RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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 2.7×10^{-5} (or 2.75×10^{-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-WPCRNDROPON-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 SFTM in the Wet Handling Facility. For assembly drops involving the SFTM 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.

1. RESPONSE

The areas for further explanation referred to in the RAI are excerpted and discussed in the response subsections:

1.1 PART (A)—COMPONENT FAILURE PROBABILITY CONSISTENCY WITH ACTIVE COMPONENT DATABASE

(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.

1.1.1 Interlock Failure Modes for Various PCSA Scenarios

- Explain how the failure probability of 2.7×10^{-5} (or 2.75×10^{-5}) and the error factor of 5 account for the interlock failure modes for the various scenarios identified throughout the preclosure safety analysis.

Response: There are two inquiries within this RAI: (1) how the failure mode accounts for interlock failures in the Preclosure Safety Analysis (PCSA) model and (2) what is the justification of the mean failure rate and error factor used for the interlock failure mode.

There are two failure modes associated with interlock failures given in the "YMP Active Comp Database_final 8 August 2008.xls" in Attachment H of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. The database is hereinafter referred to as the YMP Active Comp Database. The two failure modes are:

1) **Failure on Demand (FOD)**—This failure mode represents failure of a device to perform the function required when called upon to do so. The values stated for failures on demand have no time element and are not recognized as failures until the device is called upon to perform (i.e., change state or perform an action). Examples of these types of failures include the failure of a standby pump to start when demanded or the failure of an interlock to block an undesired signal.

2) **Failure per Unit of Time or Failure Rate (FOH)**—This failure mode represents failures of an operating component over a unit time period. These failures are immediately recognized when they occur, as the component is active and the process stops or cannot perform its intended function when the failure occurs. An example of

this failure mode is the failure of a pump to continue running once it has successfully started. However, this failure mode is not used for interlock failures in the Canister Receipt and Closure Facility (CRCF) event sequence quantification, and therefore will not be addressed further in this response.

In the YMP Active Comp Database (BSC 2009a, Attachment H), the interlock failure mode associated with a failure probability of 2.75×10^{-5} is IEL-FOD, interlock failure on demand. The RAI asks for justification of the use of this failure probability throughout the analysis. As shown in Table 1, this failure probability was appropriately used in the PCSA fault tree models to describe failures that occur in conjunction with another action (generally, an undesired operator action or a spurious signal) that would cause an undesired outcome unless the action is blocked by the interlock. In this context, the interlock failure mode used in the PCSA fault tree models is the failure to prevent an undesired result until the necessary prerequisite conditions are met. If the interlock fails to prevent the undesired result from occurring when challenged, the interlock is deemed to have failed when demanded (or "failed on demand").

Table 1. Interlock Functions

Basic Event Using IEL-FOD Template	Associated Fault Trees	Function
060-GATE-IEL001--IEL-FOD	060-INTERLOCK-FAILURE	Block limit switch malfunction
060-CTM--IMEC125-IEL-FOD	GATE-36-60	Block CTM hoist motor control failure
	GATE-36-7	Block CTM hoist motor control failure
	ESD9-MCO-LIDIMP	Block CTM hoist motor control failure
	GATE-36-132	Block CTM hoist motor control failure
	GATE-36-58	Block CTM hoist motor control failure
	GATE-20-2	Block CTM hoist motor control failure
	ESD9-DSNF-LIDIMP	Block CTM hoist motor control failure
	ESD9-HLW-LIDIMP	Block CTM hoist motor control failure
	ESD9-TAD-LIDIMP	Block CTM hoist motor control failure
060-CR---IELSKT--IEL-FOD	060-18-SLIDE-GATE-DIR-EX	Block inadvertent open command from PLC
060-CTM--SLIDGT2-IEL-FOD	GATE 36-7	Block inadvertent close command from PLC
060-CR---IEL00A--IEL-FOD	060-9-ST-SPURMOVE	Block operator error
	060-9-CTT-SPUR-MOVE	Block operator error
	060-18-SHLDDR-DIRCT-EXP	Block inadvertent open command from PLC
060-PORTSLIDEGTE-IEL-FOD	ESD19-SHIELD-RING	Block operator error
	ESD18-TMP-SHLD-LOSS-DSTD	Block operator error
	ESD18-TEMP-SHIELD-LOSS	Block operator error
060-SLDGATE-IEL-FOD	ESD18-TMP-SHLD-LOSS-DSTD	Block operator error
	ESD18-TEMP-SHIELD-LOSS	Block operator error
060-VCTO-IEL0002-IEL-FOD	HVAC007	Block operator error
060-PWRPRTGATINT-IEL-FOD	060-9-WPTT-SPURMOVE	Block operator error
26D-##EG-FLITLKA-IEL-FOD	EP-ITS-DG-A-17	Prevent improper operation of diesel fuel

Basic Event Using IEL-FOD Template	Associated Fault Trees	Function
		transfer pumps
26D-##EG-FLITLKB-IEL-FOD	EP-ITS-DG-B-17	Prevent improper operation of diesel fuel transfer pumps
060-WPTT-IELDK3--IEL-FOD	060-EQUIP-MOVE-LOAD	Block spurious control system signal
	060-9-WPTT-SPURMOVE	Block operator error
060-SPMRC-IEL011-IEL-FOD	060-1-SPMRC-COLLISION	Block operator error
060-SPMTT-IEL102-IEL-FOD	060-1-SPMTT-COLLISION	Block operator error
060-CTM-BRIDGETR-IEL-FOD	060-8-TWO-CTMS-COLLIDE	Block control system failure
060-CTM-BRIDGMTR-IEL-FOD	GATE-20-94	Block spurious control system signal
	GATE-36A-1	Block spurious control system signal
060-CTM-HSTTRLLY-IEL-FOD	GATE-20-94	Block spurious control system signal
	GATE-36A-1	Block spurious control system signal
060-CTM-SBELTRLY-IEL-FOD	GATE-20-94	Block spurious control system signal
	GATE-36A-1	Block spurious control system signal
060-CR---IEL00B--IEL-FOD	060-9-ST-SPURMOVE	Block spurious control system signal
	060-9-CTT-SPUR-MOVE	Block spurious control system signal
	060-18-SHLDDR-DIRCT-EXP	Block spurious control system signal
060-VCTO-IEL0001-IEL-FOD	HVAC007	Block operator error
060-WPTT-IEL001-IEL-FOD	060-WPTT-PRE-TIL	Block improper application of power to tilt motor
	060-WP-IMPACT	Block operator error
060-WPTT-IEL003--IEL-FOD	060-WPTT-PRE-DEPARTURE	Block spurious control system signal
060-CRWT-IEL0001-IEL-FOD	060-CRWT-RS00000-FAILURE	Block spurious control system signal

NOTE: CTM = canister transfer machine; PLC = programmable logic controller.

Table 1 shows that the basic event "interlock fails on demand" was applied consistently for all similar functions throughout the PCSA fault tree models. In this sense, interlock failure is modeled to capture the specific failure mode that contributes to the overall system failure. In the cases shown in Table 1, it is a failure to block or prevent an undesired action from occurring.

The response to the second inquiry provides justification of the mean failure rate and error factor used for the interlock failure.

The DOE utilized failure data from widely accepted industry data sources such as *Nonelectric Parts Reliability Data—1995* (Denson et al. 1994) (hereinafter, NPRD-95) and *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations* (IEEE Std. 500-1984, Reaffirmed, 1991) (hereinafter, IEEE 500) to establish failure probabilities for functional failures. These sources provide component failure data representative of operational experience from both military and industrial applications. These sources are reviewed by the analyst to determine what data sources or datasets from these sources will provide the closest approximation of a component failure rate expected when the repository facilities are placed into operation. Following construction, the performance of the systems and components will be monitored to confirm their reliability is consistent with the applicable analyses.

Some failure rates given in NPRD-95 are identified by the Reliability Analysis Center as "roll-up" values. A "roll-up" data entry is one where the failure rate is derived from multiple data sources using the data merge algorithm described in Section 1 of NPRD-95. The PCSA treats a roll-up value as a central tendency that represents the multiple datasets that compose it.

The interlock value used in the PCSA was a roll-up value from NPRD-95 and was treated as the estimated mean (i.e., central tendency). As explained in more detail in Section 1.6 of this response, an error factor of 5 was judged appropriate because, although an interlock is a well understood component, it is used in an environment for which there is limited specific experience.

1.1.2 Canister Transfer Machine Slide Gate Interlock Failure, Obstruction Detection Failure

- 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.

Response: Figure B4.4-11 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a) is Sheet 9 of the canister transfer machine Drop Fault Tree that begins with Figure B4.4-3. This figure is the portion of the fault tree that identifies failures that result in the canister being dropped due to a collision with objects in the lift path. This particular figure addresses the potential for the canister transfer machine shield bell slide gate to obstruct the lift path. This obstruction is detected through the use of an interlock to detect the slide gate position to ensure that the slide gate is fully open before the lift is allowed to begin. If the slide gate is not fully open, it represents an obstruction in the lift path. The interlock constitutes a permissive that indicates that there is no obstruction because the slide gate has fully opened.

1.1.3 Canister Transfer Machine Slide Gate Interlock Failure, Movement with Slide Gate Open

- 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.

Response: The slide gate interlock prevents the shield skirt from being raised until the slide gate is fully closed. The canister transfer machine trolley and bridge motors are prevented from operating until the shield skirt is fully raised. Thus, failure of the canister transfer machine slide gate position interlock would allow the operator to raise the skirt and move the canister transfer machine before the slide gate is fully closed.

1.1.4 Interlock Failure Probability, Application throughout Surface Facilities

- 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.

Response: The interlock failure rate derived from NPRD-95 is a time-based failure rate. An appropriate duration is needed to establish a failure probability. An estimated average duration between operational demands on the interlock was selected, based on a review of facility operations described in process flow diagrams and throughput analyses. On average over the lifetime of a facility, any specific activity (e.g., cask unloading, canister transfer) would take approximately one shift or 8 hours. This value was used for this failure probability only. The distribution assigned to these data was lognormal with an error factor of 5. This accounts for the potential variability of both failure rate and the estimated duration of 8 hours.

Assumptions such as these are applied consistently because the PCSA model takes advantage of the template feature within SAPHIRE. This feature ensures the data are applied consistently to each component type and failure mode combination specified in the analysis through the component naming scheme. The last seven characters of the basic event name identify the component type and the component failure mode. The SAPHIRE database contains templates for each component type and failure mode. Assumptions such as these are incorporated into the template data, which are then assigned to all components of the given type experiencing that specific failure mode.

1.2 PART (B)—CONSISTENCY OF IMPLEMENTING COMPONENT CRITERION WITH DATA IN THE ACTIVE COMPONENT DATABASE

(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.

Response: The process that ensures the data are applied consistently is as follows:

1) The fault trees are developed first, defining the basic events that require data.

2) The data analyst uses the guidance of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, p. C-20) to search for and select the most applicable data for the component failure mode.

In the absence of failure mode specific information, the total (all-modes) failure rates are used, which is a conservative aspect of the analysis. As with any risk analysis, this process uses the analyst's judgment combined with confirmatory reviews performed by independent analysts in accordance with project quality procedures. These data are documented in the YMP Active

Comp Database (BSC 2009a, Attachment H) for a given component type and failure mode. This information is then transferred to a template in the SAPHIRE database for that component type and failure mode. The analyst then assigns that template data to the specific component type and failure mode in the fault tree basic event. This is accomplished by using the last seven characters in the basic event ID; the characters identify the component type and the failure mode (e.g., IEL-FOD for interlock failure on demand).

1.2.1 Component Criterion Implementation, Canister Transfer Machine Holding Brake Failure to Hold

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.

Response: The canister transfer machine "holding brake failure to hold" (BRK-FOH) failure data was obtained from NPRD-95 "Generic Data Source". The electric brake failure rate data provided in NPRD-95 were obtained from a report describing field test data for an electric brake found on the AN/BQQ-5 bow-mounted spherical array sonar acoustic systems mounted on U.S. Navy nuclear submarines. Information for this component provided in NPRD-95 includes the national stock number and manufacturer. This item is described as "a device operated by electromechanical means which functions to bring to rest mechanically and/or hold at rest a load." Based on the function of the canister transfer machine electric emergency brake modeled in the PCSA, the electric brake failure data were deemed appropriate for use because the canister transfer machine electric brake is designed to hold the hoist cable or cable reel in place with a load at the end of the cable when there is a loss of power, which is similar to the design of the electric brake described in the source data.

1.2.2 Component Criterion Implementation, Canister Transfer Machine Load Cell Pressure Sensor Failure on Demand

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.

Response: The canister transfer machine load cell pressure sensor failure information was obtained from NPRD-95. The pressure sensor data in NPRD-95 were obtained from maintenance records for pressure sensors used in commercial applications that are ground fixed and provide for emergency power generation or for heating, ventilation, and air conditioning (and supporting equipment). Pressure sensor failure data in NPRD-95 is provided from eight sources. These sources include data collected from hospital facilities located in La Mesa, California and San Diego, California; data collected from a data facility located in Baltimore, Maryland; as well as the source mentioned in the RAI (a hotel, motel, casino, or resort facility located in Coronado, California). When multiple industry data sources are available for a component, an empirical Bayesian approach was used to develop prior distributions that represent the variability found across industrial applications as described in *Canister Receipt and Closure Facility Reliability*

and Event Sequence Categorization Analysis (BSC 2009a, Section 4.3.3). Eight sources of information were applied to this failure rate but they were numerically aligned such that the analysis results concentrated around a single value with little uncertainty. In such instances, as stated in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Section 4.3.3.1), the distribution is modeled using the data source that yields the most diffuse information, which would yield the largest uncertainty. For the load cell pressure sensor failure, this corresponds to the source citing two failures in 0.0894×10^6 operational hours (Denson et al. 1994), which was the information from Coronado.

1.2.3 Component Criterion Implementation, Canister Transfer Machine Sheaves Failure or Grapple Failure on Demand

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.

Response: The failure data for the canister transfer machine sheaves failure and the canister transfer machine grapple failure information was obtained from NPRD-95 under the part description "frame, structural, crossmember." This was determined to be the appropriate analogue for the structural failure aspects of the sheave and grapple reliability.

The data in NRPD-95 for the "frame, structural, crossmember" failure was obtained from a data source titled "Maintenance Management System (MIMMS) 5-ton cargo truck listing of components replaced." This data source contains data extracted from the Marine Corps Integrated Maintenance Management System database and consists of part replacement data at the first level of maintenance. The part populations listed in the part detail section are listed per vehicle rather than the entire fleet population. In addition, the data are reported on a per mile basis (rather than a per unit time basis) requiring an average velocity associated with the canister transfer machine to convert to a per unit time. A speed of two miles per hour was deemed appropriate for this conversion since this value is conservative (by approximately an order of magnitude) relative to the allowed canister transfer machine motion, which is 10 to 20 feet per minute.

1.2.4 Component Criterion Implementation, Probability of Collision for the Site Prime Mover

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.

Response: The data used are considered conservative because their use results in a higher probability of collision than would occur at the repository. The human failure event analysis of a

vehicle collision (rail car, truck trailer, horizontal cask transfer trailer, or site transporter) with an auxiliary vehicle or a structure, system, or component (SSC) is presented in Appendix E of *Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis* (BSC 2009b). The data used in this analysis are summarized in Tables E6.2-2 and E6.2-3 in Appendix E of the analysis. As described in the analysis (BSC 2009b), historical data were used to calculate the preliminary value of the basic event mean probability. These historical data were associated with the use of escort vehicles as well as vehicle travel incidents at speeds of 40 miles per hour or less. These data are taken from higher-risk environments than are expected to be found on repository roadways. The speeds at the repository will be very slow (on the order of a few miles per hour) and the use of speed-limited escort vehicles will greatly reduce the likelihood of an on-site collision. Therefore, the use of higher risk environment data (more congested traffic at higher speeds) conservatively represents the occurrences of human failure events on intra-site roadways on which speeds are limited by design.

1.3 PART (C)—JUSTIFICATION OF NUREG-1774 FAILURE DATA FOR THE CRCF WASTE PACKAGE HANDLING CRANE

(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-WPCRNDROPON-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.

Response: The Waste Package Handling Crane is classified as non-Important to Safety (ITS) under nonseismic loads. This crane is not used to handle nuclear waste; it is used to place an empty waste package onto the waste package transfer carriage. It is, therefore, not a risk significant component with respect to the PCSA.

SAR Section 1.2.2.2.1 provides the rationale for the safety classification and principal code selection for the cranes used in the surface facilities. SAR Table 1.2.2-10 lists the surface facility cranes and provides the following information: safety classification, ASME standard and crane type, and design basis ground motion level. Meeting the requirements of ASME NOG-1-2004 for a Type II crane places the waste package handling crane in the category of non-single-failure-proof cranes as identified in NUREG-1774, *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002* (Lloyd 2003). NUREG-1774 information may be divided into single-failure-proof, non-single-failure-proof, and nonspecified; the latter two categories are applicable to the waste package handling crane.

1.3.1 NUREG-1774 Failure Data Applicability, Waste Package Handling Crane Classification

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.

Response: The waste package handling crane will meet the requirements of an ASME NOG-1-2004 Type II crane (SAR Section 1.2, Table 1.2.2-10); it will not be a single-failure-proof crane. The two phrases "Meets NUREG-0612," or "Meets 0612 crane upgrade requirements" are intended to indicate that the cranes identified as such are single-failure-proof consistent with the classifications in NUREG-1774. Data used to develop the failure probabilities for the waste package handling crane excluded all data associated with cranes that met NUREG-0612 basic or upgrade requirements.

The determination of the number of challenges to non-single-failure-proof cranes was performed in the manner described in Section C1.3 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a):

> "…NUREG-1774 (Ref. C5.26, Table 12, pp. 61–63) provides a list of the nuclear power plants that had upgraded their cranes to single-failure-proof status consistent with licensee response to U.S. Nuclear Regulatory Commission (NRC) NRC Bulletin 96-02 (Ref. C5.9) which requested specific information relating to their heavy loads programs and plans consistent with the recommendations of NUREG-0554 (Ref. C5.34). This information was used to constrain the denominator of the number of very heavy load lifts from NUREG-1774 (54,000) by using a percentage of percent of nuclear power plants reporting single-failure-proof cranes out of total plants (43/109).
>
> Conversely, a separate category of non-single-failure-proof cranes for the waste package handling cranes was developed using the remaining percentage (66/109) to adjust the number of lifts…"

This division of the 54,000 heavy load lifts into lifts by single-failure-proof and non-single-failure-proof cranes results in 32,698 lifts of heavy loads by non-single-failure-proof cranes.

1.3.2 NUREG-1774 Failure Data Applicability, Drop Value for Waste Package Handling Crane Design and Operations

> 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.

Response: Of the events identified in NUREG-1774, three events were determined to be applicable to the waste package handling crane; these three events involved heavy load drops from non-single-failure-proof cranes. Two of these events were associated with the operation of cranes without a specified classification and one was associated with the operation of a non-single-failure-proof crane. The designation of the cranes involved in these events is based on the information provided by the licensees in response to NRC Bulletin 96-02 (Crutchfield 1996); this

information is presented in Tables 12 and A1 of NUREG-1774. The three events are summarized in Table 2. The detail design and operation of the heavy lift cranes will be encompassed within the population of cranes represented in NUREG-1774.

Table 2. Summary of NUREG-1774 Crane Events

Location	Date	Event
Ginna	Jul-69	An assembly was dropped (due to a crane brake failure), which included the core barrel, the thermal shield, lower core plate, and attached internals weighing about 82 metric tons (90 tons). The assembly was partially supported during its fall by the crane brake. The assembly tilted slightly as it fell approximately 1.8 m (6 ft) to a temporary storage support, which acted as an energy absorber. Evaluation of the event indicated that the crane motor overheated, the electromagnetic brake failed, and a backup mechanical brake was removed as part of a modification by Westinghouse.
Indian Point 3	Jan-71	The reactor vessel weighing approximately 402 metric tons (443 tons) underwent an unscheduled descent while it was being hoisted prior to its placement. It was not clear what caused the descent. Two failures occurred: (1) the crane cable and (2) the pinion gear bracket to base plate welds on the hoist mechanism itself. The order of the failures was not known. The time of the descent was certified to be between 15 and 60 seconds. It was concluded that no damage to the pressure vessel occurred as a result of the incident.
Indian Point 3	Oct-90	While lifting the upper core support structure weighing approximately 54 metric tons (60 tons), two fuel assemblies were found to be attached. One of the assemblies dropped into a retrieval basket when the brakes on the overhead crane were applied. A guide pin on each assembly was bent. The guide pins were most likely damaged during the previous refueling outage.

1.3.3 NUREG-1774 Failure Data Applicability, Two-Block Value for Waste Package Handling Crane Design and 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.

Response: Of the events identified in NUREG-1774, one two-block event was determined to be applicable to the waste package handling crane: a two-block initiated heavy load drop from a non-single-failure-proof crane. This event was associated with the operation of a crane without a specified classification. The designation of the crane involved in this event is based on the information provided by the licensees in response to NRC Bulletin 96-02 (Crutchfield 1996); it is presented in Tables 12 and A1 of NUREG-1774. The two-block event associated with a non-single failure proof crane is summarized in Table 3. The detail design and operation of the heavy lift cranes will be encompassed within the population of cranes represented in NUREG-1774.

Table 3. Summary of NUREG-1774 Applicable Two-Block Event

Location	Date	Event
Palisades	1970	23 metric ton (25-ton) capacity auxiliary hoist on a polar crane two-blocked when the operator bypassed the interlocks, parting the cable, resulting in the control rod drive mechanism support tube, hoist sheave, and hook to fall (0.95 metric ton (1.05 tons)). Drop/slip distance was 6.7 to 7.9 m (22 to 26 ft).

1.4 PART (D)—JUSTIFICATION OF NUREG-1774 FAILURE DATA AND FRAMATOME DATA FOR THE WET HANDLING FACILITY SPENT FUEL TRANSFER MACHINE

(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).

Response: As stated in SAR Section 1.2.5.2.2.6, the spent fuel transfer machine is classified as a Type I crane in accordance with ASME NOG-1-2004. Type I cranes typically have features such as load path redundancy, conservative design factors, overload protection, redundant braking systems, overtravel limit switches, and other protective devices to make the likelihood of a load drop extremely small.

A basic assumption of the PCSA and the SAR is that SSCs designed and purchased for the repository will be representative of the population of SSCs in United States industry-wide reliability information sources. Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population. System-level information, such as crane load-drop rates from the industry-wide information sources, is used. It is appropriate to use such information because it represents similar pieces of equipment at the system level. In addition, drawing from a wide spectrum of sources takes advantage of many observations, which yield better statistical information regarding the uncertainty associated with the resulting reliability estimates. As the repository operates, facility-specific information will be applied to this variability using a Bayesian update method.

NUREG-1774 and *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study—1985–1999* (Framatome ANP 2001) summarize industry-wide load drop information for the types of cranes representative of the spent fuel transfer machine. Individual events were screened to determine applicability to the spent fuel transfer machine.

1.4.1 Use of Post-2001 Data

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).

Response: The referenced data sources contain all of the crane drop information used to develop the crane load drop probabilities used in the facility analysis. No post-2001 data were found that were considered applicable. No other data are cited or used.

1.4.2 Fuel Assembly Slips

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.

Response: As noted on line 675 of the YMP Active Comp Database (BSC 2009a, Attachment H), the mean value (5.15×10^{-6}) was based on spent fuel drops only. Fuel assembly drops within the Wet Handling Facility pool are part of Category 2 event sequences and have very small offsite doses that are well within the performance objectives of 10 CFR 63.111(b)(2). Fuel assembly slips do not have the potential for a release and, therefore, are not initiating events.

1.4.3 Drop Events from 1985 to 2002

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.

Response: Seven of the twelve events identified for the period from 1985 to 2002 are drops associated with fuel pool handling operations. These events are identified in Table 4. In each of these events, it was determined that the cause of the event could be applicable to operation of the spent fuel transfer machine. In these events, the drop was caused by a mechanical or operator-related failure of either the transfer crane or of the attachment mechanism (e.g., grapples). These are failures that could be applicable to the Wet Handling Facility spent fuel transfer machine. The single event included in this list that is of unknown cause (the April 1997 event at Waterford) resulted in a fuel assembly drop during movement in the spent fuel pool.

Table 4. Drops Associated with Fuel Pool Handling Operations

Event	Date
Quad Cities 1	Sept. 1989
North Anna 1	Jan. 1990
Byron 2	Sept. 1990
Sequoyah 1	June 1993
Vermont Yankee	Sept. 1993
Waterford	April 1997
North Anna 1	Mar. 2001

The five events excluded are either drops not associated with fuel transfer machine operations or events associated with activities not performed at the Wet Handling Facility. The five excluded events from Table 4 of NUREG-1774 that occurred between 1985 and 2002 are: (1) a container of fuel assemblies fell off a transfer cart, (2) two fuel assemblies were found attached to the

upper core support structure during a lift and one assembly dropped, (3) fuel was damaged, not dropped, during an event, (4) an assembly shipping container was inadvertently lifted and dropped, and (5) fuel assemblies fell from their metal container due to rigging issues. Therefore, these five events were excluded.

1.4.4 Events Identified as an Upper Bound

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.

Response: The upper bound of 17 drop events is based on the total number of drop events involving a grapple occurring over the period of the study, including events from 1969 through 2002. These 17 events from Table 4 of NUREG-1774 are presented in Table 5.

Table 5. Events Identified as an Upper Bound from NUREG-1774 Data

Events Applicable to Spent Fuel Transfer Machine Operations that Occurred Before 1985			Drop Events Associated with Fuel Pool Handling Operations	
Event	**Date**		**Event**	**Date**
Pilgrim	Jan. 1974		Quad Cities 1	Sept. 1989
Millstone 1	Sept. 1974		North Anna 1	Jan. 1990
Duane Arnold	June 1975		Byron 2	Sept. 1990
Humbolt Bay	June 1975		Sequoyah 1	June 1993
Brunswick 2	March 1976		Vermont Yankee	Sept. 1993
Brunswick 2	March 1976		Waterford	April 1997
Peach Bottom 3	Jan. 1977		North Anna 1	Mar. 2001
Prairie Island 1	Jan. 1981			
Turkey Point 4	April 1983			
Hatch 1	Oct. 1984			

1.4.5 Likelihood of an Assembly Drop When Transferring Spent Fuel Versus New Fuel

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.

Response: Fuel drops were considered if they involved operations similar to spent fuel transfer machine operations in the Wet Handling Facility. No consideration for the age of the fuel was taken in selecting the events to consider.

1.5 PART (E)—EXPLANATION OF USE OF BAYESIAN ESTIMATION TO COMBINE MULTIPLE DATA SOURCES

(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.

Response: When multiple industry data sources are available for a component, an empirical Bayesian approach was used to develop prior distributions that represent the variability found across industrial applications, as described in the CRCF categorization analysis (BSC 2009a, Section 4.3.3). The sources of information applied to this failure rate were numerically aligned such that the analysis results concentrated around a single value with little uncertainty. In such instances, as stated in the CRCF categorization analysis (BSC 2009a, Section 4.3.3.1), the distribution is modeled using the data source that yields the most diffuse information, which would yield the largest uncertainty. In the example cited (interlock failure on demand), the median estimate of the five sources was chosen to be representative of the mean failure rate. This resulted in a mean failure rate 2.75×10^{-5} per hour with an error factor of five.

1.6 PART (F)—TECHNICAL BASIS FOR ERROR FACTORS USED IN DISTRIBUTIONS OF ACTIVE COMPONENT FAILURE DATA

(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.

Response: In general, the guidelines established for assigning error factors to an expert-estimated value used in the PCSA were as follows:

- If the component was well known and had a long history in well-defined and controlled environments, it was assumed that the uncertainty was small and an error factor of three would be assigned.

- If the component was well-known but was being utilized in an environment that was new, the response of the component in the new environment would be less certain and an error factor of five was assigned.

- For components that did not have much or any operating history in existing operating environments and the operating environment was one that was new or evolving, an error factor of ten was assigned to represent the lack of knowledge and experience.

This is consistent with the DELPHI approach in IEEE Std. 500-1984 (1991), *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*.

1.7 PART (G)—JUSTIFICATION OF MEAN FAILURE RATE OF A RADIATION MONITOR

(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."

Response: Two information sources for the component radiation sensor with a run-time failure mode are identified in the YMP Active Comp Database (BSC 2009a, Attachment H). One source is vendor information (Laurus Systems [n.d.]), which states that the mean time between failures will be on the order of approximately 50,000 hours. This value provides an upper bound or high estimate for the failure rate. The inverse of this value is conservatively taken as an estimate of the mean failure rate, 2×10^{-5} failures per hour. Since no estimate of the range was given, an error factor of five was assigned (see Section 1.6, above). The second data source for radiation sensors is IEEE Std. 500-1984 (1991) (p. 607). Under the designation for all failure modes, the low, recommended (i.e., best estimate), and high failure rates are 8.88, 14.35, and 19.88 failures per 10^6 hours, respectively. The high value was incorrectly recorded in the YMP Active Comp Database (BSC 2009a, Attachment H) as 1.99×10^{-6} per hour. If the high and low values are correctly used for these percentiles, the error factor estimate has a value of 1.5. However, the error factor was calculated as 0.5 due to the transcription error. This transcription error resulted in the addition of a note to the database stating that an error factor of 0.5 was calculated. The error factor entered in the component database has the value of 2.0. This value is conservative relative to the correct error factor of 1.5 based on the high and low values.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

ASME (American Society of Mechanical Engineers) 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* ASME NOG-1-2004. New York, New York: American Society of Mechanical Engineers. TIC: 257672.

BSC (Bechtel SAIC Company) 2009a. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

BSC 2009b. *Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis*. 000-PSA-MGR0-00900-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0008.

BSC 2008. *Mechanical Handling Design Report-Spent Fuel Transfer Machine*. 050-30R-HT00-00100-000 REV 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080312.0015.

Crutchfield, D.M. 1996. "Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment." NRC Bulletin 96-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. Accessed July 21, 2009. ACC: MOL.20080213.0021. URL: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1996/bl96002.html

Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995.* NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.

Framatome ANP (Advanced Nuclear Power) 2001. *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study—1985–1999*. Lynchburg, Virginia: Framatome Advanced Nuclear Power. ACC: MOL.20011018.0158.

IEEE (Institute of Electrical and Electronics Engineers) Std. 500-1984 (Reaffirmed 1991). *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 256281.

Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

Laurus Systems [n.d.]. "rad-D FAQ." Ellicott City, Maryland: Laurus Systems. Accessed July 24, 2009. TIC: 259965. http://laurussystems.com/Service/rad-D_faq_ver409.pdf

NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

NRC 2007. *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis—Level of Information and Reliability Estimation.* HLWRS-ISG-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.

Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data*. NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.

Siu, N.O. and Kelly, D.L. 1998. “Bayesian Parameter Estimation in Probabilistic Risk Assessment.” *Reliability Engineering and System Safety, 62,* 89-116. New York, New York: Elsevier. TIC: 258633.

Zentner, M.D.; Atkinson, J.K.; Carlson, P.A.; Coles, G.A.; Leitz, E.E.; Lindberg, S.E.; Powers, T.B.; and Kelly, J.E. 1988. *N Reactor Level 1 Probabilistic Risk Assessment: Final Report.* WHC-SP-0087. Richland, Washington: Westinghouse Hanford Company. ACC: MOL.20080207.0021.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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-TEMPSHIELD-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.

1. RESPONSE

The areas for further explanation referred to in the RAI are excerpted and discussed in the response subsections below:

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.

Response: The preclosure safety analysis (PCSA) is based on the design as it exists at a specific point in time. The representation of event sequences in the PCSA is consistent with the design and operations of the geologic repository operations area (GROA) facilities, as documented in the reference design documents cited in the six event sequence development analyses and the six event sequence reliability and categorization analyses that are referenced in the SAR. The PCSA is consistent with both the operations and the design of the GROA facilities within the context of the design evolution. As the design evolves, there are procedures and processes in place to ensure that the design evolution does not materially impact the event sequence quantification or the analysis results and conclusions. As the design evolves, there are procedures and processes in place to ensure that the PCSA is periodically updated to accurately reflect the design. Updates to the Nuclear Safety Design Bases (NSDB), procedural safety controls, and the SAR will be made at the appropriate time.

The process for classifying structures, systems, and components (SSCs) as important to safety (ITS) or non-ITS is described in SAR Sections 1.6.1, 1.6.2, and 1.9. SAR Table 1.9-1 presents the SSCs that have been classified as ITS in the PCSA. Classification as ITS is based on the specific preclosure safety functions that the SSCs perform and whether they are relied upon to prevent (i.e., reduce the probability of) the occurrence of an event sequence or mitigate the consequences of an event sequence, as demonstrated in the event sequence analyses. The preclosure safety functions relied upon in the NSDB and associated ITS SSCs are presented in SAR Tables 1.9-2 through 1.9-7. These tables identify ITS SSCs at a high level of assembly (e.g., a large piece of equipment such as the canister transfer machine (CTM)). The design presented in Section 1.2 of the SAR describes the ITS and non-ITS portions of the design in more detail. For example, the subsidiary ITS SSCs for the CTM are included in the process and instrumentation diagram for this SSC (see SAR Figure 1.2.4-51). The PCSA fault trees include SSCs within the CTM that, if failed could lead to failure of the safety function.

1.1 APPLICATION OF OPERATIONS AND MAINTENANCE ACTIONS WHEN DEVELOPING INITIATING EVENTS

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

1.1.1 Bypass on the Canister Transfer Machine When Lid is Lifted for non-Dual-Purpose Canisters

- 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

- 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.

Response: There are multiple inquiries imbedded in this request. The first inquiry concerns the statement in *Canister Receipt and Closure Facility Event Sequence Development Analysis* (BSC 2008) that an interlock is manually bypassed when the lid is lifted for non-dual-purpose canisters (DPC). The statement on Page B-6 of the event sequence development analysis (BSC 2008) reflects the conceptual design of the slide gate interlocks that existed at the time the document was developed and approved. As the slide gate system design developed, it became apparent that the conceptual design objectives of minimizing the potential for uncontrolled exposure could be achieved with a simpler design that did not require the bypass. Consequently, the bypass was removed from the design, and its function was removed from the PCSA models. The event sequence development analysis (BSC 2008) will be revised to reflect design changes that were captured in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a).

The second inquiry concerns why there are differences between two apparently similar fault trees. The fault trees in question (ESD18-TEMP-SHIELD-LOSS and ESD18-TMP-SHLD-LOSS-DSTD in the Canister Receipt and Closure Facility (CRCF) SAPHIRE Model (BSC 2009a, Attachment H)) address loss of shielding during canister transfers. One branch of these trees concerns a loss of shielding resulting from the operator failing to close the CTM slide gate before raising the shield skirt and moving the CTM. This occurrence is captured in event 060-OpFailSG-HFI-NOD (BSC 2009a, Table E6.5-1). The justification for the preliminary value assigned to this event includes the following statement found in Table E6.5-1 in the event sequence categorization analysis (BSC 2009a): “because this interlock may be bypassed during normal maintenance, the bypass is explicitly modeled in HFE 060-OpFailRstInt-HFI-NOM.” In the ESD18-TEMP-SHIELD-LOSS fault tree, the human failure event 060-OpFailRstInt-HFI-NOM (BSC 2009a, Table E6.5-1) was inadvertently omitted from the “Slide Gate Opens and CTM Moves” branch of the fault tree. Rectifying the omission increases the probability of the ESD18 event sequences for DPCs, high-level radioactive waste (HLW) canisters, multicanister overpacks (MCOs), and transportation, aging, and disposal (TAD) canisters as shown in Table 1.

Table 1. Changes in ESD 18 Event Sequence Probability

Waste Form	Total Cut Set Value without Failure to Restore Interlock	Total Cut Set Value with Failure to Restore Interlock
DPC	3.0×10^{-3}	6.4×10^{-3}
HLW canister	8.5×10^{-2}	1.8×10^{-1}
MCO	3.9×10^{-3}	8.4×10^{-3}
TAD canister	1.3×10^{-1}	2.8×10^{-1}

The DOE standard canister waste form ESD18 event sequence probability does not change as the failure to restore interlock event is already contained in the ESD18-TMP-SHLD-LOSS-DSTD fault tree. From the table above, it is evident that the increase associated with consideration of "failure to restore" does not alter the event sequence categorization.

The third inquiry concerns the modeling of interlocks and interlock failures due to maintenance activities. The examples given in the RAI are Figures B4.4-11 and B9.4-1 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a). Figure B4.4-11 is Sheet 9 of the "CTM Drop Fault Tree" and Figure B9.4-1 is the "Typical Direct Exposure Fault Tree due to Shield Door or Slide Gate Opening." In the former case, there is a failure to restore following maintenance included in the event; in the latter case, there is not. The approach for modeling interlocks and their restoration following maintenance is provided in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Attachment E, Section E6.0.2.1). The analysis notes that the interlocks were generally modeled explicitly in the fault tree instead of being imbedded in the human reliability analysis and that the preliminary interlock failure value implicitly accounts for the failure to restore an interlock after maintenance if that interlock is difficult to bypass and is not bypassed during normal maintenance. From Table 2, it is apparent that interlock failures were modeled consistently with the criteria above, limiting the "failure to restore" event to models covering slide gate operation. In all other cases, the failure to restore following maintenance event was considered to be imbedded in the component failure rate.

Table 2. Interlock Cross-reference

Interlock Failure Basic Events	Associated Fault Trees	Associated Fail to Restore Event in Fault Tree?	Justification
060-GATE-IEL001--IEL-FOD	060-INTERLOC-FAILURE	No	Failure to restore imbedded in basic event
060-CTM--IMEC125-IEL-FOD	GATE-36-60	No	Failure to restore imbedded in basic event
	GATE-36-7	No	Failure to restore imbedded in basic event
	ESD9-MCO-LIDIMP	No	Failure to restore imbedded in basic event
	GATE-36-132	No	Failure to restore imbedded in basic event
	GATE-36-58	No	Failure to restore imbedded in basic event

Interlock Failure Basic Events	Associated Fault Trees	Associated Fail to Restore Event in Fault Tree?	Justification
	GATE-20-2	No	Failure to restore imbedded in basic event
	ESD9-DSNF-LIDIMP	No	Failure to restore imbedded in basic event
	ESD9-HLW-LIDIMP	No	Failure to restore imbedded in basic event
	ESD9-TAD-LIDIMP	No	Failure to restore imbedded in basic event
060-CR---IELSKT--IEL-FOD	060-18-SLIDEGATE-DIR-EXP	Yes	Interlock considered susceptible to fail to restore
060-CTM--SLIDGT2-IEL-FOD	GATE 36-7	No	Failure to restore imbedded in basic event
060-CR---IEL00A--IEL-FOD	060-9-ST-SPURMOVE	No	Failure to restore imbedded in basic event
	060-9-CTT-SPUR-MOVE	No	Failure to restore imbedded in basic event
	060-18-SHLDDR-DIRCT-EXP	No	Failure to restore imbedded in basic event
060-PORTSLIDEGTE-IEL-FOD	ESD19-SHIELD-RING	Yes	Interlock considered susceptible to fail to restore
	ESD18-TMP-SHLD-LOSS-DSTD	Yes	Interlock considered susceptible to fail to restore
	ESD18-TEMP-SHIELD-LOSS	Yes	Interlock considered susceptible to fail to restore
060-SLDGATE-IEL-FOD	ESD18-TMP-SHLD-LOSS-DSTD	Yes	Interlock considered susceptible to fail to restore
	ESD18-TEMP-SHIELD-LOSS	No	Failure to restore imbedded in basic event
060-PWRPRTGATINT-IEL-FOD	060-9-WPTT-SPURMOVE	No	Failure to restore imbedded in basic event
26D-##EG-FLITLKA-IEL-FOD	EP-ITS-DGA-17	No	Failure to restore imbedded in basic event
26D-##EG-FLITLKB-IEL-FOD	EP-ITS-DGB-17	No	Failure to restore imbedded in basic event
060-WPTT-IELDK3--IEL-FOD	060-EQUIP-MOVE-LOAD	No	Failure to restore imbedded in basic event
	060-9-WPTT-SPURMOVE	No	Failure to restore imbedded in basic event
060-SPMRC-IEL011-IEL-FOD	060-I-SPMRC-COLLISION	No	Failure to restore imbedded in basic event
060-SPMTT-IEL102-IEL-FOD	060-1-SPMTT-COLLISION	No	Failure to restore imbedded in basic event
060-CTM-BRIDGETR-IEL-FOD	060-8-TWO-CTMS-COLLIDE	No	Failure to restore imbedded in basic event

Interlock Failure Basic Events	Associated Fault Trees	Associated Fail to Restore Event in Fault Tree?	Justification
060-CTM-BRIDGMTR-IEL-FOD	GATE-20-94	No	Failure to restore imbedded in basic event
	GATE-36A-1	No	Failure to restore imbedded in basic event
060-CTM-HSTTRLLY-IEL-FOD	GATE-20-94	No	Failure to restore imbedded in basic event
	GATE-36A-1	No	Failure to restore imbedded in basic event
060-CTM-SBELTRLY-IEL-FOD	GATE-20-94	No	Failure to restore imbedded in basic event
	GATE-36A-1	No	Failure to restore imbedded in basic event
060-CR---IEL00B--IEL-FOD	060-9-ST-SPURMOVE	No	Failure to restore imbedded in basic event
	060-9-CTT-SPUR-MOVE	No	Failure to restore imbedded in basic event
	060-18-SHLDDR-DIRCT-EXP	No	Failure to restore imbedded in basic event
060-VCTO-IEL0001-IEL-FOD	HVAC007	No	Failure to restore imbedded in basic event
060-WPTT-IEL001-IEL-FOD	060-WPTT-PRE-TIL	No	Failure to restore imbedded in basic event
	060-WP-IMPACT	No	Failure to restore imbedded in basic event
060-WPTT-IEL003--IEL-FOD	060-WPTT-PRE-DEPARTURE	No	Failure to restore imbedded in basic event
060-CRWT-IEL0001-IEL-FOD	060-CRWT-RS00000-FAILURE	No	Failure to restore imbedded in basic event

1.1.2 Entrance of Operators into the Transfer Room during Normal Activities

- 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.

Response: The canister transfer operations are controlled and conducted from the facility control room. No operator access is allowed during canister transfers of any waste forms. Following completion of a transfer, access to the Canister Transfer Room is controlled and will only occur infrequently for activities such as maintenance. The event 060-OpStageRack1-HFI-NOD was quantified in the event sequence categorization analysis (BSC 2009a, Section E6.5.3.4.6.1) to address the likelihood that shielding (e.g., port slide gates), which is expected to be in place, may not have been restored to its shielding position following transfer of a canister to a staging rack. This analysis notes that an operator entering the Canister Transfer Room for normal operations, such as routine maintenance when a staging port slide gate has been inadvertently left open, could be exposed to radiation streaming from the uncovered port.

1.2 QUANTIFICATION AND IMPLEMENTATION OF BASIC EVENTS IN FAULT TREES

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

1.2.1 Demands Placed on the Canister Transfer Machine Holding Brake

- 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.

Response: The total number of each waste form handled is accounted for in the initiating event tree. For example, the event DPC in the initiating event tree CRCF-ESD09-DPC in the CRCF SAPHIRE model (BSC 2009a, Attachment H) is "Number of DPCs moved during preclosure period." This event is given a value of 346, which is the total number of DPCs estimated to be handled over the lifetime of the facility. Separate initiating event trees are included in the CRCF SAPHIRE model for each waste form (e.g., CRCF-ESD09-DSTD, CRCF-ESD09-HLW). The total number of each waste form handled is quantified in the same manner, using the name of the waste form given in the first event in the initiating event tree for that waste form.

The number of demands on a piece of equipment during a waste handling evolution depends on the waste form involved and the operation being performed. This information is included in the fault trees. In the case of the CRCF-ESD09-nnn (where nnn represents the waste form) initiating event trees, the event sequences where failure of the holding brake is relevant are only those branches that involve a drop where the holding brake is a contributing factor to the drop (i.e., a holding brake failure is not a contributor, for example, to the "Canister Drop > Operational Height" or "Spurious Movement" branches of the event tree). The specific branches where the holding brake failure is a contributing factor are "Canister Drop at Operational Height," "Object Dropped on Canister," and "Canister Dropped Inside Bell."

The fault trees quantifying these events were developed to account for the number of specific demands on the equipment for each transfer of a given waste form. For example, a TAD canister is lifted from the transportation cask into the CTM shield bell. At the completion of the lift, the holding brake engages. The CTM then moves the TAD canister over the waste package in the waste package loading room where the holding brake disengages and the TAD canister is lowered into the waste package. There is one demand on the holding brake during this sequence. For the same TAD canister, the lid is removed from the transportation cask and the waste package lid is subsequently placed on the waste package after the TAD canister has been placed in the waste package. In this case, the number of objects lifted is two, each possessing the potential to be dropped onto the TAD canister. Consequently, there are two demands on the holding brake that are associated with lifting a heavy object that has the potential to damage the TAD canister if dropped.

The events that are incorporated into the fault trees to account for these demands are given in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Table 6.3-11). The events are listed as follows:

060-CTMOBJLIFTNUMBER—This event represents the number of object (lid) lifts the CTM must accomplish for waste forms that rely on the CTM to remove the transportation cask lid and install the waste package inner lid. The value assigned to this event is 2, representing the two opportunities to drop an object on the canister during the transfer of a canister from the cask to a waste package.

060-CTMOBJLIFTNUMBERD—This event represents the number of object (lid) lifts the CTM must accomplish for waste forms that have the transportation cask lid removed by the cask handling crane before the cask is moved into the Cask Unloading Room where the CTM will remove the canister without having to first remove the transportation cask lid. The value assigned to this event is 1, representing the single opportunity to drop an object on the canister during the transfer of a canister from the cask to a waste package.

060-LIFTS-PER-TAD-CAN—This event represents the number of lifts associated with the transfer of a TAD canister from a transportation cask to a waste package. The value assigned to this event is 1, representing the opportunities for the malfunction of a CTM component to result in a drop of the canister during its transfer from the cask to a waste package.

060-LIFTS-PER-MCO-CAN—This event represents the number of lifts associated with the transfer of an MCO from a transportation cask to a waste package. The value assigned to this event is 1, representing the opportunities for the malfunction of a CTM component to result in a drop of the canister during its transfer from the cask to a waste package.

060-LIFTS-PER-HLW-CAN—This event represents the number of lifts associated with the transfer of an HLW canister from a transportation cask to a waste package. The value assigned to this event is 1.2, representing the opportunities for the malfunction of a CTM component to result in a drop of the canister during its transfer from the cask to a waste package. The value of 1.2 accounts for the fraction of HLW canisters that will be lifted twice (i.e., 20% of the canisters will be staged prior to being transferred to a waste package) during its movement from the transportation cask to a waste package. This event is explained in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Table 6.3-11).

060-LIFTS-PER-DSNF-CAN—This event represents the number of lifts associated with the transfer of a defense spent nuclear fuel (SNF) canister from a transportation cask to a waste package. The value assigned to this event is 2, representing the opportunities for the malfunction of a CTM component to result in a drop of the canister during its transfer from the cask to a waste package. This event also accounts for the transfer to the staging area before final transfer to the waste package.

060-LIFTS-PER-DPC-CAN—This event represents the number of lifts associated with the transfer of a DPC from a transportation cask to a waste package. The value assigned to this event

is 1, representing the opportunities for the malfunction of a CTM component to result in a drop of the canister during its transfer from the cask to a waste package.

In summary, the number of lifts for each waste form and each initiator is identified in Table 3. The number of demands on CTM components (including brakes) is typically 2 per lift.

Table 3. Number of Lifts per Initiator For Each Waste Form

Waste Form	Initiator: Number of Drops at Operational Height	Initiator: Object Dropped on Canister	Initiator: Canister Dropped Inside Bell
DPC	1	1	1
Defense SNF canister	2	2	2
HLW canister	1.2	2	1.2
MCO	1	2	1
TAD canister	1	2	1

1.2.2 Quantification of Slide Gate Operation per Canister or Object Lift

- 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.

Response: The ESD18 fault trees (BSC 2009a, Attachment H) are used to evaluate the likelihood that shielding is compromised during a canister transfer. Events contributing to this likelihood associated with the port slide gate are in the 060-OPER-DIR-EXP branch of the ESD18 fault trees in the SAPHIRE model (BSC 2009a, Attachment H). The single event in this branch of these fault trees associated with the operation of the port slide gate is 060-OPCTMDIREXP1-HFI-NOD, which evaluates operator failure to close the slide gate after the placement of a canister into a staging rack prior to raising the shield skirt and moving the CTM away from the port. The port slide gate is opened and closed once in this process. The port slide gate is then opened again to remove the canister and then closed once the canister is removed.

1.2.3 Accounting for Object Lift Value and Fault Trees for Canister Drop for the Canister Transfer Machine and the Waste Package Crane

- 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.

Response: The entry in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Table 6.3-11) states "During transfer of DOE Std. canister, HLW, MCO or TAD from the TC to the waste package (WP), the CTM lifts a lid and the WP crane lifts a lid over the cask. Therefore, a value of 2 is assigned to this basic event." There are two opportunities to drop a lid on a canister during a canister transfer. The first opportunity

occurs when the transportation cask lid is removed from the transportation cask by the CTM. The second opportunity occurs when the waste package inner lid is placed on the waste package after the canister has been transferred to the waste package. The waste package inner lid is placed on the waste package by the CTM. Both opportunities to drop an object on a canister result from CTM lifts. The waste package crane is not involved in either of these lifts or the canister transfer operation.

1.2.4 Equipment and Activities to Reduce Probability of Direct Exposure during Dual-Purpose Canister Cutting Operations

- 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.

Response: The events in Table E6.7-1 are part of *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009b, Section E6.7), "Analysis of HUMAN FAILURE Event Group # 7: DPC Cutting." This group evaluates human failure events linked to operations and initiating events associated with DPC cutting. The event described in *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009b, Table E6.7-1) is "Operator causes loss of shielding during DPC cutting;" the example given describes the operator incorrectly installing the DPC shield ring (BSC 2009b, p. E-221). The DPC shield ring is relied upon during DPC cutting to shield workers from direct exposure. The associated activity is operator placement of the shield ring. Improperly installing the shield ring results in exposure to the worker. The complete analysis involves consideration for numerous contributors, such as failure to install, failure to notice the installation failure, failure to install properly, failure to perform radiation monitoring, and failure to notice the improper installation, as well as other contributors. All of these occurrences are attributed to the operator causing a loss of shielding during DPC cutting operations.

1.2.5 Steps in Cask Preparation Activities for Dual-Purpose Canisters in the Canister Receipt and Closure Facility

- 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."

Response: A detailed analysis of this activity including a justification for its inclusion for detailed analysis begins on page E-91 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a) for the "Analysis Of Human Failure Event

Group #3: Cask Preparation and Movement To Cask Unloading Room" base case scenario. The preliminary analysis in Table E6.3-1 (BSC 2009a, p. E-89) specifically identified this particular activity for this scenario. The detailed analysis of events associated with this scenario begins on page E-80 of the analysis. In this section, the specific steps the operator is expected to follow are outlined and potential failures are identified and quantified. The statement in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Section E6.3.3.2.3) simply describes one of the environmental conditions considered in the full analysis of this event. It does not imply that repository activities are conducted without procedures; it only acknowledges that the operators will have procedures but may not have them available in-hand as they perform this activity because this is considered a skill-based activity. Consequently, the operators will be relying on their experience and training, which includes training on the procedure for installing the lift fixture.

1.3 ACCOUNTING FOR SIMILAR OPERATIONS IN DIFFERENT FAULT TREES AND HUMAN FAILURE EVENTS

(c) Explain how different fault trees and human failure events account for operations that appear to be similar.

Response: Responses to the specific instances cited below demonstrate that for the cases specified, as well as the analysis in general, there are differences associated with different waste forms and operating steps. The analysis was conducted at a level of detail that accounted for such differences for similar but not identical operations.

1.3.1 Differences between Processing DOE Standardized Canisters and Other Waste Forms

- 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-TEMPSHIELD-LOSS (for other waste forms).

Response: Differentiation among waste forms is required to allow for potential differences in waste form parameters and characteristics that could impact the analysis, such as different grapples, different lifting fixtures, different lifting steps (e.g., with yoke or without yoke), different cask preparation steps, different staging requirements, different breach probabilities, different waste packages, and different source terms. This differentiation allows the models to incorporate waste form-specific information, providing a more accurate evaluation of event sequence probabilities.

In the cases of ESD18-TMP-SHLD-LOSS-DSTD and ESD18-TEMP-SHIELD-LOSS in the SAPHIRE model (BSC 2009a, Attachment H), the difference is that an additional event (060-OPSTAGERACK-HFI-NOD) is included in ESD18-TMP-SHLD-LOSS-DSTD to account for exposures resulting from operator errors associated with staging a DOE standard canister.

1.3.2 Differences in Failure Probabilities for Closing Port Gate and Other Canister Staging Operations

- 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).

Response: 060-OpCTMImpact1-HFI-COD (BSC 2009a, Section E6.5.3.4.4.1) is the event titled "Operator moves the CTM while canister or object is below or between levels". One of many events evaluated as a contributor to the quantification of this event is the event titled "Operator Fails to Close Port Slide Gate". 060-OPStageRack1-HFI-NOD (BSC 2009a, Section E6.5.3.4.6) is the event titled "Operator Causes Direct Exposure during Canister Staging." This event is evaluated in the context of the operator failing to ensure that procedurally required shielding (i.e., closure of the slide gate) is accomplished following the placement of a canister in the staging rack.

The actions are not identical and the difference is explained in the response to RAI 2.2.1.1.3-3-031. The common performance conditions and other factors considered by the analyst for each event are listed in the analysis given in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a, Section E6.5.3.4.4.1 for 060-OpCTMImpact1-HFI-COD and Section E6.5.3.4.6 for 060-OPStageRack1-HFI-NOD). Differences between 060-OpCTMImpact1-HFI-COD, "Operator Moves the CTM while Canister or Object Is Below or Between Levels," and 060-OPStageRack1-HFI-NOD, "Operator Causes Direct Exposure during Canister Staging," stem from two additional common performance conditions in the latter (working conditions and availability of procedures), with a minimal effect on quantification (0.008 versus 0.01). Given the overall uncertainty in the fundamental models and the high degree of analyst judgment during a human reliability analysis, either action could be legitimately analyzed with either set of common performance conditions, with minimal effect on event sequence probability.

1.4 CONSIDERATION OF SIMULTANEOUS OPERATIONS IN THE CANISTER RECEIPT AND CLOSURE FACILITY WHEN DEVELOPING INITIATING EVENTS

(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.

Response: Within the CRCF, there are two CTMs and parallel paths that appear to allow the simultaneous transfer of two canisters containing similar or different waste forms. The design

and operational intention, however, is to use only one path at a time to transfer canisters within the unloading and waste package positioning rooms. Permanent shield walls in place between rooms/areas to reduce normal operating exposures preclude an operation in one room from exposing workers in another. Shield doors are interlocked so that direct exposure from one room to another is not a Category 1 event sequence. These interlocks are included in the appropriate fault trees for which direct exposure is an end state.

In the preparation area, only one rail cask can be physically handled at a time. There is only enough space to park one railcar, and there is one designated cask preparation platform to access the cask once it has been transferred to a canister transfer trolley. Simultaneous transfers to and from two site transporters cannot occur due to space, equipment, and resource limitations.

For example, cask preparation operations would not occur simultaneously in the site transporter vestibule and in the Cask Preparation Room. When canisters are in the Canister Transfer Room, the shield bell and skirt provides shielding such that personnel could be present. However, they would not normally be in that room. The two paths of the CRCF are not intended as simultaneous, parallel operating paths. One path could be set up to process large canisters (e.g., TAD canisters) and the other could be set up to process small diameter canisters (e.g., DOE standard canisters). Each line would be used as needed, but there would not be two canisters in the same stage of transfer at the same time. Table 4, summarizes the exposure potential associated with operations in each major operational area within the CRCF.

Table 4. Direct Exposure Potential in Waste Handling and Adjacent Areas

CRCF Operating Area	Room Number	Direct Exposure Potential
Site Transporter Vestibule	1027	All canisters in the Site Transporter Vestibule will be in an aging overpack. There are no operations conducted in this area that could result in an unplanned exposure to an individual in this area or an adjacent area. Normal operations in adjacent areas do not expose any sources that could result in an unplanned exposure in the Site Transporter Vestibule. The only potential contributors to an unplanned exposure in this area would result from breaches of the aging overpack boundary, which are addressed in ESD02.
Rail Car Vestibule	1036	All canisters in the Rail Car Vestibule will be in a transportation cask. There are no operations conducted in this area that could result in an unplanned exposure to an individual in this area or an adjacent area. Normal operations in adjacent areas do not expose any sources that could result in an unplanned exposure in the Rail Car Vestibule. The only potential contributors to an unplanned exposure in this area would result from breaches of the transportation cask shielding, which are addressed in ESD01.

CRCF Operating Area	Room Number	Direct Exposure Potential
Prep Area	1026	All canisters in the Prep Area will be in either a transportation cask or aging overpack. Transportation cask or aging overpack lid removal for attaching a lift fixture to a DPC is the only normal operation conducted in this area that temporarily removes shielding that could result in an unplanned exposure to an individual in this area or an adjacent area. The field resulting from this operation is a loosely collimated beam directed toward the roof over the Prep Area facility which is approximately 60 feet above the top of the cask. This field is expected and procedures controlling access to potential exposure areas during this operation will be in place. Normal operations in adjacent area that could result in an unplanned exposure in the Prep Area are canister transfers conducted in one of the Cask Unloading Rooms (1023 or 1024). These occurrences are addressed in ESD18.
Cask Unloading Room	1023	All canisters in an Cask Unloading Room will initially be in either a transportation cask or aging overpack that will provide shielding until the canister is transferred into the CTM shield bell. Transportation casks or aging overpacks containing DPCs will have the lid removed, resulting in a loosely collimated vertical beam as described above. Once the cask or aging overpack is in the Cask Unloading Room, the shield door between the Prep Area and the Cask Unloading Room is closed. Areas adjacent to this Cask Unloading Room on the first floor are the other Cask Unloading Room (1024) hallways 1005 D, E, and F, and the Prep Area. The other Cask Unloading Room and hallways are separated from this Cask Unloading Room by shield walls that preclude exposure to these areas during canister transfers. The shield door between the unloading room and the Prep Area provides shielding that prevents exposures to personnel in the Prep Area during canister transfer operations. Inadvertent opening of this shield door is addressed in ESD18. The area adjacent to this room on the second floor is the Canister Transfer Room (2004). Shielding between this Cask Unloading Room and the Canister Transfer Room is provided by the Cask Unloading Room ceiling/transfer room floor. Once the shield door between the Cask Unloading Room and the Prep Area is closed, the CTM shield bell is moved over the transfer port, the shield bell skirt is lowered and the port slide gate is opened. Although personnel are not expected to be in the Canister Transfer Room (2004) during the transfer, shielding is provided by the shield skirt, the CTM bell, and the Canister Transfer Room floor. Once the canister is transferred to the CTM shield bell, the CTM slide gate is closed, providing shielding after the shield skirt is raised to move the CTM. The only exposure potential from operations associated with the Cask Unloading Room would result from equipment malfunctions or operator error and are addressed in ESD18 and 060-18-SHLDDR-DIRCT-EXP.

CRCF Operating Area	Room Number	Direct Exposure Potential
Cask Unloading Room	1024	All canisters in an unloading room will initially be in either a transportation cask or aging overpack that will provide shielding until the canister is transferred into the CTM shield bell. Transportation casks or aging overpacks containing DPCs will have the lid removed, resulting in a loosely collimated vertical beam as described previously. Once the cask or aging overpack is in the Cask Unloading Room, the shield door between the Prep Area and the Cask Unloading Room is closed. Areas adjacent to this Cask Unloading Room on the first floor are the other Cask Unloading Room (1023) hallways 1005 D, E, and F, and the Prep Area. The other Cask Unloading Room and hallways are separated from this Cask Unloading Room by shield walls that preclude exposure to these areas during canister transfers. The shield door between the unloading room and the Prep Area provides shielding that prevents exposures to personnel in the Prep Area during canister transfer operations. Inadvertent opening of this shield door is addressed in ESD18. The area adjacent to this room on the second floor is the Canister Transfer Room (2004). Shielding between this Cask Unloading Room and the Canister Transfer Room is provided by the Cask Unloading Room ceiling/transfer room floor. Once the shield door between the Cask Unloading Room and the Prep Area is closed, the CTM shield bell is moved over the transfer port and the shield bell skirt is lowered and the port slide gate is opened. Although personnel are not expected to be in the Canister Transfer Room (2004) during the transfer, shielding is provided by the shield skirt, the CTM bell and the Canister Transfer Room floor. Once the canister is transferred to the CTM shield bell, the CTM slide gate is closed, providing shielding after the shield skirt is raised to move the CTM. The only exposure potential from operations associated with the Cask Unloading Room would result from equipment malfunctions or operator error and are addressed in ESD18 and 060-18-SHLDDR-DIRCT-EXP.
Canister Transfer Room	2004	While the canister is being transferred in the Canister Transfer Room it is in the CTM shield bell with the shield skirt slide gate closed. No additional shielding is necessary to allow access to this room although it will be access controlled and personnel do not need access to this area for the conduct of normal operations. The CTM shielding also protects personnel in areas adjacent to the Transfer Room from exposure. These areas include the 2006 Corridors, the Waste Package Closure Room (2007), Closure Equipment Rooms (2007 A and B), and the Closure Support Rooms (2003 and 2011). Areas below the Transfer Room are shielded by the Transfer Room floor. Canister grapple changes are accomplished in the Maintenance Rooms (1012 and 1033) below the Transfer Room and would not be susceptible to exposure from operations in the Transfer Room. Exposures due to equipment malfunctions or operator errors associated with Transfer Room operations are addressed in ESD18.
Waste Package Positioning Room	1018	The Waste Package Positioning Rooms (1018 and 1019) are shielded on all sides preventing personnel exposure in adjacent areas from operations conducted in the Waste Package Positioning room. Additionally, the Waste Package Transfer Trolley (WPTT) is shielded to allow personnel access if required due to equipment malfunction; however, personnel access to these rooms is controlled. When the waste package lids are being welded in place, there is a radiation field in the Waste Package Closure Room (2007); however this field is expected and the welding operation is remotely controlled and automated such that personnel access is not required. Exposures during closure due to equipment malfunctions or operator error are addressed in ESD19.

CRCF Operating Area	Room Number	Direct Exposure Potential
Waste Package Positioning Room	1019	The Waste Package Positioning Rooms (1018 and 1019) are shielded on all sides, preventing personnel exposure in adjacent areas from operations conducted in the Waste Package Positioning room. Additionally, the WPTT is shielded to allow personnel access if required due to equipment malfunction; however, personnel access to these rooms is controlled. When the waste package lids are being welded in place, there is a radiation field in the Waste Package Closure Room (2007); however this field is expected and the welding operation is remotely controlled and automated such that personnel access is not required. Exposures during closure due to equipment malfunctions or operator error are addressed in ESD19.
Waste Package Loadout Room	1015	The Waste Package Loadout Room is shielded on all sides preventing personnel exposure in adjacent areas from operations conducted in the WP Loadout Room. Additionally, the WPTT and the transport and emplacement vehicle are shielded to allow personnel access if required due to equipment malfunction; however, personnel access to this room is controlled when a loaded waste package is present.

1.5 CONSIDERATION OF FUEL ASSEMBLY COLLISIONS IN THE WET HANDLING FACILITY

(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.

Response: This question contains two parts: (1) the treatment of collisions of fuel elements during transfer, and (2) the assurance that fuel assemblies are fully lowered into place in the fuel storage rack following transfer.

Fuel element collisions are not prevented, and no equipment, components, or procedures are credited with their prevention. Such collisions may occur in the Wet Handling Facility (WHF) fuel handling pool, which reduces potential releases such that these event sequences comply with the performance objective of 10 CFR 63.111(b). Additionally, the pool is borated, which prevents criticality resulting from such collisions.

Fuel element collisions during transfer in the WHF pool are addressed by event 050-OpFuelImpact-HFI-NOD, "Operator Impacts Fuel Assembly During Transfer" (BSC 2009b, Table E6.8-1). This analysis states that the event is screened from consideration because "(1) criticality due to impact was screened out based on pool boration; criticality in this case is only an issue if it is accompanied by a loss of boration (screened out in Table 6.0-2 of the main report); and (2) airborne radioactivity release due to impact is bounded by the drop event." Consequences of the fuel assembly collision events are bounded by the fuel assembly drop events. These are evaluated in event tree WHF-ESD022-FUEL (BSC 2009b, Figure A5-36). SAR Tables 1.8-30 and 1.8-31 show that Category 2 event sequences that involve fuel assembly drops meet the 10 CFR 63.111(b) performance objectives.

Proper seating of an SNF assembly in the storage rack is considered to be an integral part of the insertion operation. Improper seating was not identified as an event sequence initiating event because it would not lead to a radiological consequence.

1.6 CASK OR ASSEMBLY TRANSFER SAFE LOAD PATHS

(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.

Response: The term "safe load path" as used in the PCSA differs from the concept of safe load path as defined in NUREG-0612, *Control of Heavy Loads at Nuclear Power Plants* (NRC 1980). The focus of NUREG-0612 is on minimizing the consequences of a potential heavy load drop by avoiding movement over safe shutdown equipment or over irradiated fuel. In the repository waste handling facilities, the heavy loads themselves typically contain irradiated fuel, and the focus of the repository fuel handling activities is on minimizing the likelihood of collisions and drops involving waste containers as they are being moved within the facility.

The consequences of potential collisions involving waste containers are controlled by the NSDB that limit the speeds of mechanical handling equipment such as the cask handling cranes and the cask transfer trolleys. As a result, the waste containers in transit have very low kinetic energies, and potential collisions do not result in a release of radioactivity. The concept of safe load paths is invoked in the PCSA as part of the determination of the contribution of human error to the probability of a collision event.

The observance of safe load paths is not relied upon to prevent or mitigate the consequences of event sequences. The establishment and use of safe load paths is a nuclear industry "best practice" that is implemented at the repository to reduce the likelihood that an operator error will initiate a collision event.

Fuel assembly and cask handling in the surface facilities is performed by the equipment described in the following paragraphs. Except where indicated, non-ITS instrumentation and controls are used to control and limit load movement. Safe load paths will be identified in the operating procedures or associated drawings as part of detailed design.

- **Spent fuel transfer machine**—The designation of safe load paths for the spent fuel transfer machine will restrict fuel assembly movements to the desired travel paths between the DPC unloading location, the TAD canister loading locations, and the SNF staging racks.

- **Cask handling crane**—Each of the waste handling facilities has a cask preparation area, where an arriving transportation cask is moved by the cask handling crane from its conveyance to a waiting cask transfer trolley or, in the case of the WHF, to a preparation station. Cask transfers typically require one or two horizontal crane movements and travel distances are short, generally less than 50 feet. The designation of safe load paths will restrict cask movements to the open floor areas between the conveyance and the cask destination. In the WHF, this approach also applies to cask movement by crane between work stations and to and from the pool.

- **Cask transfer trolley**—In each of the waste handling facilities, cask transfer trolleys operate in a straight line between a cask preparation area and a location where a waste canister is unloaded from the cask. In the WHF, the cask transfer trolley is also used in a similar manner to load a waste canister into a shielded transfer cask. Travel distances are short, and the straight line travel path is the safe load path. Guide rails and an end stop are provided inside the unloading rooms to aid in centering the cask transfer trolley under the cask transfer port. These features also aid in keeping the cask transfer trolley on its safe load path.

Cask handling equipment operating in the vicinity of the WHF decontamination pit and the pool are the cask handling crane and the cask transfer trolley. The crane carries casks over the pit and the pool as part of operations. Non-ITS zone controls prevent the cask handling crane from inadvertently carrying a load over the pool or over the SNF staging racks without deliberate operator action. It is not possible for the cask transfer trolley to inadvertently come into proximity with the decontamination pit or the pool because of the circuitous path that it would be required to traverse. In addition, cask transfer trolley travel is limited by the length of its umbilical air line.

1.7 INCLUSION OF SPECIFIC ACTIONS IN INITIATING EVENTS FOR THE CANISTER RECEIPT AND CLOSURE FACILITY

(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.

Response: There are four requests in the above statement. The first three questions are specific to each of the actions identified below and request the following information: (1) explain how each of the actions listed below were addressed in the initiating events analysis, (2) describe any equipment and components involved with these actions, and (3) explain if these actions are

included in the hazards and operability (HAZOP) analysis. The fourth question is generic in nature and involves explaining how DOE determined it had identified all risk-significant hazards and initiating events for all preclosure operations.

The answers to the first three questions are provided below. In response to the fourth question, the DOE employed a comprehensive approach for identification of initiating events that employed both master logic diagrams and HAZOP methodologies. This was accomplished by performing a detailed review of each facility's processes and operations. Each facility's processes and operations were then segmented into discrete elements delineated by completion of a process step within the overall process such as unloading the transportation cask from a railcar. Each of these elements was then analyzed using master logic diagrams to identify hazards and initiators associated with the activity. After the master logic diagrams were finished, a HAZOP analysis of the processes was performed to confirm the adequacy and comprehensiveness of the findings of the master logic diagrams. This methodology is summarized in SAR Section 1.6 and explained in detail in Sections 4 and 6 in the set of event sequence development analyses (e.g., BSC 2008).

1.7.1 Cask Alignment in the Cask Unloading Room Prior to Unloading a Cask

1) Alignment of cask in the Cask Unloading Room prior to unloading a cask by the Canister Transfer Machine.

Response:

- **Initiating Event Identification and Inclusion In the HAZOP Analysis**—Cask alignment in the Cask Unloading Room was identified in the master logic diagram as CRC-1604 "Canister strikes port edge CTM slide gate or wall leading to canister drop" in *Canister Receipt and Closure Facility Event Sequence Development Analysis* (BSC 2008, Figure D16, p. D-17). Table 10 in this analysis, "Listing of Internal Initiating Events," provides a cross-reference to the associated HAZOP table, where this event was addressed, and also shows the event sequence diagram figure addressing the event. Cask alignment was identified in HAZOP Node 14.

- **Initiating Event Analysis**—In the fault tree, misalignment is assumed to occur; the fault tree evaluates a failure to mitigate the collision. The events evaluated in quantifying these failures are under gate 36-23-3, titled "failure of weight limit control to stop hoist," in the gate-36-58 subtree portion of ESD9-*nnn*-DROP fault trees in the SAPHIRE model where "nnn" represents the code for the waste form (e.g., TAD canister, DPC) in the event sequence diagram name.

Actions and Equipment Involved—The cask and aging overpack unloading operations are performed in the Cask Unloading Room. The cask and aging overpack are positioned under the facility transfer port using a cask transfer trolley and a site transporter, respectively. A cask pedestal is positioned and secured onto the cask transfer trolley platform center. A cask is placed on the pedestal center and secured. Guide features (recessed surface area/guide pins) are provided on both the cask transfer trolley platform

and pedestal top for cask centering on the cask transfer trolley. The cask transfer trolley holding the cask is moved into the Cask Unloading Room and the cask center is aligned with the transfer port center using two removable floor-mounted side guides and the end stop. The cask transfer trolley is capable of positioning a cask center within 0.5 inches of the transfer port center.

The CTM is equipped with a computer vision system that provides precise object positioning information. This system is very similar to the system presently used in La Hague, France for a similar application. A video image of the object is taken, software translates the information into x- and y- coordinates, and information is fed to an encoder feedback system to drive the bridge and hoist trolley/grapple to engage with the lifting feature on the canister to perform a canister loading/unloading operation. None of this equipment is credited in preventing a misalignment or for quantifying event sequences.

1.7.2 Waste Package Alignment in the Waste Package Positioning Room Prior to Loading a Waste Package

2) Alignment of the waste package in the Waste Package Positioning Room prior to loading a waste package using the Canister Transfer Machine.

Response:

- **Initiating Event Identification and Inclusion In the HAZOP Analysis** —Waste package alignment in the Waste Package Positioning Room was identified using the same event used to identify cask misalignment in the Cask Unloading Room, event CRC-1604 (BSC 2008, Figure D16). This event is under the branch of the master logic diagram that accounts for damage occurring when a canister is raised or lowered by the CTM. Misalignment is not specifically or uniquely considered; the event of concern involves impacts during raising or lowering a canister with the CTM, regardless of the cause. Table 10 in this analysis, "Listing of Internal Initiating Events," provides a cross-reference to the associated HAZOP table, where this event was addressed, and also shows the event sequence diagram figure addressing the event. Cask alignment was identified in HAZOP Node 14.

- **Initiating Event Analysis**—Contributions to event sequences where misalignment could be a contributor are considered in the CRCF-ESD09 event trees, as discussed above. These event sequences address any impacts that would result from misalignments.

- **Actions and Equipment Involved**—Loading of an empty waste package in the waste package transfer trolley is performed in the Waste Package Loadout Room. As part of this assembly/preparation operation, a predetermined reference distance between waste package center and end of the waste package transfer trolley is maintained. The alignment of empty waste package center (when the waste package is on the waste package transfer trolley) with the transfer port center (in the Waste Package Positioning Room) is achieved by the rails controlling the lateral distance

and the end stop controlling the longitudinal distance. This approach is very similar to providing x- and y- coordinates on a crane system for equipment positioning. This methodology allows for aligning the two centers within 0.1875 inches. The alignment of CTM hoist/grapple with waste package center is accomplished by using computer vision technology, as discussed previously.

1.7.3 Alignment of the Canister Transfer Machine over a Port Prior to Canister Transfer

3) Alignment of the Canister Transfer Machine over a port prior to a canister transfer.

Response:

- **Initiating Event Identification and Inclusion In the HAZOP Analysis**—All misalignments were addressed in the context of the failure to mitigate the results of a canister striking the port structures, regardless of the cause. Misalignment is not specifically or uniquely considered; the event of concern is an impact during raising or lowering of a canister with the CTM, regardless of the cause. As such, this event is also included in CRC-1604. Table 10 in this analysis, "Listing of Internal Initiating Events," provides a cross-reference to the associated HAZOP table, where this event was addressed, and also shows the event sequence diagram figure addressing the event. Cask alignment was identified in HAZOP Node 14.

- **Initiating Event Analysis**—Contributions to event sequences where misalignment could be a contributor are considered in the CRCF-ESD09 event trees. These event sequences address any impacts that would result from misalignments.

- **Actions and Equipment Involved**—The x- and y- coordinates for the transfer port center is fed to the CTM computer vision system. The CTM hoist/grapple is aligned with the transfer port center to perform the canister loading/unloading operation.

1.7.4 Use of the Guide Sleeve

4) Use of the guide sleeve as described on Page 1.2.4-29 of the SAR.

Response: The guide sleeve guides the canister into the cask, waste package, or aging overpack. The guide sleeve was not considered in the initiating events since it was incorporated into the CTM design in parallel with the development of the event sequence analysis to ensure that drops of canisters from the CTM are nearly flat-bottom drops. When incorporated into the design, no malfunctions associated with the guide sleeve were identified that would contribute to the initiating event frequency for any sequence. The drop angle is treated as part of the pivotal events in the event tree. There is no distinction made within the initiating event as to drop angle. All drops are included.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2008. *Canister Receipt and Closure Facility Event Sequence Development Analysis.* 060-PSA-CR00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080221.0008; ENG.20080314.0005; ENG.20090109.0006.

BSC 2009a. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

BSC 2009b. *Wet Handling Facility Reliability and Event Sequence Categorization Analysis*. 050-PSA-WH00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0006.

NRC (U.S. Nuclear Regulatory Commission) 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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.

1. RESPONSE

1.1 CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS AS IMPORTANT TO SAFETY

The representation of event sequences in the preclosure safety analysis is consistent with the design of the geologic repository operations area facilities as documented in the reference design documents cited in the six event sequence development analyses and six event sequence reliability and categorization analyses that are referenced in the SAR.

The process for classifying structures, systems, and components (SSCs) as important to safety (ITS) or non-ITS is described in SAR Sections 1.6.1, 1.6.2, and 1.9. SAR Table 1.9-1 presents the SSCs that have been classified as ITS in the preclosure safety analysis. Classification as ITS is based on the specific preclosure safety functions that the SSCs perform and whether they are relied upon to prevent (i.e., reduce the probability of) the occurrence of an event sequence or mitigate the consequences of an event sequence, as demonstrated in the event sequence analyses. The ITS SSC preclosure safety functions are presented in SAR Tables 1.9-2 through 1.9-7. These tables identify ITS SSCs at a high level of assembly (e.g., a large piece of equipment such as the canister transfer machine). The design presented in SAR Sections 1.2, 1.3, and 1.4 describes the ITS and non-ITS portions of the design in more detail and includes more details associated with SSC classification.

For example, the canister transfer machine is classified as ITS based on the analysis of this SSC. The subcomponents designated as ITS for the canister transfer machine are included in SAR Figure 1.2.4-51, the process and instrumentation diagram for this SSC.

The specific examples described in this RAI are excerpted and discussed in the following subsections.

1.2 CASK PREPARATION PLATFORM OPERATIONS TO PREVENT CASK LID DISPLACEMENT

(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.

The preparation platform and shield plate are designed such that inadvertent displacement of the lid (i.e., Basic Event 060-Liddisplace1-HFI-NOD) cannot occur. The cask preparation subsystem in the Canister Receipt and Closure Facility (CRCF) is described in SAR Section 1.2.4.2.1.1.3.1. For cask preparation operations in the CRCF, a cask containing a dual purpose canister (DPC) is moved to the cask preparation platform, which is located in the cask preparation area of the CRCF. The top deck of the cask preparation platform is made of steel plates with appropriate thickness and orientation to meet as low as is reasonably achievable objectives. A circular opening on the raised platform deck is provided to access casks positioned under this opening through the platform shield plate system. The associated activities for cask preparation are described in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Section E6.3).

The platform shield plate system is mounted on the cask preparation platform deck, covering the platform opening when a cask is positioned below. The shield plate system consists of a rotating shield plate with several strategically located openings (small hatches) to access various cask bolt patterns below. The bearing-mounted shield plate is rotated using a drive system, similar to a rotating table, which allows access to any bolt on a cask positioned under the cask preparation platform. The platform shield plate system, located on two rails, is equipped with a drive system to allow it to move away from the platform deck opening, thereby providing complete access to the cask top below. Both the cask preparation platform and platform shield plate system provide shielding to the operators working on the platform.

Cask preparation activities for a DPC in the CRCF involve the use of the preparation platform, the platform shield plate, and common tools. The following steps are performed by an operator to preclude inadvertently displacing a lid:

1. Position the transportation cask containing a DPC under the cask preparation platform opening.

2. Remove the first cask lid bolt via access through an appropriate shield plate hatch opening.

3. Rotate the shield plate and align the shield plate hatch opening with the next bolt on the cask lid and remove the bolt.

4. Repeat the operation for all cask bolts.

5. Move the shield plate system away from the cask platform opening for crane access to the cask top.

6. Using the 20 ton auxiliary hoist, align and place the cask lid lifting adapter on the cask lid using the tapped holes provided on the cask lid. Move the auxiliary hoist to prepare for the next operation.

7. Move the shield plate system back over the cask platform opening. Since the cask lid lifting adapter does not protrude beyond the platform opening, the shield plate system movement will not impact and displace the lid adapter.

8. Since the cask lid lifting adapter is completely protected by the shield plate and not accessible to the crane rigging above, insert a long-reach tool/torque tool through the shield plate hatch opening to secure the cask lid lifting adapter to the cask lid.

As stated in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Tables E6.3-1, 6.4-1, and E6.8-1), due to the design of the preparation platform, improperly stowed rigging during this operation does not catch the lid lift fixture. The design includes a raised platform and a shield plate such that the cask is recessed underneath the platform and protected by the shield plate. Because the cask is always surrounded by the platform and the top is below the platform deck, loose or improperly stored rigging cannot come into contact with the cask except through the access port that is normally covered by the shield plate. When the plate is moved aside to allow a lid lift fixture to be moved into place by the auxiliary hoist, the cask is still below the platform deck, and only the center portion of the lid can be accessed through the uncovered access port while the lid lift fixture is being placed. During this operation, rigging can only come into contact with the top of the lid, which does not have any protrusions or edges that the rigging could catch on. The sides of the lid and cask cannot be accessed, as they are covered by the platform and platform deck.

The CRCF cask preparation platform is classified as ITS, as shown in SAR Table 1.9-1, as a result of the seismic event sequence analysis. The safety function relied upon for this ITS SSC (protect against platform collapse) is presented in SAR Table 1.9-3. As described above, the design of the cask preparation platform is such that it cannot cause an initiating event associated with lid displacement.

1.2.1 Inadvertent Opening of Transport and Emplacement Vehicle Doors

(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.

The preclosure safety analysis determines the probabilities of event sequences leading to direct exposure, including exposure caused by inadvertent opening of the Transport and Emplacement Vehicle (TEV) shield doors. The failure of the ITS mechanical switch or interlock (such that power is not removed) is part of the fault tree analysis and has a low occurrence frequency. Inadvertent actuation of the TEV shield doors, leading to direct exposure of personnel, has been determined to be a Category 2 event sequence (for which worker dose calculations are not required).

The TEV is classified as ITS, as shown in SAR Table 1.9-1. The safety functions relied upon for the TEV are presented in SAR Table 1.9-7, including the safety function of protecting against direct exposure of personnel. To accomplish this safety function, the TEV design incorporates an onboard hardwired ITS shield door (permissive) interlock that interrupts power to the shield door locks and motors when deactivated and prevents the operator from unlocking or opening the shield doors. This ITS interlock is engaged by an ITS mechanical switch that is located on the TEV in such a manner that its actuation is accomplished mechanically by an ITS stationary actuating bracket located on the TEV rails inside a waste handling facility loadout room or in a turnout of an emplacement drift. Once the ITS mechanical switch is activated, power is re-established to the ITS shield door interlocks so that the operator can open the shield doors via commands sent through the non-ITS programmable logic controller. Confirmation that the shield door control is available is visually indicated to the operator on the human–machine interface console in the Central Control Center Facility (CCCF). A signal generated by the ITS interlock contactor closure and opening is sent via the on-board non-ITS PLCs to the non-ITS Digital Control and Management Information System located in the CCCF for the purpose of TEV monitoring only. The function of preventing inadvertent opening of shield doors is accomplished by a hardwired ITS interlock that does not need confirmation in any way. Operation of the interlock and the TEV is explained in more detail below.

During a waste package loadout operation in the Initial Handling Facility or a CRCF, the TEV is controlled by an onboard non-ITS programmable logic controller system and monitored from the CCCF. As the TEV enters the facility loadout room, its forward motion engages the mechanical actuating bracket, thereby changing the interlock switch position, allowing power to be applied to the TEV front shield door locks. Following switch actuation, unlocking and opening of the front shield doors is permitted upon operator command. The front shield doors are unlocked and

opened, and the rear shield door is raised. The base plate is extended, and the shielded enclosure is lowered to accept the waste package on its emplacement pallet. Following the waste package loading operations, the facility exterior shield doors are opened, and the TEV exits the facility. As the TEV exits the loadout room, the ITS mechanical switch position is deactivated (changed to the open position) by the mechanical actuation bracket, thereby interrupting power to the shield door locks. This action prevents a spurious signal from inadvertently opening the shield doors during transit.

A similar operation takes place during emplacement. After the TEV stops at the emplacement access doors, various positional sensors and devices onboard establish a positional data point. The emplacement access doors are opened long enough to admit the TEV into the drift. When the TEV enters the emplacement drift, the stationary actuating bracket operates the ITS switch, closing the contact, thereby allowing unlocking of the front shield doors and the raising of the rear shield door. The waste package emplacement operations follow.

In summary, for waste package loadout and emplacement operations, the TEV shield doors are interlocked (through the use of an ITS mechanical switch) to remove power upon exiting a facility or an emplacement drift; power is restored upon entering an emplacement drift or facility. Confirmation of the signal is not relied upon to prevent inadvertent shield door opening; therefore this function is not ITS.

1.2.2 Transport and Emplacement Vehicle Shield Door Interlock

- 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.

A description of the TEV ITS mechanical switch and its operation is provided in the response to the first bullet of part (b) of this RAI. Before exiting the facility loadout room, assurance that the ITS mechanical switch that allows power to be applied to the shield door locks and motors has been deactivated is confirmed by a signal sent by a TEV programmable logic controller to the human–machine interface console in the CCCF. In addition, the operator will be required to implement a confirmation test by attempting to unlock and open the TEV shield doors before the TEV exits a loadout room (under conditions that have precluded personnel access). Inability to unlock and open the doors upon operator command confirms that the ITS mechanical switch is deactivated. In addition to instrumentation readings, observation that the TEV shield doors are not open is visually provided by cameras in the loadout room. These confirmation activities and the associated confirmation equipment are non-ITS as they are not relied upon to prevent an event sequence. Only the mechanical interlocks are ITS for the safety function of preventing the doors from opening.

Continuous monitoring of the TEV functions is provided by the TEV programmable logic controller. Should a step not be completed properly, the programmable logic controller either stops and aborts the sequence or executes the step identified for improper step completion; in either case, a message is provided to the CCCF operator. Inadvertent activation of the ITS interlock during transfer from the loadout room to the emplacement drift is prevented by locating the ITS mechanical switch on the TEV in such a manner (e.g., a recessed switch) that activation can only be accomplished mechanically by the stationary actuating brackets attached to the TEV rails. In addition, rocks or debris on or near the TEV rails that could conceivably activate the ITS mechanical switch would be detected by the TEV cameras or the TEV range detectors. The TEV also incorporates rail sweepers to remove debris from the track to avoid inadvertent activation of the ITS mechanical switch. Finally, the TEV and its travel path are closely monitored visually during transit from the loadout room to the emplacement drift; rocks and debris would be detected by operations personnel before they could interfere with TEV operations.

1.3 SLIDE GATE MOTORS AND CANISTER DAMAGE

(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.

As seen in SAR Table 1.9-1, in the CRCF, the DOE canister slide gates; cask port slide gates; transportation, aging, and disposal canister slide gates; and waste package port slide gates are classified as ITS based on their intended safety functions. The preclosure safety functions for these slide gates are presented in SAR Table 1.9-3, including the preclosure safety function of precluding canister breach. As presented in SAR Table 1.9-3, a “preclude canister breach” safety function is listed, with an accompanying nuclear safety design basis stipulating that closure of the slide gate shall be incapable of breaching a canister. The design criteria for the CRCF slide gates are presented in SAR Table 1.2.4-4.

Slide gate motor power is limited such that a slide gate closing on a canister, canister transfer machine canister guide sleeve, or the canister transfer machine hoist rope has insufficient force to breach the canister, deform the guide sleeve, or sever the hoist rope. Specifically, based on the continuous stall torque of the drive motor, the maximum effective stress imposed on a canister wall is not permitted to exceed two-thirds of the canister material yield stress. Keeping the imposed stress below yield ensures that the canister integrity is maintained. In addition, the mechanical torque switches integral to the slide gate motors prevent canister breach by limiting the closing force, consistent with the above criteria.

1.4 CANISTER DROP INSIDE A CANISTER TRANSFER MACHINE SHIELD BELL

(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 intact 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.

The canister transfer machine slide gate is designed to withstand a 12 in. vertical drop of the heaviest canister. The stiffness of the canister transfer machine slide gate, when subject to the impact of a dropped canister, is equivalent to that of a 100-in. square, 10-in. thick, solid carbon-steel plate that is supported at an opening with a diameter of 88 in. The canister transfer machine structural and shielding components, including the slide gate and supporting structures such as the shield bell, shield bell trolley, and bridge are designed to withstand the drop impact and remain intact. The shielding would remain in place and perform its intended function. As discussed in SAR Section 1.2.2.2.9, ITS mechanical handling equipment is designed for applicable loads associated with design bases established to prevent or mitigate Category 1 and Category 2 event sequences.

1.5 CANISTER TRANSFER MACHINE ADJUSTABLE SPEED DRIVE FAILURE

(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.

The "CTM high drops from 2-blocking events" fault tree is presented in Figure B4.4-16 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009). As shown in this figure, under the top event is an OR gate linking two gates: "op event with two block event" (the canister must be lifted above normal heights associated with a lift) and "two block related failures" (features designed to limit the drop height must fail).

The "Failure of the ASD" AND gate is shown under Gate 36-184 ("op event with two block event") in the fault tree presented in Figure B4.4-17. This gate is under the "op event with two block event" side of the fault tree. The intent of this gate is to indicate the failure of the adjustable speed drive to stop the lift of a canister by the hoist; it is not to indicate failure of the adjustable speed drive to provide control.

As indicated in the fault tree, for this intermediate event to occur, the optical sensor detecting that the canister is above the slide gate must fail and the operator must have initiated the lift of the canister such that it eventually proceeds to the two-block height (if it is accompanied by failure of the two limit switches). Normally, the optical sensor at the bottom of the shield bell that is hard-wired to the adjustable speed drive will erase the lift command once the canister has cleared the sensor. In the absence of the signal to erase the lift command, the adjustable speed drive will fail to stop the hoist prior to the canister reaching the adjustable speed drive stop point, thereby contributing to the potential for a lift toward the two-block height.

Failure of the adjustable speed drive component is captured under the AND gate titled "two block related failures" (GATE-36-200). As seen in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Figure B4.4-18), a basic event titled "CTM Hoist ASD controller fails" (under the OR gate titled "mechanical faults cause canister to be raised too high") represents the failure of the adjustable speed drive component.

1.5.1 Canister Transfer Machine Hoist System Component Failures

- 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.

The interlock and brake solenoid are ITS fail-safe components that ensure that the system either remains in, or reverts to, a safe state in the event of failure of either component. The holding brake will engage if either component fails.

Electric motor failure will be detected by one of several means described below, which are dependent on the mode of failure and will result in the hoist brake being set to stop hoist movement in each case. In the case of motor overheating, motor winding resistance temperature detectors will detect a high motor winding temperature condition and activate the adjustable speed drive stop command to stop hoist motion and engage the hoist brake. If power is lost to the system, the hoist brake solenoid will de-energize, causing the hoist brake to set. If power is lost to the motor only, or if a mechanical coupling fails, the most likely result would be an increased hoist speed while lowering. This would be detected by the overspeed switch, which will cause the hoist brake and emergency hoist drum brake to set. These protective defense-in-depth features are present in accordance with the requirements of ASME-NOG-1-2004, *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)* for Type I cranes.

The non-ITS canister hoist position encoder is a direct input to the adjustable speed drive; it will stop the adjustable speed drive at a designated automatic speed drive stop point. This stop point is lower than that of the first upper travel limit switch. Therefore, if the encoder fails, the first upper travel limit switch will stop hoist movement. This encoder signal is treated the same as a programmable logic controller input to the adjustable speed drive and is, therefore, not credited to preclude any event sequence in the canister transfer machine fault trees.

1.5.2 Canister Transfer Machine Hoist Holding Brake and Electric Motor Response to Adjustable Speed Drive Signal

- 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.

The logic for the adjustable speed drive is presented in SAR Figure 1.2.4-55. When a control signal is given to raise or lower the hoist, the adjustable speed drive "hoist raise command" or

"hoist lower command" will be activated, provided that all the system interlocks for that command are in a permissive state. When either the "hoist raise command" or "hoist lower command" is activated, the "hoist stop command" is deactivated, which in turn activates the "energize coil to release holding brake" command to disengage the hoist holding brake. In the absence of any command to raise or lower the hoist, the adjustable speed drive "hoist stop command" remains active, which in turn keeps the holding brake solenoid in a de-energized state to keep the holding brake engaged. These protective defense-in-depth features are present in accordance with the requirements of ASME-NOG-1-2004 for Type I cranes.

1.5.3 Adjustable Speed Drive Control Software Failure

- Explain how DOE accounts for failure associated with the control software on the ASD.

An adjustable speed drive is a commonly used device that includes an embedded microprocessor, programmed in firmware, to govern the operation of the unit. The firmware is inaccessible to the adjustable speed drive user. However, the operating parameters can be set via an interface menu on the unit. The controls are considered to be integral to the unit, and industry data on reliability used in the preclosure safety analysis applies to the unit as a whole, not its individual components (both hardware and firmware). Failure of the adjustable speed drive embedded control software is, therefore, not considered as a separate failure mechanism in the preclosure safety analysis.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

ASME (American Society of Mechanical Engineers) NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672.

BSC (Bechtel SAIC Company) 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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-TEVDOORHFI-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 7.94×10^{-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

- 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 1.74×10^{-3}. The MathCad file, "HC FOD Hand Controller Demand Failure.xmcd" shows a mean value of 2.85×10^{-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-HLWFAIL-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-LIDIMPACT," 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.

1. RESPONSE

The representation of failure events documented in Section 6 and Attachment E of the Preclosure safety analysis documents is consistent with the SAPHIRE models in Attachments B and H of these documents because Section 6 was derived from SAPHIRE results and Attachment E provides the human reliability inputs to the SAPHIRE models. Examples of this consistency are provided in the responses to the individual examples cited in the RAI.

The sections of the RAI are excerpted and discussed in the response subsections:

1.1 TRANSPORT AND EMPLACEMENT VEHICLE INITIATING EVENT PROBABILITY FOR INADVERTENT SHIELD DOOR OPENING

(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.

The event "prolonged immobility," does not result in shielding loss (as further discussed in the response to RAI 2.2.1.1.3-3-018) and therefore, does not result in an event sequence with an increase in radiological exposure, as defined in 10 CFR 63.2. There are no important to safety

(ITS) structures, systems, or components (SSCs) required to prevent prolonged immobility. Consequently, an initiating event probability for prolonged immobility is not risk significant and does not contribute to the transport and emplacement vehicle (TEV) design bases.

1.1.1 Discussion Regarding Programmable Logic Controller, Mission Time, and Human Failure Event

(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.

1.1.1.1 How Spurious Operation of the Programmable Logic Controller Captures Failure Modes

A programmable logic controller spurious operation failure mode is represented in the SHIELD-DOOR fault tree (BSC 2009b, Figure B1.4-36) by a basic event titled "PLC Spurious Op – TEV Doors." This basic event represents a programmable logic controller failure in which a spurious signal is sent from the programmable logic controller to open the TEV shield doors. Spurious operation is defined as a failure that inadvertently initiates an undesired open signal. As such, this basic event encompasses all failure modes from the PLC that could result in an open signal. This value was derived by using the geometric mean of the hourly failure rate of programmable logic controllers obtained from *Nonelectronic Parts Reliability Data 1995* (Denson 1994) and *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment* (SAIC 2002, Table E2-2). These sources provide information on the cumulative failure rate involving all modes of SSC failure (hardware and software). This value was then adjusted to account for the percentage of the overall hourly failures that resulted in an undesired signal. This percentage was obtained from *Failure Mode/Mechanism Distributions 1997* (Crowell 1997), which provides a distribution of the cumulative failure rate over failure modes or mechanisms.

1.1.1.2 Independence of Programmable Logic Controller and Interlock

The programmable logic controller and ITS interlocking mechanical switch are functionally and physically independent of each other. The interlock is a mechanical switch actuated by a bracket on the rail when the TEV enters or leaves an emplacement drift or a facility loadout area (see also the response to RAI 2.2.1.1.3-3-011 (b) for additional information). The interlock is hardwired within the electrical circuits for unlocking the front shield door locks (shot bolts) and for raising the rear shield door. The switch contact must be closed for power to be applied to these actuators. When outside the waste package loadout areas and emplacement drifts, the ITS switch contact is open so the TEV shielded enclosure doors cannot open until the TEV is either

in a facility loadout area or an emplacement drift. The TEV is remotely actuated and monitored by operators in the Central Control Center Facility (CCCF) using the Digital Control and Management Information System interfacing to the onboard redundant programmable logic controller. The programmable logic controller is used only to implement equipment operations as directed by the operator; it does not perform ITS functions, and it is not relied upon to prevent or mitigate an event sequence. Consequently, the programmable logic controller is not identified as ITS. Since the programmable logic controller and ITS mechanical switch are independent of one another and are of diverse designs, there is no common cause or common mode failure mechanism (e.g., single point failure) associated with the PLC or the ITS interlock that could lead to inadvertent opening of the TEV shield door.

1.1.1.3 Non-ITS Programmable Logic Controller Single Point Shield Door Failure

As described above, the programmable logic controller is non-ITS because it is not relied upon to prevent or mitigate an event sequence. The preclosure safety analysis (PCSA) includes programmable logic controller failures as contributors to inadvertent opening of the shield doors; however, the previously described interlock prevents power from being applied to the shield door actuators independent of the programmable logic controller, any independent malfunction of the programmable logic controller, software or hardware, can not cause the doors to inadvertently open.

1.1.2 Transport and Emplacement Vehicle Inadvertent Shield Door Opening 4-Hour Mission Time

- 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.

The conservative estimate of time required for the TEV to transit from a facility loadout area to inside an emplacement drift is 8 hours. During the transit, opening of the shielded enclosure doors is prevented by a hardwired interlock that interrupts power to the door locks. This switch changes position at the beginning and end of the transit. The position of the switch (open or closed) is indicated in the control room. The transit time can then be considered equivalent to a test interval for the interlock. Because the failure probability of the interlock is uniformly distributed over this interval, the average unavailability is $1/2\lambda t$ (Vesely 1981). This is represented in the analysis as a mission time-based expression of λT, where $T = 1/2t$, and $t =$ 8 hours. If 8-hours (t) is used instead of 4-hours (T), the point estimate approximately doubles from 1.4×10^{-7} to 2.8×10^{-7}, with the mean increasing from 1.15×10^{-7} to 2.30×10^{-7}. This does not impact the event sequence categorization or the conclusions of the analysis.

1.1.3 Transport and Emplacement Vehicle Human Failure Event Assumption Tracking

- DOE describes a human failure basic event (i.e., 800-HEE0-TEVDOORHFI-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.

1.1.3.1 Meaning of Term "Semiautomatically"

The term "semiautomatically" is used to describe the interaction between the operator and TEV automated control circuitry. The programmable logic controller includes programming for various operational sequences for the TEV. These sequences may be short and simple or may be collections of simple sequences; branching may be provided based upon sensed conditions. The operator in the CCCF causes an operational sequence to be performed by verifying the programmable logic controller is in the programmed mode, selecting the operational sequence to be performed and then giving the command to initiate the sequence. The programmable logic controller then executes the steps associated with that sequence, including the verification that any required control permissives are met for the steps. Should a step not be completed properly, the programmable logic controller either stops and aborts the sequence or (if in the programming) executes the step identified for improper completion. In either case, a message is provided to the CCCF operator. The operator also has the capability to stop the sequence at any time. Upon completion of the sequence, the programmable logic controller identifies completion to the operator, who then determines the next appropriate command for the TEV, in accordance with operating procedures and repository and TEV conditions.

1.1.3.2 Assumption Tracking

Control features in the event titled "800-HEE0-TEVDOORHFI-NOD" (e.g., operator training, controls being distinct) are not tracked through formal engineering procedures; although operators will be trained, the details of this training are not yet known. TEV controls are designed based on man-machine interface design (*IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations* (IEEE Std 1023-1988)); these guidelines provide that controls should be designed to be distinctive between groups and arranged by importance and frequency of use. Furthermore, consistent with the configuration management system, design changes are checked against PCSA assumptions for consistency. Formal tracking has been provided for the semiautomatic controls for opening the shield doors; descriptions of these controls can be found in *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle* (BSC 2008, Sections 2.5.2 and 3.3.15).

1.1.4 Transport and Emplacement Vehicle Immobility—Programmable Logic Controller

(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.

The response to RAI 2.2.1.1.3-3-018 demonstrates that prolonged immobility does not result in shielding loss. The event "prolonged immobility," therefore, does not result in an event sequence with an increase in radiological exposure, as defined in 10 CFR 63.2, and there are no ITS SSCs required to prevent prolonged immobility (see Section 1.2.2 of this response).

1.1.4.1 How Programmable Logic Controller Spurious Operation Captures All Failure Modes That Could Result in Prolonged Immobility

A programmable logic controller spurious operation failure mode is represented in the SHIELD-STOP fault tree (BSC 2009b, Figure B1.4-35) by a basic event titled "800-HEE0-PLCSPD1-PLC-SPO". This basic event represents a programmable logic controller failure in which a spurious stop signal is sent from the programmable logic controller to the drive motors. As such, this basic event encompasses all failure modes from the PLC that could result in an open signal. Spurious operation is defined as a failure that inadvertently initiates a stop signal; this is estimated in the failure rate data sources identified in the "YMP Active Comp Database.xls" (BSC 2009b, Attachment H) as a control component inadvertently sending a signal. This value was derived by using the geometric mean of the hourly failure rate of programmable logic controllers obtained from *Nonelectronic Parts Reliability Data 1995* (Denson 1994) and *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment* (SAIC 2002, Table E2-2). These sources provide information on the cumulative failure rate involving all modes of SSC failure. This value was then adjusted to account for the percentage of the overall hourly failures that resulted in an undesired signal. This percentage was obtained from *Failure Mode/Mechanism Distributions 1997* (Crowell 1997), which provides a distribution of the cumulative failure rate over failure modes/mechanisms.

1.1.4.2 Failures That Could Result in the Transport and Emplacement Vehicle Going to an Immobile State

The only interlock associated with the TEV in the current design is the ITS mechanical interlock that prevents the doors from opening when the TEV is between a facility loadout area and the emplacement drift. This interlock interrupts power to the shield door locks, and it cannot impact any other TEV controls. If a control permissive or programmable logic controller malfunctions,

then the operator in the CCCF would be alerted of the failure, existing and potential conditions would be evaluated, and subsequent actions would be determined and implemented. This failure is accounted for in the speed control spurious operation "800-HEE0-PLCSPD1-PLC-SPO" event. Other credible sources of TEV immobility, such as loss of power or third rail failure, have been identified and included in the aforementioned SHIELD-STOP fault tree.

1.1.4.3 Programmable Logic Controller is Not Identified as ITS; Software Errors That Could Result in Immobility

The programmable logic controller is not classified as ITS, and it performs no safety functions. However, software as part of the programmable logic controller could potentially result in some degree of TEV immobility ranging from slow or intermittent travel along the rail to complete immobility. In such a case, a retrieval vehicle would be used to retrieve the TEV if prolonged immobility was anticipated. As described above, this is not an initiating event of an event sequence because shielding degradation would not occur.

1.1.4.4 Transport and Emplacement Vehicle Fan Failure

- 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.

The current TEV design does not include a ventilation fan since thermal calculations have concluded that a ventilation fan on the TEV is not needed to maintain waste packages or TEV shielding below stated thermal limits (see response to RAI 2.2.1.1.3-3-018). Immobility simply stops operation until the TEV can be unloaded and removed to the Heavy Equipment Maintenance Facility for repair. Consequently, this event (fan failure) was not incorporated into the analysis. In light of the thermal results, the prolonged stop of the TEV is no longer an initiating event and, as such, fault tree SHIELD-STOP is a conservative model.

1.1.4.5 Transport and Emplacement Vehicle Overspeed Sensors

- 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.

The data used in *Nonelectronic Parts Reliability Data 1995* (hereinafter, NPRD-95) (Denson et al. 1994, Section 2, p. 182) are given under the heading of "Sensor, Speed". They are derived from a document entitled "Failure Rate Data of Temperature Sensors." However, the information given in the part details section of NPRD-95 (Denson et al. 1994, Section 3, p. 464) for the speed sensor indicates the data were based on part number "627504 – X, manufactured by Garret Mfg. Ltd." The style is listed as "DC10 APU," which is an auxiliary power unit on DC-10 aircraft, which use speed sensors to maintain the rotational speed of the auxiliary power unit. Because the

authors of NPRD-95 classified the data as pertaining to speed sensors and the underlying source document and part number lend credence to this classification, it was used as such in the PCSA.

1.1.4.6 Transport and Emplacement Vehicle Third Rail Failure

- 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.

The spreadsheets entitled "third rail failure estimate.xls" and "track (yard) accident rates.xls" are provided with this response. "Track (yard) accident rates.xls" contains the information from the Federal Railroad Administration Office of Safety Analysis "Train Accident Rates" (FRA 2009). These data can be obtained directly from the Federal Railroad Administration database by filtering for all railroads with yard tracks with a 3-year comparison from 2006 for the accident cause "Truck, Roadbed and Structures."

The information on this website is applicable to failure of the third rail used by the TEV, as it provides information concerning the hazards and risks that exist on the nation's rail yards. The Federal Railroad Administration collects information on railroad accidents and incidents that occur in every state related to railroads under its jurisdiction and is required by law to report and keep records for development of risk reduction programs. As such, this information was found to be applicable to use for the third rail of the TEV, as the repository tracks will be of the population represented in this database.

1.1.4.7 Loss of Offsite Power

- For loss of offsite power, DOE identifies a mean failure probability of 7.94×10^{-6}. Explain how this value was determined.

The mean failure probability is the probability that power will be lost for 2 hours, assuming a loss of offsite power annual frequency of 3.48×10^{-2} (*Subsurface Operations Reliability and Event Sequence Categorization Analysis,* (BSC 2009b, Section 6.0.2.2)). This annual frequency can be converted to an hourly frequency by dividing by 8,760 (i.e., the number of hours in a year). Multiplying this result by 2 hours yields approximately 7.94×10^{-6}. Two hours was estimated to be the time it would take to resolve the situation.

1.1.4.8 Transport and Emplacement Vehicle Fault Tree Mission Times

- 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.

As described previously in this RAI response and in the response to RAI 2.2.1.1.3-3-018, prolonged immobility is not an initiating event for an event sequence because there is no expectation of increased radiological exposure from shielding degradation. This conclusion arises from steady state temperatures during periods of immobility, which have been shown to stay below the degradation temperature of the shielding. Immobility simply stops operation until the TEV is removed to the Heavy Equipment Maintenance Facility for repair.

The SHIELD-STOP fault tree (BSC 2009b, Figure B1.4-35) was constructed treating third rail failure as a random failure during transit (λt) over the mission time. An 8-hour time represents the duration of a TEV travel from the surface facility to the emplacement drift. Programmable logic controller failures and overspeed sensors are monitored, and faults associated with these components are quantified based on their average unavailability over the mission time. The average unavailability is $1/2\ \lambda t$. In this case, the average unavailability was determined by halving the mission time (resulting in 4 hrs) in the database. See also Section 1.1.2 of this RAI, which describes the halving of the mission time per the $1/2\ \lambda t$ equation.

1.2 SITE PRIME MOVER

1.2.1 Site Prime Mover Governor Within a Facility

(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

A detailed discussion of the site prime movers is provided in the response to RAI 2.2.1.1.7-8-010. A summary description of the site prime movers follows.

There are three prime mover vehicles discussed in the SAR. A hybrid diesel-battery powered switcher locomotive is used to move multiple rail cars. The locomotive carries too much diesel

fuel to be allowed to enter buildings. However the waste handling facilities can accept a railcar pushed into the building when the railcar has a buffer car connected between the cask railcar and the locomotive. The locomotive is governed to limit its top speed to 9 mph.

A second prime mover vehicle is the truck tractor for moving truck casks on standard trailers. The event sequence analysis models a hybrid vehicle that is powered by a diesel engine when outdoors and by electric motor when the truck tractor enters the buildings that take trailer casks. In the facility, the truck tractor is operated by electric motor and gear drives that limit the speed. The limited speed of this vehicle is 2.5 mph.

The third prime mover is the mobile railcar mover capable of moving one or more loaded railcars. The event sequence analysis models a hybrid vehicle that is powered by a diesel engine when outdoors and by electric motor when the mobile railcar mover enters buildings with a railcar and cask. The mobile rail car mover is operated by electric motor when entering buildings. The electric motor and gear drives limit the speed. The limited speed of this vehicle is 2.5 mph.

It is correct that the governor would not be involved with the movement of a prime mover within a facility; however, the fault tree considers the potential for malfunctions of the governor as the vehicle enters the vestibule where it will be stopped and transitioned from diesel to electric power.

1.2.2 Data Conversion to Site Prime Mover Applicability

- 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.

Component reliabilities for the speed control failure (governor) and the pneumatic brake failure used in the development of the fault trees for the site prime mover in *Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis* (BSC 2009b), are based on a 2 mph speed. Table 6.9-1 of the analysis provides a design basis that limits the speed of the site prime mover to 9 mph within the geologic repository operations area. During the development of the "YMP Active Component database.xls" (BSC 2009b, Attachment H), the design speed limit for most vehicles was 2 mph. Because of uncertainty in this value, the error factor of 181 assigned to governor failure rate was established to cover a range of operating speeds that encompasses the 9 mph speed of the prime mover.

Therefore, the uncertainty bounds around the database mean values capture potential deviations in the speed of site vehicles.

1.2.3 Remote Control System Failure

- 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 1.74×10^{-3}. The MathCad file, "HC FOD Hand Controller Demand Failure.xmcd" shows a mean value of 2.85×10^{-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.

In reviewing Figure B1.5-9 of *Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis* (BSC 2009b), it was determined that the event in Figure B1.5-9 that corresponds to "Remote Control Transmits Wrong Signal" is ISO-SPMTT-HC001-HC—FOD. The value assigned to this event is 1.740×10^{-3}. This value corresponds to the value of 1.74×10^{-3} with an error factor of 83.9 given in the MathCad file "HC FOD Hand Controller Demand Failure.xmcd" (BSC 2009b, Attachment H). The value 2.85×10^{-3} with an error factor of 142.7 could not be found in the aforementioned MathCad file nor in the "YMP Active Comp Database.xls" (BSC 2009b, Attachment H).

In developing the PCSA database, a search of data sources was made to find applicable data across industries for each component type and failure mode included in the PCSA models. The following explains how the hand held controller demand failure rate was developed:

Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis (BSC 2009a, Section 3.2.1) states:

> Equipment and SSCs designed and purchased for the Yucca Mountain repository are of the population of equipment and SSCs represented in United States industry-wide reliability information sources. Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population…. It is appropriate to use such information because it represents similar pieces of equipment at the system level. In addition, drawing from a wide spectrum of sources takes advantage of many observations, which yield better statistical information regarding the uncertainty associated with the resulting reliability estimates.

On the basis of this assumption and the need to select the most applicable data available, a spectrum of controller data was identified and combined using Bayesian analysis to produce a distribution within which the hand held controller failure would be expected to reside.

Four failure probabilities were used for the component "Hand Held Radio Remote Controller (HC)" with failure mode failure on demand, as identified in "YMP Active Comp Database.xls" (BSC 2009b, Attachment H). Three of these probabilities were taken from *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Canavan 2004, page C-7, Table C-3): (1) a dead man stop handle (failure to stop), (2) an emergency stop button (failure to stop), and (3) a controller (mechanical jamming). This report describes radiological risks and consequences to individuals from a bolted cask containing spent fuel from a pressurized water reactor while the cask is on site. While the equipment types and operating environment might not be identical to the anticipated repository case, these could be used as surrogate information because the controllers and the operational situations would be similar to those at the waste handling facilities.

The remaining failure data was taken from *Nonelectronic Parts Reliability Data 1995* (Denson 1994, p. 2-125) for a joystick assembly from military experience. These data were included in part to provide a range of values for controllers within which the "HC FOD" data would reasonably reside.

An empirical Bayesian estimation was performed using these data, with the maximum likelihood estimate calculated in the supporting MathCad file, "HC FOD Hand Controller Demand Failure.xmcd" and shown in *Intra-Site Operations and BOP Reliability and Event Sequence Development Analysis* (BCS 2009c, Figure B1.5-9) with a mean value of 1.74×10^{-3} and error factor of 83.9. This error factor reflects a wide range of controller experience and, therefore bounds the problem such that it can be considered that the hand held controller performance is contained within these bounds.

1.3 HEAVY LOAD DROP ONTO HIGH-LEVEL RADIOACTIVE WASTE

(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.

1.3.1 Lid Drop onto High-Level Radioactive Waste

(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-HLWFAIL-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-LIDIMPACT," and Figure A5-43 of BSC, 2008b identifies this initiating event as branch #2.

Neither of the initiating events referred to as "Branch #2" or "Branch #6" in Table 6.0-2 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a) is screened out. A portion of Branch #6 associated with lid drop is screened out, as described below.

The "CRCF-ESD09-HLW" initiator event tree (BSC 2009a, Figure A5-43) identifies initiators associated with transferring a high-level radioactive waste (HLW) canister with the canister transfer machine from a transportation cask to a waste package or staging area for eventual transfer to a waste package. The event tree depicting the canister and facility response to this initiator is titled "RESPONSE-CANISTER1" (BSC 2009a, Figure A5-21). The two branches in "CRCF-ESD09-HLW" addressed in this inquiry are Branch #2 labeled "Impact with Lid Removal," and Branch #6 labeled "Object Dropped on Canister." Branch #2 depicts the situation in which the canister transfer machine may lift the transportation cask containing the HLW canister and subsequently drop it. Branch #6 depicts the situation in which a heavy object may drop onto the cask. Both of these branches transfer to the "RESPONSE-CANISTER1" event tree, which can link to different fault trees to quantify the response specific to the initiating event.

The probability that a transportation cask could be partially lifted and then dropped is quantified in initiating event "ESD9-HLW-LIDIMP" (Branch #6) (BSC 2009a, Attachment H). The response to this initiator is represented by the "RESPONSE-CANISTER1" event tree. The first pivotal event, "CANISTER," in this event tree is quantified with the "ESD9-HLW-LIDIMP-CAN" fault tree. The basic event "09-HLW-FAIL-LID-IMPACT" within this fault tree is "HLW Canister Fails from Dropped Cask." This basic event is used to quantify the probability that the HLW canister inside the transportation cask fails, given that the transportation cask is partially lifted off of the cask transfer trolley and drops back onto the cask transfer trolley during removal of the transportation cask lid. However, the canister transfer machine does not have the capacity to lift a cask with HLW canisters inside. The cask, therefore, will undergo little or no movement. This places insignificant stress on the HLW canisters, which have been demonstrated by tests to survive a 30-ft drop. Failure of HLW canisters in this situation (for the basic event "09-HLW-FAIL-LID-IMPACT") is physically unrealizable and assigned a value of zero.

To further clarify, "CRCF-ESD09-HLW" (BSC 2009a, Figure A5-43) is the event tree graphically depicting the initiators associated with transferring an HLW canister to a waste package or staging area. The event "09-HLW-FAIL-LID IMPACT" is used to quantify the fault tree "ESD9-HLW-LIDIMP-CAN" that quantifies the "CANISTER" pivotal event in the "RESPONSE-CANISTER1" event tree when the initiator is branch #2 of event tree "CRCF-ESD09-HLW."

1.3.2 Drop of Object onto Canister Initiator Event Tree

(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).

Branch #2 of the initiator event tree "CRCF-ESD09-HLW, Impact with Lid Removal" (BSC 2009a, Figure A5-43), refers to the potential for the cask being lifted and then dropped if operators attempt to remove a transportation cask lid and the lid binds or failed to remove one or more of the lid bolts before staging the cask below the canister transfer machine for lid removal and unloading. Branch #6 of the initiator event tree "CRCF-ESD09-HLW, Object Dropped on Canister," refers to the potential for a heavy object being dropped onto a canister during the transfer operation. The designs of the codisposal waste package and the transportation casks for HLW or DOE spent nuclear fuel (SNF) canisters ensure a lid drop will not impact the canisters inside. Consequently, lid drops are screened out of the quantification of Branch #6 and the associated response tree "RESPONSE-CANISTER1." Branch #6, however, quantifies a drop of either an HLW canister or DOE SNF canister onto a HLW canister.

1.3.3 Drop of Object Onto Canister Initiator Event Tree

(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.

Branch #6, "Object Dropped on Canister," is evaluated with the "ESD9-HLW-DROPON" fault tree. There are two instances in which something other than a lid can be dropped on a canister. First, during the time that the canister transfer machine is being positioned to grapple the canister, the grapple can drop. Second, during the time the canister transfer machine is lifting one canister from a transportation cask or into a waste package, a canister can drop. Basic events in the fault tree "ESD9-HLW-DROPON" quantify the likelihood that a drop could occur. The fault tree accounts for both opportunities with basic event "060-CTMOBJLIFTNUMBER."

1.4 TRANSPORT AND EMPLACEMENT VEHICLE RUNAWAY INITIATING EVENT CONSIDERATION

(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.

TEV runaway is screened out as an initiating event in *Subsurface Operations Reliability and Event Sequence Categorization Analysis* (BSC 2009b, Table 6.0-2) but included as a contributor to impact event sequences during transit. However, the TEV runaway, by itself, has a probability beyond the Category 2 event sequence threshold and does not require an associated dose consequence analysis.

The TEV runaway mentioned in *Subsurface Operations Reliability and Event Sequence Categorization Analysis* (BSC 2009b, Table 6.0-2) was screened out as an initiating event on the basis of a probability of occurrence of 1.7×10^{-5} during the preclosure period, which is beyond the Category 2 event sequence threshold. The TEV runaway was screened out as an initiating event in initiator event tree "SSO–ESD–03–SEQ–2–3," for the collision or derailment of the TEV, Branch #2 (BSC 2009b, Table 6.0-2). However, TEV runaway was included as a small contributor to another event tree, designated as initiator event tree "SSO-ESD-02" (BSC 2009b, Figure A5-3), which considers a TEV runaway in initiating event "TEV impact during transit," Branch #3. This initiating event input is represented by fault tree "TRANSIT-IMPACT" and it is linked to event tree "SSO-ESD-02." The "TRANSIT-IMPACT" fault tree developed in *Subsurface Operations Reliability and Event Sequence Categorization Analysis* (BSC 2009b, Section B1.4.4) models impacts to the TEV during transit and, as such, includes the possibility of a TEV runaway as one of the ways of impact during transit. This is modeled by the use of subtree "RNWY-INIT" described as "initiator for TEV runaway," which is an input to the top event OR gate "TRANSIT-IMPACT" (BSC 2009b, Figure B1.4-26). Other impacts to the TEV during transit consist of a worker driving a vehicle into the side of a TEV and a TEV collision with an object along the rail line.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2008. *Mechanical Handling Design Report: Waste Package Transport and Emplacement Vehicle*. 000-30R-HE00-00200-000 REV 003. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080725.0012.

BSC 2009a. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

BSC 2009b. *Subsurface Operations Reliability and Event Sequence Categorization Analysis.* 000-PSA-MGR0-00500-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0009.

BSC 2009c. *Intra-Site Operations and BOP Reliability and Event Sequence Categorization Analysis*. 000-PSA-MGR0-00900-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0008.

Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and AnalysisReport.* 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.

Crowell, W.; Denson, W.; Jawoski, P.; and Mahar, D. 1997. *Failure Mode/Mechanism Distributions 1997.* FMD-97. Rome, New York: U.S. Department of Defense, Reliability Analysis Center. TIC: 260074.

DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment.* MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.

Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995.* NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.

FRA (Federal Railroad Administration) 2009. "Train Accident Rates." Federal Railroad Administration Office of Safety Analysis. http://safetydata.fra.dot.gov/OfficeofSafety/publicsite/query/inctally2.aspx, last accessed on July 24, 2009.

IEEE Std 1023-1988(R2004). 2005. *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.* New York, New York: Institute of Electrical and Electronics Engineers. TIC: 258586.

SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.* Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.

Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; and Haasl, D.F. 1981. *Fault Tree Handbook.* NUREG - 0492. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 208328.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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).

1. RESPONSE

This response demonstrates that subcriticality is maintained in the Wet Handling Facility (WHF) pool for normal operations and end-states of event sequences with a significant margin even under hypothetical boron dilution scenarios.

The preclosure safety analysis, which includes criticality safety, will be maintained throughout the design, construction, and operational periods. Detailed design for construction will be evaluated for effects on the safety analysis and the potential identification of additional hazards, initiating events, and event sequences. Therefore, as the design evolves including piping layouts, sprinkler locations, hoses and hose connections, flow rates, etc., if necessary, the boron dilution analysis will be updated to confirm that the current criticality safety analysis bases remain valid, and, if needed, additional design and operational requirements will be established.

1.1 WHF POOL AND NONBORATED WATER SOURCES

The WHF pool contains approximately 1.4 million gallons of borated water (BSC 2008, Section 6.1.1). The pool minimum required boron concentration is 2,500 mg/L of boron enriched to 90 atom % in ^{10}B (SAR Section 1.14.2.3.3.4). If nonborated water is added to the pool, the boron concentration will be diluted, and the remaining boron concentration fraction can be calculated as follows:

$$\text{Remaining boron Concentration Fraction} = \frac{1.4}{1.4 + \text{nonborated water volume in millions of gallons}} \qquad \text{(Equation 1)}$$

The sources of nonborated water available to the WHF are fire suppression water, potable water and deionized water. The raw water storage tank with a capacity of 850,000 gallons does not have a direct pathway to the WHF. As described in SAR Section 1.6.3.4.7, raw water is pumped from the raw water storage tank to the deionized water system where the raw water will be prepared for use within the surface facilities. Other water systems are insignificant sources due to their limited volume (e.g., chilled water).

The water-based double-interlocked preaction fire suppression system within the WHF is supplied with water from fire water Loop 1, which has four storage tanks with a capacity of 300,000 gallons each (SAR Section 1.4.3.2.1.1). This results in a maximum total of 1.2 million gallons of nonborated fire suppression water potentially available to the WHF.

The potable water system stores treated potable water in a 230,000 gallon tank (SAR Figure 1.4.4-7). Potable water is supplied to various locations within the WHF, including bathrooms, eye wash/safety showers, and work stations.

The deionized water supply system is the only nonborated water system with a direct pathway to the WHF pool. The deionized water storage tank has a capacity of 19,600 gallons (SAR Figure 1.4.4-9).

The freeboard volume of the pool is approximately 137,000 gallons. This volume is based on four feet of freeboard in the pool at the normal operation height, and pool areal dimensions of 75 ft × 61 ft (BSC 2008, Section 6.4.9). The sources of nonborated water with volumes greater than 137,000 gallons are the fire suppression system and the potable water system. Neither of these systems is connected directly to the pool or pool piping, and the only flow path is through runoff into the pool, which would not be at a significant velocity. Once the freeboard volume is filled, water flow would follow the path of least resistance away from the pool. Therefore, the maximum possible dilution is limited to the freeboard volume, which would result in a remaining boron concentration fraction greater than 91%.

1.2 CONSIDERATION OF BORON DILUTION IN THE HAZOP, MLDS, AND EVENT SEQUENCES

1.2.1 Screening of Boron Dilution as an Initiating Event

The basis for screening boron dilution as an initiating event is provided in Table 6.0-2 of *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a), which states, in part:

> The only water source in Room 1016 is the deionized water system and this system does not have enough water to dilute the boron concentration to levels to cause criticality. ….the maximum amount of water that can be drained from the de-ionized water system due to a pipe rupture is 19,600 gallons. The WHF pool contains 1.4 million gallons of water. …. The addition of 19,600 gallons reduces the boron concentration by 1.4%. … the minimum required concentration of soluble boron in the pool is 2500 mg/L of boron enriched to 90 atom % ^{10}B. For all normal WHF pool operations, subcriticality is maintained crediting no more than 15% of this minimum required soluble boron concentration. Hence, there is a factor of safety of 85%/1.4% = 60.7; and water dilution is not a credible scenario leading to criticality in the WHF pool for normal operations.

The deionized water system, containing 19,600 gallons, is the only water source considered in the boron dilution initiating event screening because the deionized water system is the only source of nonborated water available to the WHF pool during normal operations. Other sources of nonborated water are associated with event sequences, where boron dilution is considered as a pivotal event.

The 15% pool boron concentration fraction required for maintaining subcriticality for normal operations is conservatively based on bounding fuel characteristics (e.g., fresh fuel enriched to 5 wt% ^{235}U). Pressurized water reactor assemblies are conservatively modeled as Westinghouse 17 × 17 and Babcock & Wilcox (B&W) 15 × 15 fuel assemblies. Boiling water reactor assemblies are conservatively modeled as General Electric 7 × 7 and Advanced Nuclear Fuel 9 × 9 fuel assemblies. These four assembly designs have been shown to be the most reactive designs in various potential preclosure configurations (SAR Section 1.14.2.3.2.1.1). To reduce the analysis dependence on specific assembly designs, the fuel pin pitch is optimized to the most reactive configuration within the fuel basket tubes or assembly channels for both normal operations and end-states of event sequences.

In order to dilute the boron concentration to levels resulting in a boron concentration fraction less than 15%, greater than seven million gallons ([1.4/0.15] – 1.4) of nonborated water would have to mix with the pool borated water. The total volume of nonborated water available to the WHF is less than 1.5 million gallons.

Therefore, boron dilution is screened out in the hazard and operability (HAZOP) evaluation and master logic diagrams (MLDs) as an initiating event because boron dilution, in the absence of other independent initiating events, does not initiate a sequence of events that could potentially lead to a criticality (BSC 2009b, Table E-23, Node 22.29). However, boron dilution is included as a pivotal event.

1.2.2 Quantification of the Boron Sufficiency Pivotal Event and Role of PSC-9

The boron sufficiency pivotal event is associated with event sequences that could potentially impact geometry, interaction, and performance of fixed neutron absorbers as well as boron dilution. The basis for the failure probability of 1×10^{-6} assigned to the boron sufficiency pivotal event is provided in Table 6.3-9 of *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a). This failure probability is based in part on PSC-9, which requires sampling of the pool water to ensure that the minimum required boron concentration of 2,500 mg/L in the pool is maintained. However, the primary basis for this failure probability is that, for event sequences that include this pivotal event, the required boron concentration fraction to maintain subcriticality is less than 53% (Section 1.2.3). Even under hypothetical conditions that result in filling the entire freeboard volume of the pool with approximately 137,000 gallons of nonborated water, the end boron concentration fraction would remain above 91%. Therefore, the failure probability of 1×10^{-6} for the boron sufficiency pivotal event is reasonable because boron dilution to the levels that might be insufficient to maintain subcriticality during these event sequences is physically unrealizable.

The implementation details of PSC-9 are provided in the response to RAI 2.2.1.1.7-7-002.

1.2.3 Minimum Required Boron Concentration Fraction for End-States of Event Sequences

End-states of event sequences associated with handling and movement of casks, canisters and individual assemblies, with potential impact on geometry, interaction, or performance of fixed

neutron absorbers, are modeled with the same fuel characteristics described in Section 1.2.1 with optimized fuel pin pitch for a range of flux trap gap widths and varying credit for fixed neutron absorbers from 75% to complete omission. As shown in Figures 43 through 92 of *Nuclear Criticality Calculations for the Wet Handling Facility* (BSC 2007), the minimum required boron concentration fraction needed to maintain subcriticality (i.e., maximum k_{eff} below the upper subcritical limit of 0.93) for the various potential configurations for end-states of event sequences ranges between 0% and 30%[1]. Greater than three million gallons of nonborated water would be required to reduce the pool boron concentration fraction to less than 30%. The total volume of nonborated water available to the WHF is less than 1.5 million gallons.

The limiting seismic event sequences important to criticality safety in the WHF pool result in a tipover of a truck cask, a shielded transfer cask containing a DPC, or a shielded transfer cask containing a transportation, aging, and disposal (TAD) canister with a mean probability of occurrence of 2×10^{-4} over the preclosure period (BSC 2009c, Table 6.7-4). The criticality safety analysis conservatively considered that these event sequences result in spent nuclear fuel spilling out of the truck cask, DPC, or TAD canister forming a reflected pile of fuel pins. Table 1 presents the minimum required boron concentration fraction as a function of separation between fuel pins for a pile of 4,992[2] fuel pins (conservatively modeled with 71 × 71 array of 5,041 fuel pins) as representing a tip over of a DPC containing 24 B&W 15 × 15 assemblies, which were determined to be the limiting canister and assembly designs. Table 1 also provides the nonborated water volume necessary to dilute the pool water to reach the minimum required boron concentration fraction.

[1] Note that the values presented in these Figures are the minimum required natural boron concentration in mg/L. To convert these values to boron concentration fraction, they need to be divided by 2500, which is the minimum required boron concentration, and by 4.5, which is the ratio of 90% ^{10}B to the natural abundance of ^{10}B (19.9%). Values above 22% are based on extrapolations of the trends in these Figures.

[2] 24 B&W 15 × 15 assemblies with 208 fuel pins, 16 guide tubes and one instrumentation tube per assembly.

Table 1. Minimum Required Boron Concentration Fraction for Seismic Event Sequences

Pin pitch[a] (cm)	Minimum required ^{10}B enrichment[b]	Minimum required boron concentration fraction[c]	Necessary nonborated water volume addition to reach concentration fraction (thousands of gallons)[d]
1.13	81%	90%	154
1.20	75%	83%	289
1.34	58%	64%	779
1.49	43%	48%	1,520
1.63	34%	38%	2,259
1.87	23%	25%	4,160
2.09	Natural	< 22%	> 4,964

[a] BSC 2007, Attachment 2, *MCNP Files.zip*. Pin pitch is taken from files BW15PinArrayC_0.8_20_70_ino, BW15PinArrayC_0.8_30_70_ino, BW15PinArrayC_0.8_50_70_ino, BW15PinArrayC_0.8_75_70_ino, BW15PinArrayC_0.8_100_70_ino, BW15PinArrayC_0.8_150_70_ino, BW15PinArrayC_0.8_200_70_ino, respectively.

[b] BSC 2007, Attachment 2, Spreadsheet *Simple Geometry Results.xls*, Worksheet *BW15 Pin results*. The minimum required ^{10}B enrichment values are linearly interpolated for $k_{eff}+2\sigma$ of 0.93 for the cases reflected with Concrete.

[c] Fraction of the minimum boron concentration of 2,500 mg/L boron enriched to 90 atom % in ^{10}B.

[d] These values are calculated using Equation-1.

Given the presence of multiple grids along the fuel assemblies, the intact pin pitch is expected to remain unchanged for the end-states of these event sequences, and the required boron concentration fraction to maintain subcriticality for this end-state is 53% as interpolated from Table 1 for the intact assembly pin pitch of 1.44 cm (BSC 2007, Table 5).

Even if all the fuel assemblies hypothetically collapse into the most reactive configuration, subcriticality is maintained, crediting 90% of the minimum required boron concentration. In order to dilute the pool boron concentration to 90% of the minimum required concentration, 154,000 gallons of nonborated water would have to enter the pool (Table 1), which is greater than the freeboard volume of the pool of 137,000 gallons, and therefore, judged to be physically unrealizable.

1.2.4 Consideration of the Boron Sufficiency Pivotal Event for DPC Fill Operations

The DPC is sampled, vented, cooled if necessary, filled and flushed with borated water prior to cutting open the final DPC lid and prior to placement in the pool. The borated water piping is connected with and processed through the WHF pool borated water treatment system (SAR Section 1.2.5.1.2.1) and cannot be physically connected to the deionized or potable water systems. Therefore, the only source of water available for DPC fill operations is the pool borated water. The minimum required boron concentration fraction is less than 15% for normal operations with DPCs and less than 30% for the conservative representations of end-states of event sequences impacting geometry and interaction without credit for fixed neutron absorbers. In order to dilute the boron concentration to levels resulting in a boron concentration fraction less than 30%, greater than three million gallons of nonborated water would have to mix with the

pool borated water. The total volume of nonborated water available to the WHF is less than 1.5 million gallons. Therefore, a boron sufficiency pivotal event is not considered in the analysis of DPC fill operations.

1.3 CONSIDERATION OF EVENTS THAT COULD CAUSE BORON DILUTION

1.3.1 Internal Flooding

Internal flooding is caused by either actuation of the fire suppression system or failure of water-carrying pipes or valves associated with chilled water, hot water, potable water, or other water systems. There is no fire suppression coverage over the pool area and drains will divert flood water away from the pool. Even under hypothetical conditions that result in filling the entire volume of freeboard in the pool with nonborated flood water (i.e., 137,000 gallons), the resulting boron concentration fraction would be greater than 91%, which is higher than the concentration fraction required for normal operations (less than 15%), end-states of handling and movement event sequences (less than 30%), and end-states of seismic event sequences (less than 53%).

1.3.2 Inadvertent Reduction of Injected Boron

Soluble boron is injected into the pool through the boric acid makeup system when the boron concentration in the pool water is reduced below the minimum required concentration of 2,500 mg/L. The majority of boron loss from the pool is due to periodic use of pool water for resin sluicing and from small quantities of pool water left in transportation casks and DPCs after being emptied of borated pool water. The loss of boron is not expected to be significant. The operation of the boric acid makeup system involves mixing the boron to be added with deionized water in the boric acid makeup tank and then pumping the contents of the tank into the pool water treatment, cooling, and cleanup system return piping. The boric acid makeup system tank is sized with a capacity of 1,244 gallons. To reach a boron concentration fraction below 53%, the boric acid makeup system must inadvertently inject the tank volume of nonborated water into the pool over 1,000 times. The inadvertent addition of over 1,000 makeup tanks full of nonborated water into the WHF pool without detection is considered not credible.

1.3.3 Under-Enrichment of Injected Boron

Because, the only boron available within the geologic repository operations area is the enriched boron, there is no potential to inadvertently use natural boron. Procured boron will be accompanied with the necessary material data sheets to demonstrate that the boron shipped to the repository meets the 90 atom % ^{10}B enrichment requirement. In addition, each shipment will be tested upon receipt to ensure that the boron is of the required enrichment.

1.3.4 Nonhomogeneity of Mixing

Nonhomogeneity of mixing could occur if the dissolved concentration approaches saturation levels. The solubility of boric acid in water as a function of temperature is provided in Table 2 (Lide 2005). As described in SAR Section 1.2.5.3.2.2, the pool water is maintained at 75°F during normal operations, at which the saturation level is greater than 9,000 mg/L. Even at much

cooler temperatures than could be experienced in the WHF pool, the saturation boron concentration is significantly higher than the minimum required concentration of 2,500 mg/L.

Table 2. Solubility of Boric Acid in Water

Temperature		Boric Acid	Boron Concentration
(°C)	(°F)	(g/100g water)	(mg/L)[a]
0	32	2.61	4567
10	50	3.57	6247
20	68	4.77	8347
25	77	5.48	9590
30	86	6.27	10972
40	104	8.10	14175

NOTE: [a]These values are calculated by dividing the boric acid concentration by 0.175, which is the ratio of the atomic mass of boron to boric acid; then converted from (g/100g water) to (mg/L) by multiplying by 10,000.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2007. *Nuclear Criticality Calculations for the Wet Handling Facility.* 050-00C-WH00-00100-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071212.0001.

BSC 2008. *Pool Water Treatment and Cooling System.* 050-M0C-PW00-00100-000-00C. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080212.0002.

BSC 2009a. *Wet Handling Facility Reliability and Event Sequence Categorization Analysis.* 050-PSA-WH00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0006.

BSC 2009b. *Wet Handling Facility Event Sequence Development Analysis.* 050-PSA-WH00-00100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0005.

BSC 2009c. *Seismic Event Sequence Quantification and Categorization Analysis.* 000-PSA-MGR0-01100-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0013.

Lide, D.R., ed. 2005. *CRC Handbook of Chemistry and Physics.* 86th Edition. Boca Raton, Florida: CRC Press. ISBN: 0-8493-0486-5.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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.

1. RESPONSE

Based on the clarification telephone call with the NRC on April 22, 2009, this response addresses the RAI by providing a general discussion of the technical basis for the selection of different human reliability analysis (HRA) methods and specific examples. These examples include but are not limited to those specifically requested in the RAI.

1.1 TECHNICAL BASIS FOR SELECTION OF DIFFERENT HRA METHODS

As stated in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Appendix E, Section E3.2.7.2, Selection of Quantification Model), the selection of a specific quantification method for the failure probability of an unsafe action is based upon the characteristics of the human failure event (HFE) quantified. The characteristics considered in the selection of the quantification method for each HFE include those discussed in Section E5.1.1 of the event sequence categorization analysis (BSC 2009). These HFE characteristics from Section E5.1.1 are the following:

1. The three temporal phases used in probabilistic risk assessment modeling:
    A. Pre-initiator
    B. Human-induced initiator
    C. Post-initiator.
2. Error modes:
    A. Errors of omission

B. Errors of commission (EOCs).

3. Human failure types:

   A. Slips/lapses

   B. Mistakes.

4. Informational processing failures:

   A. Monitoring and detection

   B. Situation awareness

   C. Response planning

   D. Response implementation.

Appendix E.IV, Section 3, item D under Assessment of Available Methods of the event sequence categorization analysis (BSC 2009) discusses the rationale for using the various approaches. Rather than using only one of the three context or cognition-driven methods for all the detailed quantification, different methods were used based on their fit to the actions modeled. The *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification* (CRA 2006) and *Cognitive Reliability and Error Analysis Method, CREAM* (Hollnagel 1998) approaches include different Generic Task Types (GTTs) and Cognitive Function Failures (CFFs) as well as different performance-shaping factors and adjustment factors, which allow a broader spectrum of applicability of these task types and factors for the array of analyzed actions. *HEART - A Proposed Method for Assessing and Reducing Human Error* (Williams 1986) is a predecessor of NARA and corollary method that was also considered to be appropriate for use, although the more current NARA was given preference in the PCSA HRA. There are unsafe actions within the Yucca Mountain Project HFEs that best fit the NARA approach and others that best fit the CREAM method. In addition, for a small number of unsafe actions that were not modeled by either the NARA or CREAM approaches (primarily in the area of unusual acts of commission), a third method determined from Technique for Human Error Rate Prediction (THERP), *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report* (Swain and Guttmann 1983), is used. Specifically, in the modeling of dependence between actions, NARA specifically endorses the THERP approach. In the case when simple, procedure-driven unsafe actions occur within an HFE during step-by-step tasks, THERP was implemented because it is based on observations of human performance in the completion of manipulations without the need to know the root causes or motivations for the performance (e.g., how often does an operator turn a switch to the left instead of to the right).

The level of specificity in the description of the GTTs and CFFs requires that the HRA team make technically suitable selections when applying them to a specific case. While repository operations differ from those of traditional nuclear power plants, the analytical preference was to use NARA since it was targeted towards nuclear plant situations, and was therefore considered to

be more applicable to the repository than the other selected methods. As described above, a broader base of unsafe actions than NARA accommodates was needed for the array of human actions needed for the preclosure safety analysis HRA. The NARA GTT descriptions are slightly more descriptive and precise using examples of tasks in the nuclear power plant environment relevant to each GTT. However, they are limited to the general areas of Task Execution, Ensuring Correct Plant Status, Alarm/Indication Response, and Communication. CREAM CFF descriptions are less specific and represent broad categories of actions (e.g., Observation not Made, or Action out of Sequence). These broader categories, such as Observation, Interpretation, Planning and Execution, had wide applicability to the Yucca Mountain Project situations and contexts.

The expert judgment approach from *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)* (NRC 2000) also provided a structured framework for the use of judgment for human error probability (HEP) value estimation per the American Society of Mechanical Engineers probabilistic risk assessment standard.

In summary, the technical basis for the selection of a specific quantification approach (NARA, CREAM, THERP, or ATHEANA expert judgment) for any specific task (i.e., unsafe action) within a given HFE comes down to the determination by the analysis team as to which of the approaches had a generic task that most closely fit the specific task in the HFE. Each HFE was initially quantified by one member of the team using that approach. It was then reviewed independently by the other members of the team. Comments were discussed and a final resolution agreed to by team members. The HFE was then reviewed once again by an independent HRA expert, and any comments about method selection were resolved between the reviewer and the team. Therefore, the selection process was judgment based, and the adequacy of the selection rests entirely on the expertise and adequacy of the team, the independent reviewer, and the process applied. Examples of the selection of different HRA methods are provided in Section 1.2.

1.2 JUSTIFICATION FOR USE OF MULTIPLE HRA QUANTIFICATION METHODS

Based on the results of the NRC clarification telephone call regarding subpart (b) of the RAI, Section 1.1 above provides an overview of the approach to the selection of different HRA methods. Section 1.2 applies the principles described in that overview to specific examples.

Consistent with the ATHEANA method, an HFE is broken down into the various scenarios that lead to the failure. Then, each scenario is further broken down into specific required human actions and their applicable procedures, along with the systems and components that must be operated during performance of each action. While the HFE scenario provides a common context, equipment interactions and performance-shaping factors, each unsafe action reflects a particular cognitive process and/or task implementation that requires specific consideration by the analysts for quantification. Therefore, each unsafe action was evaluated against the GTT descriptions from NARA with insights from HEART EPC descriptions and compared to the CFFs in CREAM to find the most appropriately matched method in terms of action type, situation, and intent.

Each method used is well researched, well founded, and when applied properly to the quantification of a task, a reasonable result is obtained. Although the basis for each model is different, the most applicable GTT across both models was selected. The HRA team did not want to limit the scope of the analysis to only those unsafe actions for which any single model applied, but did strive for consistency of method application when applied to different facilities or to different but similar processes. There is precedent for using different methods, for example, for cognitive and procedural tasks. Therefore, the selection of one method versus another was based on the specific unsafe action being quantified. Consistent with the emphasis of each method, the actions quantified with CREAM tended to be more cognitive in nature, requiring operator evaluation and decision-making, while the actions quantified with NARA tended to be errors in routine task execution or in checking/setting operational status (such as placing a control in a particular position).

An example of how a combination of methods was used within the same scenario is the following, which utilizes NARA, CREAM, empirical equipment data, and ATHEANA expert judgment. The descriptions below demonstrate that a thorough evaluation of each unsafe action, considering the scenario context and the task-specific elements, was conducted during the analysis.

BSC 2009, Section E6.5.3.4.2.3, HFE Group #5 Scenario 1(c) for 060-OpCTMdrop001-HFI-COD

In this scenario, some variations of canister transfer machine (CTM) activities require heavy objects to be moved over the canister; some lids are removed, and waste package inner lids are also installed. The operator causes drop of an object, such as the cask lid or waste package inner lid, onto the canister during CTM operations, through the following steps (BSC 2009, Section E6.5.3.4.2.3):

1. Operator leaves adjustable speed drive (ASD) in maintenance mode OR operator places ASD in canister mode OR ASD height control fails.

2. Operator fails to notice lift is taking too long OR operator “locks” lift button into position.

3. Load cell overload interlock fails.

4. Mechanical failure of hoist under overload causes lid drop.

Operator Leaves ASD in Maintenance Mode—The ASD controls the height of the lift. Before beginning the lifting process, the operator should ensure that the ASD is in the lid lift mode. It could be in maintenance mode because of activities performed in the days between canister transfers. It is not clear how often this would occur, so for the purpose of this analysis, the bounding case is that the ASD is always in maintenance mode between canister transfers. This exaggerates the opportunity for an unsafe action.

The operator must change the mode prior to the lid lift. In doing this, the operator could either fail to change the mode (miss this step in the process) or erroneously place it in the canister lift mode, either of which results in the ASD trying to lift the lid too high and impacting the bottom of the bell. The third way this could occur is simply a mechanical failure of the height control set point of the ASD.

The CTM operator is supposed to set the CTM system to the appropriate lift mode prior to performing a lift. This is fundamental to the operation, not simply a step in a procedure that can be missed. The initial action to set the mode is quite simple, so the only realistic way that the operator can leave the ASD in maintenance mode is to completely fail to take any actions to set the CTM system for a lift. This failure can be represented by NARA GTT B3.

- GTT B3: Set system status as part of routine operations using strict administratively controlled procedures. The baseline HEP is 0.0007.

  This operation is part of a fundamental and simple action taken prior to performing a lift, consistent with setting a system status as part of routine operations and is performed under optimal conditions. It is therefore consistent with the intent and description of GTT B3. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The baseline HEP is used without adjustment.

Operator leaves ASD in maintenance mode = 0.0007

Operator Places ASD in Canister Lift Mode—Given that a CTM operator has correctly decided to set the CTM system status prior to operations, the appropriate operating mode also needs to be selected. There are only two modes to choose from: lid lift and canister lift. The ASD control is a screen where the operator can scroll between the choices to pick the appropriate lift mode. The act of selecting the wrong mode from these two can be best represented by task execution error NARA GTT A1.

- NARA GTT A1: Carry out a simple single manual action with feedback. Skill-based, and therefore not necessarily with procedures. The baseline HEP is 0.005.

- This operation is performed under optimal conditions. It is early in the operation, and the operator is active, so it is too early in the task for boredom to set in. The ASD control system requests confirmation from the operator (e.g., “You have selected canister lift. Confirm Y/N”), which is the feedback referred to in NARA GTT A1. The baseline HEP is used without adjustment, and GTT A1 was selected as the most appropriate match for the actual operation since the action of interest involves the operator simply selecting an operational mode from the control screen and obtaining feedback through the control system request for confirmation. There are no complex cognitive processes that would fit the categories cited in CREAM.

Operator places ASD in canister lift mode = 0.005

ASD Height Control Fails—This is a mechanical failure of the ASD controller. (This event is an equipment failure and does not have a human component to its failure rate. The demand failure rate for the ASD is from the Attachment C Active Component Failure Database.)

ASD height control fails = 3.4×10^{-5}

Operator Fails to Notice Lift is Taking Too Long—Lifting the lid takes on the order of a few minutes, whereas lifting the canister takes on the order of ten minutes. Because the operator holds the lift button or the lift stops, there is an opportunity to notice that the hoist has not stopped when expected and to release the button and stop the hoist, either before the lid contacts the interior of the bell or before it begins to overload the system. Realistically, the operator would have on the order of 30 seconds between when it should stop and when it would be too late. The hoist position indicator and camera view are in front of the operator on the control panel.

The operator is supposed to hold the lift button until the lift automatically stops. This operation has been performed many times in the past by the operator, and the operator has an instinctive feel for how long the lift takes. If an operator feels it is taking too long, the operator need only look at the camera and the indicators on the control panel for verification. Failing to recognize this situation can be represented by CREAM CFF I3 because the definition of CFF I3 of delayed interpretation (not made in time) reflects the time factor involved in the scenario and the operator failure to notice the extended timeframe of the lift and failure to respond in time. The NARA GTTs do not adequately reflect the cognitive issues of evaluating the situation and how long the lift should take, The CREAM CFF I3 baseline HEP was adjusted by the following common performance conditions (CPCs) with values not equal to 1.0:

- CFF I3: Delayed interpretation (not made in time). The baseline HEP is 0.01.
- CPC “Working Conditions”: The operator has optimal working conditions in the CRCF Control Room. The CPC for an interpretation task with advantageous working conditions is 0.8.

Applying these factors yields the following:

Operator fails to notice lift is taking too long = $0.01 \times 0.8 = 0.008$

Operator “Locks” Lift Button into Position—Another way that the lift would go too long is if the operator were to use some inventive means to “lock” the button in place. The CTM lifts are a tedious task and require holding the button in place for long periods of time. There is no locking feature associated with the ASD that would keep the button in place; however, it is not inconceivable that, after many lifts have been done without an ASD failure, an operator would develop a creative technique to accomplish this. Since the operator develops trust in the ASD and the other system interlocks, the operator would not believe that the deviation is unsafe, and it would free up time to prepare for subsequent steps or to perform other duties.

The operator is supposed to hold the lift button until the lift automatically stops. However, it is always possible to rig something up that would hold the button in place, relieving the operator of the perceived "inconvenience" of holding it. The HRA team believes that the preferred methods do not provide baseline HEPs for such unsafe actions. Therefore, the ATHEANA expert judgment approach is used. In considering the judgment, HEART and NARA do provide some insight into the existence of EPCs that can affect this unsafe action, such as the following:

- A mismatch between an operator's model of the world and that imagined by a designer—The designer considers the "push-and-hold" as a safety feature that keeps the operator's attention on the operation. The operator considers it as an unnecessary inconvenience in what should be an automated function.

- A mismatch between real and perceived risk—Locking the button removes a layer of safety provided by the operator monitoring operations, but the operator perceives the reliability of the limits and interlocks as such that there is no additional risk involved (HEART EPC 12).

- Little or no independent checking or testing of output—A single operator is operating the CTM from a remote location. No one is looking over the operator's shoulder (HEART EPC 17).

- An incentive to use other, more dangerous procedures—Holding the button means that the operator's ability to accomplish other work is limited. The operator can be more efficient (e.g., planning for future activities, completing paperwork) by trusting the control system to complete the task (HEART EPC 21, NARA EPC 15). (Explanatory Note: The operator is not paying sufficient attention to the task at hand and trusts that the control system will stop the lift at a particular point – this is considered by the analysts to be a dangerous process.)

- Operator under load, boredom—Holding a button when one fully expects that the system automatically controls the operation is not very challenging (NARA EPC 13).

- Little or no intrinsic meaning in a task—The operator really has to wonder why the system was not designed to simply perform the operation on its own. The operator could come to consider the "push-and-hold" feature as a poorly thought out design flaw (HEART EPC 28).

Taking this as a whole, the HRA team judged that the operator locks the button in place about 10% of the time (which can be interpreted as some operators doing it quite frequently and other operators less or not at all). However, this action is not unrelated to prior failures in this scenario. An operator who fails to set the CTM system status (leaves the ASD in maintenance mode) has already demonstrated a predilection towards rushing and perhaps a bias towards short-cuts for the particular lift. Therefore, the HRA team judged that the success or failure of this task is related to the way in which the ASD failure occurs. If the failure occurs as a result of leaving the ASD in maintenance mode, the HEP for locking the button in place is twice the baseline (0.2). If it occurs for either of the other two reasons, the HEP is one-half the baseline (0.05).

Operator “locks” lift button into place (ASD left in maintenance) = 0.2

Operator “locks” lift button into place (ASD placed in canister mode or fails mechanically) = 0.05

The above examples demonstrate the application of the various quantification methods to each specific HFE based on an assessment of the actions, processes and performance-shaping factors involved.

1.3 JUSTIFICATION FOR USE OF NARA FOR 060-OPDPCSHIELD1-HFI-NOW, SCENARIO 1B (BSC 2009, SECTION E6.3.3.4.2.2)

In this scenario, the operator fails to properly shield the dual-purpose canister while installing the canister lift fixture, leading to direct exposure. The following postulated unsafe actions are involved in this scenario: (1) Shield plate crew member opens shield plate while crew bolts canister lift fixture, or (2) crew fails to notice shield plate movement in time OR shield plate crew member fails to respond to warnings from crew.

The shield plate has two modes: a normal travel mode (forward and reverse) and a jog mode (forward and reverse). The jog mode only allows the plate to move very slowly and in small increments. The shield plate operator uses the travel mode to move the shield plate completely over the cask port until it reaches the end stop. The jog function is then used for fine control of the shield plate to line up the shield plate with the bolt holes in the canister lift fixture. To open the shield plate, the shield plate operator again uses the normal travel mode until it reaches the end stop at the other end of the platform. Before opening or closing the shield plate, the shield plate operator ensures that the path of the shield plate is clear of personnel.

The first unsafe action of this event is “Shield plate crew member opens shield plate while crew bolts canister lift fixture,” which involves the movement of the shield plate while the crew are either on or very close to the plate itself conducting bolting operations. The designated shield plate operator is trained to ensure that the shield plate and path are cleared of personnel before moving the shield plate.

Once the canister lift fixture is on the dual-purpose canister and the shield plate is closed, the plate is not supposed to be opened for the remainder of the operations. Therefore, this error is considered to be an EOC, but would be a slip type of error rather than a mistake, meaning that it would be caused by an attention failure rather than an error in diagnosis or cognition.

Because the analytical preference was to use NARA, NARA was considered first and GTT A5 for a “completely familiar, well-designed, highly practiced routine task performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential errors” was recognized as a potential match. However, GTT A5 was premised on a task execution error, which was not an exact match for the shield plate movement action, although it provided a conservative HEP for the action. So, GTT A5 was "put on hold" while the team reviewed CREAM and THERP to see if there was any better match. However, the error types developed in CREAM are associated with cognitive

processes, including Observation, Interpretation, Planning and Execution, none of which were considered to be appropriate in this case.

Therefore, the remaining option was THERP. As the quantitative analysis states in BSC 2009 Section E6.3.3.4.2.2, none of the THERP EOCs in Table 20-12 were considered to be appropriate since they primarily refer to actions where the operator intends to perform an action (e.g., flip a switch or turn a knob) but instead performs a different action (e.g., flips the wrong switch or turns the knob the wrong way).

The most applicable match remained GTT A5 from NARA. While it was recognized that the unsafe action was not a task execution error, this GTT was considered the most appropriate since it described the operation the best and was still conservative when applied to this failure, because no task regarding the shield plate is actually being performed in this step.

As with much of the preclosure safety analysis HRA, this is a case of analytical judgment being used to apply the appropriate quantification method task types to the specific case at hand and documenting these judgments.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

CRA (Corporate Risk Associates) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique.* CRA-BEGLPOW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM.* 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.

NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.

Swain, A.D. and Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report.* NUREG/CR-1278.Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.

Williams, J.C. 1986. *HEART - A Proposed Method for Assessing and Reducing Human Error. 9th Advances in Reliability Technology Symposium - 1986.* Bradford, England: University of Bradford. TIC: 259862.

Williams, J.C. 1988. "A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance." [Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants]. Pages 436–450. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 259864.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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).

1. RESPONSE

1.1 EXPLANATION OF ROLE OF INFORMATION PROCESSING MODEL IN HRA

The information processing model described in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Appendix E, Section E.5.1.1.) is based on the discussion in Chapter 4 of *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis* (*ATHEANA*) (NRC 2000). This information processing model is used to analyze crew cognition and behavior, and assists in the qualitative understanding of the human failure events (HFEs) and unsafe actions. The information processing model is not a quantification model itself, but it influences the selection of the quantification method for the human reliability analysis (HRA), as described in the response to RAI 2.2.1.1.3-3-022.

Assessment of HFEs can be guided by a model of higher-level cognitive activities, such as an information processing model. Elements of the information processing model used for the Yucca Mountain Project HRA, based on the discussion in Chapter 4 of ATHEANA (NRC 2000), are described below. The relation of these elements to the HFE examples in the preclosure safety analysis is discussed in Sections 1.1.1 through 1.1.4 of this response.

- **Monitoring and detection**—Both of these activities are involved with extracting information from the environment. Also, both are influenced by the characteristics of the environment and the person's knowledge and expectations. Monitoring that is driven by the characteristics of the environment is called data-driven monitoring. Monitoring that is implemented due to a person's knowledge or expectation is called knowledge-driven monitoring. Detection can be defined as the onset of realization by operators that an abnormal event is happening.

- **Situation awareness**—This is the process by which operators construct an explanation to account for their observations. The result of this process is a mental model, called a situation model that represents operators' understanding of the present situation and their expectations for future conditions and consequences.

- **Response planning**—This is the course of action that the process operators decide to take, given their awareness of a particular situation. Often (but not always) these actions are specified in procedures.

- **Response implementation**—These are the activities associated with physically carrying out the actions identified in response planning.

1.1.1 Monitoring and Detection

An example of knowledge-driven monitoring, or monitoring implemented due to a person's knowledge or expectations, is found in the following unsafe action:

BSC 2009, Section E6.5.3.4.2.1, HFE Group #5 Scenario 1(a) for 060-OpCTMdrop001-HFI-COD

This HFE involves the operator causing a drop of an object onto the canister during canister transfer machine (CTM) operations.

In this particular scenario, (1) crew member improperly installs the grapple, (2) the preoperational check fails to note the improper installation, (3) the primary grapple interlock gives a false positive signal, (4) the operator fails to notice the bad connection between the hoist and the grapple through the camera, and (5) the grapple/lid drops from the hoist and strikes the canister.

Preoperational Check Fails to Notice Improper Installation—There are two crew members responsible for preparing the CTM for each operation. Each crew member has a distinct set of assignments, although they collaborate when needed and are expected to check each other's work. The second crew member checks the first crew member's installation of the grapple, which provides an opportunity for the error to be detected. Maintenance crew members are trained in various tasks required for preparing the CTM for canister transfer. For this reason, the second crew member also has a set of activities to perform, and so checking the first crew member is a secondary function. In addition, the existence of the grapple/hoist interlock can lead to an expectation that any error can be detected.

The second crew member would have helped initially with the connection of the grapple to line it up but would then move on to other things. At best, the second crew member performs a cursory check at the end of the CTM preparation. Since the second crew member was involved in the early stages, there is a bias that the job was done correctly. It is concluded that the level of dependence is high. The baseline human error probability (HEP) for checking routine tasks without a checklist, is determined from Technique for Human Error Rate Prediction Table 20-22, item (2) of *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278 (Swain and Guttmann 1983), which is 0.2. However, for this high dependence action the applicable HEP is from Technique for Human Error Rate Prediction Table 20-21, item (4)(e), which is 0.6.

Preoperational check fails to note improper installation = 0.6

1.1.2 Situation Awareness

An example of an activity that represents operators' understanding of the present situation and their expectations for future conditions and consequences is given in the following scenario's unsafe action:

BSC 2009, Section E6.5.3.4.4.2, HFE Group #5 Scenario 3(b) for 060-OpCTMImpact1-HFI-COD

This HFE deals with the operator moving the CTM while a canister or object is below or between levels.

In this particular scenario, (1) the operator puts the CTM in the lid lift mode (for dual-purpose canisters), (2) the operator fails to notice that the lift stops too soon, (3) the operator fails to close the port slide gate OR fails to notice that it does not fully close, (4) the operator fails to close the CTM slide gate OR fails to notice that it does not fully close, and (5) the CTM slide gate interlock fails.

Operator Fails to Notice that Port Slide Gate Does Not Fully Close—In this portion of the scenario, the port slide gate does not close all the way because the canister is in the way. The operator has visible feedback on the failure of the gate to close because the open indication on the control panel stays on and the closed indication also comes on and stays on. Both lights on at the same time signify that the port is neither fully open nor fully closed. The problem can be easily confirmed by looking at the camera or checking the status of the light curtain at the bottom of the bell. This unsafe action can be represented by Nuclear Action Reliability Assessment Generic Task Types (GTT) C1, (*A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique* (CRA 2006)), adjusted for the following error producing conditions:

- GTT C1: **Simple response to a range of alarms/indications providing clear indication of situation** (simple diagnosis required). The baseline HEP is 0.0004.

- EPC 3: **Time pressure**. The full affect EPC would be ×11, but this applies only in cases where there is barely enough time to complete a task, and rapid work is necessary. In this case, the time pressure is more abstract, in that there is a desire to keep the process moving for production reasons, but not a compelling one. The APOA anchor for 0.1 is that the operator feels some time pressure, but there is sufficient time to carry out the task properly with checking. This appears reasonable for this task, so the APOA is set at 0.1.

- EPC 13: **Operator underload/boredom**. The full affect EPC would be ×3, which applies to a routine task of low importance, carried out by a single individual, for several hours. The APOA anchor for 0.1 is for low difficulty, low importance, single individual, for less than one hour. This appears reasonable for this task, so the APOA is set at 0.1.

The situation awareness is provided to the operator by the visible feedback from the control panel light, the camera view, and the light curtain. These indications should permit him to notice the status of the port slide gate and were factored into the analysts' selection of the GTT related to a "clear indication of the situation."

1.1.3 Response Planning

An example of an unsafe action related to an operator deciding on a course of action, given his awareness of a particular situation, is the following:

> **BSC 2009, Section E6.5.3.4.2.4, HFE Group #5 Scenario 1(d) for 060-OpCTMdrop001-HFI-COD**

This HFE involves the operator causing a drop of an object onto the canister during CTM operations.

In this scenario, (1) the cask transfer trolley (CTT) is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice the lid tilt and continues the lift OR the operator "locks" the lift button into position, (4) the lid catches and jams in the port, (5) the load cell overload interlock fails, and (6) mechanical failure of the hoist under overload causes the lid to drop.

Operator Fails to Notice that CTT Is Not Sufficiently Centered—The CTM operator centers the CTM grapple over the cask lid lift fixture using a two-step process. First, the CTM operator does a rough alignment using the bridge and trolley position indicators and sets the bell and shield skirt in place. Then the operator opens the cask port and performs a fine alignment using a camera alignment system. [As stated in BSC 2009, Section E6.5.1.1, horizontal movement and final alignment of the CTM with the cask, waste package, and staging ports is potentially a highly automated process. However, to be conservative, the manual horizontal movement process is analyzed here, generically relying on a visual alignment system and camera for alignment confirmation.] The operator is not looking for perfect alignment but would expect it to be close. At this point, the operator would have the opportunity to question the distance needed to move the hoist into position. Possible operator perspectives include: (1) the position is not off by much, (2) the initial placement of the bell is in question and it is repositioned (which may be easier to accomplish than asking another crew member to move the CTT), or (3) the position of the CTT is not off center by enough to make a difference.

In this task, the CTM operator roughly centers the CTM over the cask port, lowers the shield, and opens the port and CTM gates. The operator needs to more accurately locate the grapple over the lid by moving the hoist within the bell. At this time, the operator has an opportunity to judge if the amount of movement required to align the grapple is too much for the lid to clear the edges of the port during the lift. In this case, it is not so much an observation error (the operator can not help but observe the relative locations of the grapple and lid) or a diagnosis error (the operator knows the canister is not perfectly centered), but rather a decision error, in which the operator decides that it does not matter that the cask is not centered ("it's close enough"). This can be represented by *Cognitive Reliability and Error Analysis Method, CREAM* (Hollnagel 1998) Cognitive Function Failure (CFF) I2, adjusted by the following Cognitive Performance Conditions (CPCs) (with values not equal to 1.0):

- CFF I2: **Decision error** (either not making a decision or making a wrong or incomplete decision). The baseline HEP is 0.01.

- CPC "Available Time": [per CREAM (pages 12 and 20), the probability of the operator responding (correctly) increases as time goes on, so available time can have an effect on performance reliability. It refers to the time that has elapsed since the beginning of the event, rather than the subjectively available time.] With regard to the general level of time pressure for the task and the situation type, it would be easy to believe [based on the human reliability analysts' judgment] that there is adequate time since the consequences of taking more time are (from a safety perspective) insignificant.

However, from a production perspective, this would be a significant setback since the CTM operator would have to get the CTT crew back to move the CTT, which is a time-consuming process. This time pressure could bias the operator towards a decision that "it's close enough." The CPC for an interpretation task with continuously inadequate available time is 5.0.

Applying these factors yields the following:

Operator fails to notice that CTT is not sufficiently centered = $0.01 \times 5 = 0.05$

The operator's perception of the situation regarding the position of the CTT leads to different response planning in terms of his subsequent action (such as repositioning the bell or deciding that the CTT is not sufficiently off center to make a difference). This was factored into the qualitative understanding of the action and the selection of the CREAM CFF I2 Decision error as the appropriate quantification category.

1.1.4 Response Implementation

An example of an activity involved with physically carrying out the actions identified in response planning is the following unsafe action that directly follows the one discussed above in Response Planning:

BSC 2009, Section E6.5.3.4.2.4, HFE Group #5 Scenario 1(d) for 060-OpCTMdrop001-HFI-COD

This HFE involves the operator causing a drop of an object onto the canister during CTM operations.

In this scenario, (1) the CTT is not sufficiently centered under the port, (2) the operator fails to notice that the CTT is not sufficiently centered, (3) the operator fails to notice the lid tilt and continues the lift OR the operator "locks" the lift button into position, (4) the lid catches and jams in port, (5) the load cell overload interlock fails, and (6) mechanical failure of the hoist under overload causes the lid to drop.

Operator Fails to Notice Lid Tilt—The CTM operator is able to see the lid through the camera display. When the lid strikes the ceiling of the Cask Unloading Room, it begins to tilt as the hoist continues to rise. If the cask is not properly centered, it is possible that the lid could strike the ceiling around the cask port rather than rising smoothly through the cask port. The operator has

the opportunity to notice the lid tilting before it potentially jams into the port and has the opportunity to stop the lift. The prior unsafe action of failing to notice that the cask is too far off center could still lead the operator to be somewhat more careful and observant during the lift than if it had been closer to center (e.g., like the extra care a driver might show while pulling into a narrower than normal parking space).

If the operator is looking at the camera view during the lift, then the operator has the opportunity to observe the lid contacting the ceiling of the Cask Unloading Room and tilting into the port rather than rising straight through. The most likely failure would be that the operator is not looking at the screen at the time that this occurs, which can be represented by CREAM CFF O3, adjusted by the following CPC (with value not equal to 1.0):

- CFF O3: Observation not made (omission). The baseline HEP is 0.003.

  [It should be noted that in CREAM there is a discrepancy in the values quoted for observation errors O2 and O3 (CREAM, Table 9, Chapter 9, p. 252. The National Aeronautics and Space Administration (NASA) shuttle probabilistic risk assessment (PRA) study (Hamlin, 2005) cites a mean value of 3×10^{-3} for these failure modes, which is consistent with the value found in the CREAM example (CREAM, Table 16, Chapter 9, p. 258) for O3. The changes to the original CREAM values for observation errors O2 and O3 made in the NASA shuttle PRA study reflect the correction of a typographical error in the original CREAM value. These changes were made based on a conversation with both the CREAM author and a chief scientist involved with the shuttle PRA. The HRA team in the current analysis therefore judged that the correct mean value for these failure modes is 3×10^{-3}, as cited in the shuttle PRA.]

- CPC "Adequacy of Man–Machine Interface": There are two vulnerabilities in the man-machine interface for this observation. First, there is no alarm or indicator to alert the operator. Second, the camera view is not perfect. These are inherent to this type of operation, but would make it more likely that the operator would not be looking at the screen at the time. Thus, the man–machine interface should be considered inappropriate with regard to success of this observation. The CPC for an observation task with inappropriate man–machine interface is 5.0.

Applying these factors yields the following:

Operator fails to notice lid tilt = $0.003 \times 5 = 0.02$

The observations by the operator and the opportunities for action provided by these observations factor into the response implementation and were used to identify the qualitative factors of the action as well as the selection of CFF O3 as the appropriate quantification category.

In summary, the information processing model contains four elements that characterize the types of evaluations operators conduct prior to taking unsafe actions: monitoring and detection,

situation awareness, response planning, and response implementation. The understanding of these evaluations within the context of the HFE scenarios assisted the analysts in selecting among the available GTTs and CFFs described in the quantification methods.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

CRA (Corporate Risk Associates) 2006. *A User Manual for the Nuclear Action Reliability Assessment (NARA) Human Error Quantification Technique.* CRA-BEGLPOW-J032, Report No. 2, Issue 5. Leatherhead, England: Corporate Risk Associates. TIC: 259873.

Hamlin, T.L. 2005. *Space Shuttle Probabilistic Risk Assessment – Human Reliability Analysis (HRA) Data Report*. VOL. III, Rev. 2.0. Washington, D.C.: NASA. ACC: MOL.20080311.0023.

Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Method, CREAM.* 1st Edition. New York, New York: Elsevier. TIC: 258889. ISBN: 0-08-0428487.

NRC 2000. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA).* NUREG-1624, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 252116.

Swain, A.D. and Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report.* NUREG/CR-1278.Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 246563.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 25:

> Provide information on what common factors (and potential differences) there [are] 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.

1. RESPONSE

1.1 INTRODUCTION

As stated in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Attachment E, Section E6.0.2.2), crane-drop-related human failure events were not explicitly quantified because the probability of a crane drop due to human failure is incorporated into historical data used to provide general failure probabilities for drops involving various crane/rigging types. Specifically, the primary data source, *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002* (Lloyd 2003) (NUREG-1774), states: "Of the estimated 54,000 very heavy load lifts at operating plants since the issuance of NUREG-0612, three very heavy load drops were identified. These three very heavy load drop events occurred because of human error." Therefore, the application of this data to only the equipment failure portion of the models was considered appropriate, and including the human failure portion would be double-counting.

The rationale for the application of empirical crane data was twofold: (1) *Interim Staff Guidance HLWRS-ISG-02, Preclosure Safety Analysis — Level of Information and Reliability Estimation* (NRC 2007a) accepts the use of higher level data whenever sufficient and applicable (system level rather than subsystem or component level); and (2) consistent with the strategy of the preclosure safety analysis (PCSA), as wide a range of empirical equipment experience as possible was evaluated since it was considered that the repository will fall within that range. A significant amount of crane experience exists within the commercial nuclear power industry and other applications, and that experience is relevant to similar operations at the repository. Further, the repository is expected to have training for crane operators and maintenance programs similar to those utilized at nuclear power plants.

The primary insight gained from the review of the generic crane data was that operator error was an integral contributor to the generic crane drop data. Also, parsing the generic data into separate categories of human-caused versus equipment-related failures would be difficult to validate based upon the sparse information provided. Therefore, an attempt to develop a crane equipment-only related failure rate from the generic data and a separate human error rate using detailed human reliability analysis was not considered as a justifiable approach.

The only exception to the use of empirical data versus human reliability analysis modeling was for the case of drops from the canister transfer machine (CTM); these were explicitly modeled because the operation and construction of the CTM are sufficiently different from standard industry cranes and a separate analysis was therefore warranted.

1.2 JUSTIFICATION FOR THE USE OF EMPIRICAL DATA FOR CRANES SIMILAR TO INDUSTRY

The basis for relying upon industry empirical data for equipment and human reliability quantification and of cranes is based upon the following:

1. The repository crane designs and maintenance and operations plans are similar to those at NRC-licensed commercial nuclear power facilities. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Section 3.2) states that equipment and structures, systems, and components (SSCs) designed and purchased for the repository are part of the population of equipment and SSCs represented in United States industry-wide reliability information sources. Furthermore, the uncertainty in reliability is represented by the variability of reliabilities across this population.

   Industry-wide data for cranes was taken from *Control of Heavy Loads at Nuclear Power Plants – Resolution of Generic Technical Activity A-36* (NRC 1980) (NUREG-0612), *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002* (Lloyd 2003) (NUREG-1774), and *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Canavan et al. 2004) (EPRI 1009691). NUREG-1774 includes several appendices that contain crane data from the Occupational Safety and Health Act Administration, the U.S. Navy, Licensee Event Reports, and from the results of a fault tree analysis. EPRI 1009691 provides estimates from Savannah River Site crane experience in addition to a fault tree analysis. Information from these sources was evaluated in terms of quality, applicability to the repository, and to ensure that the events cited included both equipment failures and human failures.

2. Similarity between the repository cranes and those in industry is ensured by application of the latest nuclear crane industry codes and standards (ASME NOG-1-2004; ASME NUM-1-2004) to the design, maintenance, and operation of repository cranes. The aforementioned industry codes and standards are endorsed by the NRC in *NRC Regulatory Issues Summary - Clarification of NRC Guidelines for Control of Heavy Loads* (NRC 2007c) for single-failure proof cranes at proposed commercial nuclear power plants, as well as for existing NRC-licensed facilities that propose to upgrade their cranes to single-failure proof cranes.

   NUREG-1774 provides a list of the nuclear power plants that upgraded their cranes to single-failure-proof status consistent with licensee responses to *Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment* (Crutchfield 1996, NRC Bulletin 96-02), which requested specific information relating to their heavy loads programs and plans. This information was used to identify relevant data (single-failure-proof crane data) for use in the PCSA crane drop data calculations.

3. *Preclosure Safety Analysis – Human Reliability Analysis* (NRC 2007b, HLWRS-ISG 04) discusses the need for justification of generic data use, particularly as applied to crane drops. However, as with many generic data sources, the level of specificity provided in the crane data documents does not support an evaluation to the extent described in HLWRS-ISG-04 (NRC 2007b). The most detailed crane drop event descriptions are contained in NUREG-1774 (Lloyd 2003), which devotes approximately a paragraph to discussing each event. The PCSA included a review of this crane drop event data to ensure that the cranes involved in the drop incidents were single-failure proof cranes consistent with the ASME NOG-1-2004 requirements of the cranes to be used at the geologic repository operations area (GROA). This screening process was performed to ensure that the event data applied to the PCSA was relevant to the crane types and operations that would be conducted at the repository. Nevertheless, the available information was not sufficient to provide details on factors and controls that influence human performance during crane operation. Therefore, the reasons for past unsafe human actions could not be specified as indicated in HLWRS-ISG-04 (NRC 2007b), and the analysis used the most applicable data possible from the available sources.

4. NUREG-1774 (Lloyd 2003) provides reliability information for US commercial nuclear cranes and is based upon more than 30 years of industry operating experience. Based on the discussion in item 3 above, NUREG-1774 (Lloyd 2003) represents the majority of the cranes at the Yucca Mountain repository. This information includes both equipment and human failure events, thus Yucca Mountain repository-specific equipment and human failure models are not needed to supplement the NUREG-1774 (Lloyd 2003) experience based information.

1.3 USE OF MODELING FOR CRANES NOT SIMILAR TO INDUSTRY CRANES

HLWRS-ISG-02 (NRC 2007a) states that the reliability estimate of a crane or other canister handling system at the GROA could be justified by comparison with the experience and reliability data of similar handling systems used in industry. However, there may be insufficient system-level data applicable to some important to safety SSCs, or existing system-level data may not be completely applicable to its unique GROA operations. In these cases, the reliability estimate is justified by analogous data at the next level down, typically for the subsystems or individual components of the SSCs.

Examples of repository conveyances that are unique (i.e., not similar to the commercial nuclear power facility cranes) are the CTM, the waste package transfer trolley and the cask transfer trolley. Of these, the only crane is the CTM.

NUREG-1774 (Lloyd 2003) was not directly relied upon in the reliability analyses for the CTM (or its subsystems or features). Rather, the CTM failure analysis was “built-up” using components similar to those on ASME NOG-1-2004 cranes with their accompanying component-level reliability data.

Although NUREG-1774 (Lloyd 2003) was not directly applicable to the CTM, it is recognized that NUREG-1774 (Lloyd 2003) provides general insights applicable to nearly all nuclear crane designs, maintenance, and operations.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

ASME (American Society of Mechanical Engineers) NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder)*. New York, New York: American Society of Mechanical Engineers. TIC: 257672.

ASME NUM-1-2004. 2005. *Rules for Construction of Cranes, Monorails, and Hoists (with Bridge or Trolley or Hoist of the Underhung Type)*. New York, New York: American Society of Mechanical Engineers. TIC 259317.

BSC (Bechtel SAIC Company) 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report*. 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.

Crutchfield, D.M. 1996. "Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment." NRC Bulletin 96-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.19970910.0006.

Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

NRC (U.S. Nuclear Regulatory Commission) 2007a. "Preclosure Safety Analysis—Level of Information and Reliability Estimation." Interim Staff Guidance HLWRS-ISG-02. Washington, DC: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.

NRC 2007b. "Preclosure Safety Analysis—Human Reliability Analysis." Interim Staff Guidance HLWRS-ISG-04. Washington, D.C.: Nuclear Regulatory Commission. ACC: MOL.20071211.0230.

NRC 2007c. *NRC Regulatory Issues Summary - Clarification of NRC Guidelines for Control of Heavy Loads*. NRC-RIS-2005-25, Supplement 1. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC 1980. *Control of Heavy Loads at Nuclear Power Plants*. NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

RAI Volume 2, Chapter 2.1.1.3, Third Set, Number 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.

1. RESPONSE

RAIs 2.2.1.1.3-3-027 through 2.2.1.1.3-3-031 and the responses constitute an interrelated group in that they request explanations of the methods and results of the qualitative analyses of the human reliability analysis. This response builds on previous responses within this group.

Consistent with the discussion during the NRC clarification telephone conference call on April 22, 2009, this response provides a description of the vulnerabilities identified and used to develop the results requested and then uses an example scenario to describe typical results from the analysis. The analytical process is consistent with the NRC and industry published guidance for these activities. This response provides examples responsive to the NRC request, whereby the results that justify the identification of potential vulnerabilities are provided in conjunction with the application of accepted methodologies.

1.1 IDENTIFICATION OF POTENTIAL VULNERABILITIES IN THE HUMAN RELIABILITY ANALYSIS

In the human reliability analysis, "vulnerabilities" are the context and factors that influence human performance and constitute the characteristics, conditions, rules, and tendencies that pertain to all the scenarios analyzed in detail. The identification of potential vulnerabilities is part of the preclosure safety analysis (PCSA) human reliability analysis process that began with the development of base-case scenarios, which represent the most realistic description of expected facility, equipment, and operator behavior for the selected operations. The base-case scenarios are described conceptually in Section E3.2.2 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009) and developed in detail in sections E6.X.1 (where X is the human failure event group number). The base case scenario provides a basis from which to identify and define deviations from expected performance for each operation evaluated by the PCSA human reliability analysis. As NUREG-1880, *ATHEANA User's Guide* (Forester et al. 2007) states, "The intent of such a description is to provide a basic understanding of the progression of events associated with the scenario, and to denote key characteristics that add to its understanding. In other words, the description is intended to identify 'what is going on in this scenario,' from the perspective of what the operators would see and experience if they were actually involved in the scenario of interest."

Vulnerabilities are identified through an information collection step that defines the context in which scenarios that deviate from the base case are identified. An overview of identification of vulnerabilities is discussed in *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009, Attachment E, Section E3.2.5) as Step 5 of the ATHEANA process used to perform the human reliability analysis.

NUREG-1880 states that the purpose of Step 5 is to identify and characterize factors that could contribute to crew performance when responding to the various accident scenarios, with the main interest being the identification of factors that could create potential vulnerabilities in the crew's ability to respond to the scenario(s) of interest and increase the likelihood of the human failure events or unsafe actions identified in Step 4. Step 5, therefore, provides information that is critical to modeling the context of the human failure events/unsafe actions, quantifying the events, and searching for important deviation scenarios. Thus, Step 5 corresponds to the collection and assessment of the qualitative aspects (e.g., perform an analysis, evaluate performance shaping factors, consider timing, assess dependencies) of the human reliability analysis.

In particular for the PCSA, the analysts began the process by looking for inherent characteristics of the operating crews (e.g., team dynamics, strategies for implementing procedures) or the crew's knowledge base (informal rules, expectations or biases based on training, learned response tendencies, etc.), which could contribute (either positively or negatively) to the human failure event or unsafe action of concern. This knowledge and information base was taken in the context of each specific human failure event being evaluated. It included not only the internal state of knowledge of the operator (i.e., what the operator inherently knows), but also the state of the information provided (e.g., available instrumentation, plant equipment status).

During the deviation analysis performed in the subsequent Step 6 of the ATHEANA human reliability analysis process, analysts examined the various nominal scenarios for potential variations in plant or situational conditions that might capitalize on the vulnerabilities identified in Step 5, or might create new vulnerabilities and lead to a strong error forcing condition. An error forcing condition is a situation that arises when particular combinations of performance shaping factors and plant conditions create an environment in which unsafe actions are more likely to occur.

For those human failure events requiring detailed analysis, the first step in the ATHEANA approach to detailed quantification was identifying and characterizing factors that could create potential vulnerabilities in the crew's ability to respond to the scenarios of interest and might result in human failure events or unsafe actions.

These vulnerabilities were identified through analytical activities including, but not limited to, the following:

1. The facility familiarization and information collection process discussed in the event sequence categorization analysis (BSC 2009, Section E4.1), including crane operating experience in NUREGs, Navy Crane Center quarterly and safety reports, DOE operational experience, nuclear plant Licensing Event Reports and EPIX data from the Institute of Nuclear Power Operations database, and Scientech/Licensing Information Service data on Independent Spent Fuel Storage Installation events (1994 through 2007).

2. Discussions with subject matter experts from a wide range of areas, as described in the event sequence categorization analysis (BSC 2009, Section E4.2).

3. Insights gained during the performance of the other PCSA tasks (e.g., initiating events analysis, systems analysis, and event sequence analysis).

Vulnerabilities pertaining to those aspects of the operations that relate to potential human failure scenarios relevant to the human failure events in each group were documented for each human failure event group as "Assessment of Potential Vulnerabilities" in the event sequence categorization analysis (BSC 2009, Section E6.X.3.2), where X is the human failure event group number.

The general categories of vulnerabilities identified and documented are:

- Operating Team Characteristics
- Operation and Design Characteristics
- Formal Rules and Procedures
- Operator Tendencies and Informal Rules
- Operator Expectations, such as anticipatory actions and consequences of failure.

1.2 EXAMPLE VULNERABILITY IDENTIFICATION

In the specific example of human failure event Group Number 3, "Cask Preparation and Movement to Cask Unloading Room," the vulnerabilities identified in the event sequence categorization analysis (BSC 2009, Section E6.3.3.2) are the following:

E6.3.3.2.1 Operating Team Characteristics

Crew Members—There are several crew members involved in the installation of the canister lift fixture. One predesignated crew member operates the platform shield plate. This crew member, referred to here as the shield plate operator, is trained as to when the shield plate must be opened or closed. When the operations require the shield plate to be moved, the shield plate operator informs the other crew members on the platform that the shield plate is going to be moved. The other crew members confirm that the shield plate is in the proper position before continuing on to the next step of the operation. All crew members are expected to have the proper training commensurate with nuclear industry standards, followed by a period of observation by a qualified operator or supervisor until each operator is proficient.

Radiation Protection Worker—The radiation protection worker is a fully certified health physics technician, whose job is to monitor radiation from the cask during movement. The radiation protection worker is responsible for stopping operations if high radiation levels are detected or if there is a situation that would lead to direct exposure.

E6.3.3.2.2 Operation and Design Characteristics

Preparation operations are slow and tedious, and they promote complacency. The position of the shield plate is very visible. The shield plate is opened to place the canister lift fixture on the dual-purpose canister (DPC), and it is then closed to bolt the fixture. The shield plate remains closed while the DPC is transferred to the Cask Unloading Room.

Shield Plate Operations—The shield plate has two modes: a normal travel mode (forward and reverse) and a jog mode (forward and reverse). The jog mode only allows the plate to move very slowly and in small increments. The shield plate operator uses the travel mode to move the shield plate completely over the cask port until it reaches the end stop. The jog function is then used for fine control of the shield plate to line up the shield plate with the bolt holes in the canister lift fixture. To open the shield plate, the shield plate operator again uses the normal travel mode until it reaches the end stop at the other end of the platform. Before opening or closing the shield plate, the shield plate operator ensures that the path of the shield plate is clear of personnel.

E6.3.3.2.3 Formal Rules and Procedures

Procedures—There are no written, formal procedures that the crew has in front of them during cask preparation; the knowledge of the process and operating skills for how to handle a DPC come from training.

E6.3.3.2.4 Operator Tendencies and Informal Rules

Observation and Communication—The shield plate operator communicates the actions to other crew members throughout this operation. The entire crew should be aware of the process and order of operations.

E6.3.3.2.5 Operator Expectations

Anticipatory Actions—The preparation process is simple but time consuming. There can be a tendency for the crew to focus on future tasks while preparing the DPC.

Consequences of Failure—The cask is not lifted in this step, and a shield plate is over the cask, so the threat of radiation release or physical injury is very low in this procedure. The crew expects failures to be relatively inconsequential, which promotes complacency in the operations.

In summary, the key vulnerabilities for this scenario are:

Negative

- Complacency due to slow and tedious operations and a low threat of radiation release/exposure or physical injury
- Lack of reference to a procedure during the actions; reliance on knowledge and skills of the operators

Positive

- Communication of actions and crew awareness of operations steps
- Crew training and period of observation prior to participation in operations
- Visibility and slow movement of shield plate

- Shield plate operator ensures that the path of the shield plate is clear of personnel prior to opening or closing it

- Radiation protection workers stop operations out of concern for their own personal safety and that of their crew members if high radiation levels are detected or if there is a situation that would lead to direct exposure.

Similar vulnerability descriptions are provided for each human failure event group for which detailed analysis is conducted in the event sequence categorization analysis (BSC 2009, Sections E6.X.3.2). The identification of vulnerabilities results from careful application of a process that is consistent with NRC endorsed and accepted analytical practices, and they are representative of analyses performed for other activities and industries.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2009. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0004.

Forester, J.; Kolaczkowski, A.; Cooper, S.; Bley, D.; and Lois, E. 2007. *ATHEANA User's Guide*. NUREG-1880, Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20090714.0001.