RAI Volume 2, Chapter 2.1.1.6, First Set, Number 2:

Explain how DOE applied the criteria identified on SAR pages 1.9-6 and 1.9-7 to designate components within an ITS system or subsystem ITS or non-ITS. Some examples needing clarification follow:

- DOE identifies differential pressure switch, "PDS 0148 A" as ITS in SAR Figure 1.2.4-101 on page 1.2.4-317 and describes on SAR page 1.2.4-60 that the heating, ventilation, and air-conditioning (HVAC) exhaust system transfers to the standby fan automatically on detection of high or low differential pressure across the HEPA filter plenums. Explain how DOE accounts for this differential pressure switch when calculating the mean probability that the HVAC system becomes unavailable (SAR Table 1.9-3 on page 1.9-68).

- DOE describes on page E-117 of BSC, 2008ac that, "The ASD (*Adjustable Speed Drive*) is equipped with a semi-automated system for lifts." DOE continues on page E-117 of BSC, 2008ac by describing that, "In the canister lift mode, the operator sets the mode and pushes/holds the lift button; the ASD lifts to the proper height and stops." DOE shows in SAR Figure 1.2.4-51 (Sheet 2 of 3) on page 1.2.4-213 that the ASD is ITS and it receives a signal from the canister hoist position encoder. Explain if the encoder is ITS and explain if there is other equipment involved with lifting to the proper height and stopping that is also ITS but is not shown on the diagram.

1. RESPONSE

1.1 CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS

The process for classifying structures, systems, and components (SSCs) as important to safety (ITS) or non-ITS is summarized 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 based on the criteria on SAR pages 1.9-6 and 1.9-7. This classification is based on the specific safety functions performed by the SSCs that are relied upon to preclude (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 safety functions relied upon by the ITS SSCs are presented in SAR Tables 1.9-2 through 1.9-7, along with their controlling parameters and values. The tables in SAR Section 1.9 list ITS SSCs at a high level of assembly; these SSCs are usually composed of many components. ITS components are not specifically designated as ITS in the fault trees. Instead, they are designated as ITS in the drawings, tables, and text of SAR Sections 1.2 through 1.5. The fault trees (or other sources) that form the basis for the controlling parameters and values are referenced in the column labeled "source" in Table 6.9-1 of each of the six facility reliability and event sequence categorization analyses. Only those components and supporting SSCs necessary to fulfill the safety function are classified as ITS.

For example, the canister transfer machine (CTM) is classified as ITS based on the analysis of this SSC. The safety functions designated in SAR Table 1.9-3 include, but are not limited to, protect against drop, protect against drop of a load onto a canister, and protect against spurious movement. The source analyses for these safety functions are fault tree models CTM-DROP---ALL-HEIGHTS, CTM-DROP-ONTO-CASK, and CTM-SHEAR, respectively, as indicated in Table 6.9-1 of *Canister Receipt and Closure Facility Reliability and Event Sequence Development Analysis* (BSC 2009a). These fault trees include those components that are relied upon to reduce the probability of drops, such as hard-wired interlocks and adjustable speed drives. Because these components are relied upon to reduce the frequency of an event sequence, they are classified as ITS in accordance with the criteria presented on page 1.9-6. The model also includes non-ITS programmable logic controllers because their spurious operation can result in inadvertent CTM movements. Because the correct operation of the programmable logic controllers is not relied on in the fault tree model to prevent an event sequence or mitigate the consequences of an event sequence, they are classified as non-ITS. The CTM components classified as ITS are annotated as such on the process and instrumentation diagram for this SSC, as shown in SAR Figure 1.2.4-51.

1.2 DIFFERENTIAL PRESSURE SWITCH AND HVAC SYSTEM UNAVAILABILITY

The Canister Receipt and Closure Facility (CRCF) heating, ventilation, and air-conditioning (HVAC) system fault trees are provided in Appendix B of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a). A transcription error has resulted in Figure B7.4-3 presenting an incorrect image. The fault tree for the ITS confinement HVAC system, titled "Delta Pressure Not Maintained in CRCF Facility," is correctly presented in Figure B7.4-3 of the *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009b). The remainder of the figures identified in this response can be correctly obtained from *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a). The gate to the right in this fault tree ("Loss of HEPA filtered exhaust from operating and standby trains" (gate HVC002)) is the gate of interest to determine the effect of the loss of differential pressure switch PDS 0148 A.

As seen in Figure B7.4-5, a loss of high-efficiency particulate air (HEPA) filtered exhaust occurs if there is a loss of flow from both the operating train (Train A), as shown under gate HVCA001, and the standby train (Train B), as shown under gate HVAC005. Following gate HVAC005 to Figure B7.4-6, one of the causes of the loss of HEPA-filtered flow from the standby train (Train B) is the failure of the standby train (Train B) to start. One of the causes of this failure is a mechanical or electrical failure (gate HVAC15). As seen in Figure B7.4-8, the causes of failure of Train B to start due to mechanical or electrical failures can be the Train B exhaust fan failing to start or the Train B exhaust fan controls failing to provide a start signal (gate HVC047). One of the three potential causes of failure of gate HVC047 is the basic event 050-VCT0-FANBASD-CTL-FOD, titled "Train B ASD start logic signal fails." This basic event encompasses the failure of differential pressure switch PDS 0148 A. Failure of the start logic signal to the Train B adjustable speed drive has a probability of 2×10^{-3} to one significant digit.

The contribution of basic event 050-VCT0-FANBASD-CTL-FOD to the "HEPA Filtered Flow Not Maintained" fault tree is found in Table B7.4-3 in Appendix B of *Canister Receipt and*

Closure Facility Reliability and Event Sequence Categorization Analysis (BSC 2009a). The basic event "Train B ASD start logic signal fails" (event 050-VCTO-FANBASD-CTL-FOD) is coupled in a cutset with the basic event titled "Exhaust fan in Train A fails" (event number 060-VCTO-FAN00A-FAN-FTR). This cutset has a probability of 1×10^{-4} (to one significant digit); the contribution of this cutset to the overall fault tree probability is 0.26%. The probability of this cutset is small because of the decision to rely on the adjustable speed drive (shown in SAR Figure 1.2.4-101) to reduce its probability.

1.3 CANISTER TRANSFER MACHINE LIFT ADJUSTABLE SPEED DRIVE AND CANISTER HOIST POSITION ENCODER

The logic for the CTM canister hoist is presented in SAR Figure 1.2.4-55. When a control signal is made 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 (a permissive is a condition that must be met before a piece of equipment can be operated or a sequence step can be performed). 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 the 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. An optical sensor above the slide gate will cause the adjustable speed drive to issue a "hoist stop command." Failing that, ITS interlocks (or limit switches) for high and high-high lift levels will shut off power to the hoist and cause the brakes to engage.

The 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. Failure of the adjustable speed drive is a basic event in the CTM drop fault trees found in Figures B4.4-7 and B4.4-18 in BSC 2009a. An adjustable speed drive has at least a factor of 10 higher probability of failure than an encoder (Table C4-1 of BSC 2009a) and failure would cause the encoder signal to be ignored. The encoder is not modeled in these fault trees and is classified as non-ITS because its success or failure is insignificant to the initiating event probability.

SAR Figure 1.2.4-51 (Sheet 2 of 3) on page 1.2.4-215 is a process and instrumentation diagram for the CTM; the set of 3 diagrams depicts the major pieces of equipment involved with CTM operations. This equipment includes both ITS and non-ITS components and subcomponents. Although the non-ITS canister hoist position encoder is not shown on Sheet 2, it is shown on Sheet 3 (SAR Figure 1.2.4-51 (Sheet 3 of 3) on page 1.2.4-217). The CTM components that are relied upon to preclude (reduce the probability of) the occurrence of an event sequence or mitigate the consequences of an event sequence are annotated as ITS on these figures. These components include adjustable speed drives, interlocks, sensors, and switches. There are no other CTM components associated with lifting a canister to the proper height and stopping the hoist that have been classified as ITS and are not shown on these diagrams.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

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. *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.

RAI Volume 2, Chapter 2.1.1.6, First Set, Number 5:

> Explain how DOE quantified event sequences involving filtered and unfiltered radionuclide release in the Receipt Facility (RF). DOE identifies that the HVAC system in the RF is non-ITS (SAR page 1.2.6-17); however, DOE identifies event sequences involving filtered radionuclide release (e.g., ESD06-TAD-SEQ3-RRF in SAR Table 1.7-9 on page 1.7-78).

1. RESPONSE

As described in SAR Sections 1.6 and 1.7, event sequence analysis includes the identification and quantification of initiating events, pivotal events, and end states. Each event sequence, therefore, is associated with an end state even for event sequences that do not rely on all of the events to achieve a probability that is beyond Category 2. The event sequences for the Receipt Facility (RF) that involve radionuclide release (e.g., ESD06-TAD-SEQ3-RRF) have a probability that allows for categorization of these event sequences as beyond Category 2 without reliance on the confinement heating, ventilation, and air-conditioning (HVAC) system for filtration. The confinement HVAC system, therefore, is not classified as important to safety for the RF. However, the event sequences still display a filtered and unfiltered release depending on whether or not the confinement HVAC system fails.

As described in Section 4.3.2.1 of *Receipt Facility Event Sequence Development Analysis* (BSC 2008), event sequence diagrams depict the logical progression of event sequences from the initiating event up to, and including, an end state. Eight mutually exclusive end states are considered in the event sequence diagrams, two of which are radionuclide release–filtered and radionuclide release–unfiltered. The "CONFINEMENT" pivotal event in the RF event trees (provided in Attachment G of *Receipt Facility Event Sequence Development Analysis* (BSC 2008)) models the success or failure of the HVAC system to maintain confinement and perform filtering of the radionuclide release.

Event sequence ESD06-TAD-SEQ3-RRF has the highest probability, 4×10^{-5} over the preclosure period, of all event sequences involving a release of radioactive material (BSC 2009, Table G-2). This event sequence is associated with successful confinement HVAC system operation; the end state for this event sequence is radionuclide release–filtered. The event sequence ESD06-TAD-SEQ5-RRU includes failure of the confinement HVAC system and a radionuclide release–unfiltered end state. This event sequence has a probability of 1×10^{-6} over the preclosure period. If no credit is taken for the performance of the HVAC system (the probability of failure of the HVAC system is hypothetically assigned a value of unity), then the event sequence probability would be that of ESD06-TAD-SEQ3-RRF. Because ESD06-TAD-SEQ5-RRU has a probability that would be categorized as "Beyond Category 2" without relying on the confinement HVAC system, the confinement HVAC system in the RF is not classified as important to safety.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2008. *Receipt Facility Event Sequence Development Analysis*. 200-PSA-RF00-00100-000-00A CACN 002. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080211.0006; ENG.20080314.0004; ENG.20080828.0011.

BSC 2009. *Receipt Facility Reliability and Event Sequence Categorization Analysis*. 200-PSA-RF00-00200-000-00B. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0010.