REQUEST FOR ADDITIONAL INFORMATION
VOLUME 2 - Preclosure
CHAPTER 2.1.1.3 - Identification of Hazards and Initiating Events
SET 3 (RAIs #1 to #33)

The following questions pertain to DOE's assessment of external hazards that is used to support its Preclosure Safety Analysis (PCSA) in the Safety Analysis Report (SAR). This information is needed to assess whether or not DOE has demonstrated compliance with 10 CFR 63.112(b), (c), and (d), which require DOE to include in the PCSA (SAR sections 1.6 and 1.7) an identification and systematic analysis of naturally occurring and human-induced hazards, the data used, and the technical basis for either inclusion or exclusion of these hazards in the safety analysis. In addition to the SAR, these questions also refer to other preclosure documents referenced in the LA and on the docket. Unless otherwise specified, references cited in the following RAIs are from SAR section 1.7.

RAI #1

a) Provide a technical basis for excluding ash fall hazards from large-volume (> 1 km^3), explosive, silicic (rhyolitic) eruptions with a probability of occurrence at least 1 in 10,000 during the 100-year preclosure period to develop the design-basis roof loads for the repository facilities in SAR Section 1.6.3.4.3.

b) Provide the detailed analysis that demonstrates that the probability of exceeding a roof live load of 21 lb/ft^2 is less than 6.4×10^{-8} per year, as indicated in SAR Section 1.6.3.4.3. Elsewhere in the SAR, DOE references the document BSC (2004) but this has not been provided.

SAR Section 1.1.6.3 uses a 100,000-year cut-off for ash fall hazards from silicic volcanic eruptions. DOE has not justified selecting a 100,000-year limit to screen out at least two large silicic eruptions, reported to have occurred within the past 700,000 years in the Western United States (Perry and Crowe, 1987), to develop the roof-load from volcanic ash fall for the repository facilities. If a similar size eruption occurred during the preclosure period, it could deposit 1 m [3 ft 3 in] or more of ash at the Yucca Mountain site, depending on the distance from the repository to the eruption site and prevailing wind conditions at the time of eruption (Perry and Crowe, 1987, p. 11). This thickness of ash fall exceeds significantly the design-basis roof load in SAR Section 1.6.3.4.3. Additionally, an ash-fall of 1 m or more would also affect the passive cooling of the aging overpacks.

References:

BSC 2004. "Ash Fall Hazard for North Portal Operations Area Facilities." CAL–WHS–GS–000001 Rev 00A. Las Vegas, Nevada: Bechtel SAIC Company.

Perry, F.V. and B.M. Crowe, B.M. 1987. “Preclosure Volcanic Effects: Evaluations for a Potential Regulatory Site at Yucca Mountain, Nevada.” Los Alamos, Nevada: Los Alamos National Laboratory.

RAI #2

(a) Provide a technical basis for the estimated input parameters used in the flood frequency analysis using the HEC–1 hydrological model.

(b) Provide the flood frequency analysis and any other supporting information that justifies DOE’s conclusions for its external flooding assessment. DOE references the following documents, but these have not been provided:

BSC 2004. “Hydrological Engineering Studies for the North Portal Pad and Vicinity.” 000–00C–CD04–00100–000–00A. Las Vegas, Nevada: Bechtel SAIC Company.

BSC 2008. “Flood Hazard Curve of the Surface Facility Area in the North Portal Pad and Vicinity.” 000–PSA–MGR0–01900–000–00A. Las Vegas, Nevada: Bechtel SAIC Company.

RAI #3

Provide a technical basis for DOE’s assessment of loss of cooling capabilities at the surface facilities. They are needed to assess whether loss of cooling can initiate an event sequence at the repository facilities. DOE references the following documents but these have not been provided:

BSC 2007. “Thermal Evaluation of the CRCF-1 Lower Transfer Room Cells.” 060-00CDS00-00100-000-00A. Las Vegas, Nevada. Bechtel SAIC Company.

BSC 2008a. “Pool Water Treatment and Cooling System.” 050-M0C-PW00-00100-00000C. Las Vegas, Nevada: Bechtel SAIC Company.

BSC 2008b. “WHF and RF Thermal Evaluation.” 000-00C-DS00-01200-000-00A. Las Vegas, Nevada. Bechtel SAIC Company.

RAI #4

Explain why DOE used structural failure data from the International Atomic Energy Agency (2003) to screen out structural failure by tornadoes rather than using data from Texas Tech University (2006).

Section A3.4 of BSC (2008d), as referenced in SAR section 1.6, screens out structural failure from tornado strikes at 95 percent probability of occurrence using the data provided by the International Atomic Energy Agency (2003). However, as discussed in Section A3.4 of BSC (2008d), the structural failure probability would be above the screening threshold if data from Texas Tech University (2006) were used.

References:

International Atomic Energy Agency 2003. “External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide.” Safety Standards Series No. NS–G–1.5. Vienna, Austria: International Atomic Energy Agency.

Texas Tech University 2006. “A Recommendation for an Enhanced Fujita Scale (EF-Scale).” Revision 2. Lubbock, Texas: Texas Tech University, Wind Science and Engineering Center.

RAI #5

Provide the analysis referenced in SAR Section 1.6.3.4.4 High Winds and Tornadoes that documents the development of straight wind hazard curve DOE used to support its PCSA. This information is needed to determine whether the estimated 3-second gust straight wind speed for the million-year recurrence interval adequately estimated. DOE references the following document but this has not been provided:

BSC 2007. “Straight Wind Hazard Curve Analysis.” 000–00A–MGR0–00100–000–00A. Las Vegas, Nevada: Bechtel SAIC Company.

RAI #6

Provide the technical basis for screening out mass wasting and landslide, identified in SAR Table 1.6–8 External Event Identification and Crosswalk to Assigned Categories, as potential initiators of event sequence in the repository facilities. DOE excluded these events in SAR Section 1.6.3.4.2 Nonseismic Geologic Activity by stating that necessary topographic and geologic conditions do not exist. However, geologic records and recent observations show mass wasting events continue to occur at the repository site area. SAR Sections 1.1.7.2.1 and 1.1.7.2.2 describe storm-triggered debris flow on the South hill slope of Jake Ridge and storm-triggered mass wasting events around Midway Valley. SAR Section 1.1.4.1.2.2 describes a plan to construct two diversion channels to protect the GROA from floodwater and debris flow originated from Exile Hill; however, design details and adequacy of the design were not provided.

RAI #7

Define and provide justification for screening out the following external hazards, identified in SAR Table 1.6–8 External Event Identification and Crosswalk to Assigned Categories, as being the potential initiator of event sequences:

(a) Rockburst
(b) Soil Shrink-Swell Consolidation

(c) Static Fracturing
(d) Geochemical Alterations
(e) Perturbation of Groundwater System
(f) Thermal Loading
(g) Undetected Past Human Intrusions
(h) Barometric pressure
(i) Extreme weather and climate fluctuation.

DOE identified these as potential hazards but did not provide any description of these or a technical basis for screening these out.

RAI #8

Provide the technical bases to demonstrate that potential hazards from nearby facilities, as documented in SAR Section 1.6.3.4.8 Nearby Industrial or Military Facility Accidents, were properly screened out. Also, provide information to demonstrate that the analyses are supported by current, up-to-date information. Specific examples include, but are not limited to:

- No rationale has been provided for the conclusion that ground motions at Yucca Mountain repository from nuclear tests at the repository would be bounded by moderate to large earthquakes in the region or the activities associated with the program to defeat military missions protected in tunnels and hardened deeply buried facilities would not affect the repository.
- No justification is provided for why an accidental detonation of the "maximum high explosive device" at the Device Assembly Facility or the tests performed at U-1a Complex/Lyner Complex or the tests with high explosives performed at the Big Explosives Experimental Facility would not initiate an event sequence at the repository.
- No basis is provided for the conclusion that the probability of an explosion in Area 27 complex is one in 10,000,000 per year.
- No justification is provided for why Storage and Disposition of Weapons-Usable Fissile Materials would not affect the repository.
- No basis is provided for the conclusion that the worst sequence from an accident at the Joint Actinide Shock Physics Experimental Research would be minor local contamination.
- Information provided for the Next Generation Radiographic and Magnetic Flux Compression Generation Facilities relies on a conceptual description in an environmental impact statement published in 1996.

RAI #9

Justify the applicability of failure data (failure modes, failure probability etc.) used in the SAPHIRE models (see, for example, “YMP Active Comp Database.xls” included in Attachment H to BSC, 2008b for the active equipment or components of the Canister Receipt and Closure Facility). Specifically,

(a) Demonstrate that a probability of failure for equipment or a component used in the PCSA is consistent with the failure mode quantified in the active component. Examples include, but are not limited to:

- Explain how the failure probability of 2.7 x 10^{-5} (or 2.75 x 10^{-5}) and the error factor of 5 account for the interlock failure modes for the various scenarios identified throughout the preclosure safety analysis.
- Figure B4.4-11 of BSC, 2008b identifies Canister Transfer Machine (CTM) slide gate interlock failure and associates it with obstruction detection failure; Table B4.4-6 of BSC, 2008b describes the failure as, “CTM slide gate interlock failure.” It is not clear how a failure of this interlock contributes to obstruction detection failure.
- Figure B9.4-1 of BSC, 2008b identifies CTM slide gate interlock failure and associates it with the slide gate being open and the CTM moving, Table 6.3-1 of BSC, 2008b describes the failure as, “Slide Gate Interlock Fails.” It is not clear how a failure of this interlock contributes to the CTM moving with the slide gate open.
- For the interlock failure probability, explain how the assumption of one demand every 8 hours is applicable throughout the surface facilities and explain how assumptions such as these are tracked to ensure the failure probability is applied correctly.

(b) Demonstrate that DOE consistently implemented the criterion (i.e., matching the component type and failure mode from the data source to the basic event in the fault tree), identified on Page C-15 of BSC (2008b), in developing the failure data included in the file “YMP Active Comp Database.xls” included in Attachment H to BSC (2008b) and in other data sets. Examples of instances where the implementation of this criterion is unclear include, but are not limited to:

1) For the Canister Transfer Machine holding brake failure to hold (BRK-FOH), DOE includes a description for the data source that refers to the AN/BQQ-5 system installed on the SSN-690.
2) For the Canister Transfer Machine load cell pressure sensor failure on demand, (SRP-FOD), DOE includes a description for the data source that refers to data collected from a hotel, motel, casino, or resort facility located in Coronado, CA.
3) For the Canister Transfer Machine sheaves failure (BLK-FOD) or the Canister Transfer Machine grapple failure on demand (GPL-FOD), DOE includes a description for the data source that refers to a 5-ton cargo truck in which the data was converted from miles to hours using a factor of 2 miles per hour.
4) To estimate the probability of a collision developed for the Site Prime Mover, DOE considers the use of escort vehicles and information for vehicle travel on

roads with speed limits between 20 and 45 mph. Explain how these data are applicable to operations involving the Site Prime Mover (and other vehicles) on intra-site roadways.

(c) Justify the applicability of the failure data from NUREG-1774 to the Waste Package (WP) Handling Crane in the Canister Receipt and Closure Facility. For example, DOE assigns a mean probability for a drop of 1.05×10^{-4} (Basic event 060-WPCRN-DROPON-CRW-DRP in Table 6.3-1 of BSC, 2008b) and a mean probability for a two-block event of 4.49×10^{-5} (Basic event 060-WPCRN-DROPON-CRW-TBK in Table 6.3-1 of BSC, 2008b), based on data from NUREG-1774. However, it is not clear how the NUREG-1774 data are applicable to the WP handling crane. Instances requiring clarification include:

1) Table 12 in NUREG-1774 lists the facilities and the crane type. It does not classify cranes in all cases as single-failure-proof and non-single-failure-proof. It uses terminology such as, "Meets NUREG-0612," or "Meets 0612 crane upgrade requirements." Explain how the Waste Package Handling Crane meets the classifications identified in NUREG-1774.
2) For the drop value, explain how the events identified in NUREG-1774 relate to the Waste Package Handling Crane, its design, and its operations.
3) For the two-block value, explain how the event in NUREG-1774 relates to the Waste Package Handling Crane, its design, and its operations.

(d) Justify the applicability of the data from NUREG-1774 and "Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999" (Framatome, 2001) to the Spent Fuel Transfer Machine in the Wet Handling Facility. For assembly drops involving the Spent Fuel Transfer Machine in the Wet Handling Facility, DOE assigns a mean failure probability of 5.15×10^{-6}. This value is based on data from NUREG-1774 and Framatome (2001). Instances requiring clarification include:

1) Explain how information since 2002 has been considered in the analysis and explain how DOE has considered available data in addition to that contained in NUREG-1774 and Framatome (2001).
2) Explain how DOE has considered fuel assembly slips in addition to fuel assembly drops. For example, Page A-29 of NUREG-1774 refers to a load slip involving fuel assemblies. In addition, Page A-44 of NUREG-1774 indicates a fuel bundle drifted past its stop point and contacted the refueling floor.
3) In calculating the mean failure probability, DOE considered seven drop-events from 1985 to 2002; however, NUREG-1774 identifies twelve events in Table 4 during that period. Explain which events DOE identified and explain why those events pertain to drops in the Wet Handling Facility from the Spent Fuel Transfer Machine.
4) DOE identifies seventeen events as an upper bound on the number of drops. Explain what events DOE identified for this upper bound and why those events

pertain to drops in the Wet Handling Facility from the Spent Fuel Transfer Machine.

5) Explain how DOE considered the likelihood of an assembly drop when transferring spent fuel versus transferring new fuel since drops involving both spent fuel and new fuel are identified in NUREG-1774.

(e) Explain how the selection of one failure distribution, when several sources of data are available, is consistent with the use of Bayesian estimation to combine multiple data sources, as described on Page 143 of BSC (2008b). For example, for interlock failure on demand (i.e., IEL FOD), five distributions are identified in "YMP Active Comp Database.xls." Rather than combining the data from these multiple sources, DOE only used one data source.

(f) Provide the technical basis for the error factors used in the resulting distributions for active component failure data when exposure data are not available. For example, for interlock failure on demand (i.e., IEL FOD), as indicated in, "YMP Active Comp Database.xls" included in Attachment H to BSC (2008b), five distributions are identified which do not include exposure data. Each of the distributions has an error factor equal to 5.

(g) For basic event 050-OpDPCShield2-HFI-NOW (Operator Causes Loss of Shielding during DPC Cutting) justify that the radiation monitor has a mean failure rate of 2×10^{-5} failures per hour. DOE indicates this failure rate is based on a vendor brochure (Item SRR-FOH in "YMP Active Comp Database.xls" included in Attachment H to BSC 2008h). Provide the vendor information to show how this failure rate was determined. In addition, explain how DOE determined the error factor for this failure rate. DOE considered data from the Institute of Electrical and Electronics Engineers, Inc. (IEEE) Standard 500 (1991) for a radiation sensor but did not use this information as indicated in file, "YMP Active Comp Database.xls." The file, "YMP Active Comp Database.xls" included in Attachment H to BSC, 2008h shows a value for the upper limit that appears to be erroneous (e.g., the upper limit is less than the mean and the lower limit.) and the description for this item indicates that, "Calculated EF of 0.5 would not run in MathCad Bayesian Estimation therefore used EF of 2."

Framatome ANP (Advanced Nuclear Power). 2001. "Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999." Lynchburg, Virginia: Framatome Advanced Nuclear Power.

RAI #10

Demonstrate that the representation of events in the preclosure safety analysis is consistent with the operations at the GROA facilities. When operations are described and equipment is described with the operations, it is not always clear if the equipment is being credited with safety and should be identified as important to safety (ITS). If a structure, system, or component (SSC) is being relied upon to perform a safety function in an operation, identify that SSC and state whether or not it is ITS. Areas requiring further explanation include:

(a) Demonstrate that operations and maintenance actions were applied consistently when developing initiating events. Some examples follow:

- Page B-6 of BSC, 2008a indicates that the slide gate interlock is bypassed on the CTM when the lid is lifted for non-DPC canisters. For the ESD18 initiating event fault tree, DOE considers failure to reset the interlock following maintenance as a basic event in the case of a DOE Standardized Canister but does not include this basic event for waste forms other than the DOE Standardized Canister. In addition, it is not clear how DOE considers the failure to restore the interlock during normal operations as a result of bypassing it for lid removal.
    - Figure B4.4-11 of BSC, 2008b identifies CTM slide gate interlock failure but does not include consideration for operator failure to reset the interlock following maintenance.
    - Figure B9.4-1 of BSC, 2008b identifies CTM slide gate interlock failure and includes consideration for operator failure to reset the interlock following maintenance.
- For human failure event, 060-OpStageRack1-HFI-NOD, the description in BSC, 2008b indicates that a worker enters the Transfer Room during normal activities. Explain when operators enter the Transfer Room during normal activities for each of the waste forms being processed.

(b) Demonstrate that the quantification of basic events and their implementation in the fault trees is justified in terms of the operations being performed. For example,

- It is not clear how many demands are placed on the Canister Transfer Machine holding brake per canister lift or object lift and how the combination of these two events is performed consistently in, for example, the CRCF ESD09 fault trees.
- It is not clear how many times the port slide gate is operated per canister or object lift in, for example, the CRCF ESD18 fault trees.
- Explain how the value for object lifts (e.g., 060-CTMOBJLIFTNUMBER in Table 6.3-11 of BSC, 2008b) and the associated fault trees involving a drop onto a canister account for both the Canister Transfer Machine and the Waste Package Crane that is referred to in Table 6.3-11 of BSC, 2008b.
- Explain how the operations, described at Table E6.7-1 of BSC, 2008h for basic event 050-OpDPCShield2-HFI-NOW, are consistent with the description on page E-195 of BSC, 2008h. Clearly identify the equipment and activities that are relied on to reduce the probability that a worker from receiving a direct exposure.

- For cask preparation activities in the Canister Receipt and Closure Facility involving a dual purpose canister (DPC), explain the steps in the operation that are credited with preventing an operator from causing loss of shielding while installing the DPC lift fixture (060-OpDPCShield1-HFI-NOW). DOE indicates the following on Page E-82 of BSC (2008b): "There are no written, formal procedures that the crew has in front of them during cask preparation; the procedures for how to handle a DPC come from training."

(c) Explain how different fault trees and human failure events account for operations that appear to be similar. Examples include, but are not limited to:

- Explain the difference between processing DOE standardized canisters and the other waste forms that are being accounted for in initiating event trees ESD18-TMP-SHLD-LOSS-DSTD (for DOE standardized canisters) and ESD18-TEMP-SHIELD-LOSS (for other waste forms).
- Explain why the probability that an operator fails to close a port slide gate is 0.01 for Basic Event 060-OpCTMImpact1-HFI-COD but is 0.008 for 060-OPStageRack1-HFI-NOD (refer to pages E-150 and E-165 of BSC, 2008b).

(d) Explain how DOE considered simultaneous operations in the Canister Receipt and Closure Facility when developing initiating events for the facility. This includes activities in the Preparation Area, Transfer Room, and Loadout Room. For example, explain how DOE considered the potential for personnel that may be performing activities associated with one Canister Transfer Machine (for example, grapple removal) to get an exposure due to someone else's failure to perform some activity associated with operations related to the other Canister Transfer Machine.

(e) Explain how fuel assembly collisions (i.e., an assembly collides with some object or with another assembly) were considered in the Wet Handling Facility. Identify the equipment, components, or procedures that are credited with preventing fuel assembly collisions. Explain how DOE ensures that an assembly is fully lowered into its location in the staging rack.

(f) For all of the handling equipment that is used in the surface facilities to transfer an assembly or a cask (e.g., the Cask Transfer Trolley and the Cask Handling Crane in the Wet Handling Facility) identify the safe load paths and identify the equipment, components, or procedures that are relied on to prevent the equipment from operating outside its safe load path. For example, for WHF-ESD14-DPC, the description of the event sequence involves the movement of a cask containing a DPC from the Unloading Room to the Preparation Station. The human error description associated with this event sequence involves the use of two guide rails and an end stop to keep the Cask Transfer Trolley on the safe load path in Table E6.5-1 on Page E-93 of BSC, 2008h. Explain where the guide rails are and where the safe load paths are for operation of the Cask Transfer Trolley in the Wet Handling Facility. Justify that handling equipment cannot inadvertently come in proximity to the Decontamination Pit, the pool, or other facility structures and what measures are in place to prevent the handling equipment from moving to these areas.

(g) Explain how the following actions were included in the initiating events for the Canister Receipt and Closure Facility and what equipment and components are credited with these actions. Explain if these actions were included in the HAZOP analyses that were performed and explain how DOE determines that it has identified all of the hazards and initiating events for all preclosure operations.

1) Alignment of cask in the Cask Unloading Room prior to unloading a cask by the Canister Transfer Machine.
2) Alignment of the waste package in the Waste Package Positioning Room prior to loading a waste package using the Canister Transfer Machine.
3) Alignment of the Canister Transfer Machine over a port prior to a canister transfer.
4) Use of the guide sleeve as described on Page 1.2.4-29 of the SAR.

RAI #11

Demonstrate that the representation of events in the preclosure safety analysis is consistent with the design of the GROA facilities. If an SSC is being relied upon to perform a safety function in an operation, identify that SSC and state whether or not it is ITS. Specific examples requiring further explanation include:

(a) For cask preparation activities in the Canister Receipt and Closure Facility involving a dual purpose canister (DPC), demonstrate that the design of the preparation platform and shield plate prevent an operator from inadvertently displacing the lid (i.e., Basic Event 060-Liddisplace1-HFI-NOD). Identify the actions and their order that are being performed and identify the SSCs involved with screening this basic event and specify whether or not they are identified ITS.

(b) Justify that the Transport and Emplacement Vehicle (TEV) doors cannot be inadvertently opened while transferring a waste package to the underground. The following needs clarification:

- DOE indicates the doors are prevented from being actuated unless the TEV is, "… near to the WP loadout area or an emplacement drift" (BSC, 2008l). DOE indicates that the front shield door interlocks are disengaged, "… after receiving confirmation on positioning from control" (BSC, 2008l). Explain what this confirmation entails, what systems and equipment are involved, and whether or not they are ITS.
- DOE describes a stationary actuating bracket located along the rail lines at the waste handling buildings or inside the emplacement access doors that is used to deactivate the TEV shield door interlock on entry and activate it on exit via an ITS switch located on the TEV. Explain how DOE determines that the interlock is

activated on exit from a waste handling building and how DOE determines that the interlock is not inadvertently deactivated during transit, and what actions the TEV takes or operations personnel take if the interlock is not active during transit.

(c) Justify the assertion that slide gate motors have insufficient power to significantly damage a canister. DOE describes in Table 6.0-2 of BSC, 2008b that damage to a canister resulting from a side impact of a slide gate is screened out based on the motors on the slide gates having insufficient power to significantly damage a canister. Clarify whether the slide gate motor power is reflected in the determination of SSCs ITS.

(d) DOE describes in Table 6.0-2 of BSC, 2008b that a canister drop inside the shield bell of the Canister Transfer Machine with the slide gate closed would be subsumed by drops from the operational height. Explain if credit is taken for the slide gate, shield bell, and shield bell trolley to maintain their integrity and support a canister that is dropped within the shield bell. It is not clear if, for example, the shielding would remain in tact and whether or not a direct exposure could occur. It is not clear if the shield bell, shield bell trolley, slide gate, and any associated components are designed to support the full weight of a canister.

(e) For the Canister Transfer Machine Adjustable Speed Drive (ASD), explain how the failure of the ASD is captured by the failure probability of the, "Canister above CTM slide gate optical Sensor" failure shown in Gate 36-184 ("op event with two block event") fault tree included as Figure B4.4-17 of BSC, 2008b.

- Figure 1.2.4-51 of the SAR shows not only connections involving the, "Canister Clear of Slide Gate" sensors but also connections to an interlock, brake solenoid for the holding brake, electric motor, and canister hoist position encoder. Explain if failure of these other components can affect the system.
- Explain how the holding brake and electric motor shown in Figure 1.2.4-51 of the SAR respond to a signal from the ASD.
- Explain how DOE accounts for failure associated with the control software on the ASD.

RAI #12

Demonstrate that the description of failure events described in Section 6 and Attachment E of BSC 2008l (and BSC 2008b, BSC 2008d, BSC 2008f, BSC 2008h, and BSC 2008j) are consistent with the SAPHIRE models documented in Attachments B and H. Specific examples include:

a) Justify the initiating event failure probability for the TEV involving the inadvertent opening of TEV shield doors and prolonged immobility resulting in shielding loss. Instances requiring clarification include:

(1) For inadvertently opening shield doors, DOE considers human error, interlock failure, and spurious operation of the Programmable Logic Controller (PLC) or shield door actuators.

- Explain how spurious operation of the PLC captures all the failure modes from the PLC that could result in a signal to open the doors. Explain if the interlock and the PLC are independent, or if there is a dependency, explain if this dependency can result in a single point of failure. Clarify if the PLC is identified ITS and explain if software errors can result in the inadvertent opening of TEV shield doors.
- DOE assigns a mission time of 4 hours for most of the basic events having a time-based failure rate [Page 113 of BSC (2008l)] and associates this mission time with loading a waste package in a facility or emplacing it in a drift. DOE identifies an 8-hour mission time for transit. Provide justification for assigning a 4-hour mission time to basic events involving inadvertently opening the TEV doors.
- DOE describes a human failure basic event (i.e., 800-HEE0-TEVDOOR-HFI-NOD) in Table E6.2-2 of BSC, 2008l in which operators are assumed to be highly trained, the shield doors are opened semiautomatically, and the control for opening the shield doors is expected to be, "quite distinct from the other TEV controls" (BSC, 2008l). Explain what is meant by "semiautomatically" and explain how the assumptions included in this human failure event (e.g., control for opening the shield doors being quite distinct) are tracked to ensure they are incorporated into the design.

(2) For prolonged immobility, DOE considers TEV fan failure, PLC spurious operation, overspeed sensor failure, loss of offsite electrical power, and failure of the third rail system.

- Explain how spurious operation of the PLC captures all the failure modes from the PLC that could result in prolonged immobility. Explain if there are any other failures such as the failure of an interlock which could also result in the TEV going to an immobile state. Clarify if the PLC is identified ITS and explain if software errors can result in prolonged immobility.
- Explain how the TEV fan failure is accounted for. Page B1-41 of BSC, 2008l identifies failure of the TEV fan as a basic event; however, Table B1.4-9 of BSC, 2008l does not include TEV fan failure as a basic event.
- For the overspeed sensor failure, DOE includes failure rate data pertaining to temperature sensors as indicated in, "YMP Active Comp Database.xls" included in attachment H to BSC, 2008l. Clarify how temperature sensor data is applicable to overspeed sensors on the TEV.
- For the third rail failure, DOE includes information from the Federal Railroad Administration Safety Data website. DOE refers to calculations in, "third rail failure estimate.xls" referenced in, "YMP Active Comp Database.xls" included in attachment H to BSC, 2008l. Provide "third rail failure estimate.xls;" provide the information referred to on the Federal

Railroad Administration Safety Data website; and explain how the information on this website is applicable to failure of the third rail resulting in prolonged immobility of the TEV.

- For loss of offsite power, DOE identifies a mean failure probability of 7.94 x 10^{-6}. Explain how this value was determined.
- DOE assigns a mission time of 4 hours for most of the basic events having a time-based failure rate [Page 113 of BSC (2008l)] and associates this mission time with loading a waste package in a facility or emplacing it in a drift. DOE identifies an 8-hour mission time for transit. Provide justification for assigning a 4-hour mission time to basic events involving prolonged immobility and provide justification for assigning both 4-hour and 8-hour mission times to basic events in the same fault tree in which prolonged immobilization of the TEV is modeled.

b) For collisions involving the Site Prime Mover while entering a facility, explain how the SAPHIRE model captures the failure of the Site Prime Mover. The following information is not clear:

- Explain how the governor, identified in the fault tree model, is involved during movement into a facility. DOE describes on Page B1-22 of BSC, 2008j that the maximum speed of the Site Prime Mover is controlled by a governor on the diesel engine for outside movement; however, for in-facility operations, speed is controlled by the physical limitations of the drive system. Our understanding is that the governor would not be involved with the movement into a facility based on the information on page B1-22 of BSC, 2008j.
- For speed control failure and brake failure, DOE calculates mean failure probabilities based on data for a 5 ton cargo truck and converts the data from miles to hours using a factor of 2 mph. Explain how this conversion relates to the Site Prime Mover given that it is limited to 9 mph within the GROA and 2.75 mph while approaching handling facilities as described on Page 1.2.8-37 of the SAR.

For control system failure, DOE identifies the possibility that the remote control transmits the wrong signal as shown in Figure B1.5-9 of BSC, 2008j. This figure shows a mean probability of 1.74 x 10^{-3}. The MathCad file, “HC FOD Hand Controller Demand Failure.xmcd” shows a mean value of 2.85 x 10^{-3} and error factor of 142.7. Clarify how DOE determined the distribution for this basic event. In developing the distribution, DOE considered failures associated with a dead man stop handle, the emergency stop button controller failure to stop on demand, mechanical jamming of a controller, and speed selector failure. Explain how these component failures relate to the failure modes identified for the remote control transmitting the wrong signal.

c) Justify that the correct initiating event branch was screened out for the case of a drop of a heavy object onto an HLW canister identified as branch #6 of the initiator event tree (i.e., CRCF-ESD09-HLW) described in Table 6.0-2 of BSC, 2008b, p. 101. Instances requiring clarification include:

(1) Explain if branch #2 in Figure A5-43 of BSC (2008b) is being screened out. Justify a value of 0 for basic event “HLW Canister Fails from Dropped Cask” included in Table 6.3-8 of BSC, 2008b, p. 180.

- One of the basic events for CRCF-ESD09-HLW is identified as 09-HLW-FAIL-LID-IMPACT. Table 6.3-8 of BSC, 2008b identifies this basic event as, “HLW Canister Fails from Dropped Cask,” associates a value of 0 for it, and specifies the condition as, “HLW Canister fail-Dropped lid.” In addition, Table A4.9-3 of BSC, 2008b, p. A-53 associates the initiating event, “ESD9-HLW-LIDIMP,” with basic event “09-HLW-FAIL-LID-IMPACT,” and Figure A5-43 of BSC, 2008b identifies this initiating event as branch #2.

(2) Explain the difference between branch #2 and branch #6 of the initiator event tree and explain whether or not DOE screened branch #6 as indicated in Table 6.0-2 of BSC, 2008b.

- Page B4-43 of BSC, 2008b under Section B4.4.3, “Drop of Object onto Canister,” indicates that, “Transfer operations using the CTM entail the possibility of inadvertent drops of objects onto canisters. Cask lids, handling equipment and auxiliary grapples are handled during the canister transfer process.” Figure A5-43 identifies, “Object Dropped on Canister,” as branch #6 of the initiator event tree. In addition, page A-50 of BSC, 2008b in Section A4.9.1, “Initiating Events for CRC-ESD-09,” indicates that an impact associated with lid removal, “… covers the potential impact during cask or aging overpack lid removal due to a human failure to remove all of the lid bolts.” Our understanding is that this is branch #2 of the initiator event tree (Figures A5-42 and A5-43 of BSC, 2008b). In this same section, for an object dropped on a canister, this initiating event “… covers the potential impact to the canister due to the drop of a heavy object (e.g., cask lid) by the CTM.” Our understanding is that this is branch #6 of the initiator event tree (Figures A5-42 and A5-43 of BSC, 2008b).

(3) Explain how branch #6 of the initiator event tree (CRCF-ESD09-HLW) accounts for the drop of a HLW canister or DOE SNF canister onto a HLW canister as described in Table 6.0-2 of BSC, 2008b.

d) Clarify whether a TEV runaway initiating event has been screened out in BSC 2008l. Table 6.0–2 shows SSO–ESD–03–SEQ–2–3 has been screened out due to low probability of occurrence, but SSO-ESD-02 appears to include consideration of a TEV runaway event.

RAI #13

Identify where in the referenced source documents the initiating events listed in SAR Table 1.6-3 can be identified and how these are linked to the Master Logic Diagrams. For example, it is not clear how to trace through the SAR and supporting documents, “Impact from platform operations – 1” separately from “Impact from platform operations – 2” identified in this table on page 1.6-54 of the SAR.

RAI #14

Justify that event sequence frequencies accurately capture the frequency for events or bound the frequency for events that may span more than one waste form and potentially more than one facility. For example, ESD18 in the Canister Receipt and Closure Facility involves a direct exposure during transfer operations with the Canister Transfer Machine. There are separate event sequence frequencies for different waste forms; however, the events are similar regardless of the waste form. In addition, ESD12A in the Initial Handling Facility also involves a direct exposure during transfer operations with the Canister Transfer Machine. The events are similar in this case, regardless of whether the event is in the Canister Receipt and Closure Facility or the Initial Handling Facility.

RAI #15

(a) Confirm that all of the supporting files for the SAR were completed. Explain the comments in File “000-PSA-MGR0-00900-000a09-Mar-11-2008.xls” included in Attachment H to BSC, 2008j:

- On tab, “Data Page,” with reference to, “TC w/UCSNF,” a note indicates, “changed Feb 26, per MVF, Waiting for documentation that UCSNF comes in only on TT.”
- On tab, “ESD01,” a box indicates, “No UCSNF on Railcars,” and a note indicates, “Pending referencable documentation that states UCSNF arrives only on truck trailers.”

(b) For the SAPHIRE files provided as Attachment H to BSC, 2008h (and similar documents), explain which ones are applicable to the review and confirm that work has been completed on the SAPHIRE models in particular for files having the word, “Draft” in their title. Some examples follow:

- The SAPHIRE files for the IHF include, “IHF FOR LA.SRA” and “IHF.SRA.”
- The SAPHIRE files for Intrasite fault trees include, “intrasite Oct 07.sra” and “INTRASITE-FEB-08.SRA.”

- The SAPHIRE files for the WHF include, “WHF – Vol. II Draft.sra” and “WHF---VOL-II-DRAFT.SRA.”
- The SAPHIRE files for the Subsurface include, “FaultTreesCRCF.sra” and “YUCCA-MOUNTAIN.SRA.”

RAI #16

Demonstrate that internal flooding for surface facilities is appropriately screened from consideration. Specifically,

(a) Justify that the screening of internal flooding in the surface facilities is supported by the design of the individual facilities and the design of equipment in the facilities. DOE screens internal flooding in the surface facilities. As part of the screening argument, DOE indicates that, “Casks are elevated … [at] all times at least five feet above the floor by railcar, truck, or canister transfer trolley” [BSC, 2008b and BSC, 2008h]. Clarify the height of the cask at Preparation Station #1, Preparation Station #2, and the TAD canister closure station of the Wet Handling Facility.

(b) Justify that the screening argument for internal flooding is applicable to each of the surface facilities and identify the components and equipment that are relied on to prevent internal flooding and state whether or not they have been identified as ITS. DOE provides a similar argument for screening internal flooding in each of the surface facilities. It is not clear that the screening argument takes into account the differences among the facilities. For the Wet Handling Facility, the screening argument is on Page 104 of BSC, 2008h.

- Explain how DOE considers workers being exposed due to the rupture of piping that is part of the Pool Water Cooling Subsystem. DOE indicates on page 1.2.5-37 of the SAR that, “The pool water cooling heat exchangers are located in Room M001, 20 ft above the ground floor.” In addition, on page 1.2.5-42 of the SAR, DOE indicates that, “… pool equipment is stationed at elevations above the pool ….”
- Explain how DOE considers failure of the pool level control in terms of internal flooding. On page 1.2.5-40 of the SAR DOE refers to automatic controls, the digital control and management information system (DCMIS), an alarm in the Central Control Center, the ability to open the makeup valve from the facility operations room, and manual local operation of a bypass valve.

(c) Justify the inherent assumption that hardwired interlocks would not be susceptible to failure due to internal flooding and water impingement during an internal flooding event. On page 105 of BSC 2008b, DOE has considered potential hot shorts in control boxes from flooding; however, DOE has credited the hardwired interlocks between the Canister Transfer Machine’s slide gate, shield bell skirt, and shield doors to prevent any inadvertent motion, even during an internal flooding event.

RAI #17

(a) Justify why the doors of the emplacement drifts, discharge pump, construction barrier, and shotcrete seal would not be classified as items important to safety in SAR Table 1.9–1 Preclosure Safety Classification of SSCs. As part of the screening argument for internal flooding in the subsurface facilities, DOE has identified emplacement drift doors that would prevent water splash from contacting waste packages, barriers at the front of each emplacement drift, a discharge pump that would pump water out of the tunnel, a construction barrier, and Shotcrete seal (BSC, 2008l). In addition, on page 101 of BSC (2008l), DOE indicates that, "In the event of a flood, portal security personnel can isolate flow to the tunnel (underground communications are provided during construction operations)."

(b) Explain what anecdotal information was obtained on water pipe breaks in construction tunnels and define what was meant by "unusual" in terms of performance requirements in BSC, 2008l (page 101, 3rd full paragraph).

(c) Justify the conclusion that the amount of water available for internal flooding is insufficient to rise to the waste package elevation in the emplacement drifts. This is needed to assess whether failure of water supply pipes to the Tunnel Boring Machine could cause water build up high enough on the construction side of the isolation barrier. The accumulated water may flow down the access main to the emplacement side and enters the drifts with emplaced waste packages. Calculations provided in BSC, 2008l, Section 6.04 seems to assume that the isolation barrier is always at the intersection of the emplacement drift and access main, which is inconsistent with the information in SAR Section 1.3.1.2.7 and SAR Figure 1.3.1–12. The calculations could have underestimated the potential maximum water levels as a result of this assumption.

(d) Justify why a loaded Transportation and Emplacement Vehicle (TEV) near the intersection of the access main and emplacement drift would not be affected during an internal flooding event. This is needed to assess whether an internal flooding event can affect a loaded TEV during transit in the subsurface facility.

RAI #18

Provide the maximum residence time of a waste package in a TEV without exceeding the maximum operating temperature for TEV shielding. The applicant identifies thermal degradation of the TEV shielding as a potential occurrence if a loaded TEV were to stop for an extended period of time (BSC, 2008l, Section B1.4.5). The applicant estimated about 8.5 occurrences of extended stoppage of the TEV during the preclosure period

(BSC, 2008l, Calculation “Subsurface Quantification BACKCHECK UPDATE LOCKED 03-10-08.xls”) but screened out this branch of event tree SSO-ESD-04 on the basis of a zero probability for loss of shielding. The applicant screened out thermal degradation of the TEV shielding because of a requirement established by the applicant that the shielding be designed to sustain the thermal loading for all waste package loadings over an extended period of time without significant degradation of the shielding function. The design requirement, however, includes undefined terms such as “extended period of time” and “significant degradation”.

RAI #19

Provide information on probability of occurrence of an initiating event related to improper material selection for neutron absorber plates/tubes.

According to SNL (2007) Section 6.2.6, the WHF pool CSNF staging racks would contain neutron absorber plates. Many canisters and casks containing neutron absorber plates/tubes will be processed in WHF, will be filled up with and/or immersed in water. SNL (2007) Section 6.3.2 analyses estimate that material selection error during manufacturing process may exceed 10^{-4} per selection event (i.e., single plate/tube manufacturing). This analysis is used to quantify the improper performance of the neutron absorber plates (SNL, 2008, p. 6-823). The total number of manufactured plates used in canisters and casks (i.e., number of selection events) is expected to be very large. If wrong (i.e., out-of-specification) material is selected for neutron absorber plates used in the WHF pool, in canisters, and casks to be processed at WHF, the neutronic reactivity of the corresponding system might potentially increase reducing subcriticality margin of safety.

Sandia National Laboratories 2007. "Analysis of Mechanisms for Early Waste Package/Drip Shield Failure". ANL–EBS–MD–000076 Rev 00. Las Vegas, Nevada: Sandia National Laboratories.

Sandia National Laboratories 2008. “Features, Events, and Processes for the Total System Performance Assessment: Analyses.” ANL–WIS–MD–000027. Rev. 00. Las Vegas, Nevada: Sandia National Laboratories.

RAI #20

a. Justify how ‘boron dilution’ was considered in event sequences, HAZOP, and MLD. Identify any boron dilution initiated event sequences.
b. For screening of boron dilution as an initiating event, explain why DOE did not consider:

1. Introduction of non-borated water into the pool in the WHF internal flooding screening argument,
2. Inadvertent reduction of injected boron,
3. Under enrichment of injected boron (Ex: using natural boron by mistake),
4. Boron dilution/loss of concentration when evaluating dual purpose canister fill water.

c. Describe in detail how PSC-9 is implemented and justify the frequency of failure of the planned safety controls. It appears that these are administrative controls and even if independent, it is unclear how these would justify screening this out. Provide the basis for the PSC-9 development if the boron dilution event initiating event was screened out in SAR Table 1.7-1.

d. Justify the handling of the potential criticality condition as accounted for in HAZOP and explain and justify what is considered as part of the “Adequate boration concentration in pool maintained” and why it or a similar pivotal event/parameter is not used for fill water (Nodes 18 and 21).

SAR Section 1.14.2.3.3.3 references Table 1.7–1 that justifies screening stating that “There are no water sources in the WHF that could lead to a decrease of the boron concentration in the WHF pool to a level posing a criticality concern during normal operations.” No justification is provided for this statement. According to the SAR Section 1.6.3.4.7 there are three underground wells which supply an 850,000-gal water storage tank. This water will be used as makeup water for the WHF pool, for fire-suppression system, and for chilling HVAC system. BSC (2008h) Section 6.0.4 lists fire-suppression system, “water carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems” as potential sources of water in WHF. The screening basis presented in Table 6.0.2, however, lists only an insignificant source of water in Room 1016. The inadvertent increase of water flow from the makeup system, influx of water from chilling HVAC system or fire suppression system, clogged drainage system, the decrease of the amount of injected boron, under-enrichment of boron, and non-homogeneity of boron dilution in water might potentially lead to effective dilution of the neutron absorber or overflow. No information is provided on whether inadvertent reduction of injected boron and/or under-enrichment of injected boron are potential initiating events.

The possibility of boron dilution was not considered in the HAZOP or MLD evaluation of the DPC fill water. The applicant analyzes other events and parameters related to DPC fill water in Figure D-16 and Table E-19 of BSC (2008g).

RAI #21

Demonstrate that potential critical conditions that could occur without breach are accounted for in the screening process.
Justify:

1. How the IHF cask/canister mechanical handling would prevent more than two naval canisters from interacting.
2. Screening out interaction between more than four DOE SNF canisters in the CRCF, and provide information on those human actions and design solutions that are credited in screening out this initiating event.

Some of the DOE SNF does not require the introduction of moderator to reach an ‘important to criticality’ end state. However, there are no initiating events that deal with this nor is it clear how these initiating events were screened.

RAI #22

Provide the technical basis for the selection of different HRA methods. Specific questions include:

(a) DOE provides a discussion on the selection of human reliability analysis (HRA) methods for detailed quantification in Appendix E.IV of BSC (2008b). In this discussion, different HRA quantification methods are assessed to be options for use in the HRA quantification or of no use. Of the methods that are identified as options, provide information on how or why a particular method is used for a specific human failure event.

(b) Provide justification, on a human failure event (HFE)-specific basis, for the use of multiple HRA quantification methods (e.g., use of NARA and CREAM for different unsafe actions or sub-scenarios that make up an HFE).

(c) In basic event 060-OPDPCSHIELD1-HFI-NOW, Scenario 1b of BSC (2008b), justify why NARA was used to model the error of commission for the first unsafe action.

RAI #23

Demonstrate that dependencies have been adequately captured in the HRA. Specific examples include:

(a) Provide information on any consideration of historical experience that shows dependencies between an initial failure and subsequent “independent” checks.

(b) For the basic event 060-OPSTAGERACK1-HFI-NOD in BSC (2008b), explain why potential dependencies between the two unsafe actions (involving an initial failure, followed by a failure to identify this failure) have not been considered.

(c) For the HFE 060-OpDirExpose3-HFI-NOD in BSC (2008b), explain how the dependencies among the crew member events were considered in the human error probability (HEP) calculation displayed by Equation E-50 of BSC (2008b). Events A, E, and F appear to involve the same crew member, and if so, would have a dependency. It is not clear how this dependency is accounted for in the calculation.

(d) Justify the dependency analysis performed for human failure events

- For HFE Group #3, 060-OPDPCSHIELD1-HFI-NOW, Scenario 1(a) in BSC (2008b), provide explanation of apparent inconsistency between assessment of “low consequence” and crew being “directly at risk.”
- For HFE Group #3, 060-OPDPCSHIELD1-HFI-NOW, Scenario 1(b) in BSC (2008b), provide explanation why Scenario 1(b) does not include consideration of dependencies issues similar to that for Scenario 1(a).

RAI #24

Explain what role the information processing model, described in Appendix E, Section E.5.1.1.4 of BSC (2008b), played in the qualitative and quantitative HRA analyses for HFEs (generically and for specific HFEs).

RAI #25

Provide information on what common factors (and potential differences) there between cranes to be used at the repository and those used in industry. Specifically, provide information that justifies the use of empirical data to represent human-caused crane drops, as opposed to performing a repository-specific HRA analysis.

RAI #26

Justify screening out HFEs, generally (e.g., 060-LIDDISPLACE1-HFI-NOD, Table A4.17-2; although cited in this context, Section 6.1 of BSC, 2008b does not address this justification need).

RAI #27

Provide results of the qualitative HRA analyses (e.g., task analyses) that justify the identification of the potential vulnerabilities for the repository facilities (and associated activities), generally, that DOE provides in the qualitative HRA results.

RAI #28

For all HFEs, whether assigned preliminary failure probabilities or analyzed using detailed HRA methods, provide qualitative HRA analysis results on the factors that are expected to effect human reliability (e.g., performance shaping factors, operating characteristics) that are: 1) specific to different operations and initiating events (e.g., HFE group) and 2) specific to HFEs, as a opposed to the five repository-generic human performance issues identified in Section E.5.2.

RAI #29

Provide documented basis, with explicit links to qualitative HRA analysis results, that justify choices made in the application of detailed HRA quantification methods (as discussed in the detailed HRA quantification section of Appendix E). For example, what qualitative HRA analysis results justify modeling HFE 060-OPCTMDIREXP1-HFI-NOD in section E6.5.3.4.5.1 of BSC (2008b) as a "…completely familiar, well-designed, highly practiced routine task performed to the highest possible standards by high motivated, highly trained, and experienced personnel, totally aware of implications of failure…."?

RAI #30

Justify selection of generic task types (GTTs) and error producing conditions (EPCs) when using NARA methodology. In particular, the choice of NARA GTT A5, instead of A1, should be explained and justified.

RAI #31

For use of CREAM methodology, justify selection of common cause failures (CCFs) and common performance conditions (CPCs). For CPCs, especially, explain why different sets are used for different sub-scenarios that address the same operation, same operator, same locations, etc.

RAI #32

In basic event 060-OPCTMDROP001-HFI-COD, Scenario 1e in BSC (2008b), explain why the error mode of activating the wrong control was not modeled.

RAI #33

In basic event 060-OPCTMDROP001-HFI-COD, Scenario 1e in BSC (2008b), provide information to explain why the error mode of skipping operational steps is modeled with CREAM as "action performed out of sequence."