste package not breached (if dropped from surface or during trip in).

The associated event tree is Figure 9-6.

The event tree for this activity sequence is shown as Figure 9-6. The second event on the list is conditional on the first; it considers a double fault in which the waste package is dropped when transitioning to wireline support only and the gate valve is also open improperly. The final event in the list is also conditional, and evaluates whether or not the package is breached as a result of the initiating event. It is applied to the combined first two faults, and individually to the next three faults.

The event tree and the fault trees presented in this section draw heavily on the earlier effort used to select wireline emplacement over drill string emplacement, as documented in Appendices A and B of the CDR (SNL 2016). The event tree is shown in Figure A-2 of the CDR, and four fault trees that generally correspond to items 1, 3, 4, and 5 in the above list are given as Figures B-1 through B-4 of the CDR.

There are a number of changes made in this evaluation. The CDR evaluated consequential costs for retrieval and recovery operations. This study only addresses radiological risk during normal operations; recovery activities that appear in the CDR such as fishing a dropped or stuck package are not included in these fault trees. The first two fault trees below are reworked to reflect the current design concepts and equipment descriptions (SNL 2016). The final conditional event was added to discern the probability of a major release of radioactive material from an end state in which the waste package may not be properly placed, but immediate radiological consequences may not exist. Even with these modifications, in many cases the fault probabilities for individual initiating events taken from the CDR apply directly to equivalent events in this study.

The initial event is to transition support of the waste package at the surface to wireline alone, by disengaging the side latch devices. Figure 10-34 presents the fault tree for this event. Three faults are considered. A faulty wireline connection would lead to a drop onto the gate valve; the fault probability is based on the left side of Figure 10-29, using just the 10^{-6} per package probability of a faulty wireline connection (upper latch). Either a wireline break due to operating the hoist in the wrong direction or a wireline hoist runaway would also drop the waste package onto the gate valve. Probabilities for these events are drawn from the CDR data.

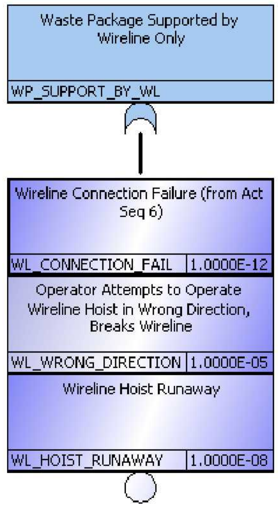


Figure 10-34. Fault tree 7.1, waste package supported by wireline only.

Because the gate valve captures the waste package after a short drop, it is probable that the impact limiter prevents release of radioactive material and consequence Category B is assigned. The waste package would remain under the wellhead shield, and worker dose exposure would be most likely be encountered during recovery operations.

Figure 10-35 depicts a conditional fault tree to consider whether the gate valve is properly closed at the time the side latches are disengaged and support transitions to the wireline system. The end state for the transition event alone would be an unbreached waste package captured by the gate valve; were the gate valve not closed the end state would be a waste package dropped from the surface into the borehole. A combination of a simple controlled operation to close the gate valve with an equally simple interlock to disallow initiation of the activity sequence without the gate valve being closed are shown in the fault tree.

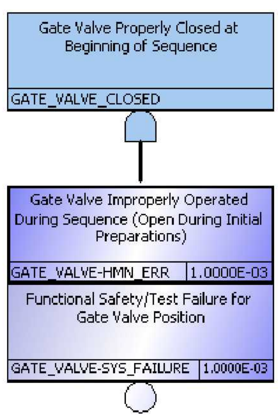


Figure 10-35. Fault tree 7.2, gate valve properly closed at beginning of sequence.

The consequence of the combined fault of a dropped package and an open gate valve depend on the final conditional event; whether or not the waste package is breached as a result of the drop.

If so, consequence Category G is encountered; if the package is not breached, the consequence is Category F.

The first of three relatively complex fault trees for wireline emplacement and retrieval considers whether the waste package is dropped during trip into the emplacement zone in the borehole. The fault tree shown in Figure 10-36 is a modification of the fault tree shown in Figure B-2 of the CDR (SNL 2016). The two main faults would be a break in the wireline and a failure of the wireline connection to the waste package. A wireline failure due to a dynamic tension event was added to the tree. Most of the event probabilities are carried over from the CDR.

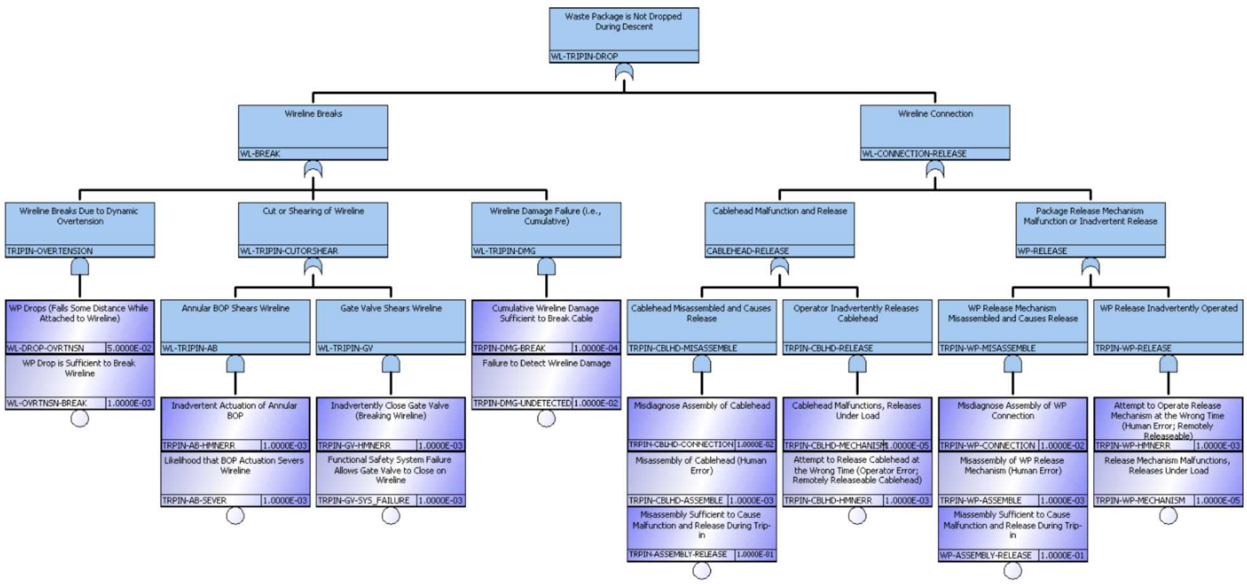


Figure 10-36. Fault tree 7.3, waste package is not dropped during descent.

Consequence of a waste package drop is Category F or Category G, depending on the final conditional event evaluating whether the waste package is breached.

Similarly, the fault tree that evaluated whether the waste package is successfully delivered to the emplacement zone without becoming stuck is drawn from Figure B-3 documented in the CDR (SNL 2016). As presented in Figure 10-37, the structure of the event tree is essentially unchanged; a few individual event probabilities are changed slightly. Consequence again is either Category F or Category G, depending on the final conditional event addressing waste package breach.

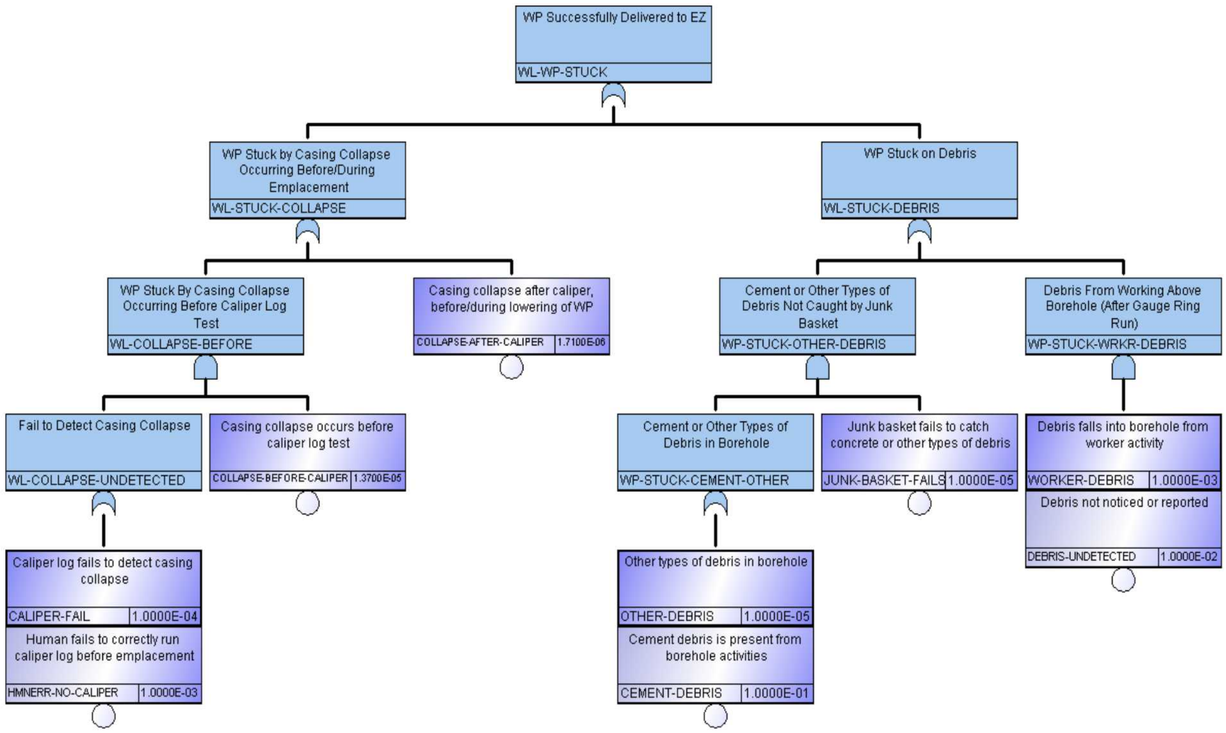


Figure 10-37. Fault tree 7.4, waste package successfully delivered to emplacement zone.

Figure 10-38 presents the fault tree for a drop of the tool string onto the previously emplaced waste package during trip out. Although the appearance of Figure 10-38 differs somewhat from the earlier Figure B-4 in the CDR (SNL 2016), the event structure is essentially the same. Several event titles have changed to reflect the current design concept, such as events addressing failures in the annular BOP and the gate valve. Some probabilities have also changed, reflecting likely failure modes for the updated equipment. In general, however, the structure and probabilities for this fault tree is based on the earlier evaluation documented in the CDR. Consequence again is either Category F or Category G, depending on the final conditional event addressing waste package breach.

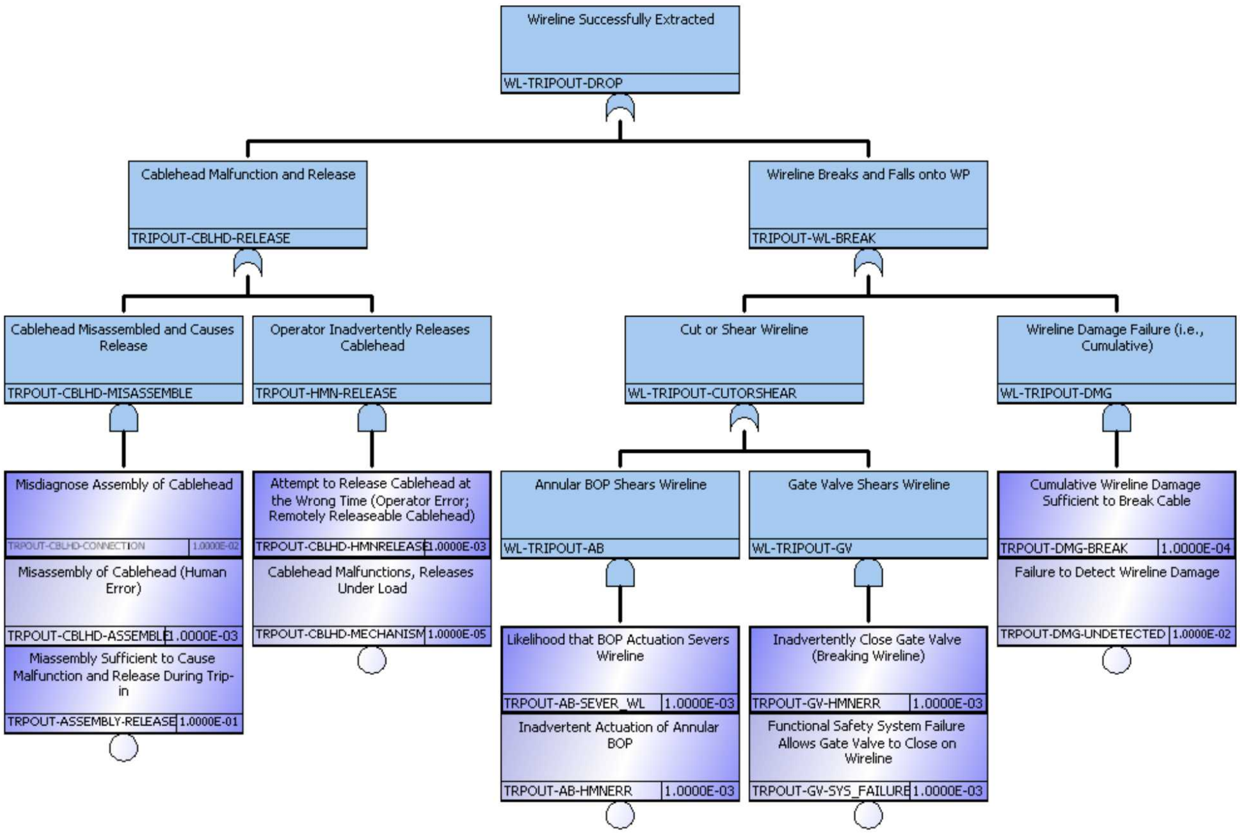


Figure 10-38. Fault tree 7.5, wireline successfully extracted.

The final fault tree is a simple conditional event, evaluating whether a waste package is breached as a result of a drop, becoming stuck, or a drop of the tool string onto the waste package during trip out. This fault, based currently on a simple probability of 0.01, is used to assess whether the consequence is Category F or Category G. Future analyses may be used to better quantify this portion of the model; separate probabilities may be developed for different triggering events.

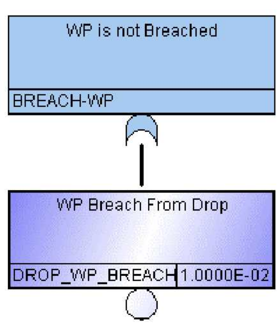


Figure 10-39. Fault tree 7.6, waste package is not breached.

The data and logic shown in the six fault trees presented in this section leads to the following failure probabilities for the events:

Drop of waste package at transition to support by wireline only	1×10^{-5}
Gate valve improperly open at time of transition to wireline support	1×10^{-6}
Waste package dropped during wireline descent	5.5×10^{-5}
Waste package not delivered to intended location in borehole	1.3×10^{-5}
Tool string dropped on emplaced waste packages during wireline trip out	4×10^{-6}
Waste package breaches as a result of a drop into borehole or tool string impact	1×10^{-2}

Risk is spread evenly over the three events that lead to a package drop. Consequences depend on conditional events that follow. For a drop at the time the package transitions to support by wireline only, the low probability of the gate valve being open improperly when the drop occurs limits the likely consequence to Category B; the relatively low probability of package breach even if the gate valve is open favors consequence Category F rather than Category G.

Similarly, the final conditional event limits the consequence to Category F in the event of a package drop, failure to deliver to intended location (stuck package), or a drop of the tool string onto the emplaced package during trip out.

Radiological consequences from a dropped package trapped by the gate valve or a borehole event without package breach would primarily be associated with worker exposure during recovery operations. The need for recovery operations following a downhole event depends on whether the package is in or above the emplacement zone; these issues are discussed further in the CDR (SNL 2016).

A series of events leading to downhole waste package breach would result in contamination of the borehole, with transport of borehole fluid providing a potential mechanism for the spread of contamination. The borehole fluid system for normal operations should be designed to immediately isolate and disposition a reasonable quantity of contaminated borehole fluid (longer term disposition of greater quantities would be addressed in a recovery plan). Immediate off-site radiological consequences from a downhole event are unlikely, but longer-term issues with recovery operations for a contaminated borehole could be more problematic.

10.8 Conditioning of Equipment for Next Use

The four subsequences for conditioning equipment for emplacement of the next package and for preparing and shipping the empty transportation cask back to the package loading site do not, in the normal operating sequence, involve handling radioactive material. Thus, there are no events encountered during the conduct of these sequences that lead to any of the radiological consequences addressed in this study. No event tree was presented in the previous section, and no event fault trees are developed here.

Incorrect performance of actions included in Activity Sequence 8 may lead to failures that have radiological consequences but occur during the execution of other activity sequences. These events are treated under the activity sequence in which they occur.

10.9 Placement of Mechanical Interval Plug

After a string of 40 waste packages has been emplaced an interval plug is used to carry the load to the host rock, so this sequence is performed at a frequency 1/40 of the main sequence. Once the bridge plug is set, package damage is not likely. Thus, this evaluation focuses on the placement of the mechanical bridge plug. The plug is placed using coiled tubing technology.

Fault trees have been prepared to assess probability of failure to accomplish four top events:

1. Insert coiled tubing and tool string into borehole.
2. Run in coiled tubing and tool string.
3. Locate tools at intended location above previously emplaced waste packages.
4. Properly set bridge plug, enabling proper cement plug and establishing load path for next waste package string.

The associated event tree is Figure 9-7.

As with the borehole qualification activity sequence, radiological risk is incurred should the coiled tubing and tool string system drop or be driven onto the previously emplaced waste packages, causing a breach of one or more of the packages. All failures are assigned consequence Category F. Although there may be more force applied to previously waste packages with coiled tubing operation than with wireline operation (due to the greater mass of the coiled tubing system), normal operation of this sequence is only conducted with packages in their intended location in the emplacement zone and the aggregate effect of impact limiters throughout the package string mitigates against package damage.

Fault trees for placement of the mechanical bridge plug resemble the trees shown for Activity Sequence 1, borehole qualification using wireline technology. The first fault tree addresses insertion of the coiled tubing and tool string into the borehole, shown in Figure 10-40. This fault tree is similar to Figure 10-1, for insertion of the borehole qualification tool string. Similar conservative fault probability values are shown.

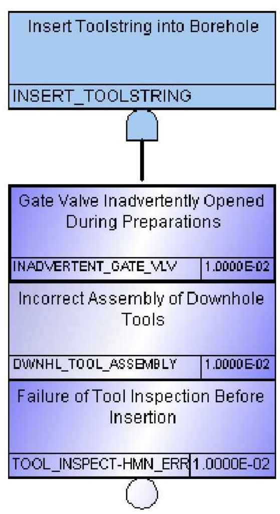


Figure 10-40. Fault tree 9.1, insert tool string into borehole.

Similarly, the structure of the fault tree for running in the coiled tubing and tool string shown in Figure 10-41 has common elements with the borehole qualification fault tree shown in Figure 10-2, except that in the case of bridge plug insertion the failures in the coiled tubing and tool string are shown separately. Moderate failure probabilities are shown, and for each branch an inspection step is used to reduce the failure probability.

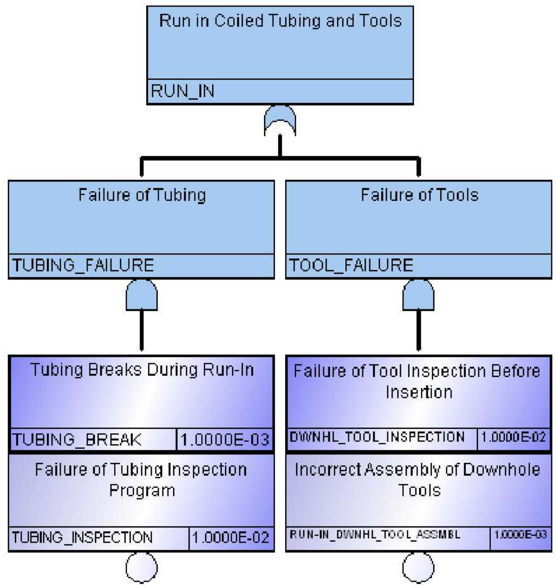


Figure 10-41. Fault tree 9.2, run in coiled tubing and tools.

The fault tree for locating the bridge plug in its intended location above the emplaced waste packages, without collision with the top waste package, is shown in Figure 10-42. Again, the structure is similar to that shown for logging the correct interval in Figure 10-3. In the case of the coiled tubing operation, slightly higher failure probabilities are assigned to the administrative control and functional safety systems used to reduce overall risk.

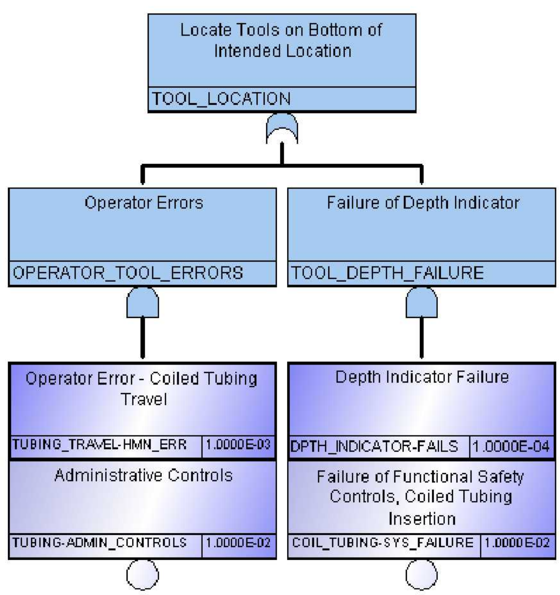


Figure 10-42. Fault tree 9.3, locate tools on bottom of intended location.

The actual setting of the bridge plug is a new event, with the fault tree shown in Figure 10-43. As this tree evaluates the overall effectiveness of load transfer to host rock, it includes both a branch for bridge plug operation and a side branch for cement placement. The focus of the tree is on near-term protection against damage to the waste packages, rather than long-term performance. Thus, either the bridge plug or the cement plug provides protection and rather conservative failure probabilities are indicated.

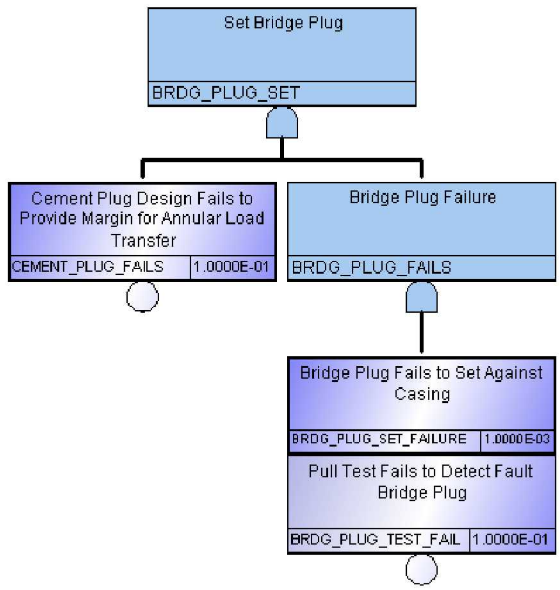


Figure 10-43. Fault tree 9.4, set bridge plug.

Using the probabilities and logic shown in the fault trees, the failure probabilities for the top events are:

Drop and damage to waste package during insertion of tool string into borehole	1×10^{-6}
Drop and damage to waste package during run in of coiled tubing and tool string	2×10^{-5}
Tool string impact on waste package due to failure to properly locate string on bottom	1.1×10^{-5}
Failure to properly set bridge plug leading to excess loading on package string	1×10^{-5}

Note that the frequency of this sequence is 0.025 (once every 40 packages emplaced) compared to the frequency of the borehole qualification and package emplacement sequences. Thus, an interval plug event with a probability of 2×10^{-5} is comparable to a probability of 5×10^{-7} in the main package emplacement sequence.

Overall risk for this sequence is spread fairly evenly over the last three of the four events.

As with borehole qualification, these failures are assigned consequence Category F. Although the mass of the coiled tubing string may be substantial, the packages are in their emplacement zone, and the presence of a full string of packages means the aggregated compliance of a full set of impact limiters is available to absorb the energy of dropping the string onto the packages.

11 RISK MODEL CALCULATION RESULTS

The equation for risk is given as: *Risk = Likelihood × Consequence*, where likelihood is the frequency of some event occurring, and consequence represents some sort of danger associated with the event occurring (typically with regards to human lives, such as exposure to radiation). The PRA described here uses approximate probabilities that come from many sources, such as the CDR (SNL 2016) and the SPAR-H method for determining human error probabilities (Gertman et al. 2005). As defined in Section 9 and discussed in Section 10, consequences associated with end-states are binned qualitatively into seven categories (Table 9-1). Thus, risk is not treated quantitatively here, consistent with the purpose of the assessment which is to develop design insights (Section 1). A more complete risk analysis with quantitative treatment of consequences would require additional design information and fragility analysis. When a regulatory risk analysis is performed for nuclear projects, a level 1, 2 or 3 PRA approach as used by the U.S. Nuclear Regulatory Commission for nuclear power plants, would be an appropriate approach.

Quantification of the success and failure of the different event-tree (ET) end states in Section 9 is calculated using the top-event failure probabilities provided in Section 10. Each end state probability (and the contribution to an assigned consequence category) is calculated from the product of fault tree probabilities for the branching that leads to that end state. After the consequence category probabilities are calculated for an ET, category information is aggregated to get the total probability for each category, and category information is then aggregated across ETs to obtain the PRA model results.

Referencing the PFD (Figure 5-1) it is inferred that the different activity sequences have different levels of frequency associated with them. For example, Sequences 1 through 8 are performed on individual waste packages, and risk depends on the number of waste packages to be included in a string, borehole, or campaign. Thus, the frequency of these sequences is "per waste package" frequency. Sequences 9 and 10 are performed with a "per string" frequency.

Determining the probability of success for one borehole depends on the number of waste packages in a string and the number of strings in a borehole. For this analysis, it is assumed that there are 40 waste packages in a string, and 10 strings per borehole (Section 4). The probability of successfully completing a string of waste packages is given by

$$P(1\ WP\ Success) = P(Seq1) * P(Seq\ 3) * P(Seq\ 4) * P(Seq\ 5) * P(Seq\ 6) * P(Seq\ 7),$$

where *P(Seq#)* represents the probability of success of that specific sequence. Assuming that the success of each waste package emplacement in the borehole is independent of emplacement of other waste packages, then the probability of string success is given by

$$P(String\ Success) = P(1\ WP\ Success)^{40}$$

the number of waste packages in each string is 40. Sequence 9, placement of mechanical interval plug, follows completion of emplacement of a string of packages. Assuming that the success of each interval plug and string is independent of other plugs and strings, then the probability of success for a borehole being filled is given by

$$P(String\ and\ Plug) = P(Seq9) * P(String\ Success),$$

$$P(Borehole\ Filled) = P(String\ and\ Plug)^{10}$$

where the number of interval plugs per borehole is 10. The probabilities cited for probability of successful borehole completion follow the above equations.

This section first quantifies the consequence category probabilities for each of the activity sequence event trees and determines the probability of successful borehole completion. Following this, sensitivity analyses are presented to better understand risks associated with the entire borehole procedure.

Note that throughout this analysis, probability results are reported with as many as seven significant figures. Such precision is needed to interpret the PRA model results, particularly the "probability of success." The significant figures associated with model inputs must determine the precision of outputs, and the basic event probabilities in this assessment are broad estimates with limited data support. However, using inputs expressed with 1 or 2 significant figures, it is possible to calculate complementary probability values (e.g., $1 - \alpha$) that appear to have more precision. The discussion below does not exactly follow protocols for reporting precision, but uses complementary values to facilitate comparison of different results. The well-informed reader will recognize and address this practice in any future use of probabilities reported here.

11.1 Probabilities for Consequence Categories – Base Case

Determining the aggregated probabilities for the consequence categories proceeds in several steps. First, the branching probabilities leading to a specific end state on an ET (with assigned consequence category) are calculated individually. Next, for ETs that have several common consequence categories, those end states are aggregated into a single probability for that consequence category in that ET. Finally, the primary FTs or set of FTs that have the most significant impact on the probability of success are identified along with the primary drivers for those FTs. The identified FTs and primary drivers will be examined further in the sensitivity analysis (Section 11.2).

The term "primary driver" used here refers to basic events (generally, constituents of FTs) that have the largest influence on the calculated consequence category probabilities. Altering a primary-driver basic event will alter the fault tree probability as well. If the primary-driver basic event probability input is reduced enough (typically 2 orders of magnitude or more) then the primary driver for that FT is likely to change to a different basic event or set of basic events.

The calculations described here are referred to as the "base case analysis." This terminology is needed to differentiate between results in Section 11.1, and sensitivity analyses described in Section 11.2.

11.1.1 Borehole Qualification

The borehole qualification event tree (Activity Sequence 1) is shown in Figure 9-1 and the corresponding fault trees, along with their probabilities, are shown in Figure 10-1 through Figure 10-3. Four unique end states (including success) are possible and using the probabilities from Section 10.1, the probability of each end state is calculated. The branching of this ET may be considered "simple" because the end state probabilities are equal to the fault tree probabilities corresponding to that branch.

The aggregated probability for the Category F end state is 5.31E-05 per waste package.

The primary driver for an off-normal end state of any kind is the FT "Run in Wireline Tool String" (Figure 10-2), which is driven by a wireline break event.

Activity Sequence 1: Borehole Qualification		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99995
2	Category F	1.10E-06
3	Category F	5.10E-05
4	Category F	1.00E-06

Note that since this sequence is associated with borehole qualification, the results of this sequence will have an impact on the Sequence 7 activities (Section 6.7). The prospect of getting a waste package stuck in spite of a successful qualification was addressed previously (SNL 2016, Appendix A) and is incorporated here in Activity Sequence 7. Generally, successful and accurate borehole qualification would be expected to increase the probability of success for Sequence 7.

11.1.2 Waste Package Receipt

As noted in Sections 9.2 and 10.2 transportation of waste packages to a disposal site is to be performed using a commercially available, licensed transport system. The important features of such a system would not be modified, and its safety is beyond the scope of this assessment.

11.1.3 Transportation Cask Unloading and Move

The event tree for Activity Sequence 3 is shown in Figure 9-2 and the corresponding fault trees, along with their probabilities, are shown in Figure 10-4 through Figure 10-9. This sequence has seven unique end states, including success. The branching of this ET may also be considered simple and the end state probabilities are equal to the FT probabilities corresponding to each branch.

Activity Sequence 3: Transportation Cask Unloading and Move		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99991
2	Category B	1.00E-07
3	Category B	1.20E-05
4	Category B	2.10E-05
5	Category B	1.10E-05
6	Category B	2.10E-05
7	Category B	2.30E-05

The aggregated probability for Category B end states for this activity sequence is 8.81E-05 per WP. Except for “Roll Cradle #1 Against Interface Shield” (Figure 10-9) all FTs contribute approximately equally to reducing the probability of success for this sequence. All the contributing FT cut sets have rigging failure and crane failure as a common event.

11.1.4 Cask-to-Cask Waste Package Transfer

The event tree for the cask-to-cask waste package transfer is shown in Figure 9-3 and the corresponding fault trees, along with their probabilities, are shown in Figure 10-10 through Figure 10-19. This sequence ET has 11 unique end states with four different categorical end states. The probability for each end state and the aggregated probabilities for each consequence category are given below.

Activity Sequence 4: Cask-to-Cask Waste Package Transfer		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99991
2	Category B	1.00E-07
3	Category C	2.10E-05
4	Category C	1.10E-05
5	Category B	1.00E-06
6	Category B	1.00E-06
7	Category D	1.10E-11
8	Category C	1.20E-11
9	Category B	2.00E-05
10	Category B	1.20E-06
11	Category B	3.00E-05

- Category B = 5.33E-05 per WP
- Category C = 3.20E-05 per WP
- Category D = 1.10E-11 per WP

Four end states (end states 3, 4, 9, and 11) have larger probabilities, on the order of 10^{-5}. For those FTs contributing to those end states, operator errors are the leading contributors to the top event failure probabilities.

11.1.5 Transfer Cask Move to the Wellhead

The event tree for the transfer cask move to the wellhead is shown in Figure 9-4 and the corresponding fault trees, along with their probabilities, are shown in Figure 10-20 through Figure 10-27. Nine end states are associated with this activity sequence. The probability for each end state and the aggregated probability for each consequence category are given below.

Activity Sequence 5: Transfer Cask Move to Wellhead		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99990
2	Category C	1.10E-05
3	Category B	2.10E-05
4	Category C	2.10E-05
5	Category B	1.10E-05
6	Category B	2.10E-05
7	Category C	4.20E-10
8	Category E	4.20E-21
9	Category B	1.40E-05

- Category B = 6.70E-05 per WP
- Category C = 3.20E-05 per WP
- Category E = 4.20E-21 per WP

Several fault trees have approximately equal probability of failure, contributing to the overall probability of an off-normal outcome in this activity sequence. Similar to other fault trees, the leading contributors to top event failure are due to rigging failures, crane failures, and operator errors.

11.1.6 Wellhead Area Configuration

The event tree for the wellhead area configuration sequence is shown in Figure 9-5 and the corresponding fault trees are provided in Section 10-28 through 10-33. There are seven end states associated with this sequence. Similar to other ETs, this ET can also be classified as being "simple" (See Section 11.1.1). The end state probabilities and the aggregated probabilities for each category are provided below.

Activity Sequence 6: Wellhead Area Configuration		
End State #	**End State Consequence Category**	**Probability (per WP)**
1	Category A	0.99996
2	Category B	3.00E-07
3	Category B	1.00E-06
4	Category C	1.30E-05
5	Category B	2.00E-06
6	Category B	1.00E-06
7	Category B	2.00E-05

- Category B = 2.43E-05 per WP
- Category C = 1.30E-05 per WP

End states 4 and 7 have probabilities about an order of magnitude larger than the other end states. For end state 7 (which corresponds to the FT shown in Figure 10-28) the leading basic event drivers are operator errors (e.g., "improper radiological controls"). For end state #4 (which corresponds to the FT shown in Figure 10-31) the leading basic event driver is mechanical failure of the carousel.

11.1.7 Wireline Emplacement of a Waste Package

The event tree for emplacing waste packages is shown in Figure 9-6 and the corresponding fault trees and probabilities are shown in Figure 10-34 through Figure 10-39. There are seven end states associated with this sequence and four end state consequence categories. The end state probabilities and the aggregated probabilities for each category are provided below.

Activity Sequence 7: Wireline Emplacement of a Waste Package		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99992
2	Category F	2.73E-06
3	Category G	0.0
4	Category F	2.73E-06
5	Category G	4.35E-08
6	Category F	5.15E-05
7	Category G	0.0
8	Category B	1.00E-05
9	Category F	1.00E-11
10	Category G	0.0

- Category B = 1.00E-05 per WP
- Category F = 5.70E-05 per WP
- Category G = 4.35E-08 per WP

End states 6 and 8 have probabilities about an order of magnitude greater than the other end states. For end state 6, the primary top event leading to this end state is the drop of a waste package during descent (Figure 10-36). The primary driver in Figure 10-36 is wireline breaking due to dynamic overtension. For end state 8, the fault tree leading to this end state is the dropping of the waste package while supported by the wireline only with the gate valve properly closed. The primary driver for the dropping of the waste package while supported by wireline only (Figure 10-34) is a human error event.

11.1.8 Conditioning of Equipment for Next Use

As noted in Sections 9.8 and 10.8, the activities associated with this sequence that can lead to failure become apparent in other sequences. For this reason, those activities are addressed in the other sequences and no analysis was performed for this particular sequence.

11.1.9 Placement of Mechanical Interval Plug

The event tree for placement of mechanical interval plug is shown in Figure 9-7 and the corresponding fault trees and probabilities are provided in Figure 10-40 through Figure 10-43. There are five possible end states and two consequence categories. Similar to other ETs, this event tree is considered “simple.” The end state probabilities are given below.

Activity Sequence 9: Placement of Mechanical Interval Plug		
End State #	End State Consequence Category	Probability (per WP)
1	Category A	0.99996
2	Category F	1.00E-05
3	Category F	1.10E-05
4	Category F	2.00E-05
5	Category F	1.00E-06

The aggregated probability for Category F is 4.20E-05 per WP. End states 2 through 4 are approximately equally probable, but the primary basic events responsible for their failure probabilities differ. For end state 4, which corresponds to the FT in Figure 10-41, tubing or tool failure have equal probability of failure. For both types of failure, operator diagnosis is the primary cause of the failure. Operator errors are also the primary drivers for the probability of end state 3. The failure probability of end state 2 is equally driven by two basic events (Figure 10-43), failure of the pull test and failure of the cement plug design.

11.1.10 Aggregated Probabilities for Loading All Packages in a Borehole and Completing the Emplacement Zone

The aggregated probabilities for each of the different consequence categories are shown in Table 11-1 and Table 11-2. Consequence category B has the highest probability per borehole (among Categories B through G). This is partly because Category B occurs in the ETs for every sequence except for sequences 1 and 9 (those without any waste package handling). Category F and Category C also have high probabilities per borehole as they appear in three of the several ET sequences. The sensitivity analysis investigates means by which these probabilities can be reduced and to what degree.

The probability of radiological exposure during the DBFT is zero because test packages would contain no radioactive material. However, the results provide insight as the to the approximate likelihood of a mishap such as a drop. Using the string probability information from Table 11-1, the probability of successfully emplacing fewer than 40 test packages in the DBFT, is greater than 98% (by comparison to success for a string of 40). Probability of a cask/package drop at the surface is dominated by Category C (0.031% for a string of 40). Probability of dropping a package or other equipment downhole without a package breach, is dominated by Category F (0.044% for a string of 40). These are rough-order-of-magnitude estimates, since the equipment used for the DBFT could be different from that developed for a disposal campaign. For example, a mobile crane might be used to position the transfer cask over the wellhead for DBFT activities, whereas a fixed headframe and gantry crane could be used for disposal operations as assumed in this assessment.

Table 11-1. Aggregated probabilities at stages in the DBD process.

Consequence Category	Probability (per WP)	Probability (per string)	Probability (per interval plug)	Probability (per borehole)
Category A	0.99956	0.98237	0.99996	0.83673
Category B	2.43E-04	9.66E-03	-	9.25E-02
Category C	7.70E-05	3.08E-03	-	3.03E-02
Category D	1.10E-11	4.40E-10	-	4.40E-09
Category E	4.20E-21	0.0	-	0.0
Category F	1.10E-04	4.39E-03	4.20E-05	4.35E-02
Category G	4.35E-08	1.74E-06		1.74E-05

Table 11-2. Aggregated probabilities extended to a campaign of 30,000 waste packages.

Consequence Category	Probability (per 30,000 WPs)	Probability (per 750 plugs)	Expected Number for 30,000 WPs	Expected Number for 750 plugs
Category A	1.61E-06	0.96899	29987	749.97
Category B	9.99E-01		7.28	
Category C	9.01E-01		2.31	
Category D	3.30E-07		3.30E-07	
Category E	0.00E+00		1.26E-16	
Category F	9.63E-01	3.10E-02	3.30	3.15E-02
Category G	1.31E-03		1.31E-03	

11.2 Sensitivity Analysis on Key Parameters

The base case analysis (Section 11.1) generally used conservative estimates. The sensitivity analysis here applied less conservative estimates to examine the effect of minimizing human errors and increasing the overall reliability of the systems, structures, and components involved. One of the goals of the sensitivity analysis was to try and achieve off-normal FT probabilities on the order of 10^{-6} for the entire ET, for those activity sequences that dominate DBD system performance. The following sections highlight the changes made to FTs to achieve this order of magnitude for the analysis.

Examination of the ETs and FTs identified common basic events across all ETs, and identified FTs that had substantial impact on end-state probabilities. Common basic events that are present in many FTs include rigging failure, crane failure, and carousel failure. The reliability data on the systems, structures, and components that make up these events is extensive and often protected by industry. Probabilities used for these events are thought to be conservative in the base-case analysis, but additional reliability could be achieved. Thus, the sensitivity analysis investigates the possibility of more realistic (less conservative) estimates for the probabilities of rigging failure, crane failure, and carousel failure.

Another important, common set of events in the ETs and FTs are human errors (or operator errors). One method for quantifying human error probabilities (HEPs) is the Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) which is commonly used by the NRC for nuclear power plant PRA (Gertman et al. 2005). HEPs have been identified throughout this analysis as being the primary driver for many fault tree probabilities. Given the lack of information that may influence performance shaping factors (PSFs) for a borehole site, the generic HEPs for diagnosis and corrective action, values of 1.00E-02 and 1.00E-03 respectively, have been used throughout the base case analysis. According to the SPAR-H worksheets, if all PSFs were positive (i.e., a value less than or equal to one), then the HEPs for diagnosis and action can be reduced to 1.00E-06 and 1.25E-06, respectively. These values represent the "best-case scenario" that can be achieved in borehole operations.

Due to the conceptual nature of the current report, a thorough sensitivity study and uncertainty analysis are not performed. The sensitivity analyses performed here identify the primary contributions to activity sequence failures, and identify areas where the conceptual design may be improved to further increase the probability of successful borehole completion.

11.2.1 Borehole Qualification

As noted in Section 11.1.1, the most influential FT in this sequence is the "Run in wireline tool string" FT shown in Figure 10-2. The most significant basic event probability in this FT is associated with the wireline breaking and has a probability of 5.10E-05 in the base case analysis. If the reliability of the wireline could be increased to 1.00E-06, then the overall success for this sequence could be significantly improved.

Applying the increased reliability for the wireline, successful operation for this sequence increases to 0.9999969 (versus 0.9999469 in the base case analysis). The aggregated probability for Category F is decreased to 3.10E-06 (versus 5.31E-05 in the base case analysis). Furthermore, the overall effect on the probability of success for completing the borehole is increased from 0.8367314 to 0.8536349.

11.2.2 Waste Package Receipt

No sensitivity analyses were performed because no base case analysis was performed.

11.2.3 Transportation Cask Unloading and Move

Rigging failure and crane failure were identified in Section 11.1.3 as the primary drivers for several of the FT probabilities. Both events have probabilities of 1.00E-05. For this sensitivity analysis, those probabilities were reduced to 1.00E-06. This affected FTs in Figures 10-4 through 10-8, as well as the end states that are associated with these FTs (end states 3 through 7).

Increasing the reliability of the rigging and the crane increased the probability of success from 0.9999119 to 0.9999839. The aggregated probability for Category B is decreased to 1.61E-05 with the increased rigging and crane reliability (base case analysis was equal to 8.81E-05). Successful borehole completion probability is increased to 0.8611799 for this sensitivity case (0.8367314 for the base case analysis).

11.2.4 Cask-to-cask Waste Package Transfer

Section 11.1.4 identified that FTs with probabilities on the order of 10^{-5} had operator diagnosis/actions as the primary drivers. As discussed above SPAR-H HEPs can be reduced as far as 1.00E-06 for diagnosis and 1.25E-06 for actions. The sensitivity analysis for this sequence applied these best-case scenario HEPs to the FTs.

The branching for the FT "Remove shield plug from transport cask" (Figure 10-10) has two branches and one basic event that are operator dependent. The redundancy for each of the configuration branches of the FT (failure of cradle #1 configuration and failure of shield plate configuration) allows for the probability to be reduced by reducing the HEP or the failure of the functional safety system. However, improper removal of the shield plug has no redundancy and results in a single-event cut set for this FT. Similarly, the "Configure upper shield and upper latch assembly" FT (Figure 10-12) and the "Install lower shield plug in transfer cask" FT (Figure 10-18) have cut sets with only one event in the cut set, which are human error events. The "Move shield plate and cradle #1" FT (Figure 10-17) has redundancy in this sequence, similar to Figure 10-10. The sensitivity analysis for this sequence only considers reduced human error probabilities, although performance of the functional safety system might also be improved.

By decreasing the HEPs as discussed previously, the probability of success was increased from 0.9999147 to 0.9999907. The aggregated probabilities for this sensitivity analysis are listed to the right of the arrow (→) below and all decreased except for Category D due to the FT associated with this consequence category not being affected by sensitivity case.

- Category B = 5.33E-05 → 7.08E-06
- Category C = 3.20E-05 → 2.26E-06
- Category D = 1.10E-11 → 1.10E-11

Probability of successful borehole completion increased to 0.8625452 with HEPs decreased to the best-case scenario HEPs.

11.2.5 Transfer Cask Move to the Wellhead

The sensitivity analysis for this sequence applies sensitivities for both rigging/crane failure and operator errors. For HEPs, the best-case scenario probabilities described at the beginning of this section are applied. Additionally, the rigging/crane failure probability of 1.00E-06 is also applied to this set of FTs. The effected FTs are Figure 10-20 through Figure 10-22, and Figure 10-24 through Figure 10-27.

Applying these sensitivity values to this sequence, the probability of success was increased from 0.9999010 to 0.9999897. The aggregated probabilities for this sensitivity analysis are listed to the right of the arrow (→) below.

- Category B = 6.70E-05 → 8.25E-06
- Category C = 3.20E-05 → 2.00E-06
- Category E = 4.20E-21 → 2.00E-30

The probability of successful borehole completion increased from 0.8367314 to 0.8669680 for this sensitivity case.

11.2.6 Wellhead Area Configuration

The success probability for this sequence can be improved with increased carousel reliability and applying the HEPs for the best-case scenario.

In the base case analysis, carousel mechanical failure was assigned a probability of 1.00E-05. If the reliability of the carousel could be improved to 1.00E-06, then the probability of the FT in Figure 10-31 could be decreased from 1.30E-05 to 4.00E-06. For the adaptation of HEPs into the FTs, the FT in Figure 10-28 could be reduced from 2.00E-05 to 2.50E-08.

The overall effect of these two sensitivities is that the probability of success for this sequence is increased from 0.9999627 to 0.9999917. The aggregated probabilities for this sensitivity analysis are listed to the right of the arrow (→) below.

- Category B = 2.43E-05 → 4.32E-06
- Category C = 1.30E-05 → 4.00E-06

The probability of successfully filling the borehole under this sensitivity case increased to 0.8464856.

11.2.7 Wireline Emplacement of the Waste Package

Two of the three primary FTs discussed in Section 11.1.7 have HEPs as the main drivers (FTs in Figure 10-34 and Figure 10-37). Applying the HEPs for the best-case scenario to those FTs, both FTs are reduced an order of magnitude.

Figure 10-36 is most significantly impacted by the dynamic overtension branch. For this branch of the FT, both events must occur. Thus, reducing the probability for either will reduce the overall top event probability. If the probability of a waste package dropping some distance can be reduced to 1.00E-03, as might be the case for a plumb vertical borehole with smooth casing, then the overall FT probability can be reduced to 6.00E-06, versus 5.50E-05 probability in the base case.

Applying these sensitivity values to the FTs, the probability of success for this sequence is increased from 0.9999182 to 0.9999860. The aggregated probabilities for this sensitivity analysis are listed to the right of the arrow (→) below.

- Category B = 1.00E-05 per WP → 1.26E-06
- Category F = 5.70E-05 per WP → 8.95E-06
- Category G = 4.35E-08 per WP → 9.32E-09

The probability of successfully filling the borehole with this sensitivity analysis applied increased from 0.8367314 to 0.8597192.

11.2.8 Conditioning of Equipment for Next Use

No sensitivity analysis performed since no base case analysis was performed.

11.2.9 Placement of Mechanical Interval Plug

This sequence has several FTs with the primary drivers being HEPs. Using the best-case scenario HEPs described above, the FT probabilities are reduced by at least an order of magnitude. The one FT that is not affected by the HEPs is Figure 10-43, for which the primary drivers are failure of the cement plug design and failure of the pull test to detect a faulty bridge plug. These probabilities were decreased from 1.00E-01 to 1.00E-02 for this sensitivity analysis.

Applying these sensitivities to event tree for this sequence, the probability of success was increased from 0.9999580 to 0.9999989. The aggregated probability for Category F was decreased from 4.20E-05 to 1.11E-06. Because this FT only affects one plug for each string of WPs, the effect on the probability of borehole completion was minor with an increase to 0.8370736.

11.2.10 Overall Process

The base case analysis performed in Section 11.1.10 calculated the overall borehole process, as shown in Table 11-1 and Table 11-2. Table 11-3 represents the same calculation but with all the sensitivity values discussed in Section 11.2 applied. As seen in the table, the most significant effect of the sensitivity values is that the probability of a successful borehole completion increases from 0.8367314 to 0.9758306.

Table 11-3. Aggregated probabilities at stages in the DBD process, for best-case analysis.

Consequence Category	Probability (per WP)	Probability (per string)	Probability (per interval plug)	Probability (per borehole)
Category A	0.9999389	0.9975575	0.9999989	0.9758306
Category B	3.70E-05	1.48E-03	-	1.47E-02
Category C	8.27E-06	3.31E-04	-	3.30E-03
Category D	1.10E-11	4.40E-10	-	4.40E-09
Category E	2.00E-30	0.00E+00	-	0.00E+00
Category F	1.21E-05	4.82E-04	1.11E-06	4.82E-03
Category G	9.32E-09	3.73E-07	-	3.73E-06

Nearly all the consequence categories show a decrease in the probability with the sensitivity values applied, except for Category D that experienced no change. Category D is only present in the ET for Activity Sequence 4 (Section 9.4) and is affected by FTs for "Cask-to-cask waste package transfer" (Figure 10-13) and "Waste package integrity maintained" (Figure 10-15). Thus, Category D is highly sensitive to the values of these FTs. If a lower failure probability is desired, then these FTs should be revisited.

12 EXTERNAL HAZARDS

External initiating events derive from causes other than maintaining, plugging, and sealing a disposal borehole, or from handling and emplacing waste packages. A previous analysis (Hardin and Peretz 2017) selected seismic ground motion as the principal external hazard, for generic (non-site specific) assessment, at these intensities:

- **Category 1 (expected to occur at least once during 50-year operations)** – The design basis seismic event is estimated to have 2% probability of occurring in 50 years, corresponding to peak horizontal acceleration of 0.16 g. This hazard level is less likely than Category 1 (for a 50-year disposal project) and therefore is conservative for *magnitude* (but the Category 1 probability level of ≥ 0.02 per year should be used for *frequency*). This hazard level is reasonably consistent with conditions of tectonic stability that have been prescribed for deep borehole disposal locations.
- **Category 2 (less than 1 chance in 10^4 during 50-year operations)** – By definition this event has annual probability of 2×10^{-6}. A peak horizontal acceleration of 0.5 g was selected *ad hoc*, which corresponds to a moderate-to-severe earthquake that is rare in a tectonic province with moderate tectonic stability. Such a hazard level is greater than much of the conterminous U.S., but is an order of magnitude less than tectonically active regions.

The period of peak ground motion is likely to be in the range of 0.3 to 1 sec, with the possibility of spectral amplification depending on site conditions (e.g., low-velocity sediments overlying high-velocity crystalline basement). Strong motion spectra would be needed for seismic design, especially for components with potential for resonance (e.g., headframe).

Extreme ground motion (greater than 0.5 g) at the Category 2 level (500,000-year recurrence) may be possible at a particular site, and should be verified. Peak horizontal acceleration is generally greater than vertical acceleration, but a combined vector-sum loading should be considered in structural calculations.

Hazard from fault rupture that accompanies seismic activity is excluded (Hardin and Peretz 2017) because rupture is generally small for more frequent events, or limited to preexisting faults that can be avoided based on site investigations.

Lightning was also identified as a potential external initiating event, but excluded on the basis that adverse conditions will be predicted, detected, and mitigated (Hardin and Peretz 2017). Lightning strikes are strongly associated with, although not limited to, predictable extreme weather such as thunderstorms and hurricanes. It can be detected in real time at distances of 100 miles or more, giving warning for suspension of vulnerable operations. In lightning-prone regions protection can be added to system components such as the headframe and wireline system, to further reduce the likelihood of critical damage such as breaking the wireline cable during downhole operations. Combining mitigation measures with limited exposure vulnerability (i.e., fractional duration of vulnerable operations) lightning can be excluded (beyond Category 2) if the aggregate annual probability of lightning-initiated event sequences resulting in critical damage is less than 2×10^{-6}.

Wind strength and direction are more predictable, and waste handling and emplacement operations can be suspended if predicted wind speed exceeds a design threshold (e.g., 25 knots).

Wind design criteria such as ASCE-7 (ASCE 2005; FEMA 2007) are used with appropriate categorization and importance factors, to design critical facilities even in tornado- and hurricane-prone areas, special wind areas, and flat, open terrain. To prevent wind-caused damage to equipment, it is assumed that appropriate shelters (e.g., berm protection) are available for waste transport vehicles and portable equipment (e.g., crane, wireline rig).

Other hazards excluded in the previous report (Hardin and Peretz 2017), based on analysis or assumption, include landslide, volcanism, flooding, aircraft crash, nearby industrial/military accidents, hazardous materials, external fire, and meteorites/satellites.

12.1 Seismic Ground Motion

This section analyzes the potential for DBGM-1 (2,500-year recurrence, bracketing Category 1 events) and develops another design basis (DBGM-2) that serves to exclude event sequences beyond Category 2.

The approach first performs a "crosswalk" to qualitatively assess the extent to which each of the high-level internal initiating events (Section 7) could be initiated by concurrent seismic ground motion (Section 8.2.1). The approach goes on to estimate exposure duration for key activity steps and activity sequences (Section 8.2.2). Exposure durations are used to calculate conditional probabilities for seismic event sequences corresponding exactly to the probability level for Category 2 (10^{-4} for the overall disposal campaign of 30,000 waste packages) and assuming maximum fragility. In other words, because of limited exposure duration, some activity sequences can be designed to withstand weaker ground motion than the 500,000-year events discussed previously, and still have seismic event sequence probabilities less than 10^{-4}. These bounding estimates for seismic initiating event probability are then used to define DBGM-2 at two levels corresponding to surface operations (DBGM-2A at 100,000-year recurrence) and wellhead/borehole operations (DBGM-2B at 200,000-year recurrence).

In the approach described above, supporting equipment is included implicitly in seismically initiated event sequences based on internal events. For example, the mobile crane, cradle operation, cask-to-cask transfer, headframe hoist, and wireline system are all assumed to default to arrested, safe shutdown conditions in the event of extreme ground motion, or failure of their respective power supplies. However, additional and separate treatment of the vulnerability of supporting equipment to ground motion allows a more explicit review that can include modes such as a crane damage and tip-over, headframe structural stability, wireline system seismic response, and power supply reliability. A similar analysis of exposure duration and bounding seismic event probabilities, is developed for supporting equipment (Section 8.2.3).

Finally, summary event sequence diagrams (ESDs) are developed for graphical presentation of external seismic-initiated events (Section 8.2.4). In summary, the evaluation of seismic events shows that there are three broad categories of seismic risk present, associated with: 1) surface handling of waste packages using relatively brief activity sequences; 2) downhole operations requiring longer duration; and 3) support functions that must be maintained over nearly the full duration.

12.2 Crosswalk to Internal Initiating Events

The sixty internal initiating events identified in Section 7 and discussed in Section 8 lead to a wide range of event sequences and failed states. Event trees that use selected initiating events from this set (Section 9) also include basic and pivotal events that further increase the range of outcomes. Accordingly, transparent examination of seismic system response begins with how ground motion could affect the likelihood for each of these initiating events.

The assessment of seismic sensitivity is qualitative, but with justification (Table 12-1). Event sequences are designated “low” or “high” sensitivity, with the basis provided. Thus, the analysis in Section 8.2.3 of exposure duration and DBGM-2, can be interpreted in terms of which event sequences could have greater seismic fragility (detailed fragility analysis would be undertaken, where necessary, in the design process).

Table 12-1. Crosswalk between potential external seismic ground motion events, and internal initiating events.

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
1. Borehole Qualification				
Wellhead				
	Wireline tool string drops from wellhead onto uppermost emplaced waste package.	Low	Limited exposure duration at the wellhead with gate valve open; slow terminal velocity of dropped tooling.	Design criteria (e.g., terminal velocity) and administrative controls.
Wireline				
	Wireline tool string drops onto uppermost emplaced waste package.	Low	Slow terminal velocity of dropped tooling; condition monitoring of wireline cable and connections.	Design criteria (e.g., terminal velocity) and administrative controls (e.g., slow logging speed and inspection of cable and connections).
	Wireline tool string strikes uppermost emplaced waste package during logging.	Low	Slow logging speed; downhole load sensing; robust waste packages.	Design criteria (e.g., analyze waste package impact resistance; load sensing downhole wireline tool) and administrative controls (e.g., logging speed).
3. Transport Cask Prep. and Move				
Lift				
	Cask topples as it is lifted off trailer cradle.	High	Vulnerable crane action during ground motion.	Design criteria (analyze maximum drop height at adverse orientation; specify pad constructed of compacted gravel) and administrative controls.
	Cask collision with object during move.	High	Vulnerable crane action during ground motion.	Design criteria (e.g., long period of pendular load oscillation; hardware limits on crane functions) and administrative controls (limit objects near path).
	Crane drops object on cask.	High	Vulnerable crane action (objects are relatively light).	Design criteria (e.g., identify limiting mass) and administrative controls (eliminate available heavy objects).
	Cask drop during move from trailer to cradle #1.	High	Vulnerable crane action during ground motion.	Design criteria (maximum drop height and adverse orientation; specify pad construction; anti-two blocking) and

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
				administrative controls.
	Crane overturns cask while on trailer.	Low	Crane action not vulnerable prior to lift.	Design criteria (e.g., cradle and yoke design; eliminate snagging hazards).
Cask Cradle Roll				
	Inadvertent movement or collision of cradle #1.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and the control/functional safety system (e.g., control and limit timing of movement).
	Cradle #1 with transport cask derails or tips over.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and the control/functional safety system (e.g., control timing, speed, and range of movement).
Shield Plug Handling				
	Inadvertent movement of shield plug during move.	Low	Robust cask design; plug not handled during move.	Design criteria (e.g., secure shield plug restraints), and administrative controls (plug is not handled during move).
	Inadvertent removal of shield plug during preparations.	Low	Plug not handled during preparation.	Administrative controls (plug is not handled during prep. on trailer).
4. Cask-to-Cask Transfer				
Cask Cradle Roll				
	Inadvertent move of cradle away from interface shield with shield plug in place.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and the control/functional safety system (e.g., control and limit timing of movement).
	Inadvertent move of cradle away from interface shield with shield plug dislodged.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.), administrative controls (e.g., as-built testing of restraints), and the control/functional safety system (e.g., control and limit timing of movement).
	Cradle and cask dislodged during package transfer.	Low	Robust seismic design; limited duration of exposure.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., as-built testing of supports and restraints).
Shield Plug Handling				

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
	Incorrect configuration during removal of transport cask shield plug.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., simple design; seismic specs.) and administrative controls (prevent and mitigate human error).
	Incorrect configuration during insertion of transfer cask lower shield plug.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., secure plug connection with simple mechanism; seismic specs.) and administrative controls (prevent and mitigate human error).
	Incorrect configuration of transfer cask upper shield plug components.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., simple design; seismic specs) and administrative controls (prevent and mitigate human error).
	Improper placement of cask plugs in interface shield slide.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., retain plugs in slide; seismic specs.) and administrative controls (prevent and mitigate human error).
Interface Shield Slide Action				
	Incorrect movement of cask, cradle, and shield components during move.	Low	Robust seismic design.	Design criteria (seismic specs.) and the control/functional safety system (e.g., system safe shut down if configuration is incorrect, or may deviate during a seismic event).
Latch Action/Package Movement				
	Improper side latch action (damage to waste package).	Low	Robust design prevents improper action.	Design criteria (e.g., side latch seismic specs.) and administrative controls (test side latch function during transfer)
	Improper shield configuration during latching and waste package transfer operations.	Low	Principally human error, which has limited duration of exposure.	Design criteria (e.g., simple design; seismic specs.) and administrative controls (mitigate human error).
	Improper upper latch action (damage to waste package).	Low	Robust design prevents improper action.	Design criteria (e.g., upper latch seismic specs.) and administrative controls (test upper latch function during transfer)
	Package scrapes and drags through sliding shield (damage	Low	Robust seismic design; limited duration of	Design criteria (e.g., seismic specs.) and functional safety (e.g., limit push/pull force; safe shut down).

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
	to waste package).		exposure.	
5. Transfer Cask Move to Wellhead				
Lift				
	Shield plug falls out of cask during lift.	High	Plug clamped in place; robust cask design (see drop event).	Design criteria (e.g., robust design; seismic specs.), functional safety (e.g., identify unsafe condition before lift), and administrative controls (e.g., prevent incorrect operation).
	Shield plug and waste package fall out of cask during lift.	Low	Plug clamped in place; waste package retained by redundant latches; robust seismic design.	Design criteria (e.g., robust design; seismic specs.), functional safety (e.g., identify unsafe condition before lift), and administrative controls (e.g., prevent incorrect operation).
	Cask topples while lifting off cradle #2.	High	Vulnerable crane action during ground motion.	Design criteria (e.g., analyze adverse drop; seismic specs.), the control/functional safety system (e.g., control when ready for lift), and administrative controls (prevent incorrect operation).
	Cask collision with object during move.	High	Vulnerable crane action during ground motion.	Design criteria (e.g., long period of pendular load oscillation; hardware limits on crane functions) and administrative controls (e.g., limit objects near path).
	Crane drops object on cask.	High	Vulnerable crane action (objects are relatively light).	Design criteria (e.g., identify limiting mass) and administrative controls (e.g., eliminate available heavy objects).
	Cask drop during move from cradle #2 to wellhead.	High	Vulnerable crane action during ground motion.	Design criteria (analyze drop damage for adverse conditions), the control/functional safety system (e.g., response to ground motion), and administrative controls (prevent incorrect operation).
	Improper placement of cask in carousel (damage to cask).	High	Vulnerable crane action during ground motion.	Design criteria (e.g., use guides) and administrative controls (e.g., detect and mitigate damage to lower shield plug).
Wellhead				
	Toppling of transfer cask on pit	High	Vulnerable crane action	Design criteria (analyze drop damage for adverse conditions),

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
	shield assembly.		and wellhead operations during ground motion.	the control/functional safety system (e.g., control order of steps to secure cask), and administrative controls.
	Pit or shield mechanical failure.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., as-built testing after setup, prior to waste operations).
6. Wellhead Configuration				
Wellhead				
	Improper movement of carousel (damage to cask).	Low	Robust seismic design; interlocks.	Design criteria (e.g., seismic specs.; restraining device) and the control/functional safety system (e.g., lockout carousel movement).
	Failure of supports and tie-downs (cask topples).	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and administrative controls (prevent incorrect operation).
	Failed connection to wellhead flange (damage to cask).	Low	Robust seismic design.	Design criteria (e.g., robust flange design), the control/functional safety system (e.g., automatically evaluate tightening torque), and administrative controls (detect and mitigate damage to flange on cask).
Wireline				
	Improper shielding configuration during tool string installation.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., upper shield designed to prevent assembly errors) and administrative controls (prevent and mitigate human error).
	Improper tool string installation (damage to waste package).	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., robust latch) and administrative controls (e.g., perform pull test against side latches, before use; prevent and mitigate human error).
	Improper lubricator installation (cask damage or loss of shielding).	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., robust latch) and administrative controls (e.g., prevent and mitigate human error).
	Tight wireline pulls cask over during carousel rotation.	Low	Principally human error, with limited duration of exposure.	Design criteria (e.g., include wireline geometry and pull in seismic specs.) and administrative controls (e.g., prevent and mitigate human error).

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
Latch Action/Package Movement				
	Latches and tool string fail (package drops).	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., maintain redundancy and pull test latches before use).
	Stuck upper latch (damage to waste package).	Low	Robust seismic design.	Design criteria (e.g., design for recovery; seismic specs.) and administrative controls (e.g., identify conditions that lead to damage).
Upper Shield Plug Handling				
	Shield plug components stuck.	Low	Robust seismic design.	Design criteria (e.g., design for recovery; seismic specs.) and administrative controls (e.g., identify precursors).
	Entire upper shield plug dislodges as upper latch is removed.	Low	Principally human error; robust seismic design.	Design criteria (e.g., passive features prevent incorrect operation) and administrative controls (e.g., prevent and mitigate human error).
	Radiological controls or supplemental shielding not in place.	Low	Principally human error; robust seismic design.	Design criteria (e.g., seismic specs. on shielding) and administrative controls (e.g., prevent and mitigate human error).
Lower Shield Plug Handling				
	Improper pit shield configuration as lower shield plug is removed.	Low	Interlocks to detect and mitigate human error; robust seismic design.	Design criteria (e.g., seismic specs.), the control/functional safety system (e.g., alignment), and administrative controls (e.g., detect and mitigate errors).
	Lower shield plug falls during removal.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.), the control/functional safety system (e.g., verify operation), and administrative controls (e.g., detect and mitigate errors).
7. Waste Package Emplacement (and retrieval) by Wireline				
Latch Action/Package Movement				

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
	Drop waste package onto gate valve.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., pull test wireline attachment).
Wellhead				
	BOP closes (damages waste package, tool string, or wireline).	Low	Robust seismic design.	Design criteria (e.g., establish that BOP cannot damage waste package, tool string, or wireline cable), and administrative controls (e.g., facilitate recovery).
	Gate valve closes during wellhead operations (damage to waste package).	Low	Robust seismic design.	Design criteria (e.g., gate valve cannot damage package), and administrative controls (e.g., facilitate recovery).
	Waste package scrapes and drags on wellhead components.	Low	Robust seismic design.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., detect and correct damage).
Wireline				
	Waste package drops from surface into borehole.	Low	Robust seismic design (wireline connections).	Design criteria (e.g., seismic specs.) and administrative controls (e.g., pull test wireline attachment).
	Waste package drops during trip in.	Low	Cable compliance and slow logging speed.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., pull test wireline attachment before use).
	Waste package gets stuck during trip in.	Low	Limited seismic loads on guidance casing.	Design criteria (e.g., seismic analysis of casing) and the control/functional safety system (e.g., suspend trip on ground motion).
	Wireline and tool string dropped on package during trip out.	Low	Cable compliance and slow spooling speed.	Design criteria (e.g., seismic specs.) and administrative controls (e.g., pull test wireline attachment before use).
Borehole Events				
	Waste package driven uphole by fluid “kick” (stuck or damaged).	Low	Robust borehole design.	Deploy BOP and fluid control valves.
	Thermal event from waste heating (during wireline hold) causes unstable conditions (boiling).	Low	Ground motion has a minor effect on fluid level.	Design criteria (e.g., analyze conditions leading to boiling) and administrative controls (establish operational controls).

Activity Sequence	Internal Initiating Events	Greater Prob. w/ Ground Motion?	Basis	Mitigation
9. Mechanical Bridge Plug Setting				
Wellhead				
	Downhole tool assembly drops onto uppermost waste package.	Low	Robust seismic design (coiled tubing tool connections).	Design criteria (e.g., terminal velocity of bridge plug) and administrative controls (test connections before use).
Coiled Tubing				
	Coiled tubing and downhole assembly drops onto uppermost waste package.	Low	Robust seismic design; limited tubing injection speed.	Design criteria and administrative controls (e.g., test connections before use; monitor and mitigate wear condition of coiled tubing).
	Coiled tubing and tools strike the uppermost waste package on trip in.	Low	Robust seismic design; limited duration of exposure.	Design criteria (e.g., analyze waste package impact resistance) and administrative controls (e.g., injection speed).

12.3 Exposure Duration Analysis

Following the general approach detailed in BSC (2008b), the seismic exposure duration is estimated for each activity sequence that is associated with an internal initiating event. Thus, for each internally-based initiating event (Table 12-1), the activity sequences and constituent activity steps are identified (Table 12-2). Then the duration of each step is estimated, and these are summed to find the durations for each activity sequence. Note that inspection steps are not included because of short duration, and also that some steps are concurrent and therefore excluded from the tallies for activity sequences (italics in Table 12-2).

The additional probabilistic safety margin represented by fractional exposure duration, is used to calculate a new level of concern for seismic ground motion at the Category 2 probability level (10^{-4} probability over the 50-year duration of a large-scale disposal campaign). The calculation follows

$$p' = 10^{-4}/(N \times D)$$

where

p'	=	Probability level of concern (yr^{-1}) for seismic events (take reciprocal for recurrence)
10^{-4}	=	Category 2 threshold probability for event sequences (per 50-year campaign)
N	=	Number of waste packages (30,000 per 50-year campaign)
D	=	Exposure duration (yr) per waste package

A lower bound on the value of p' is 2×10^{-6} yr^{-1} (maximum recurrence 500,000 years) which is the event that gives an integrated probability of 10^{-4} over the assumed duration of a disposal campaign (50 years; see Section 4).

Events affecting handling and emplacement of each waste package are treated as independent even though as many as five boreholes are assumed to be active at once in the disposal campaign (Section 4). This assumption may not be conservative because the process flow has been disaggregated into activity sequences that are not likely to be synchronized among boreholes.

The results (Table 12-2) show the relationship of activity sequence duration to the seismic hazard level that should be considered in design. The table lists activity sequences and corresponding hazard categories; then the associated internal initiating events, then the activity steps associated with the initiating events. Durations for the steps are estimated and summed upward to subtotals for each activity sequence (except for steps that overlap in time which are shown in italics). The overall duration of handling and emplacement activities is summed at the end of the table (except for mechanical bridge plugs which are set at intervals of approximately 40 waste packages).

The results show two levels of possible concern for design. Surface handling structures, systems, and components (SSCs) can be designed to weaker ground motion (~100,000-year recurrence) than SSCs used in downhole activities (~200,000-year recurrence) because of exposure duration. These are designated DBGM-2A and DBGM-2B, respectively, in this report.

Table 12-2. Duration of exposure to ground motion, for activity sequences associated with internal initiating events.

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
1. Borehole Qualification		**Sum durations for steps below.**	**5.25**	**5.6E-06**	**1.8E+05**
Wellhead					
	Wireline tool string drops from wellhead onto uppermost emplaced WP.	1.2 Assemble the qualification tool, string consisting of a gauge ring, junk basket and other tools such as a casing collar locator, onto the wireline, along with an appropriate fluid seal system. 1.3 Attach lubricator (riser) to the wellhead flange, ready to accept the qualification tool string and grease seal, and verify that the lower gate valve is closed. 1.5 Open the lower gate valve and allow the borehole fluid to achieve a steady elevation/pressure.	1	2.9E-05	3.4E+04
Wireline					
	Wireline tool string drops onto uppermost emplaced WP.	1.6 Run the gauge ring and junk basket down and up borehole.	4	7.3E-06	1.4E+05
	Wireline tool string strikes uppermost emplaced WP during logging.	1.6 Run the gauge ring and junk basket down and up borehole.	0.25	1.2E-04	8.6E+03
3. Transport Cask Prep. and Move		**Sum durations for steps below, except those that overlap (italics).**	**2.75**	**1.1E-05**	**9.4E+04**
Lift					
	Cask topples as it is lifted off trailer cradle.	3.7 Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.	0.25	1.2E-04	8.6E+03
	Cask collision with object during move.	3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.	0.25	1.2E-04	8.6E+03

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
	Crane drops object on cask.	3.3 Remove the trailer cover and doors and set into a laydown area, using a crane. 3.4 Remove the impact limiters from the transportation cask while it is secured to the trailer, using a crane, and set them in a laydown area. 3.6 Remove the fixtures securing the cask to the trailer, and attach a crane-supported yoke to the cask trunnions.	2	1.5E-05	6.9E+04
	Cask drop during move from trailer to cradle #1.	3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask. 3.9 Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.	0.25	1.2E-04	8.6E+03
	Crane overturns cask while on trailer.	*3.6 Remove the fixtures securing the cask to the trailer, and attach a crane-supported yoke to the cask trunnions.* *3.7 Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.*	*0.5*	*5.8E-05*	*1.7E+04*
Cask Cradle Roll					
	Inadvertent movement or collision of cradle #1.	*3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.* *3.9 Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.* *3.11 Prepare the end plug for removal, and roll cradle #1 into position against the transfer shield.*	*0.5*	*5.8E-05*	*1.7E+04*
	Cradle #1 with transport cask derails or tips over.	*3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.* *3.9 Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the yoke, and secure cask to cradle.* *3.11 Prepare the end plug for removal, and roll cradle #1 into position against the transfer shield.*	*0.5*	*5.8E-05*	*1.7E+04*

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Shield Plug Handling					
	Inadvertent movement of shield plug during move.	*3.7 Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.* *3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.* *3.9 Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.*	*1*	*2.9E-05*	*3.4E+04*
	Inadvertent removal of shield plug during preparations.	*3.7 Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.* *3.8 Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.* *3.9 Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.*	*1*	*2.9E-05*	*3.4E+04*
4. Cask-to-Cask Transfer		**Sum durations for steps below, except those that overlap (italics).**	**2**	**1.5E-05**	**6.9E+04**
Cask Cradle Roll					
	Inadvertent move of cradle away from interface shield with shield plug in place.	4.19 Roll cradle #1 away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved. 4.23 Roll cradle #2 with the loaded transfer cask away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved.	0.5	5.8E-05	1.7E+04
	Inadvertent move of cradle away from interface shield with shield plug dislodged.	*Steps 4.5 through 4.22.*	*2*	*1.5E-05*	*6.9E+04*
	Cradle and cask dislodged during package transfer.	*Steps 4.5 through 4.22.*	*2*	*1.5E-05*	*6.9E+04*

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Shield Plug Handling					
	Incorrect configuration during removal of transport cask shield plug.	*4.5 Detach and pull the end shield from the transportation cask into the sliding shield, using appropriate tooling to align, pull, and secure the plug in the sliding shield.*	*0.5*	*5.8E-05*	*1.7E+04*
	Incorrect configuration during insertion of transfer cask lower shield plug.	*4.21 Push the transfer cask lower shield plug into position in the transfer cask, using appropriate tooling.* *4.22 Engage the Grayloc® clamp on the bottom of the transfer cask to the lower shield plug, and verify engagement.*	*0.5*	*5.8E-05*	*1.7E+04*
	Incorrect configuration of transfer cask upper shield plug components.	*4.10 Release the flange from the package latch subassembly on the transfer cask top plug, and attach the extension shaft to the transfer latch subassembly.* *4.16 Attach the flange to the package latch subassembly, and attach the flange to the transfer cask top shield plug. Leave the latch subassembly attached to the waste package.*	*0.5*	*5.8E-05*	*1.7E+04*
	Improper placement of cask plugs in interface shield slide.	4.18 Position the sliding shield plate in its third position, with the transfer cask lower shield plug in the slide shield ready for insertion.	0.5	5.8E-05	1.7E+04
Interface Shield Slide Action					
	Incorrect movement of cask, cradle, and shield components during move.	4.4 Position the sliding shield plate in its first position, ready to receive transportation cask end shield plug. 4.8 Position the sliding shield plate in its second position, providing an open path between the two casks. 4.13 Pull the waste package through the interface shield assembly until it is in position in the transfer cask, and the extension shaft connection is clear of the transfer cask upper plug. Monitor radiation exposure dose rates throughout this operation. 4.18 Position the sliding shield plate in its third position, with the transfer cask lower shield plug in the slide shield ready for insertion.	0.5	5.8E-05	1.7E+04

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Latch Action/Package Movement					
	Improper side latch action (damage to WP).	*4.15 Engage the side latches, securing the package in position in the transfer cask. Verify engagement of the latches.*	*0.5*	*5.8E-05*	*1.7E+04*
	Improper shield configuration during latching and WP transfer operations.	*4.10 Release the flange from the package latch subassembly on the transfer cask top plug, and attach the extension shaft to the transfer latch subassembly.*	*0.5*	*5.8E-05*	*1.7E+04*
	Improper upper latch action (damage to WP).	*4.11 Push the package latch subassembly through the interface shield assembly until it makes contact with the waste package in the transportation cask.* *4.12 Confirm latch engagement on the waste package.* *4.16 Attach the flange to the package latch subassembly, and attach the flange to the transfer cask top shield plug. Leave the latch subassembly attached to the waste package.*	*0.5*	*5.8E-05*	*1.7E+04*
	Package scrapes and drags through sliding shield (damage to waste package).	*4.13 Pull the waste package through the interface shield assembly until it is in position in the transfer cask, and the extension shaft connection is clear of the transfer cask upper plug. Monitor radiation exposure dose rates throughout this operation.*	*0.5*	*5.8E-05*	*1.7E+04*
5. Transfer Cask Move to Wellhead		**Sum durations for steps below, except those that overlap (italics).**	**1.75**	**1.7E-05**	**6.0E+04**
Lift					
	Shield plug falls out of cask during lift.	5.4 Rotate the cask into a vertical position with pins set on cradle #2, and lift the cask just above the cradle and wellhead structures. 5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.	0.5	5.8E-05	1.7E+04
	Shield plug and waste package fall out of cask during lift.	*5.4 Rotate the cask into a vertical position with pins set on cradle #2, and lift the cask above the cradle and wellhead structures.* *5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.*	*0.5*	*5.8E-05*	*1.7E+04*

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
	Cask topples while lifting off cradle #2.	5.3 Remove the fixtures securing the cask to cradle #2, and attach a crane-supported yoke to the cask trunnions (this might be a field crane, or might be a hoist on a headframe assembly).	0.25	1.2E-04	8.6E+03
	Cask collision with object during move.	*5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.*	*0.25*	*1.2E-04*	*8.6E+03*
	Crane drops object on cask.	*5.3 Remove the fixtures securing the cask to cradle #2, and attach a crane-supported yoke to the cask trunnions (this might be a field crane, or might be a hoist on a headframe assembly).*	*0.25*	*1.2E-04*	*8.6E+03*
	Cask drop during move from cradle #2 to wellhead.	*5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.*	*0.25*	*1.2E-04*	*8.6E+03*
	Improper placement of cask in carousel (damage to cask).	5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port. 5.6 Secure the transfer cask to the shield carousel, using TBD features to prevent the cask from tipping or being dislodged (features such as guy wires must allow carousel rotation and kneeling jack actuation).	0.5	5.8E-05	1.7E+04
Wellhead					
	Toppling of transfer cask on pit shield assembly.	5.6 Secure the transfer cask to the shield carousel, using TBD features to prevent the cask from tipping or being dislodged (features such as guy wires must allow carousel rotation and kneeling jack actuation).	0.5	5.8E-05	1.7E+04
	Pit or shield mechanical failure.	*5.5 Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.* *5.6 Secure the transfer cask to the shield carousel, using TBD features to prevent the cask from tipping or being dislodged (features such as guy wires must allow carousel rotation and kneeling jack actuation).*	*0.5*	*5.8E-05*	*1.7E+04*

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
6. Wellhead Configuration		**Sum durations for steps below, except those that overlap (italics).**	**3.25**	**9.0E-06**	**1.1E+05**
Wellhead					
	Improper movement of carousel (damage to cask).	Steps 6.9 through 6.26.	2	1.5E-05	6.9E+04
	Failure of supports and tie-downs (cask topples).	6.1 Ensure the transfer cask is in place on the shield plate carousel, properly secured and positioned over the lower plug handling mechanism.	0.25	1.2E-04	8.6E+03
	Failed connection to wellhead flange (damage to cask).	*6.21 Confirm cask position over the wellhead flange, and adjust position as necessary.* *6.22 Use the kneeling jacks to gently lower the cask onto the wellhead flange, while monitoring alignment of the bottom cask flange with the wellhead flange. Adjust the position of the carousel as necessary to maintain alignment as the cask is lowered.* *6.23 With the cask in contact with the wellhead flange, activate the Grayloc® clamp on the bottom of the transfer cask to complete the flange connection between the transfer cask and the wellhead.*	*1*	*2.9E-05*	*3.4E+04*
Wireline					
	Improper shielding configuration during tool string installation.	*6.9 Attach a connection sub to the transfer cask upper shield plug, to mate with the quick connector on the lower end of the lubricator.* *6.10 Make up the wireline tool string, lubricator, and grease seal assembly at ground level. Up-end the assembly under the headframe and lift it vertically with the wireline cable. Lower the assembly onto the connection sub and make the connection with the lubricator.* *6.11 Lower the tool string until it latches onto the waste package.*	*0.5*	*5.8E-05*	*1.7E+04*

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
	Improper tool string installation (damage to WP).	*6.10 Make up the wireline tool string, lubricator, and grease seal assembly at ground level. Up-end the assembly under the headframe and lift it vertically with the wireline cable. Lower the assembly onto the connection sub and make the connection with the lubricator.* *6.11 Lower the tool string until it latches onto the waste package.* *6.12 Verify that the tool string is securely latched onto the waste package.*	*0.5*	*5.8E-05*	*1.7E+04*
	Improper lubricator installation (cask damage or loss of shielding).	*6.9 Attach a connection sub to the transfer cask upper shield plug, to mate with the quick connector on the lower end of the lubricator.* *6.10 Make up the wireline tool string, lubricator, and grease seal assembly at ground level. Up-end the assembly under the headframe and lift it vertically with the wireline cable. Lower the assembly onto the connection sub and make the connection with the lubricator.*	*0.5*	*5.8E-05*	*1.7E+04*
	Tight wireline pulls cask over during carousel rotation.	*6.14 Take up wireline slack to the extent possible movement of the package is minimized but cask movements remain possible.*	*0.25*	*1.2E-04*	*8.6E+03*
Latch Action/Package Movement					
	Latches and tool string (if used) fail (package drops).	*Steps 6.15 through 6.26.*	*2*	*1.5E-05*	*6.9E+04*
	Stuck upper latch (damage to WP).	6.7 Disconnect the top latch assembly from the upper shield plug, activate the latch rod to release the assembly from the waste package, and remove the latch assembly from the upper shield plug.	0.5	5.8E-05	1.7E+04

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Upper Shield Plug Handling					
	Shield plug components stuck.	6.7 Disconnect the top latch assembly from the upper shield plug, activate the latch rod to release the assembly from the waste package, and remove the latch assembly from the upper shield plug.	0.5	5.8E-05	1.7E+04
	Entire upper shield plug dislodges as upper latch is removed.	*6.7 Disconnect the top latch assembly from the upper shield plug, activate the latch rod to release the assembly from the waste package, and remove the latch assembly from the upper shield plug.*	*0.5*	*5.8E-05*	*1.7E+04*
	Radiological controls or supplemental shielding not in place.	*6.6 Position personnel access hardware adjacent to the transfer cask, and install temporary shielding as required for removal of the latch assembly and installation of the tool string.*	*0.5*	*5.8E-05*	*1.7E+04*
Lower Shield Plug Handling					
	Improper pit shield configuration as lower shield plug is removed.	*6.15 Raise the lower shield plug handling mechanism until it engages with the shield plug.* *6.16 Activate the Grayloc® clamp on the bottom of the transfer cask to release the lower shield plug.* *6.17 Lower the shield plug handling mechanism so the shield plug is clear of the bottom flange of the transfer cask.*	*1*	*2.9E-05*	*3.4E+04*
	Lower shield plug falls during removal.	*6.16 Activate the Grayloc® clamp on the bottom of the transfer cask to release the lower shield plug.* *6.17 Lower the shield plug handling mechanism so the shield plug is clear of the bottom flange of the transfer cask.*	*1*	*2.9E-05*	*3.4E+04*
7. WP Emplacement by Wireline		**Sum durations for steps below, except those that overlap (italics).**	**5.75**	**5.1E-06**	**2.0E+05**
Latch Action/Package Movement					
	Drop WP onto gate valve.	7.2 Ensure the wireline tool string is connected waste package, and is properly tensioned. 7.6 Verify the side latches are engaged with the waste package. 7.7 Verify the wellhead gate valve is closed. 7.8 Release side latches, supporting waste package by the wireline.	0.5	5.8E-05	1.7E+04

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Wellhead					
	BOP closes (damages WP, tool string, or wireline).	Steps 7.12 through 7.18.	4	7.3E-06	1.4E+05
	Gate valve closes during wellhead operations (damage to WP).	*Steps 7.12 through 7.18.*	*4*	*7.3E-06*	*1.4E+05*
	WP scrapes and drags on wellhead components.	*7.9 Lower the package through the wellhead components, to just above the closed gate valve, while monitoring radiation dose exposure rates at the wellhead shield.*	*0.25*	*1.2E-04*	*8.6E+03*
Wireline					
	WP drops from surface into borehole *(gate valve closed).*	*7.8 Release the side latches, allowing the waste package to be supported by the wireline.* *7.9 Lower the package through the wellhead components, to just above the closed gate valve, while monitoring radiation dose exposure rates at the wellhead shield.*	0.25	1.2E-04	8.6E+03
	WP drops during trip in.	*7.10 Open the wellhead gate valve and monitor the level of fluid in the borehole.* *7.11 If necessary, add fluid to bring the borehole fluid level up to the wellhead.* *7.12 Continue to lower the waste package to the emplacement zone, monitoring depth of the package using the tool string locator, wireline runout, wireline tension, and downhole load monitoring.* *7.13 Stop the wireline when the package rests on the previous package or borehole plug (or, in the case of the initial package, the bottom of the borehole).*	*3*	*9.7E-06*	*1.0E+05*
	WP gets stuck during trip in.	*7.12 Continue to lower the waste package to the emplacement zone, monitoring depth of the package using the tool string locator, wireline runout, wireline tension, and downhole load monitoring.*	*3*	*9.7E-06*	*1.0E+05*
	Wireline and tool string dropped during trip out.	7.17 Retrieve the wireline, monitoring depth of the tool string, until the tool string is returned to the transfer cask lubricator.	1	2.9E-05	3.4E+04

Activity Sequence + Hazard Categories	Internal Initiating Events	Activity Sequence Includes These Action Steps from Process Flow Diagram	Step/ Sequence Duration (hr)	Conditional Seismic Event Prob. (per yr)	Recurrence Interval (yr)
Borehole Events					
	WP driven uphole by fluid "kick" (stuck or damaged).	*Steps 7.10 through 7.18.*	*4*	*7.3E-06*	*1.4E+05*
	Thermal event from waste heating (during wireline hold) causes unstable conditions (boiling).	(Wireline hold is not a planned activity.)			
9. Mechanical Bridge Plug Setting		**Sum durations for steps below, except those that overlap (italics).**	**4**	**7.3E-06**	**1.4E+05**
Wellhead					
	Downhole tool assembly drops onto uppermost WP.	9.3 Assemble bridge plug and squeeze packer on coiled tubing.	1	2.9E-05	3.4E+04
Coiled Tubing					
	Coiled tubing and downhole assembly drops onto upper WP.	9.6 Run coiled tubing with bridge plug into position over the last waste package.	3	9.7E-06	1.0E+05
	Coiled tubing and tools strike the uppermost WP on trip in.	*9.6 Run coiled tubing with bridge plug into position over the last waste package.*	*0.25*	*1.2E-04*	*8.6E+03*
Total Duration for Emplacement of a Single Waste Package (except mechanical bridge plug setting)			**20.75**		

12.4 Design Basis Ground Motion for Supporting Components

A similar analysis is presented for supporting equipment that is used in multiple internal event sequences and subject to degradation by seismic ground motion. These structures, systems, and components include:

- Mobile crane (transport cask preparation and moves)
- Headframe structure (transfer cask moves, wellhead configuration, and waste package emplacement and retrieval by wireline)
- Headframe hoist (transfer cask moves)
- Wireline system (borehole qualification, wellhead configuration, and waste package emplacement and retrieval)
- Power supply (on-site generators or off-site power; used to actuate cask-to-cask transfer, headframe, and wellhead functions, and to power the control/functional safety system)
- Control/functional safety system (used to control all activity sequences, including functional safety sensors, actuators, and programmable logic)

Each of these is used in several activity sequences (Table 12-3) for which exposure durations are estimated as in the previous section. The durations for each sequence are tallied, and the corresponding seismic level of concern for each SSC at the Category 2 threshold probability level is calculated. The approach is approximate because the underlying description of design and operations is conceptual, and it may be conservative to the extent that the activity steps identified in the sequences overlap in time or do not require certain supporting equipment.

The results show that supporting equipment is likely to be exposed to stronger ground motion during waste handling and emplacement operations, than the SSCs associated with internal initiating events. For event sequences at the Category 2 probability level, seismic events with recurrence in the range 300,000 to 500,000 years could be considered. Peak ground motion of 0.5 g, with recurrence of 500,000 years is designated DBGM-2C in this report.

We note that SSCs are not required to perform their functions during or after a Category 2 event, only that the overall system is required to meet regulatory limits on radiation dose and exposure to workers and the public for a single event. Supporting equipment differs from the sequences described in Table 12-2, because it must perform nearly continuously and not in a sequence of steps. Accordingly, the different SSCs (Table 12-3) perform concurrently so that seismic events are common mode initiators and interaction between impacted SSCs during and after the event must be considered.

For simplicity in consequence modeling for design, this could be interpreted to mean that SSCs can achieve safe shutdown and not interfere with each other, during or after a DBGM-2C event.

12.5 Summary of External Seismic Event Sequences

Seismic event sequences can be depicted using ESDs as shown in a set of examples (Figure 12-1 through Figure 12-4). The internally derived initiating events judged to be most sensitive to ground motion (Table 12-1) correspond to lifts of the transport and transfer casks, shown in Figure 12-1 and Figure 12-2. Seismic event sequences involving downhole activities are shown in Figure 12-3. An example diagram summarizing seismic sequences for supporting equipment is also presented (Figure 12-4).

Insights from examination of seismic hazards, and development of seismic event sequences, include the following:

- Radiological hazards (mainly direct exposure) during surface handling (e.g., lifts) that are judged to be more sensitive to seismic ground motion than downhole hazards (Table 12-1), but because of shorter duration can be designed to accommodate lesser seismic events (smaller recurrence DBGM-2A). Recovery is likely to be simpler for event sequences that involve surface handling, especially if radiological releases do not occur.
- Hazards at the wellhead and downhole (direct exposure, and potential releases downhole) that may not present immediate radiological risk to workers or the public, but which may involve stronger ground motion because of exposure duration (DBGM-2B). Damage from these hazards must be limited because of the potentially high cost and greater risk associated with recovery, especially if a waste package is breached in the borehole.
- Hazards to supporting equipment that must function nearly continuously during handling and emplacement operations, and therefore require consideration of extreme ground motion (DBGM-2C). SSCs that can perform their functions during and after a seismic event at the Category 1 probability level (DBGM-1) may not be functional after a Category 2 event, but they should be designed for safe shutdown, and to not interfere with other SSCs in the process.

Table 12-3. Duration of exposure to ground motion, for supporting equipment.

Supporting Structures, Systems, and Components	Activity Sequences Supported (Hazard Categories)	Est. Sequence Durations & SSC Total (hr)	Conditional Seismic Event Prob. (yr^{-1})	Recurrence Interval (yr)
Mobile Crane	**(Lift)**			
	Transport. Cask Prep. and Move	2.75	1.1E-05	9.4E+04
	Transfer Cask Move to Wellhead	1.75	1.7E-05	6.0E+04
	Mechanical Bridge Plug Setting	4	7.3E-06	1.4E+05
	Mobile Crane Total	8.5	3.44E-06	2.9E+05
Headframe Structure	**(Lift, Wellhead, and Wireline)**			
	Transfer Cask Move to Wellhead	1.75	1.7E-05	6.0E+04
	Wellhead Configuration	3.25	9.0E-06	1.1E+05
	WP Emplacement (and retrieval) by Wireline	5.75	5.1E-06	2.0E+05
	Headframe Total	10.75	2.7E-06	3.7E+05
Wireline System	**(Wellhead and Wireline)**			
	Borehole Qualification	4.25	6.9E-06	1.5E+05
	Wellhead Configuration	3.25	9.0E-06	1.1E+05
	WP Emplacement (and retrieval) by Wireline	5.75	5.1E-06	2.0E+05
	Wireline Total	13.25	2.2E-06	4.5E+05
Power Supply	**(Lift, Cask Cradle Roll, Shield Plug Handling, Interface Shield Slide Action, Latch Action/Package Movement, Wellhead, Wireline, and Borehole Events)**			
	Transport. Cask Prep. and Move	2.75	1.1E-05	9.4E+04
	Cask-to-Cask Transfer	2	1.5E-05	6.9E+04
	Transfer Cask Move to Wellhead	1.75	1.7E-05	6.0E+04
	Wellhead Configuration	3.25	9.0E-06	1.1E+05
	WP Emplacement (and retrieval) by Wireline	5.75	5.1E-06	2.0E+05
	Power Supply Total	15.5	2.0E-06	5.0E+05
Control/Functional Safety System	**(Lift, Cradle Roll, Shield Plug Handling, Interface Shield Slide, Latch Action, Wellhead, Wireline, and Borehole Events)**			
	Transport. Cask Prep. and Move	2.75	1.1E-05	9.4E+04
	Cask-to-Cask Transfer	2	1.5E-05	6.9E+04
	Transfer Cask Move to Wellhead	1.75	1.7E-05	6.0E+04
	Wellhead Configuration	3.25	9.0E-06	1.1E+05
	WP Emplacement (and retrieval) by Wireline	5.75	5.1E-06	2.0E+05
	Control/Functional Safety System Total	**15.5**	**2.0E-06**	**5.0E+05**

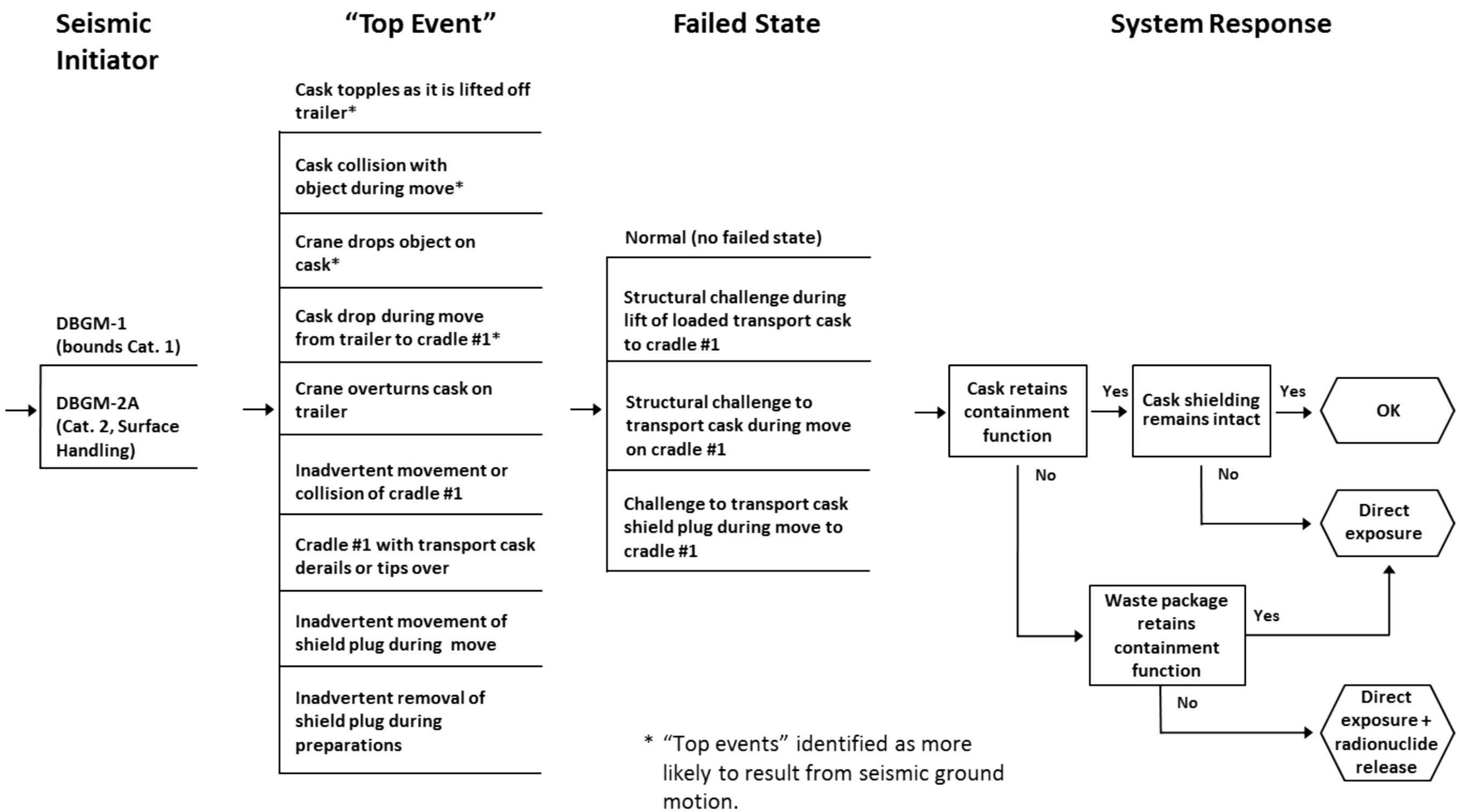


Figure 12-1. Example seismic event sequence diagram for activity sequence: Transportation cask prepare and move (all hazard categories).

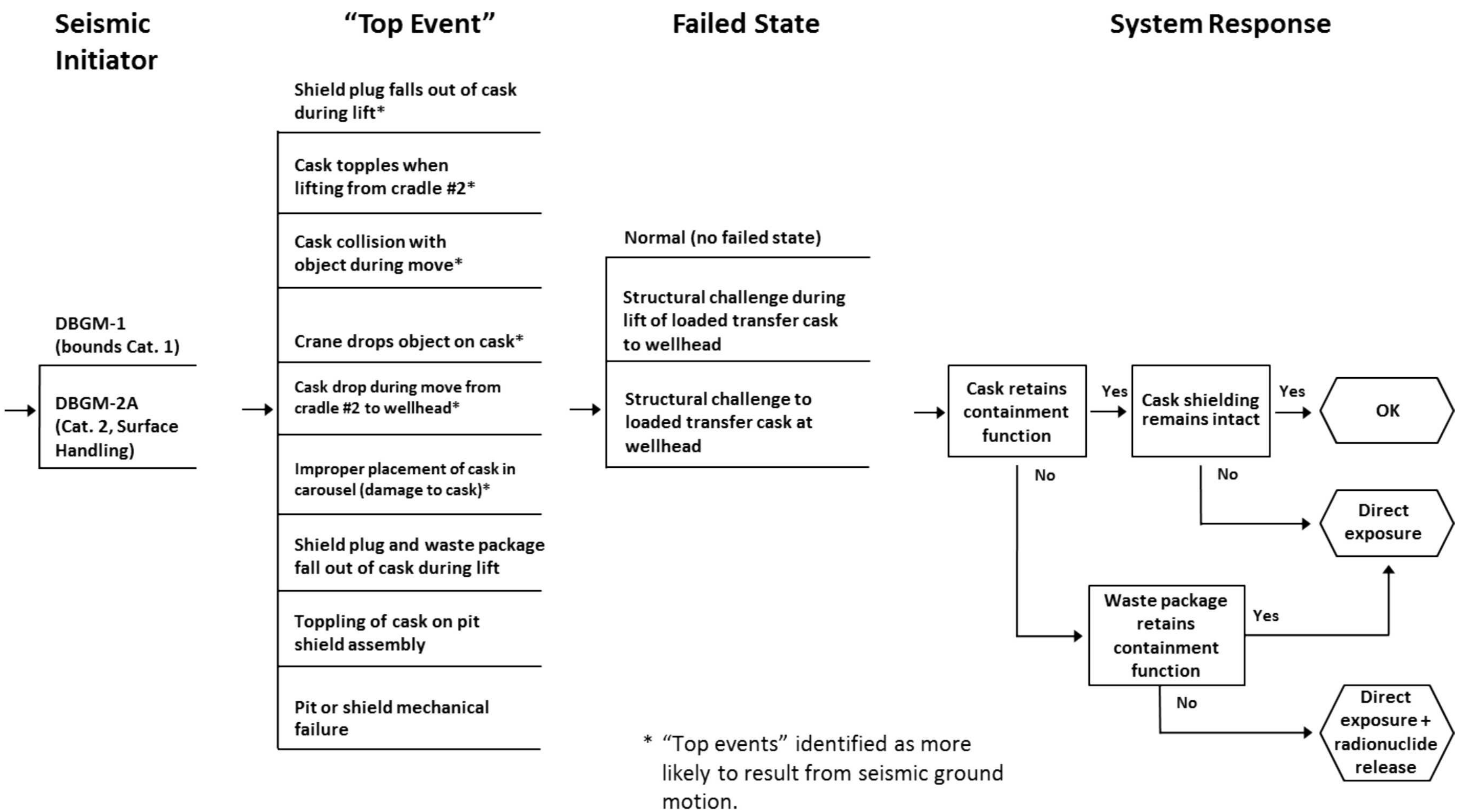


Figure 12-2. Seismic event sequence diagram for activity sequence: Move transfer cask to wellhead (all hazard categories).

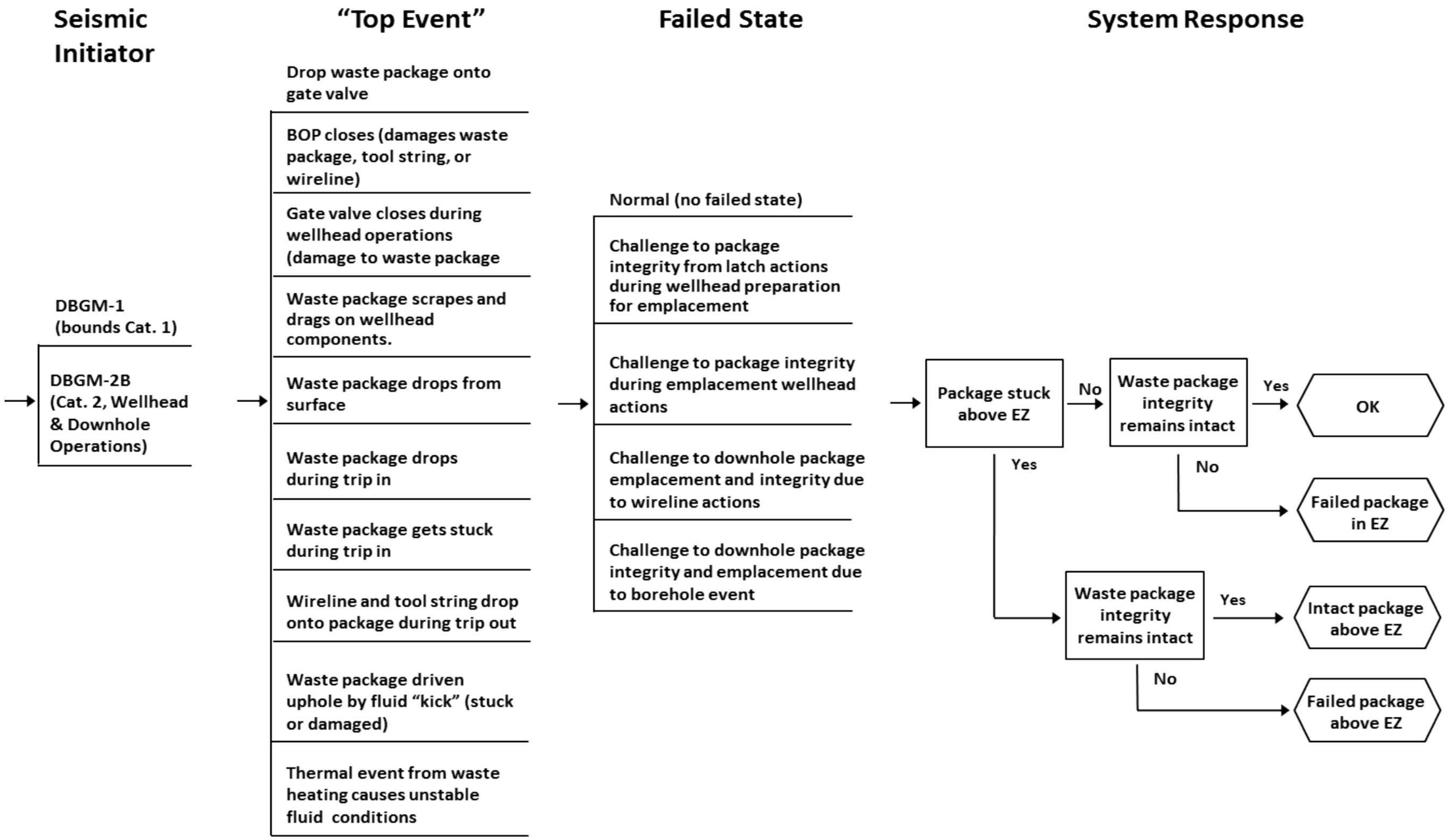


Figure 12-3. Example seismic event sequence diagram for activity sequence: Waste package emplacement and retrieval by wireline (all hazard categories).

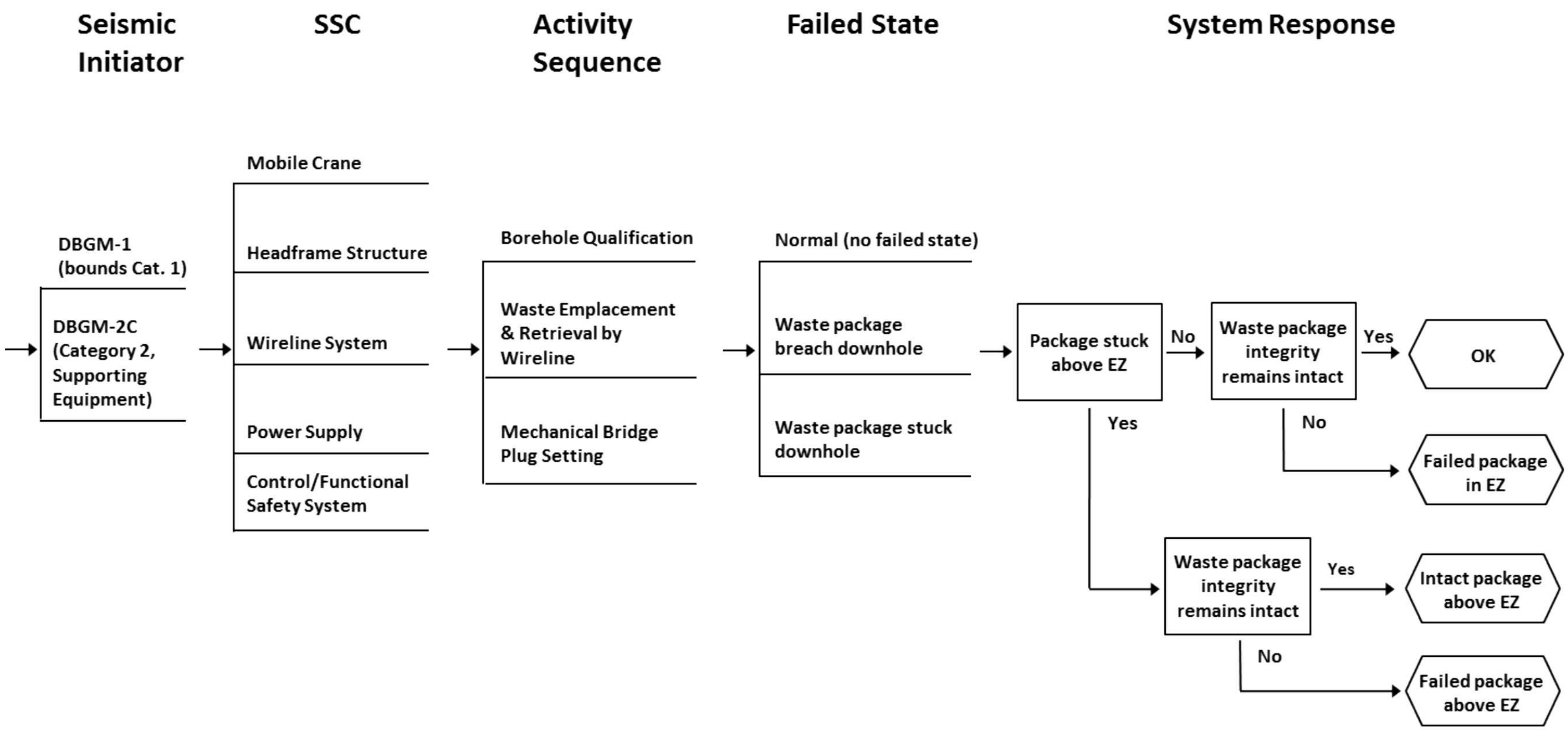


Figure 12-4. Example summary seismic event sequence diagram for supporting equipment (wireline and borehole event hazard categories)

13 DESIGN INSIGHTS

The process of identifying hazards and initiating events points toward design features that can help reduce the probability of initiating events. The following design insights will significantly improve DBD system safety:

Lift design insights – A headframe with a gantry crane places physical limits on the range of lift errors that are possible, compared to the use of a mobile or fixed point crane with a wide range of motion. The gantry crane may also be programmed to carry out specific lifts, limiting opportunities for operator error. Several stations would be arranged in line, under the gantry: cask-to-cask package transfer, washdown, and wellhead stations. A mobile crane would be used to move the transportation cask from the truck to cradle #1.

Because of the protruding flange on the transfer cask, risk of damage to a package in the event of a cask drop is likely greater for the transfer cask than for the transportation cask. The use of a gantry crane incorporated into an extended headframe structure limits helps to control possible movements, provides a more stable lift structure, and thus helps reduce risk during this operation.

Cranes should be selected with adequate lift capacity past the range of motions expected. Cranes should be designed so load movement stops on loss of power (for example, brake engagement as a response to power loss).

Cranes and hoist should include feature such as anti-two-blocking and limit switches to minimize the potential for hoist failures or excessive runout. All lift devices and rigging should be load tested on a regular approved schedule, using approved test procedures.

Cranes should incorporate load limiting devices that stop the lift at pre-set loads (e.g. at 110% of intended lift load).

All cranes should incorporate features that stop and hold the load in the event of a power (electrical or other motor) failure.

Lifts should be sufficient to reliably clear obstacles and prevent collisions, but no higher than necessary. This limits the damage that could occur as result of a drop event.

Lifts of heavy items above the cask or waste package should be avoided when practical. Design of work platforms should consider the potential for platforms or items on the platforms falling on the cask. In many cases, work platforms envisioned in this design should be reasonably lightweight or should be securely attached to the headframe assembly.

Mobile crane fuel is a potential source of fire. Safe fuel storage and collection of potential fuel leaks should be considered in the site plan.

As the design of the transfer cask progresses, the potential vulnerability of the protruding tube and flange that mates with the wellhead flange should be recognized. While maintaining clearance for the flange connection, including the remote flange clamp mechanism, cask features should minimize the potential for damage to the waste package in a vertical drop of the transfer cask onto a hard surface such as the wellhead shield plate.

Cask cradle roll design insights – A cask cradle rail system based on an integrated seismically-designed support system ensures cask alignment and minimizes the risk of counter-movements of casks in a seismic event (with potential to apply a shear force on a waste package).

Motor-driven cradle roll systems offer the potential for limiting cradle speed, and improve the interface with interlock and overall control systems. Limit switches and interlock systems can prevent travel beyond the intended range.

Once in place, cradles should be secured so they cannot move to an improper position. This is especially true when cradles are in place against the interface shield; it is also true when casks are being lifted from or lowered into a cradle. Wheel chocks, rail pins, or other constraint systems may be integrated into the interlock system.

Cradles should be tied down so they cannot topple off the rails, and casks should be tied down so they cannot be toppled off the cradle. Features may be incorporated into the cradle-rail interface, or entire cask and cradle unit tie downs may connect to a common foundation system.

Shield plug design insights – Use different fasteners for staggered shield attachments. This can help preclude accidents such as removing the entire shield plug if only the central insert was to be removed. If the two components require different tools (for example, one using hex head bolts and the other mounted with Torx screws) inadvertent disconnection of the wrong component would be more difficult.

Shield plug sequences present the opportunity for unintended shield configurations that directly lead to worker exposures. A formal radiological control program, combined with verification steps after each shield configuration change step, will be required to continually assess dose profiles. Installation of continuous radiation detectors and alarms in all work areas provide backup to surveys by radiation control technicians.

Use jigs and tools so that shield plug movements can be performed without workers at the end of the shield plug or near the side, where dose exposure rates may be highest. Jigs and tools, coupled with proper lift devices, will also ensure occupational safety and aid in maintaining control of personnel location.

Interface shield assembly design insights – The design should include an interlock system that prevents movement of casks or the shield slide under conditions that could create excessive dose exposure rates.

The interface shield assembly should be designed to preclude moving a shield plug all the way out of the shield slide, consistent with operational, recovery and maintenance requirements.

A controlled motorized drive should be used for the shield slide. The design should minimize the drive force available to the slide so inadvertent movement while the package passes through the slide cannot cause damage to the package, while ensuring sufficient force that slide movements are freely accomplished.

A manual slide movement over-ride may be necessary to address the possibility of a slide motor failure, but provide adequate lockouts are needed to ensure it is not used other than for approved recovery operations.

Latch action or package movement design insights – Hazards associated with horizontal and vertical movements are different. For a horizontal movement, friction and snagging pose the possibility that a pull operation places excessive load on the package, but a drop is not credible. For vertical movements, package drop or angular cocking would be a more serious concern; loads would be incurred when trying to pull the package back up from an undesired state.

The design should always have two package capture features in use at any time. These include the package top latch (the horizontal pull latch), the side latches, and the remote disconnect on the wireline tool string. Exceptions are when the package is in a horizontal configuration during the cask-to-cask transfer, and when it is being lowered into the borehole on the wireline.

Electric release current for the tool string release operation should be locked out until it reaches intended depth in the borehole.

Consider design features that do not allow unlatching while the latch is under load. Evaluations should ensure this does not prevent necessary response actions.

Consider implementation of interlocks to prevent inadvertent release of one system unless a second system is fully engaged.

Consider methods to periodically survey component alignment to ensure that packages cannot be caught on ledges formed between components. If appropriate, consider use of a sleeve to ensure the package has a smooth surface during the pull through the interface shield assembly (this might also help mitigate against damage from inadvertent movement of the shield slide while the package is passing through).

Consider a latch design in which the latch separates from the package at a force sufficiently above the force needed for the transfer, but not high enough to cause damage to a snagged package.

Wellhead system design insights – Wellhead components are located in a pit, with borehole and annulus fluid connections and likely valves located inside the pit. There is a possibility of pit flooding if these systems fail. As practical, wellhead components located in the pit should be designed so they can perform safety functions, and if possible normal operating functions, when immersed in water or brine.

The wellhead pit and headframe structures should be designed in common to ensure loads properly transfer from the headframe to the pit shield.

The transfer cask must withstand Category 1 ground motion without loss of function, when mounted on the wellhead carousel platform.

Fluid control valves must close when the BOP is actuated.

The functional safety system may be designed to respond to pressure "kicks," such as stopping wireline action and initiating BOP action in response to excess fluid flow at the surface or a load change downhole.

Provide an interlock to prevent gate valve closure on the waste package and wireline. Limit force on the gate valve actuator so inadvertent closure cannot damage a waste package or the wireline.

Design the kneeling jack system such that no failure can result in the transfer cask tipping near the point where the center of gravity shifts off the base. An example would be to limit the stroke of individual hydraulic jacks.

Wellhead completion is contingent on the physical behavior of a specific borehole, and with regulatory requirements in effect at the borehole site.

If practical, design the wireline tool string weak point so that it does not have sufficient force to topple the transfer cask should the wireline be taught or snagged while the cask moves on the carousel.

Wireline system design insights – Wireline systems should be designed for reliability in the event of a loss of electrical power, or in the event a fire or other event causes damage to the wireline winch and control system. Descent of the waste package requires several hours; responses to events must consider safe and stable hold points during trip in. Concerns such as heating of borehole fluid, resulting in fluid instabilities, must be addressed recognizing it may not always be practical to continue lowering (or raising) the waste package.

The use of a fixed headframe instead of a mobile crane to hold wireline sheaves for emplacement provides better reliability.

The wireline should be specified as having no splices.

Wireline sheaves should have cable capture locks to prevent jump-off.

The design should specify a hydraulic cable-tension limiter on the wireline winch, set below the downhole tool passive weak point setting, for surface operations.

The wireline winch drive, winch brakes, and hydraulic tension limiter should be integrated with the safety control (interlock) system.

The downhole weight tool output should be integrated into the safety control (interlock) system.

Use a very slow speed on trip in (maximum of 0.5 ft/sec) to avoid cable hang-up and breakage, especially at less than 1 km depth. At depths below 1 km, allow speed to increase to 2 ft/sec.

If wireline waste packages emplaced by wireline become stuck, release the wireline and mobilize a drill rig. Don't strip the wireline within pipe because the risk from losing control is greater than that from the package dropping.

Consider including both a weak point and a remotely actuated release at the cable head (in addition to the remotely operated package release).

Consider designing both the waste package remotely operated release mechanism and the remote cable head release so they are only operable without load. This ensures the waste package (or tool string) must either be on the bottom or be stuck.

Consider specifying double-redundant winch hydraulic drive and pneumatic brakes.

Specify wireline inspection standards as appropriate for the reliability expected for nuclear material operations (in addition to, or in lieu of wireline contractor standard procedures).

Incorporate a hydraulic shock absorber into the cable head to limit dynamic loads on the trip in.

Borehole construction and operation insights – Establish perforation plans for emplacement zone completion casing and guidance tie-back casing, consistent with multiple objectives including free drop terminal velocity and securing cement plugs against bedrock.

Select emplacement fluid properties and composition consistent with disposal zone completion requirements and terminal sinking velocity for the event of a dropped package.

Design waste packages for the range of temperatures that could be encountered with heat-generating waste throughout the borehole.

Design impact limiters to achieve needed performance, without contributing to the likelihood of packages getting stuck on trips in (e.g., not snagging) or after impact, on retrieval (e.g., by use of a weak point).

Include a mud check valve on the guidance casing above 3 km, to permit reverse circulation in case a package or string of packages gets stuck (with a workover rig brought onto the site for fishing).

Before every package or string of packages is emplaced, run a tool string consisting of a junk basket and gauge ring, and possibly including an acoustic caliper (for casing collapse and wear, and mud sludge buildup), a shielded gamma ray detector (detect radioactivity in fluid that would indicate a failed package), a fluid sampler (more sensitive than gamma ray detection near waste packages), and a casing collar locator (as needed).

Run a gauge ring with junk basket before bridge plug installation, and after every cement job (if not as part of the tool string run prior to each package emplacement).

The gauge ring/junk basket may be designed to limit terminal velocity, and could incorporate an impact limiter to avoid damage to emplaced waste packages in the event of a drop.

Set mechanical drillable bridge plugs with pressure on coiled tubing, in lieu of wireline bridge plugs that typically use an explosive charge.

Consider circulating borehole fluid to clean the hole, after installing a cement plug and before emplacing the next stack of packages.

Surface fluid handling equipment, including storage tanks, should be adequate to contain and isolate contaminated fluid that is produced prior to detecting a breached waste package and shutting in the borehole pending recovery operations.

Support system design insights – Many systems will require electrical power. Equipment should be designed so that loss of electrical power results in a safe state. For example, hoists and drive motors should be designed so that brakes engage upon loss of power and motions halt rather than continue under potentially degraded conditions. In some cases alternative manual actuation may be implemented after appropriate review (with physical controls, such as interlocks or lock-outs to prevent casual use) to carry an operation through to a more stable state.

Hydraulic pumps and grease supply for the injector section are likely to be electrically powered. Interlocks should be used to suspend operations on loss of hydraulic fluid pressure, or alternative power sources should be available to allow critical functions (such as BOP actuation capability) to remain available.

Control, interlock and alarm systems are generally electrically-powered. An uninterruptable power system should be considered for interlocks and alarms so protective functions are not lost upon loss of normal electrical power. Loss of the control system should result in stable shutdown of operations.

Incorporating power supply and interlock connections in the same cable and connection system ensures that a device cannot be powered without also enabling the interlock system.

Alarms should monitor and detect radiation, dispersed radioactive material, internal fire, and explosion hazards.

A fire detection, alarm and suppression system with loss-of-power capability is needed to mitigate internal fire hazards. Use of foam suppressant should be considered to immobilize hazardous material.

External events – Seismic design considerations are likely to apply to the headframe, gantry crane, and wireline upper sheave as an integrated system.

Seismic design considerations are likely to apply to the interface shield, cask cradles, and supporting rails as an integrated system.

Seismic design considerations are likely to apply to the wellhead pit as a structural element, through support of the transfer cask, to ensure adequate integrity of the stack of components from wellhead support and guidance casing tieback through the wireline components at the top of the transfer cask.

Activity sequences should be designed so that hold points between sequences are stable and minimize risk from external events.

External events that cause loss of electrical power should be considered. External events contribute to the discussion of electric power reliability, equipment design features, and interlock and alarm systems presented in the support systems category.

External events from flooding, fires, wind, and similar events may be site specific and are difficult to evaluate at this time.

General observations – An integrated functional safety system is needed to prevent or mitigate a range of potential initiating events, especially those caused by human error.

Category 1 events should not have radiological consequences significantly greater than normal operations, nor should they cause the system to generate additional radioactive waste.

An integrated functional safety system is needed to prevent or mitigate a range of potential initiating events, especially those caused by human error.

Appropriate quality requirements and checkout (beginning with the DBFT engineering demonstration activities and carried through demonstrations of field equipment with mockup packages) will identify issues in advance

This analysis focuses on events with potential radiological impact. Other occupational and industrial risks are posed, and design activities should consider other aspects of worker safety as well.

This analysis focuses on events that serve as initiating events. Other sequences performed to prepare equipment may contribute to the events identified in this analysis. This is especially true for the four segments of Activity Sequence 8, described in Table 6-8 through Table 6-11.

Design of borehole and annulus fluid management equipment, especially shut in capability, is important to safe downhole operations. Fluid control valves must close with remote actuation, concurrent with BOP closure. Fluid recovery and surge management must be designed for control of potential radiological contamination. Cleanup of contaminated fluids should be considered in the design.

The site should be designed to control contamination from a breached package at the surface and from contaminated borehole fluid that results if a package is breached downhole. Liners and other features should be used so drainage collected from operating areas, especially equipment reconditioning areas, can be collected, monitored, and treated as necessary before release.

Items Important to Safety – Each of the activity sequences considered in this assessment:

- Borehole qualification (Section 6.1)
- Transportation Cask Preparation and Move to Transfer Station (Section 6.3)
- Transfer Station Operations and Cask-to-Cask Transfer (Section 6.4)
- Transfer Cask Move to Wellhead Station (Section 6.5)
- Transfer Cask, Waste Package, Wellhead and Wireline Configuration (Section 6.6)
- Borehole Emplacement, Release, and Wireline Retrieval (Section 6.7)
- Equipment Condition for Next Use (Section 6.8)
- Setting an Interval Plug (Section 6.9)

includes major components that could be important to safety (ITS) in a regulatory risk assessment. In particular the borehole pad, cranes and hoists, equipment and fixtures at the cask-cask transfer and wellhead stations, and wireline equipment (tools, cable, hoist) would be important to safety in addition to the waste package. Also, the supporting equipment (Table 12-3) and aspects of site preparation and monitoring (Section 4) could be ITS.

14 SUMMARY

A probabilistic assessment of radiological safety has been developed that includes waste receipt, handling, transfer, emplacement in a borehole, and borehole completion. The assessment seeks to improve the conceptual design for DBD by identifying design criteria and requirements, and improved design solutions such as:

- Some off-normal events and outcomes could be avoided through the development of a single, double-ended, multi-purpose cask to be used both for waste package transportation to the site, and emplacement in the borehole.
- Safer lifts could be achieved using in-line arrangement of transfer, washdown, and wellhead stations, and using a fixed headframe for all lifts between these stations (a crane would be used to move the transportation cask from the truck to cradle #1).
- Anti-two-blocking and other crane safety features should be included for the mobile crane and fixed hoist used to lift casks and other heavy items.
- Alarms are needed for radiation, dispersed radioactive material, internal fire, and explosion hazard conditions.
- An integrated functional safety system is needed to prevent or mitigate a range of potential initiating events, especially those caused by human error.
- A fire suppression system with loss-of-power capability and foam to immobilize hazardous materials, is needed to mitigate internal fire hazards.
- The transfer cask must withstand Category 1 ground motion when mounted on the wellhead carousel platform.
- Category 1 events should not have radiological consequences significantly greater than normal operations, nor should they cause the system to generate additional radioactive waste.

The assessment is generic (non-site specific), and based on a previously developed conceptual design (SNL 2016). It serves to risk-inform design for borehole disposal of nuclear wastes in deep, crystalline, continental basement rock.

Disposal operations were modeled as a series of activity sequences populated by discrete steps, which were converted to linked event trees representing the entire disposal process end-to-end. Seven major risk categories were identified involving lifts, transfers, etc., and correlated with activity steps. Types of equipment to be used in each activity sequence were identified. The model was then reviewed to identify potential initiating events by risk category. Certain events were selected as “top events” for quantification by fault trees, and other events were designated “basic” or “pivotal” and included in fault trees or event trees. In all, seven event trees and 43 fault trees were developed for those activities directly involving nuclear waste.

Off-normal end states for the end-to-end disposal process were categorized according to the potential severity of worker exposure and the potential for radioactive material release. The frequencies of consequence categories were compared to Category 1 and 2 requirements from 10 CFR 63. Further definition of these end states (e.g., dose estimates) were deferred to a time when more definitive siting and design information is available.

The results confirm that limiting off-normal events is challenging for any process involving many repeated operations, such as could be needed for handling thousands waste packages in a disposal campaign with many boreholes. As expected, the conceptual design ensures that the calculated frequency of off-normal events is inversely related to the potential severity of consequences. Mishaps involving substantial loss of shielding or radionuclide release at the surface, are estimated to be beyond Category 2 in the aggregate (< 10^{-6} probability per repository).

Downhole mishaps resulting in release of radioactive material into the borehole fluid could be more likely (Category 2, ~10^{-3} per repository) driven by the likelihood that a package becomes stuck during emplacement and breached by fishing operations. For a smaller disposal campaign (e.g., 400 waste packages in a single borehole) off-normal events would be much more rare.

External events were also considered and seismic ground motion was selected for comparison to the Category 1 and 2 criteria. Using estimates for exposure duration associated with activity sequence steps, a design basis event (2,500-yr recurrence) was identified without a need for site-specific hazard information. Additional ground motion levels were identified as seismic design criteria for specific equipment and subsystems.

In summary, the probabilistic assessment of radiological safety for DBD operations shows that design emphasis is needed for cask design, functional safety, wellhead equipment, and improved understanding of downhole risks. The probability of a serious mishap involving loss of shielding or radioactive material release at the surface is very small. Seismic design could be important unless the DBD campaign is sited in a seismically quiescent area.

This research was performed as part of the DBFT. Based on revised DOE priorities in mid-2017, the DBFT and other research related to a DBD option was discontinued; ongoing work and documentation were closed out by the end of fiscal year FY 2017. This report was initiated as part of the DBFT and documented as an incomplete draft at the end of FY 2017. The report was finalized by Sandia National Laboratories in FY2018 without DOE funding, subsequent to the termination of the DBFT, and published in FY2019. Further DBFT work, for example, implementation of an engineering demonstration (SNL 2016), would require resumption of DBD research and development at some future time.

15 REFERENCES

Arnold, B.W., P.V. Brady, S.J. Bauer, C. Herrick, S. Pye and J. Finger 2011. *Reference Design and Operations for Deep Borehole Disposal of High-Level Radioactive Waste*. SAND2011-6749. Albuquerque, NM: Sandia National Laboratories.

ASCE (American Society of Civil Engineers, Structural Engineering Institute) 2005. *Minimum Design Loads for Buildings and Other Structures*. ASCE/SEI 7-05, Reston, VA, 2005.

BSC (Bechtel-SAIC Co.) 2008a. *Receipt Facility Event Sequence Development Analysis*. 200-PSA-RF00-00100-000-00A. February, 2008. U.S. Department of Energy, Office of Civilian Radioactive Waste Management.

BSC (Bechtel-SAIC Co.) 2008b. *Receipt Facility Reliability and Event Sequence Categorization Analysis*. 200-PSA-RF00-00200-000-00A. February, 2008. U.S. Department of Energy, Office of Civilian Radioactive Waste Management.

DOE (U.S. Department of Energy) 2008. *Yucca Mountain Repository License Application Rev. 0*. ML081560400. Las Vegas, Nevada: U.S. Department of Energy, Office of Civilian Radioactive Waste Management.

FEMA (Federal Emergency Management Agency) 2007. *Design Guide for Improving Critical Facility Safety From Flooding and High Winds: Providing Protection to People and Buildings*. FEMA 543, Chapter 3. Washington, DC, January, 2007.

Freeze, G.A., E. Stein, L. Price, R. MacKinnon and J. Tillman 2016. *Deep Borehole Disposal Safety Analysis*. FCRD-UFD-1026-000075 Rev. 0. U.S. Department of Energy, Office of Used Nuclear Fuel Disposition.

Gertman, D.I., H.S. Blackman, J.L. Marble, J.C. Byers and C.L. Smith 2005. *The SPAR-H Human Reliability Analysis Method*. NUREG/CR-6883. U.S. Nuclear Regulatory Commission. Idaho Falls, ID.

Hardin, E.H, J. Su and F. J. Peretz 2017, *Methodology for Radiological Risk Assessment of Deep Borehole Disposal Operations*. SFWD-SFWST-2017-000105, Rev 1. U.S. Department of Energy, Office of Spent Fuel and Waste Disposition.

Ma, C.W., R.C. Sit, S.J. Zavoshy and L.J. Jardine 1992. *Preclosure Radiological Safety Analysis for Accident Conditions of the Potential Yucca Mountain Repository: Underground Facilities.* SAND88-7061. Sandia National Laboratories, Albuquerque, NM.

Milstein, R.I. 2001. *Integrated Safety Analysis Guidance Document.* NUREG-1513. Division of Fuel Cycle Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC.

NAC International 2008. *NAC-LWT Legal Weight Truck Cask System – Safety Analysis Report*. Docket No. 71-9225. Revision 39. (https://www.nrc.gov/docs/ML1102/ML110260315.pdf)

NRC (U.S. Nuclear Regulatory Commission) 2015. *Safety Evaluation Report Related to Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada, Volume 2: Repository Safety Before Permanent Closure*. NUREG-1949 Volume 2. Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC.

Peretz, F. and E. Hardin 2017. *Safety and Reliability of Deep Borehole Waste Disposal Surface Activities*. SFWD-SFWST-2017-000010. U.S. Department of Energy, Office of Spent Fuel and Waste Science & Technology. May 26, 2017.

Smith, C., J. Knudsen, T. Wood and K. Kvarfordt 2012. SAPHIRE 8. Computer software. Version 1.0. Idaho National Laboratory and the U.S. Nuclear Regulatory Commission.

SNL (Sandia National Laboratories) 2016. *Deep Borehole Field Test Conceptual Design Report*. FCRD-UFD-2016-000070 Rev. 1. U.S. Department of Energy, Office of Used Nuclear Fuel Disposition.

Sprung, J.L., D.J. Ammerman, N.L. Breivik, R.J. Dukart, F.L. Kanipe, J.A. Koski, G.S. Mills, K.S. Neuhauser, H.D. Radloff, R.F. Weiner and H.R. Yoshimura 2000. *Reexamination of Spent Fuel Shipment Risk Estimates: Main Report*. NUREG/CR-6672, Vol. 1. Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, Washington, DC. March, 2000.

Vesely, W.E., F.F. Goldberg, N.H. Roberts and D.F. Haasl 1981. *Fault Tree Handbook*. NUREG-0492. Systems and Reliability Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC.

Appendix A – Cask-Drop Fragility Analysis

A.1 Background

Waste packages will be received at a DBD site within a truck-mounted transportation cask such as the LWT® cask (NAC International 2008). During the emplacement process the cask will be lifted into a vertical orientation, up to 3 m off the ground to clear the truck mounted cradle. A drop from this height would impart additional loads on the waste package. This appendix reports analysis of such an impact to assess the deceleration and shock loads experienced by the waste package inside the cask.

The calculations reported here do not include the impact limiters used for over-the-road transport of the LWT® cask. Rather, the drop represented here would occur after those impact limiters are removed, during cask handling at the DBD site. The impact limiter installed on the lower end of the waste package would still be present. As described previously (SNL 2016) the intended function of this limiter is to mitigate the impact of dropping a WP in the borehole. For a 3-m drop in air at the surface such a limiter would absorb some (but not nearly all) of the energy of the drop, as discussed below. The internal limiter concept could be modified so that it mitigates both the borehole and vertical surface drops, but this was not attempted for the calculations reported here.

The similarity of size, shielding, and end plug design, between the LWT® cask and the transfer cask, means that the drop calculations described here could be applied to the transfer cask as well. The highest lift for the transfer cask is likely to be less than 3 m because the transfer station and the wellhead station would be constructed at grade level.

An end drop is selected for analysis because most of the cask movements described for DBD operations would be done in vertical orientation. Oblique drops are also possible, as are drops of a few feet onto a steel cradle with potential for cask penetration. These cases may be undertaken in future studies.

A.2 Model Setup

The NAC LWT® cask is modeled as a 316 stainless steel cylinder (neglecting the metallic lead layer). Nominal exterior dimensions for the cask are 0.73 m (28.8 in) x 5 m (200 in). The internal cavity is 0.36 m (14.0 in) x 4.4 m (173 in) and houses the waste package. A stainless steel lid seals the internal volume. As modeled, the mass of the NAC-LWT cask is approximately 13,600kg.

The waste package used in the model is the reference waste package design (SNL 2016, Section 3) with a nominal outer diameter of 0.27 m (10.75in) and wall thickness of 0.025 m (1.00 in). The waste package is constructed from P110 casing or tubing material (yield strength 110 ksi). Aluminum centralizers secure the waste package radially within the cask. The centralizers allow some axial movement between the cask and the waste package while keeping the waste package radially centered. The waste package has an impact limiter attached as shown in Figure A-1.

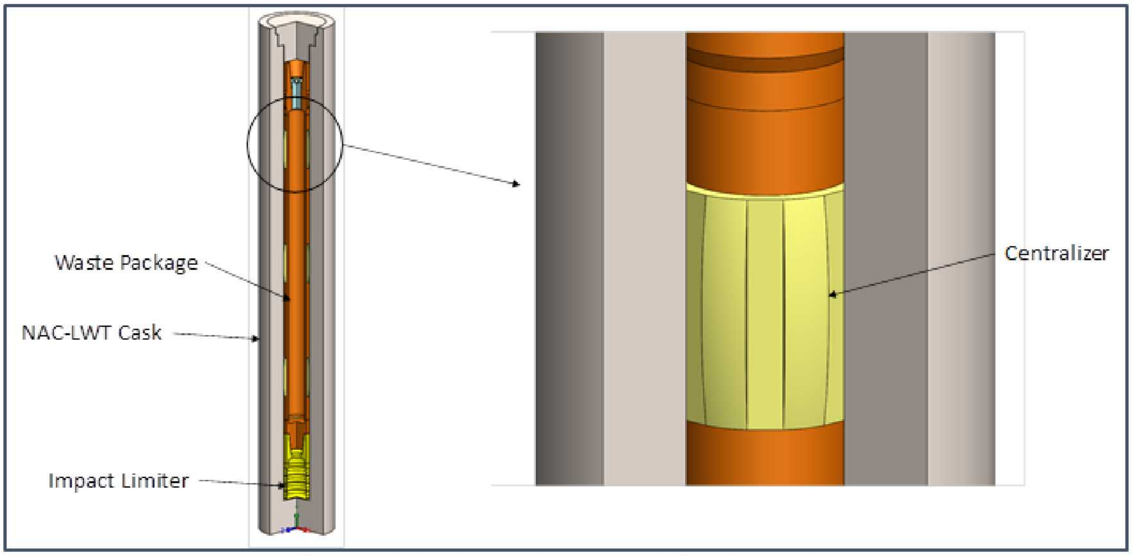


Figure A-1. Cask-drop model schematic.

The impact surface is assumed to be compacted gravel with a thickness of 0.6 m (24 in). The "stiffness" of the compacted gravel is given by the modulus of subgrade reaction (K_s) which has a wide range of values depending on the material and the condition of the surface. Stiffness values range from 300 to 450 psi/in. A nominal value of 350 psi/in was chosen for these simulations.

SolidWorks Simulation® software was used for free-body dynamic simulation. For drop test simulations, the program calculates impact and gravity loads on a rigid or flexible planar surface, with no other loads or restraints allowed. It uses an explicit time integration method, and automatically adjusts the critical time step based on the smallest element size and stability and accuracy criteria. Simulations were conducted out to 50 msec. The drop height was specified as 3m from the lowest point on the assembly which is the bottom face of the cask. The impact is assumed to be normal to the impact surface and gravity.

A.3 Results of Cask-Drop Simulation

A simulated sensor was placed on the lower interior face of the waste package to track the model results over the duration of the simulation. The sensor location is highlighted in blue as shown in Figure A-2. The speed and von Mises stress over that period are plotted as well.

The results show that the maximum stress of approximately 4,200 psi occurs around 14 msec into the impact. The stresses decrease steadily after that. This delay in the maximum stress indicates that the waste package is gradually decelerating, due in part to the compliance of the impact limiter. The stresses on the sensor face remain relatively low compared to the yield strength of the material (even modified for elevated temperature).

The stress at other locations in the assembly are also captured in the simulation. A stress plot of the entire assembly at 14 msec is shown in Figure A-3. The entire cross-section of the impact limiter has exceeded its yield strength, indicating maximum crushing and energy dissipation. Although the impact limiter is absorbing some of the energy, there are still shock loads that reverberate through the waste package. The magnitude of these short-duration stresses in the waste package body reaches nearly 20 ksi.

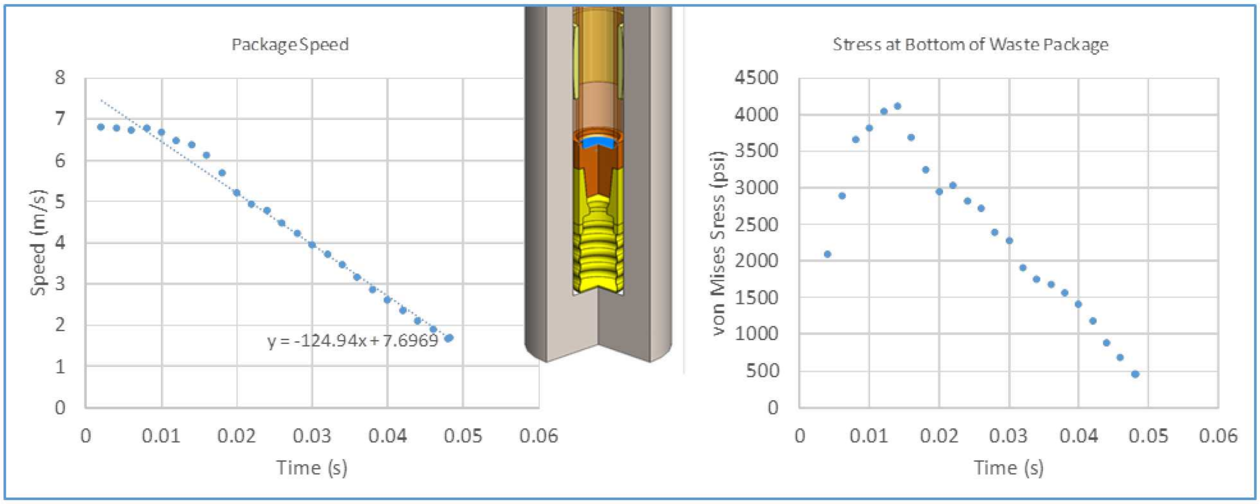


Figure A-2. Simulation results for vertical end-drop from 3 m onto compacted gravel.

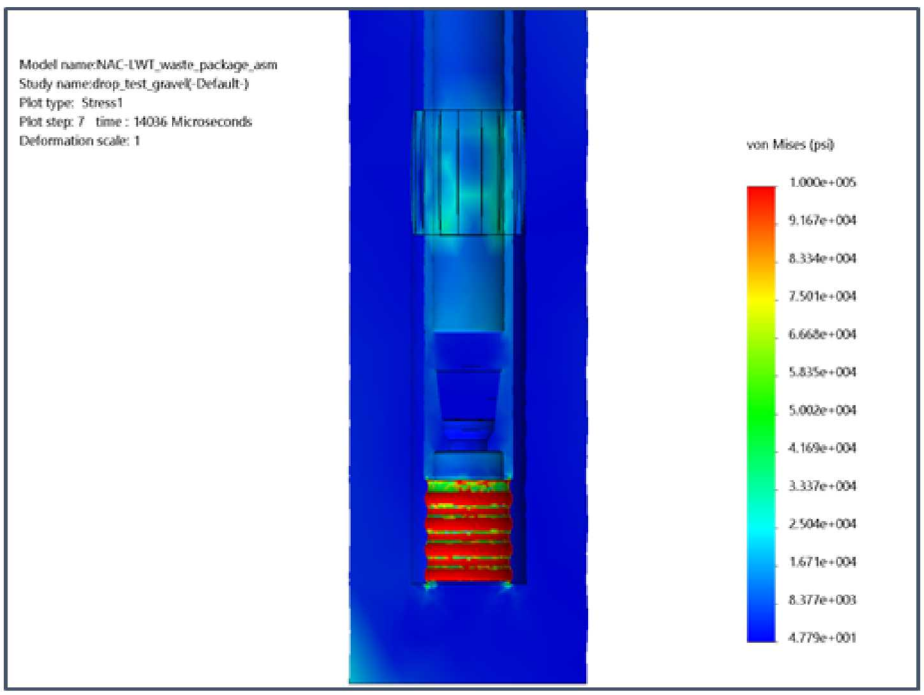


Figure A-3. Simulated stress condition (von Mises) at 14 msec for vertical end-drop from 3 m onto compacted gravel.

A.4 Analytical Solution for Cask Deceleration

Running the simulations described above to steady state (more than 50 msec) requires significant computational effort. Another approach to estimate the overall deceleration of the WP and cask is to model the assembly analytically. The impact between the cask and the ground is treated as a viscoelastic, Kelvin-Voigt impact model. Relative motion between the WP and the cask is modeled with a mass-spring-damper system. A schematic of the model is shown in Figure A-4.

The cask (m_1) and the waste package (m_2) are assumed to be connected by a spring (k_2) and a damper (b_2) (Figure A-4). The cask is connected to the impact surface with a spring (k_1) and a damper (b_1). The displacement from the neutral position for the ground surface and the WP are given by y_1 and y_2, respectively. The damping coefficients capture the energy dissipation that occurs during the impact while the spring elements represent the stiffness of the impacting surfaces.

Solving for the equations of motion for the above model results in a set of second-order ordinary differential equations (ODEs):

$$m_2\ddot{y}_2 + b_2(\dot{y}_2 - \dot{y}_1) + k_2(y_2 - y_1) = m_2 g$$

$$m_1\ddot{y}_1 + (b_1 + b_2)\dot{y}_1 + (k_1 + k_2)y_1 - k_2 y_2 - b_2\dot{y}_2 = m_1 g$$

The dot operator over a variable indicates the derivative of the variable with respect to time (or second derivative). The initial conditions are

$$y_1(0) = 0 \text{ and } y_2(0) = 0$$

$$\dot{y}_1(0) = (2gh)^{1/2} \text{ and } \dot{y}_2(0) = (2gh)^{1/2}$$

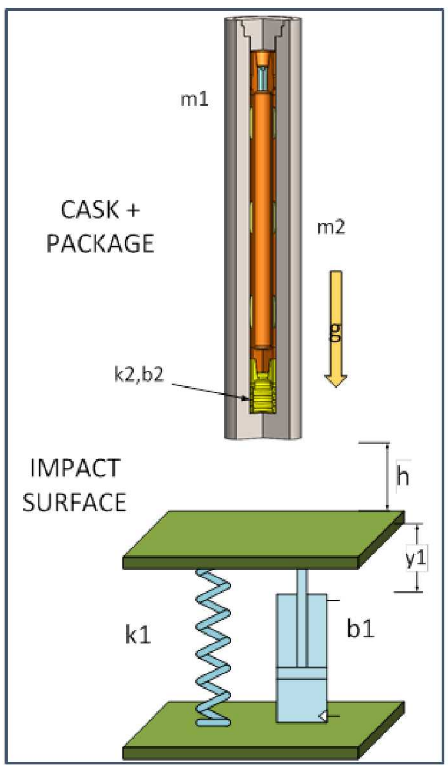


Figure A-4. Analytical model configuration.

The set of equations as solved using the ODE solver in MatLab. The span of simulation time used for analytical solution was 0 to 300 msec. The parameters and values used in the analysis are listed in Table A-1. The spring rate values are determined from the model for the impact limiter and literature for compacted gravel. The damping coefficient values were estimated in this analysis. Tests should be conducted to characterize the damping of the compacted gravel surface and the damping characteristics of the impact limiter.

Table A-1. Analytical solution model parameters and values.

Parameter	Value	Description
k_1	42.8E6 N/m²/m	Compacted gravel sub grade modulus
b_1	1E6 N-sec/m	Compacted gravel damping coefficient (estimated)
m_1	13600 kg	Mass of NAC_LWT cask
k_2	80E6 N/m	Impact limiter axial spring stiffness
b_2	1E6 N-s/m	Impact limiter damping coefficient (estimated)
m_2	1300 kg	Waste package mass
h	3 m	Drop height

Figure A-5 shows results from the analytical solution. The maximum acceleration in the cask occurs at impact and is approximately 55 g. The subsequent decay in acceleration magnitude is caused by damping in the compacted gravel surface. The maximum acceleration in the waste package occurs at approximately 10 msec after impact. This is consistent with the numerical results shown in Figure A-2 where the maximum expected stresses were predicted to occur at 14 msec.

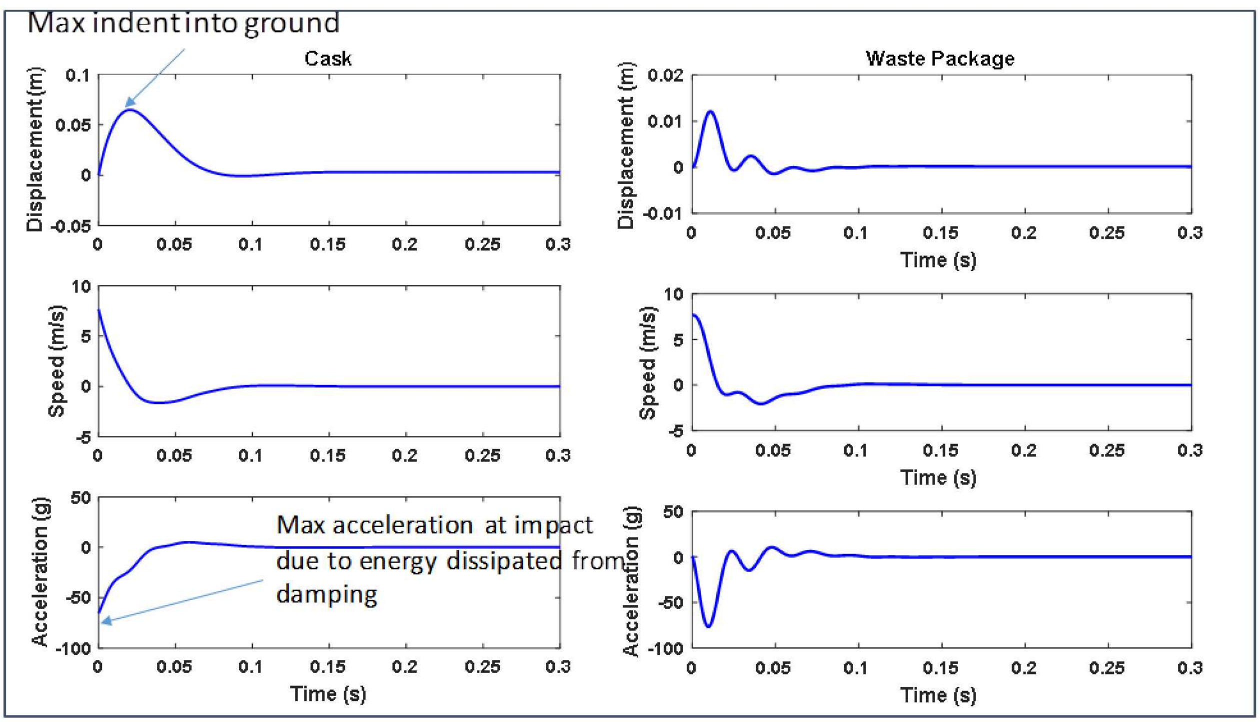


Figure A-5. Cask and waste package bulk acceleration due to impact.

Using the Kelvin-Voigt approximation it may be possible to tune the dynamic behavior of the impact based on the expected impact loading. For instance, to decrease the maximum acceleration in the WP, the impact limiter stiffness or the damping coefficient could be reduced. Although these results are in reasonable agreement with the numerical simulations, they are sensitive to the damping coefficient. Higher damping values result in larger accelerations that do not scale linearly.

Appendix B – Activity Hazard Screening Table

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
KEY												
LI	Lift											
CR	Cask cradle roll											
SP	Shield plug modification											
SS	Interface shield slide action											
LM	Latch action or package movement											
WS	Wellhead system configuration											
W	Wireline action											
V	Verify, ensure, confirm (no action)											
NS	Not selected for HAZOP (low risk)											
Sequence 1	***Borehole qualification***											
1.1	As necessary, disconnect the package placement tool string from the wireline.	Not selected	No significant potential for radiological impact									x
1.2	Assemble the qualification tool, string consisting of a gauge ring, junk basket and other tools such as a casing collar locator, onto the wireline, along with an appropriate fluid seal system.	Not selected	No significant potential for radiological impact									x
1.3	Verify that the wellhead is ready to accept the qualification tool string and fluid seal, and that the lower gate valve is closed.	Not applicable	Verification task								x	
1.4	Connect the tool string and fluid seal to the wellhead using a new gasket.	Not selected	No significant potential for radiological impact									x
1.5	Open the lower gate valve and allow the borehole fluid to achieve a steady elevation/pressure.	**HAZOP**	Base on "wellhead system"						x			
1.6	Run the gauge ring and junk basket down and up borehole.	**HAZOP**	Base on "wireline"							x		
1.7	Pull the qualification tool string into the fluid seal system, close the gate valve, and drain excess borehole fluid from the wellhead components.	**HAZOP**	Base on "wellhead system"						x			
1.8	Verify there is no radioactive contamination on the wireline or tool string as it is withdrawn from the borehole.	Not applicable	Verification task								x	
1.9	Remove and dismantle the qualification tool string and fluid seal from the wellhead and the wireline	Not selected	No significant potential for radiological impact									x
1.10	Inspect the junk basket for retrieved material, and evaluate gauge ring data to show the borehole is ready for package emplacement.	Not selected	No significant potential for radiological impact									x
Sequence 2	***Waste package receipt***											
2.1	Drive tractor-trailer with loaded transportation cask onto site	Not selected	Low risk, common activity									x
2.2	Position and park trailer, and disconnect and move tractor to designated area	Not selected	Low risk, common activity									x
2.3	Ensure trailer is secure	Not applicable	Verification task								x	
2.4	Confirm waste package data package and trailer tamper seals	Not applicable	Verification task								x	

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
Sequence 3	***Transportation cask preparation and move to transfer station***											
3.1	Ensure cradle #1 is in position to receive the transportation cask (withdrawn from the shield).	Not applicable	Verification task								x	
3.2	Ensure an empty transfer cask has been placed in cradle #2 (withdrawn from the shield).	Not applicable	Verification task								x	
3.3	Remove the trailer cover and doors and set into a laydown area, using a crane.	**HAZOP**	Base on "lift"	x								
3.4	Remove the impact limiters from the transportation cask while it is secured to the trailer, using a crane, and set them in a laydown area.	**HAZOP**	Base on "lift"	x								
3.5	Verify there is no radioactive contamination on the exterior surfaces of the transportation cask.	Not applicable	Verification task								x	
3.6	Remove the fixtures securing the cask to the trailer, and attach a crane-supported yoke to the cask pintles.	**HAZOP**	Base on "lift"	x								
3.7	Rotate the cask into a vertical position with pins set on the trailer cradle, and lift the cask just above the trailer structures.	**HAZOP**	Base on "lift"	x								
3.8	Move the cask over cradle #1, and lower the cask so the cradle rotation pins fit into pockets on the cask.	**HAZOP**	Base on "lift"	x								
3.9	Lower and rotate the cask until it rests on cradle #1 in a horizontal position, remove the handling yoke, and secure the cask to the cradle.	**HAZOP**	Base on "lift"	x								
3.10	Ensure the shield plug is in position for removal of the transportation cask shield plug	Not applicable	Verification task								x	
3.11	Prepare the end plug for removal, and roll cradle #1 into position against the transfer shield.	**HAZOP**	Combine "shield plug" and "cradle roll"		x	x						
Sequence 4	***Transfer station operations and cask-to-cask transfer***											
4.1	Ensure the transportation cask is on cradle #1, in its shielded position against the interface shield assembly.	Not applicable	Verification task								x	
4.2	Ensure the transfer cask is on cradle #2, withdrawn from the interface shield.	Not applicable	Verification task								x	
4.3	Ensure the lower shield plug for the transfer cask has been pre-positioned in the transfer shield.	Not applicable	Verification task								x	
4.4	Position the sliding shield plate in its first position, ready to receive transportation cask end shield plug.	**HAZOP**	Base on "shield slide"				x					
4.5	Detach and pull the end shield from the transportation cask into the sliding shield, using appropriate tooling to align, pull, and secure the plug in the sliding shield.	**HAZOP**	Base on "shield plug"			x						
4.6	Verify there is no radioactive contamination on accessible surfaces of the shield plug.	Not applicable	Verification task								x	
4.7	Roll cradle #2 (with the transfer cask) into its shielded position against the interface shield assembly.	**HAZOP**	Base on "cradle roll"		x							
4.8	Position the sliding shield plate in its second position, providing an open path between the two casks.	**HAZOP**	Base on "shield slide"				x					
4.9	Verify the radiation exposure dose rates around the shield are acceptable.	Not applicable	Verification task								x	
4.10	Release the flange from the package latch subassembly on the transfer cask top plug, and attach the extension shaft to the transfer latch subassembly.	**HAZOP**	Base on "shield plug" and "latch or move"			x		x				
4.11	Push the package latch subassembly through the interface shield assembly until it makes contact with the waste package in the transportation cask.	**HAZOP**	Combine "latch or move" and "shield plug"			x		x				
4.12	Confirm latch engagement on the waste package.	Not applicable	Verification task								x	
4.13	Pull the waste package through the interface shield assembly until it is in position in the transfer cask, and the extension shaft connection is clear of the transfer cask upper plug. Monitor radiation exposure dose rates throughout this operation.	**HAZOP**	Base on "latch or move"					x				

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
4.15	Engage the side latches, securing the package in position in the transfer cask. Verify engagement of the latches.	**HAZOP**	Base on "latch or move"					x				
4.16	Attach the flange to the package latch subassembly, and attach the flange to the transfer cask top shield plug. Leave the latch subassembly attached to the waste package.	**HAZOP**	Base on "shield plug" and "latch or move"			x		x				
4.17	Verify the radiation exposure dose rates at the transfer cask are acceptable.	Not applicable	Verification task								x	
4.18	Position the sliding shield plate in its third position, with the transfer cask lower shield plug in the slide shield ready for insertion.	**HAZOP**	Base on "shield slide"				x					
4.19	Roll cradle #1 away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved.	**HAZOP**	Base on "cradle roll"		x							
4.20	Verify there is no radioactive contamination in the open end of the transportation cask or on the interface shield assembly, and that radiation exposure dose rates at the interface shield assembly are acceptable.	Not applicable	Verification task								x	
4.21	Push the transfer cask lower shield plug into position in the transfer cask, using appropriate tooling.	**HAZOP**	Base on "shield plug"			x						
4.22	Engage the Grayloc® clamp on the bottom of the transfer cask to the lower shield plug, and verify engagement.	**HAZOP**	Base on "shield plug"			x						
4.23	Roll cradle #2 with the loaded transfer cask away from the interface shield assembly. Monitor radiation exposure dose rates as the cradle is moved.	**HAZOP**	Base on "cradle roll"		x							
4.24	Verify the radiation exposure dose rates at all locations around the transfer cask are acceptable.	Not applicable	Verification task								x	

Appendix A. Activity hazard screening table.												
Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
Sequence 5	***Transfer cask move to wellhead station***											
5.1	Confirm that the transfer cask, with waste package, is ready to move to the wellhead.	Not applicable	Verification task								x	
5.2	Confirm the wellhead pit shield carousel is in position over the lower plug removal station, and is ready to accept the transfer cask.	Not applicable	Verification task								x	
5.3	Remove the fixtures securing the cask to cradle #2, and attach a crane-supported yoke to the cask pintles (this might be a field crane, or might be a hoist on a headframe assembly).	**HAZOP**	Base on "lift"	x								
5.4	Rotate the cask into a vertical position with pins set on cradle #2, and lift the cask just above the cradle and wellhead structures.	**HAZOP**	Base on "lift"	x								
5.5	Move the cask over the wellhead shield carousel, and lower the cask onto the kneeling jack ring over the cask port.	**HAZOP**	Base on "lift" and "wellhead system"	x					x			
5.6	Secure the transfer cask to the shield carousel, using TBD features to prevent the cask from tipping or being dislodged (features such as guy wires must allow carousel rotation and kneeling jack actuation).	**HAZOP**	Base on "lift" and "wellhead system"	x					x			
5.7	Verify that radiation exposure dose rates are acceptable, and no radioactive contamination is present.	Not applicable	Verification task								x	
Sequence 6	***Transfer cask, waste package, wellhead and wireline configuration***											
6.1	Ensure the transfer cask is in place on the shield plate carousel, properly positioned over the lower plug handling mechanism.	Not applicable	Verification task								x	
6.2	Ensure the wellhead flange is ready to accept the transfer cask, with a new flange seal in place.	Not applicable	Verification task								x	
6.3	Verify the radiation exposure dose rates at the transfer cask are acceptable.	Not applicable	Verification task								x	
6.4	Verify the side latches are engaged with the waste package.	Not applicable	Verification task								x	
6.5	Ensure the tool string is attached to the wireline, and the lubricator and fluid seal are ready for use.	Not applicable	Verification task								x	
6.6	Position personnel access hardware adjacent to the transfer cask, and install temporary shielding as required for removal of the latch assembly and installation of the tool string.	**HAZOP**	Base on "shield plug"			x						
6.7	Disconnect the top latch assembly from the upper shield plug, activate the latch rod to release the assembly from the waste package, and remove the latch assembly from the upper shield plug.	**HAZOP**	Base on "shield plug" and "latch/move"			x		x				
6.8	Verify the radiation exposure dose rates at the transfer cask are acceptable, and adjust temporary shielding as appropriate.	Not applicable	Verification task, with response								x	
6.9	Attach a connection sub to the transfer cask upper shield plug, to mate with the quick connector on the lower end of the lubricator	**HAZOP**	Base on "shield plug"			x						
6.10	Make up the wireline tool string, lubricator, and grease seal assembly at ground level. Up-end the assembly under the headframe and lift it vertically with the wireline cable. Lower the assembly onto the connection sub and make the connection with the lubricator.	**HAZOP**	Base on "wireline" and "shield plug"			x				x		
6.11	Lower the tool string until it latches onto the waste package.	**HAZOP**	Base on "wireline"							x		
6.12	Verify that the tool string is securely latched onto the waste package.	Not applicable	Verification task								x	
6.13	Verify the radiation exposure dose rates at the transfer cask are acceptable.	Not applicable	Verification task								x	
6.14	Take up wireline slack to the extent possible movement of the package is minimized but cask movements remain possible.	**HAZOP**	Base on "wireline"							x		
6.15	Raise the lower shield plug handling mechanism until it engages with the shield plug.	**HAZOP**	Base on "shield plug"			x						
6.16	Activate the Grayloc® clamp on the bottom of the transfer cask to release the lower shield plug	**HAZOP**	Base on "shield plug"			x						

Appendix A. Activity hazard screening table.												
Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
6.17	Lower the shield plug handling mechanism so the shield plug is clear of the bottom flange of the transfer cask.	**HAZOP**	Base on "shield plug"			x						
6.18	Verify the radiation exposure dose rates at the wellhead pit shield are acceptable.	Not applicable	Verification task								x	
6.19	Ensure the wireline is sufficiently slack to accommodate cask movement, but not excessively slack as to break if the package is inadvertently released.	Not applicable	Verification task, response repeat of 6.14								x	
6.20	Rotate, and if necessary slide, the carousel to position the cask over the wellhead.	**HAZOP**	Base on "wellhead system"						x			
6.21	Confirm cask position over the wellhead flange, and adjust position as necessary.	Not applicable	Verification task								x	
6.22	Use the kneeling jacks to gently lower the cask onto the wellhead flange, while monitoring alignment of the bottom cask flange with the wellhead flange. Adjust the position of the carousel as necessary to maintain alignment as the cask is lowered.	**HAZOP**	Base on "wellhead system"						x			
6.23	With the cask in contact with the wellhead flange, activate the Grayloc® clamp on the bottom of the transfer cask to complete the flange connection between the transfer cask and the wellhead.	**HAZOP**	Base on "wellhead system"						x			
6.24	Ensure the cask is secured against movement in the vertical or horizontal (tipping) directions.	Not applicable	Verification task								x	
6.25	Verify the radiation exposure dose rates at the wellhead pit shield are acceptable.	Not applicable	Verification task								x	
6.26	Take up tension in the wireline.	**HAZOP**	Base on "wireline"							x		

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
Sequence 7	***Borehole emplacement, release, and wireline retrieval***											
7.1	Ensure the transfer cask is in place on the shield plate carousel, attached to the wellhead flange, and secured against inadvertent movement.	Not applicable	Verification task								x	
7.2	Ensure the wireline tool string is connected waste package, and is properly tensioned.	Not applicable	Verification task								x	
7.3	Ensure the lubricator and wireline fluid seal are in place.	Not applicable	Verification task								x	
7.4	Ensure the BOP is ready for operation and in open position.	Not applicable	Verification task								x	
7.5	Verify the radiation exposure dose rates at the transfer cask are acceptable.	Not applicable	Verification task								x	
7.6	Verify the side latches are engaged with the waste package.	Not applicable	Verification task								x	
7.7	Verify the wellhead gate valve is closed.	Not applicable	Verification task								x	
7.8	Release the side latches, allowing the waste package to be supported by the wireline.	**HAZOP**	Base on "latch or move" and "wireline"					x		x		
7.9	Lower the package through the wellhead, to just above the closed gate valve, while monitoring radiation dose exposure rates at the wellhead shield.	**HAZOP**	Base on "wellhead system" and "wireline"						x	x		
7.10	Open the wellhead gate valve, and monitor the level of fluid in the borehole.	**HAZOP**	Base on "wellhead system"						x			
7.11	If necessary, add fluid to bring the borehole fluid level up to the wellhead.	**HAZOP**	Base on "wellhead system"						x			
7.12	Lower the waste package through the gate valve and down the borehole to the emplacement zone, monitoring depth of the package using the tool string locator, wireline runout, wireline tension, and downhole load monitoring.	**HAZOP**	Base on "wireline"							x		
7.13	Stop the wireline when the package rests on the previous package or borehole plug (or, in the case of the initial package, the bottom of the borehole).	**HAZOP**	Base on "wireline"							x		
7.14	Verify the package is at its intended location in the borehole.	Not applicable	Verification task								x	
7.15	Send a signal to release the package from the wireline tool string.	**HAZOP**	Base on "wireline"							x		
7.16	Confirm package release by signal and/or tension on the wireline.	**HAZOP**	Base on "wireline"							x		
7.17	Retrieve the wireline, monitoring depth of the tool string, until the tool string is returned to the transfer cask lubricator.	**HAZOP**	Base on "wireline"							x		
7.18	Verify the tool string is in the lubricator, clear of the wellhead components.	Not applicable	Verification task								x	
7.19	Close the gate valve, and drain fluid from the wellhead above the gate valve.	**HAZOP**	Base on "wellhead system"						x			
7.20	Verify that radiation exposure dose rates are minimal, and no radioactive contamination is present.	Not applicable	Verification task								x	

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
Sequence 8	***Equipment condition for next use***											
8a	***Prepare wireline system for next use***											
8a.1	Ensure the transfer cask is in place on the shield plate carousel, securely fixed, with no waste package present, the wellhead gate valve closed, and drained of borehole fluid.	Not applicable	Verification task								x	
8a.2	Ensure that radiation and contamination surveys indicate no radioactive material is present.	Not applicable	Verification task								x	
8a.3	Ensure the wireline tool string is in the lubricator.	Not applicable	Verification task								x	
8a.4	Provide sufficient slack in the wireline to disconnect the fluid seal and lubricator from the transfer cask, and possibly from each other.	Not selected	No direct radiological impact									x
8a.5	Using the wireline, carefully withdraw the tool string out of the transfer cask.	Not selected	No direct radiological impact									x
8a.6	Verify no radioactive contamination is present on the tool string as it is withdrawn.	Not applicable	Verification task								x	
8a.7	Using the wireline crane or headframe, move the wireline, lubricator, and tool string to a laydown and wash area.	Not selected	No direct radiological impact									x
8a.8	Separate the tool string, lubricator, and fluid seal and wash borehole fluid residue off the components.	Not selected	No direct radiological impact									x
8a.9	Inspect the wireline termination and rebuild if necessary.	Not selected	No direct radiological impact									x
8a.10	If the next wireline application is other than waste package emplacement, disconnect the package placement tool string and prepare the wireline for an alternate tool string.	Not selected	No direct radiological impact									x
8a.11	If the next wireline application is emplacement of another waste package, rebuild or reset the remote disconnect for the next use.	Not selected	No direct radiological impact									x
8b	***Prepare transfer cask and interface shield for next use***											
8b.1	Ensure the transfer cask is in place on the shield plate carousel, securely attached and empty.	Not applicable	Verification task								x	
8b.2	Ensure the wireline tool string has been removed from the transfer cask.	Not applicable	Verification task								x	
8b.3	Ensure that radiation and contamination surveys have been completed, and no radioactive material is present in the wellhead pit or the transfer cask.	Not applicable	Verification task								x	
8b.4	Move empty cradle #2 into the washdown area, within reach of the headframe gantry crane, and secure it to prevent motion.	Not selected	No direct radiological impact									x
8b.5	Ensure there is no load on the transfer cask lower flange assembly.	Not applicable	Verification task								x	
8b.6	Connect the handling yoke to the pintles of the transfer cask using the headframe gantry crane.	Not selected	No direct radiological impact									x
8b.7	Release the Grayloc® flange clamp assembly to disconnect the transfer cask from the wellhead.	Not selected	No direct radiological impact									x
8b.8	Disconnect features used to prevent vertical and horizontal movement of the transfer cask.	Not selected	No direct radiological impact									x
8b.9	Use the kneeling jacks to separate the transfer cask from the wellhead flange.	Not selected	No direct radiological impact									x
8b.10	Verify the transfer cask is free of attachments to the wellhead or the wellhead shield or carousel assemblies, and lift the transfer cask from the wellhead shield.	Not selected	No direct radiological impact									x
8b.11	Move the transfer cask to cradle #2, and lower the cask so the cradle rotation pins fit into pockets on the cask.	Not selected	No direct radiological impact									x
	Lower and rotate the cask until it rests on cradle #2 in a horizontal position, remove the handling											

Appendix A. Activity hazard screening table.												
Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
8b.13	Remove the top shield plug, and wash borehole fluid residues from the interior of the transfer cask.	Not selected	No direct radiological impact									x
8b.14	Inspect, clean and refurbish as necessary, and replace the top shield plug and transfer latch assembly onto the top of the transfer cask.	Not selected	No direct radiological impact									x
8b.15	Inspect, clean and refurbish as necessary the lower Grayloc® flange and actuating mechanism.	Not selected	No direct radiological impact									x
8b.16	Move cradle #2, with the transfer cask, into position near (but not against) the interface shield, and seucre it to prevent motion.	Not selected	No direct radiological impact									x
8b.17	Confirm that all components are present and the transfer cask is ready to accept the next waste package.	Not applicable	Verification task								x	
8b.18	Using the crane and an appropriate open access port in the wellhead shield carousel, attach a lift fixture to the transfer cask lower shield plug and lift it off the shield plug handling fixture and out of the wellhead pit.	Not selected	No direct radiological impact									x
8b.19	Move the lower shield plug to the washdown area, and inspect and clean the shield plug.	Not selected	No direct radiological impact									x
8b.20	Verify the condition of the interface shield assembly, and pre-position the transfer cask lower shield plug in the sliding shield, using appropriate tooling.	Not selected	No direct radiological impact									x
8c	***Prepare wellhead for next use***											
8c.1	Ensure the transfer cask has been removed, the wellhead gate valve is closed, and all wellhead equipment is in a stable condition.	Not applicable	Verification task								x	
8c.2	Verify that radiation exposure dose rates are minimal, and no radioactive contamination is present.	Not applicable	Verification task								x	
8c.3	Wash borehole fluid residues and other material off the borehole equipment as appropriate, and drain the pit using the pit sump pump.	Not selected	No direct radiological impact									x
8c.4	Ensure the lower transfer cask shield plug has been removed from the shield plug handling mechanism, and confirm proper operation of the mechanism.	Not selected	No direct radiological impact									x
8c.5	Test operation of the BOP, as appropriate.	Not selected	No direct radiological impact									x
8c.6	Inspect the wellhead flange, recondition the flange as appropriate, and place a new gasket on the wellhead flange.	Not selected	No direct radiological impact									x
8c.7	Confirm operation of the wellhead pit shield assembly, including the carousel and transfer cask kneeling jacks, and position for the next operating sequence.	Not selected	No direct radiological impact									x

Appendix A. Activity hazard screening table.												
Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
8d	***Prepare transportation cask and return to waste package loading facility***											
8d.1	Ensure cradle #2 has been rolled away from the interface shield assembly.	Not applicable	Verification task								x	
8d.2	Confirm the condition of the transportation cask shield plug, and position new gaskets as appropriate.	Not applicable	Verification task, with response								x	x
8d.3	Roll cradle #1, with the empty transportation cask, into position against the interface shield assembly.	Not selected	No direct radiological impact									x
8d.4	Position the sliding shield plate in its first position, with the transportation shield plug in position for insertion into the transportation cask.	Not selected	No direct radiological impact									x
8d.5	Push the transportation cask shield plug into position in the cask, using appropriate tooling.	Not selected	No direct radiological impact									x
8d.6	Detach handling tooling and insert bolts attaching shield plug to transportation cask.	Not selected	No direct radiological impact									x
8d.7	Roll cradle #1 away from the interface shield assembly, and torque bolts attaching shield plug to cask.	Not selected	No direct radiological impact									x
8d.8	Ensure transportation cask is ready for return to waste package loading facility.	Not applicable	Verification task								x	
8d.9	Remove the fixtures securing the cask to cradle #1, and attach a crane-supported yoke to the cask pintles.	Not selected	No direct radiological impact									x
8d.10	Rotate the cask into a vertical position with pins set on cradle #1, and lift the cask just above the cradle and trailer structures.	Not selected	No direct radiological impact									x
8d.11	Move the cask over the transportation trailer, and lower the cask so the trailer cradle rotation pins fit into pockets on the cask.	Not selected	No direct radiological impact									x
8d.12	Lower and rotate the cask until it rests on the transportation trailer cradle in a horizontal position, remove the handling yoke, and secure the cask to the cradle.	Not selected	No direct radiological impact									x
8d.13	Using a crane, retrieve the impact limiters from the laydown area and attach them to either end of the transportation cask.	Not selected	No direct radiological impact									x
8d.14	Re-assemble the trailer components and verify the transportation cask is ready to move off the borehole site.	Not selected	No direct radiological impact									x

Appendix A. Activity hazard screening table.

Activity	Description	HAZOP selection	HAZOP category or rationale	LI	CR	SP	SS	LM	WS	W	V	NS
Sequence 9	***Set mechanical interval plug***											
9.1	Obtain and confirm operability of pressure-operated coiled tubing bridge plug.	Not selected	No direct radiological impact									x
9.2	Install riser on wellhead, including injector head if borehole is flowing.	Not selected	No direct radiological impact									x
9.3	Assemble bridge plug and squeeze packer on coiled tubing.	Not selected	No direct radiological impact									x
9.4	Set up coiled tubing injection.	Not selected	No direct radiological impact									x
9.5	Open gate valve and establish fluid control.	**HAZOP**	Base on "wellhead system"						x			
9.6	Run coiled tubing/bridge plug into position over last package.	**HAZOP**	Similar to "wireline"							x		
9.7	Activate bridge plug and confirm set.	**HAZOP**	Similar to "wireline"							x		
9.8	Release coiled tubing from bridge plug and confirm release.	**HAZOP**	Similar to "wireline"							x		
Sequence 10	***Set cement interval plug***											
10.1	Set squeeze packer 10 meters above bridge plug.	Not selected	No direct radiological impact									x
10.2	Obtain and mix cement for plug.	Not selected	No direct radiological impact									x
10.3	Inject cement and spacer fluids in coiled tubing.	Not selected	No direct radiological impact									x
10.4	Release packer and raise coiled tubing (rinse tubing at the surface).	Not selected	No direct radiological impact									x
10.5	Verify no radiological contamination on coiled tubing as it is pulled up.	Not selected	No direct radiological impact									x
10.6	Remove and clean coiled tubing system for next use.	Not selected	No direct radiological impact									x
10.7	Close gate valve and remove riser and injector head (if used).	Not selected	No direct radiological impact									x
10.8	Recondition the wellhead to prepare for the next emplacement sequence.	Not selected	No direct radiological impact									x

Appendix C – Equipment List and Activity Sequences

Appendix B. Equipment list and sequences in which they are used.		1	2	3	4	5	6	7	8	9	10
Transportation and reciept											
	NAC-LWT® cask with impact limiters and shield plug		x	x	x				x		
	Transportation cask trailer system with trailer cradle and tie-downs (by cask vendor)		x	x					x		
	Transportation cask lift yoke (supplied by cask vendor)			x					x		
	(roads and pads under support services)										
	(large mobile crane under headframe and cranes)										
Package transfer station											
	Shield interface with fixed plates and sliding shield, with drive moter and interlocks			x	x				x		
	Cradle #1 (transportation cask cradle)			x	x				x		
	Cradle #2 (transfer cask cradle)				x	x			x		
	Cask and cradle tiedown systems (seismic response design)			x	x	x			x		
	Interface system rails and rail footers (seismic response design)			x	x	x			x		
	Transportation cask shield plug handling equipment			x	x				x		
	Transfer cask shield plug handling equipment				x						
	Tool kit, including gaskets, ladders or light work platforms, and supplemental shielding				x	x			x		
	(small mobile crane under headframe and cranes)										
Transfer cask											
	Transfer cask body, including inner pressure tube, lift pintles, and cradle pockets				x	x	x	x	x		
	Grayloc® remote clamp with actuation system				x		x		x		
	Lower transfer cask shield plug				x		x		x		
	Upper transfer cask shield plug with removable inner plug				x		x		x		
	Package latch system with inner release rod and removable flange				x	?	x		x		
	Package latch extension rod and handling/drive hardware				x		x				
	Waste package side latch assemblies				x	?	x	x	x		
	Tool kit, including shield plug gaskets						x		x		

Appendix B. Equipment list and sequences in which they are used.		1	2	3	4	5	6	7	8	9	10
Wellhead (wellhead completion in scope of drilling contractor)											
	(borehole itself with cemented surface casing and conductor, tieback casing not in scope)										
	Wellhead baseplate	x					x	x		x	x
	Intermediate casing reducer with fluid taps	x					x	x		x	x
	Tieback casing spool piece with fluid taps (tieback welded to and supported by spool)	x					x	x		x	x
	Full-bore gate valve with remote actuator and manual over-ride	x					x	x		x	x
	Annular blowout preventer	x						x		x	x
	Hydraulic fluid and control system for annular BOP	x						x		x	x
	Spool piece connected to BOP, with Grayloc® flange at top	x					x	x	x	x	x
	Borehole cover piece (cover flange when not in use)						x		x		
	Tool kit, flange gaskets, and spare parts for BOP and gate valve						x		x		
Pit shield and transfer cask support system											
	Pit structure with footings as required to support shield plate and central post loads	x				x	x	x	x		
	Beams to support shield plate and allow slide	x				x	x	x	x		
	Pit sump, sump pump, and discharge to holdup and sampling tank (see washdown)	x						x	x		
	Pit main shield plate with slide drive and lock mechanism	x				x	x	x	x		
	Central carousel with drive and lock mechanism and central post with slide capability					x	x	x	x	x	x
	Cask support ring with hydraulic jack system, including hydraulic fluid and controls					x	x	x	x		
	Cask tie-down system					x	x	x	x		
	Transfer cask lower shield plug handling system						x		x		
	Hydraulic fluid and control system for lower cask shield plug handling station						x		x		
	Transfer cask position verification system (cameras or other position indicators)					x	x				
	Large maintenance plug with tool plugs, drive and lock mechanism										
	Lower cask shield plug station shield insert with operating features						x				
	Transfer cask opening plug	x								x	x
	Standard tool set, including mechanical reach, visual and radiation survey tools, and lights					x	x		x		
	Shield maintenance tools, consumables, and spare parts						x		x		

Appendix B. Equipment list and sequences in which they are used.		1	2	3	4	5	6	7	8	9	10
Wireline system											
	Electric wireline	x					x	x	x		
	Wireline handling system, including spool, drive motor, brake and tensioning, and controls	x					x	x	x		
	Wireline sheave above borehole, including headframe mounts and movement tracking	x					x	x	x		
	Waste package tool string (remotely-operated disconnect, locator, cable head/weakpoint)						x	x	x		
	Tool string lubricator, including mounting components for transfer cask and fluid control						x	x	x		
	Fluid control system, including mounting components and wireline interface (stuffing box)						x	x	x		
	Grease supply for borehole fluid control system (grease tube)							x			
	Borehole qualification tool string (gauge ring, junk basket, locator, cable head connection)	x									
	Borehole qualification tool string lubricator (riser) and fluid control	x									
	Wireline tool kit, tool string consumables, and spare parts						x		x		
Interval plug system (coiled tubing)											
	Coiled tubing integrated deployment system (likely truck-mounted system)									x	x
	Coiled tubing riser and fluid control system									x	x
	Mechanical plug and packer system									x	
	Plug cement and chaser fluid preparation and delivery system										x
	Coiled tubing tool kit, consumables (including mechanical plug components, spare parts									x	x
Headframe and cranes											
	Headframe spanning wellhead through transfer cask cleanout station (cradle #2)	x				x	x	x	x		
	Gantry crane (capacity)					x	x		x		
	Large mobile crane (capacity) used for cask lift			x					x		
	Small mobile crane used for miscellaneous tool and shield plug lifts	x		x	x	x	x		x	x	x
	Hooks, slings, transfer cask yoke, and general rigging			x		x	x		x	x	x
	Tool kit and mobile crane servicing equipment								x		

Appendix B. Equipment list and sequences in which they are used.		1	2	3	4	5	6	7	8	9	10
Washdown station											
	Decontamination fluid makeup and delivery								x		
	Fluid delivery lance for cleaning								x		
	Catch basin and drains								x		
	Holdup and sampling tank,treatment options, release path								x		
Borehole and annulus fluid control											
	Borehole fluid makeup	x						x		x	
	Borehole fluid tap piping, including pressure and flow controls	x						x		x	
	Annulus fluid tap piping, including pressure and flow controls	x						x		x	
	Borehole fluid recirculation sysetm, including pumps and surge capacity										
	Borehole fluid pit (lined or otherwise protected against radioactive contamination release)										
	Borehole fluid sampling, treatment and release system										
Site services (only select services identified with sequences)											
	Site grading, drainage, pads and pavement	x	x	x	x	x	x		x	x	x
	Road access and site security		x						x		
	Portable office and storage structures, with HVAC as appropriate										
	Normal electrical power (for repository scale, assumed to be feeders from regional grid)	x		x	x	x	x	x	x	x	x
	Backup electrical power										
	Potable water									x	x
	Process water (borehole fluid makeup, cleanout stations, interval plugs, etc.)	x							x		
	Fire protection (hydrants and sprinklers in select areas)										
	Fuel tanks and lubrication services (mobile cranes and other vehicles)								x		
	Central data and communications system, including interlocks and alarms	x				x	x	x		x	x
	Site lighting										

Appendix D – Example HAZOP Tables

Table E-8. HAZOP Worksheet

Facility/Operation: RF							Process: TC Unloading
Node 7: Horizontal Transfer of Cask Between Rail Car, Cask Stand and Lift Fixture or Cask Transfer Trailer							Process/Equipment: Railcar, 200-Ton Crane, Cask Stand
Guide Words: No, More, Less, Reverse, Other Than, As Well As, Part Of							Consequence Categories: Radioactive Release, Lack of Shielding, Criticality
Node Item Number	**Parameter**	**Deviation Considered**	**Postulated Cause**	**Consequence(s)**	**Potential Prevention/Mitigation Design of Operational Feature**	**Notes**	**MLD Index Number**
7.1	Speed (Crane)	(More) Cask lowers too fast	1 – Human failure 2 – Mechanical failure	Potential radioactive release	1 – Procedures and training 2 – Crane design	TC design may mitigate event, depending on passive equipment failure analysis	R-608, R-801
7.2	Speed (Crane)	(Less) Cask lowers too slow		No safety consequences			N/A
7.3	Travel (Crane)	(Other Than) Crane moves with cask lowered	1 – Human failure 2 – Mechanical failure	Potential radioactive release	1 – Procedures and training 2 – Crane design	TC design may mitigate event, depending on passive equipment failure analysis	R-610, R-803
7.4	Motor	(More) Motor temperature too high	1 – Human failure 2 – Mechanical malfunction	No safety consequences		Potential fire scenario	R-I303 thru R-I310
7.5	Maintenance	(No) Improper maintenance of crane	Human failure	No safety consequences	Maintenance program	Considered in event sequence development (event tree/FTA/HRA)	N/A
7.6	Controls (PLC)	(Other Than)		No safety consequences		Considered in event sequence development (event tree/FTA/HRA)	N/A
7.7	Vision/ Communication	(Other Than) Unclear communication	Poor operating environment	No safety consequences	1 – Crane operator training program 2 – Human factor evaluation 3 – Industrial hygiene standards	Considered in HRA	N/A
7.8	Lift	(More) Two-blocking	1 – Human failure 2 – Mechanical malfunction	Potential radioactive release resulting from drop	1 – Crane design 2 – Procedures and training	1 – TC design may mitigate event, depending on passive equipment failure analysis 2 – 20 ft or greater drop considered	R-608, R-801
7.9	Lift	(Less) Not lifted high enough to clear other structures or equipment	1 – Human failure 2 – Mechanical malfunction	Potential radioactive release resulting from drop or impact	Procedures and training		R-610, R-803
7.10	Lift	(No)		No safety consequences			N/A
7.11	Lift	(Reverse) Rapid rundown	1 – Human failure 2 – Mechanical malfunction	Potential radioactive release resulting from drop or impact	1 – Crane design 2 – Procedures and training	TC design may mitigate event, depending on passive equipment failure analysis	R-608, R-801, R-802
7.12	Speed (Crane)	(More) Crane moves faster than allowed by procedures	1 – Human failure 2 – Mechanical failure	Potential radioactive release resulting from collision with structures or equipment	1 – Crane design 2 – Procedures and training	TC design may mitigate event, depending on passive equipment failure analysis	R-610, R-803
7.13	Speed (Crane)	(Less) Crane moves too slow	1 – Human failure 2 – Mechanical failure	Potential radioactive release resulting from drop	Procedures and training	Prolonged exposure time for sequence initiation	R-801
7.14	Speed (Crane)	(Other Than) Abrupt stop	1 – Human failure 2 – Mechanical failure	Potential radioactive release resulting from collision with structures or equipment	1 – Crane design 2 – Procedures and training	TC design may mitigate event, depending on passive equipment failure analysis	R-801
7.15	Lift	(Other Than) 200-ton crane used instead of 20-ton entrance vestibule crane to remove impact limiters	Human failure	Drop of cask resulting in release	1 – Procedures and training 2 – Hook design		R-801

NOTE: Guidewords not used in this node: As Well As and Part Of.
ft = feet; FTA = fault-tree analysis; HRA = human-reliability analysis; PLC = programmable logic controller; RF = Receipt Facility; TC = transportation cask.
Events that have no direct safety consequences but may be precursors to events that occur in other nodes are noted as "No safety consequences."

Source: Original

Task: 3.7, Rotate cask to vertical and lift above trailer
Guide words: no, more, less, reverse, other than, as well as, part of

Equipment Used: Transport cask, Crane, Yoke, Transport trailer cradle
Consequence Categories: Radioactive material release, Direct exposure

Task Item Number	Parameter	Deviation considered	Postulated cause	Consequences	Potential Prevention/Mitigation Design of Operational Feature	Notes
3.7.1	Load	(More) Load lifted too heavy for crane	Failure to remove tie-downs	Drop of load leading to radioactive release	1 - Procedures and Training 2 - Crane design	Interlock between crane and tie-downs
3.7.2	Load	(Less) Load lifted too light		No safety consequences		
3.7.3	Speed (Crane and Hook)	(More or Less) Hook and crane speed not matched during lifting motion	1 - Human failure 2 - Mechanical failure	Collision leading to radioactive release	1 - Procedures and Training 2 - Crane design and below-the-hook design	Crane control could limit speed
3.7.4	Travel (Crane)	(Reverse) Travels in wrong direction	1 - Human failure 2 - Mechanical failure	Collision leading to radioactive release	1 - Procedures and Training 2 - Crane design and below-the-hook design	Crane control could limit range of motion
3.7.5	Motor	(More) Motor temperature too high	1 - Human failure 2 - Mechanical malfunction	Drop of load leading to radioactive release		Ensure motor properly rated for load
3.7.6	Motor Motive Force	(Less or No) Loss of motive force allows rapid rundown	1 - Human failure 2 - Mechanical malfunction	Collision leading to radioactive release	Crane design and below-the-hook design	
3.7.7	Maintenance	(No) Improper maintenance of crane	Human failure	Drop of load leading to radioactive release	Maintenance program	
3.7.8	Controls (PLC)	(Other Than) Control system failures	1 - Human failure 2 - Mechanical failure	Collision leading to radioactive release	Maintenance program	System to prevent crane movement without controls
3.7.9	Vision/ Communication	(Other Than) Unclear communication	Poor operating environment	Collision leading to radioactive release	Crane design and below-the-hook design	
3.7.10	Alignment	(Other Than)	1 - Human failure 2 - Mechanical failure	Drop of load leading to radioactive release	Crane design and below-the-hook design	Ensure crane footings properly set
3.7.11	Pivot Point	(Other Than) Pivot point contstraint fails	1 - Human failure 2 - Mechanical failure	Drop of load leading to radioactive release	Crane design and below-the-hook design	Ensure crane footings properly set

Note: Guidewords not used in this activity: As Well As and Part Of.

Distribution

1	MS0736	Evaristo Bonano	8840
1	MS0736	Peter Swift	8840
1	MS0736	Patrick Brady	8840
1	MS0747	David Sassani	8842
1	MS0779	Carlos Lopez	8842
1	MS0747	Geoff Freeze	8843
1	MS0747	Ernest Hardin	8844
1	MS0747	Kris Kuhlman	8844
1	MS0747	Robert MacKinnon	8842
1	MS0747	Emily Stein	8844
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories