RAI Volume 2, Chapter 2.1.1.7, Tenth Set, Number 3:

Provide the technical basis for the HVAC system mission times.

a) DOE refers to ISG-03 on page B7-9 of BSC, 2008ac with regard to a 720-hour mission time. DOE also includes a 24-hour mission time for surface nuclear confinement HVAC systems in the WHF. Explain how the mission times relate to maintenance and test intervals for the HVAC systems.

b) For components in the standby train, DOE uses a 360-hour mission time and indicates on page B7-9 of BSC, 2008ac that this mission time is used because DOE is taking into account the difference in failure rates for active and standby systems. Explain how the 360-hour mission time takes into account the differences in failure rates.

1. RESPONSE

1.1 TECHNICAL BASIS FOR THE HEATING, VENTILATION, AND AIR-CONDITIONING SYSTEM MISSION TIMES

Fault exposure times associated with important to safety (ITS) confinement heating, ventilation, and air-conditioning (HVAC) systems are representative of mission times and not the maintenance and test intervals for the HVAC systems. Component failures modeled in the HVAC systems are generally of three types: (1) failures associated with human (operator) actions, (2) component failure on demand, and (3) component failures during the required operating time (mission time) following an initiating event resulting in the breach of a waste form. One train of the HVAC system continuously operates during normal operations, while the second train is in standby. Failures that are considered in the preclosure safety analysis in the operating train of the HVAC system are limited to failures that occur after the initiating event. The operating train's status provides verification that the components within the train are properly functioning at the time of the initiating event.

Failures that would affect the active components of the standby train would prevent the initiation of operation of the component. For example, the failure of the standby exhaust fan results in a failure to start the standby train when the HVAC operation is switched from the operating train. This failure is captured in the standby exhaust fan "failure to start basic event" (BSC 2009a, Appendix B). The remaining component failures—failure of the exhaust fans to run, failure of dampers (manual and tornado) to remain open, duct rupture, speed controller failures, failure of moisture separators, and failure of high-efficiency particulate air filters (either by plugging or leakage)—are modeled as failures to continue to operate over the required mission time.

1.2 RELATION OF MISSION TIMES TO MAINTENANCE AND TEST INTERVALS

During the May 27, 2009, RAI clarification conference call, the NRC requested an explanation of standby system availability. The following discussion relates to standby system availability:

The HVAC trains are configured so that one is always operating. If the operating train is unavailable, then the control logic switches to the standby train. Furthermore, the possible unavailability of the standby HVAC train at the start of the required mission is addressed with the inclusion of two basic events in the system fault tree. In the event that an operating train has failed during normal operating conditions and the HVAC operation transfers to the standby train, the failed train will be taken out of service and placed in maintenance. One of the basic events, "050-VCTO-TRAINB-MAINT: Train B unavailable due to maintenance," is intended to address this maintenance-related unavailability of one train of the ITS HVAC. The second basic event, "050-VCTO-HFIA000-HFI-NOM: HVAC Train B control switch in wrong position," accounts for possible human errors in aligning the HVAC system prior to the initiating event (BSC 2009b, Appendix B). In this case, the standby train is placed in a configuration that precludes it from automatically starting given the failure of the operating train. Procedural Safety Control PSC-7 (SAR Table 1.9-10) states that "One train of HVAC is required to be operating and the second train is required to be in standby before commencing waste handling operations." This control limits the probability that the HVAC system will fail to start when relied upon to mitigate the consequences on an event sequence.

The mission time of 720 hours is based upon regulatory precedent for the assessment of the radiological consequences of design basis accidents. ISG-03 identifies a month as the time frame for the assessment of offsite consequences of a release following the breach of a waste form. NUREG-0800 uses 30 days for accident mitigation, restoration, control room habitability, and public dose reporting. In the systems analysis of the repository, the ISG-03 timeframe has been interpreted to mean that the systems needed to mitigate the consequences of a release must perform their required function during the 720 hours following an initiating event that results in a breach. The operations at the repository cease as a result of an event sequence, which places the facility in a safe state. The facilities are less complex than a nuclear power plant, and termination of a radionuclide release is expected to occur in much less than 30 days.

The 24-hour mission time was derived for the initiating events that resulted from failures of sampling lines during cask sampling and cooling. As stated in Section 6.2.2.7.3 of *Wet Handling Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009b), the 24-hour period was deemed sufficient because the release is a short duration, nonenergetic venting of the sampling lines into the building. This time period is used as the mission time for both trains of HVAC and again represents the time after the initiating event (leak) during which HVAC operation is required to mitigate the effects of the leak.

1.3 DIFFERENCE IN FAILURE RATES

The HVAC system mission time is 720 hours, which is the period the system is expected to exhaust air through high-efficiency particulate air filters to mitigate a release. The HVAC system operates with one train in operation (running) and a second train in standby. Should the operating train fail following an initiating event, the standby train starts and operates for the remainder of the mission time. The time-dependent failure probabilities of the components in the operating train (assumed to be Train A in the system models) are calculated using the hourly failure rate and a mission time of 720 hours. An examination of the cut sets associated with the failure of Train A of the HVAC system (modeled in the HVC002 fault tree, BSC 2009b) indicates that the

Train A failures are the result of time dependent failures; Train A component failures or the loss of offsite power event. The operating system may fail at any time during this 720-hour mission time requiring the standby system to start and operate for the remaining time necessary to complete the 720-hour mission time. The distribution of the time of failure for Train A across the 720-hour mission time is uniform; thus, the potential standby system start time is also uniformly distributed across the 720 hour HVAC system mission time. Therefore, the failure probability for Train B is calculated by using the average mission time for the standby train, 360 hours, which is consistent with Equation 9 of Section 4.3.3.1 of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a).

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 CACN 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0006; DOC.20090323.0006.

RAI Volume 2, Chapter 2.1.1.7, Tenth Set, Number 4:

For the surface nuclear confinement HVAC system, DOE identifies an interlock that prevents both HVAC exhaust trains from operating at the same time. For example, DOE identifies this interlock on page B7-5 of BSC, 2008ac. Explain the following:

a) How this interlock is included when developing the probability of failure for this system, and if this interlock can be a single point of failure for the system.

b) How the Adjustable Speed Drive (ASD) functions with the interlock. The text on page B7-4 of BSC, 2008ac indicates that the ASD shuts down the operating train; whereas, Figure 1.2.4-101 of the SAR appears to indicate that the interlock shuts down the operating train.

1. RESPONSE

The feature during normal operations (auto mode) that prevents operation of both important to safety (ITS) exhaust fans at the same time is a pair of ITS interlocks in the exhaust fan control circuitry—one in each heating, ventilation, and air-conditioning (HVAC) train. Each ITS interlock impacts the normal operation of the ITS exhaust fan in its HVAC train. The ITS interlocks receive inputs from the flow and differential pressure sensors in the associated ITS HVAC exhaust subsystem train as well as the ITS fan-tripped signal from the ITS adjustable speed drive for the ITS exhaust fan in the other train. The ITS interlock is a hard-wired device that allows the required signal to pass only if the appropriate conditions exist as listed at the end of this response. This ITS interlock is an integral part of the exhaust fan control circuitry and must function properly for the standby train to start. The ITS devices that generate the signals that lead to a start of the ITS standby exhaust fan based on running fan performance (flow or differential pressure instruments) are explicitly modeled in the HVAC system fault tree in the "HVC002" subtree for the Canister Receipt and Closure Facility (BSC 2009a) and the "HVC002" subtree for the Wet Handling Facility (BSC 2009b). The remaining control circuitry for the start signal to the standby fan (fan tripped detection) is included in the ITS exhaust fan "fail to start" basic event, 060-VCTO-FAN00B-FAN-FTS.

During off-normal operations, such as the loss of offsite power, the ITS confinement HVAC exhaust subsystem stops operating; both ITS diesel generators automatically start, and the Train A and B ITS load sequencers provide a start signal to the Canister Receipt and Closure Facility and Wet Handling Facility ITS HVAC exhaust fans. After verifying that the Train A and B ITS HVAC exhaust fans have started successfully, operators have the option to stop one fan and put it into auto mode, in accordance with procedures.

1.1 CONSIDERATION OF INTERLOCK IN DEVELOPMENT OF PROBABILITY OF FAILURE

In developing the fault trees for the HVAC system, the failure of the ITS interlocks on the start circuitry for the exhaust fans is included in the failure of the exhaust fan "fail to start" basic event, 060-VCTO-FAN00B-FAN-FTS. If the interlock had been treated as a separate basic event, its inclusion in the HVAC model would not impact the system failure probability. The interlock failure has been included in a basic event that has a failure probability of 2.02×10^{-3}. If treated separately, its failure would have been assigned a probability of 2.7×10^{-5} (BSC 2009a, Attachment B) and would appear in cut sets identical to those that contain the failure to start of the exhaust fan. The impact on the HVAC system probability of failure would be two orders of magnitude less than the failure of the exhaust fan to start.

These interlocks are not single points of failures for the HVAC system. As shown in the revised SAR Figures 1.2.4-101 and 1.2.4-102, provided in License Application Update Number 1, the differential pressure and flow signals from the operating train pass through an interlock (revised SAR Figure 1.2.4-101) to provide a signal to start the standby train upon detection of a failure of the operating train to provide the needed system performance. Depending upon the failure mode of the interlock as modeled, either no signal would be allowed to pass through the interlock or a spurious signal would be generated. If no signal is generated, the interlock failure has no impact on the operation of the operating train. If a spurious signal is generated, system operation would transfer to the standby train; the operating exhaust fan would trip, and system flow and differential pressure sensors would initiate a start of the standby train. In either case, additional failures are required to fail both trains of the HVAC system, as seen by the cut set Table B7.4-3 in the *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2009a).

1.2 FUNCTION OF THE ADJUSTABLE SPEED DRIVES WITH THE INTERLOCKS

The above-described fault tree model is consistent with the SAR Figure 1.2.4-103 depiction (in License Application Update Number 1) of the digital logic of the exhaust fans. Control for the ITS confinement areas exhaust trains is provided from the digital control and management information system (DCMIS), as well as ITS controls that are hardwired so that they cannot be affected by the DCMIS. Interfaces between ITS instruments and controls and non-ITS instruments and controls and the DCMIS are provided with electrical isolation devices such that failure of non-ITS devices will not affect the ITS function of the system.

The ITS control logic is comprised of several logic gates that receive hardwired inputs from ITS instruments and provide outputs that start the standby exhaust fan. The logic is shown in revised SAR Figure 1.2.4-103. A summary of the hardwired interlock logic is as follows:

1) An ITS differential pressure switch across the operating exhaust fan monitors the fan operation. An ITS flow transmitter and flow switch are provided in the exhaust duct to monitor airflow. A low differential pressure across the fan (indicative of fan failure), coupled with a low flow when exhaust fan operation is demanded, will initiate the stop command in the adjustable speed drive for the operating exhaust fan and the start command in the adjustable speed drive for the standby exhaust fan.

2) An ITS differential pressure switch across each filter train monitors pressure drop across the three filter plenums. A high differential pressure when exhaust fan operation is demanded (indicative of loaded filters) or low differential pressure (indicative of

breached filters), will initiate the stop command in the adjustable speed drive for the operating exhaust fan and the start command in the adjustable speed drive for the standby exhaust fan.

3) An ITS fan tripped signal for the operating exhaust fan will initiate the start command in the adjustable speed drive for the standby exhaust fan.

The appropriate command signal to the adjustable speed drives (either continue operating Train A or stop Train A and start Train B) is sent as the logic gates are satisfied. The modulating function of the adjustable speed drive does not have a command function to stop the operating train and start the standby train.

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 CACN 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20090112.0006; DOC.20090323.0006.