REQUEST FOR ADDITIONAL INFORMATION NO. 138-1704 REVISION 1

1/9/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation
Application Section: 19.1.6.1

QUESTIONS for PRA Licensing, Operations Support and Maintenance Branch 1 (AP1000/EPR Projects) (SPLA)

19-206

Justify the simplified treatment of plant operating states (POS) other than 8-1 in the US-APWR shutdown probabilistic risk assessment (PRA). In addition to generally discussing the rationale, address how each specific issue below affects the ability to obtain results and insights from the US-APWR shutdown PRA.

a. Uncertainty results are not available for total shutdown core damage frequency (CDF) or large release frequency (LRF).

b. Quantitative importance measures are not available for POS other than 8-1, so the qualitative assessment of importance used as input to the reliability assurance program (RAP) and other programs may over- or under-estimate the importance of specific equipment.

c. LRF may be overestimated, given that containment will not realistically be open in all POS.

d. The assessment of additional mitigating systems (secondary cooling by the steam generators (SG) and gravity injection (GI) from the spent fuel pool (SFP)) considers dependence between human actions, but does not carry forward equipment failures from other top events in the accident sequence that could disable the SG or GI mitigating systems.

e. Success criteria may be different for POS before and after refueling (see RAI 88, Question 19-139).

19-207

(Follow-up to Question 19-59) The response to Question 19-59 indicates that Design Control Document (DCD) Table 19.1-113 “will be revised adding the requested dispositions for all entries, and include the assumptions and insights provided in response to Question 19-27.”

a. Provide marked-up pages of an interim revision so the staff can review the proposed changes.

b. Discuss the process (e.g., internal procedure) for communicating these assumptions and insights to the developers of procedures and training.

c. State the mechanism (e.g., combined license (COL) item) for ensuring that these assumptions and insights remain valid in the PRA for the as-built, as-operated plant. (Note that the COL items provided in DCD Section 19.3.3 direct the COL applicant only to update external events and fragilities.)

d. Ensure that the revised table includes (or justifies exclusion of) all key assumptions and PRA-based insights identified in the PRA, DCD Chapter 19, and RAI responses. Several examples related to shutdown risk are (note that this list is not inclusive):

* DCD page 19.1-101: assumption related to the use of freeze seals
* DCD pages 19.1-108 to 19.1-109: key assumptions related to shutdown initiating events and system models
* DCD page 19.1-131 and PRA page 22-18: assumptions related to internal flooding during shutdown (note that PRA description is more detailed)
* PRA page 9-1: assumption that revised evaluation of operator actions can be performed as more specific design information becomes available later
* PRA page 22-20: insights from shutdown internal flooding assessment
* Response to Question 19-11: assumption that strainer plugging failure is no more likely during shutdown than at power
* Response to Question 19-26: assumption that NUMARC 91-06 will be satisfied in the shutdown response guideline
* Response to Question 19-27: insights about shutdown-related design features and key operator actions, instruments, and equipment
* Response to Question 19-45: assumptions about operator actions required to initiate reflux cooling and use of nitrogen to drain SG tubes
* Response to Question 19-45: insight that vent must be closed in certain conditions to prevent core damage
* Response to Question 19-50: assumptions about control of doors during shutdown
* Response to Question 19-63: assumptions used to justify exclusion of boron dilution as an initiating event in the shutdown PRA
* Response to Question 19-66: insight about reactor vessel penetrations
* Response to Question 19-73: assumption that indication will be available during shutdown

19-208

(Follow-up to Question 19-72) The response to Question 19-72 indicates that the DCD and PRA will be modified to revise the shutdown success criteria for safety injection (SI) and charging to match the low temperature overpressure (LTOP) technical specifications (TS) requirements in TS 3.4.12. The staff needs additional information on this ongoing effort. Specifically:

a. The staff notes that the bases for TS 3.4.12 state that “[i]f conditions require the use of more than two SI pumps or one charging pump for makeup in the event of loss of inventory, then pumps can be made available through manual actions.” This statement calls into question how many pumps can be considered available to mitigate accidents during shutdown. However, no additional discussion of these manual actions could be found in the DCD. Clearly state and justify the success criteria for SI and charging injection during shutdown in all POS, including when the pressurizer is solid and LTOP is a more serious concern. Discuss whether the operators would be expected to start SI or charging pumps, contrary to the stated TS requirement, following a loss of inventory at shutdown. Would additional pumps also be started following other initiating events for which injection is credited in the PRA? What guidance is provided to the operators on when to start additional pumps, balancing LTOP concerns with mitigation of accidents?

b. Describe the modifications that were made to the PRA in response to Question 19-72, including a list of all fault trees that were changed in both the initiating event assessment (FLML, etc.) and systems analysis.

c. Provide marked-up pages of an interim revision so the staff can review the proposed changes.

19-209

(Follow-up to Question 19-25) The response to Question 19-25 uses the frequency of manual reactor trips obtained from NUREG/CR-5750, combined with conditional probabilities that these shutdowns need drained maintenance or fuel removal, to obtain the frequency of Type A (non-drained), B (drained), and C (refueling) outages. However, page 3 of NUREG/CR-5750 states that, to be included in the study, events needed to include an unplanned reactor trip (not a scheduled reactor trip on the daily operations schedule). NUREG-1350, Volume 20, states that the average capacity factor for U.S. nuclear power plants was 92 percent in 2007. In comparison, the POS durations and frequencies from DCD Table 19.1-79 and the response to Question 19-25, respectively, indicate that the US-APWR would be shut down only 3.6 percent of the year. Therefore, it appears that the US-APWR shutdown PRA does not account for maintenance outages (planned or unplanned, although unplanned reactor trips are addressed by the sensitivity study provided in the response to Question 19-25). The staff needs additional information on the shutdown schedule to resolve this issue. Specifically:

a. Discuss how the POS durations listed in Table 19.1-79 were developed.

b. Discuss, with support from operating experience as needed, how often planned maintenance outages (not unplanned reactor trips) would be expected to occur for the US-APWR. Discuss whether these outages are expected to be drained or non-drained.

c. Provide the projected capacity factor for the US-APWR and a justification for this value.

d. Discuss how the POS durations and frequencies currently assumed in the PRA (not those provided in response to Question 19-25) compare to the projected capacity factor.

e. Revise the PRA as needed to ensure that shutdown risk is not underestimated because of low POS frequencies.

19-210

The US-APWR PRA assumes that multiple systems (e.g., residual heat removal (RHR), SI) do not need heating, ventilation, and air conditioning (HVAC) to function. Page 6A.14.4-2 of the PRA states that “according to ambient air temperature analysis, ambient air temperature will not exceed the design limit of the mitigation system during the 24 hours mission time regardless of the availability of HVAC.” The staff needs additional information on this assumption. Specifically:

a. Provide a summary and results of the ambient air temperature analysis for each room or area that is assumed not to need HVAC, and state to which systems the analysis applies.

b. Discuss the PRA studies that indicate HVAC is essential to maintain ambient air temperature below the limit for the emergency feedwater (EFW) motor-driven pumps (see page 6A.14.4-2 of the PRA). Discuss why these studies are applicable only to the EFW motor-driven pumps.

c. The responses to Questions 9.4.5-23 and 9.4.5-24 indicate that the air handling units and chilled water system are required to support primary systems that mitigate a design basis accident or transient, so they are required as part of the OPERABILITY definition in TS whenever those primary systems must be OPERABLE. Discuss the differences in assumptions and analyses that result in the HVAC systems being required for TS but not for the PRA.

d. Since the ambient air temperature could be site-specific, discuss the mechanism (e.g., COL item) for COL applicants to verify these calculations and update the PRA if necessary.

19-211

(Follow-up to Question 19-58) The response to Question 19-58 states that “[t]he section 19.2.5 of DCD which describes the accident management will be revised reflecting this RAI. Development of accident management program is one of the COL items identified in Chapter 19, and will include a shutdown response guideline as part of the program to incorporate the discussions given in NUMARC 91-06.” Provide marked-up pages of an interim revision so the staff can review the proposed changes.

19-212

(Follow-up to Question 19-68) The response to Question 19-68 states that “MHI [Mitsubishi Heavy Industries, Ltd.] will revise the shutdown PRA to use a shutdown-specific loss of offsite power (LOOP) frequency. There are certain conservative evaluations for LOOP event in the current PRA model, such as (1) the allowable time to recovery and (2) the human error of re-start RHR pump. In the revision of the shutdown PRA, to prevent the excessive conservative evaluation, MHI will also reflect the detailed evaluation related to these points.” Discuss in greater detail the nature of these “conservative evaluations” and the new detailed assessments. Provide marked-up pages of an interim revision so the staff can review the proposed changes.

19-213

The initiating event fault trees for the shutdown PRA presented in Attachment 20B of the PRA transfer to electrical system fault trees (e.g., EPS-STR69KA/B/C, EPS-69KEP(A/B/C)3, EPS-480EPC3, EPS-DCEPC3) that could not be located in the PRA. Are these fault trees the same as the electrical fault trees presented in Attachment 20A of the PRA, except that they are quantified with a one-hour mission time for the initiating event analysis? If the fault trees used for the initiating events are logically different from those presented in the PRA, provide them.

19-214

Table 19.1-80 of the DCD indicates that no outages are planned for the electrical buses, transformers, or essential service water (ESW) system during shutdown. Discuss when maintenance on these structures, systems, and components (SSC) is expected to be performed. Discuss how this maintenance is modeled in the at-power or shutdown PRA.

19-215

The OPSLOOP (consequential LOOP given a reactor trip) basic event appears in many locations in the shutdown PRA. Is an initiating event during shutdown expected to affect the offsite power grid, or does this event represent the probability of a random LOOP occurring during the accident? Discuss how the probability was derived.

19-216

The system models in the shutdown PRA appear not to include any instrumentation and control (I&C) failures (e.g., sensors, indicators, software). (One exception is the electrical system model, which includes signal and software failures related to gas turbine starting.) Discuss why these failures, which could impede the operators' understanding of shutdown events and ability to take action, are not included in the model.

19-217

The shutdown PRA fault trees include outages for several SSCs (e.g., diesel-driven and motor-driven fire suppression pumps, gas turbines, charging pumps). These out-of-service probabilities are generally in the 1E-2 to 8E-3 range and appear to be in addition to the maintenance schedule stated in DCD Table 19.1-80. Discuss the rationale for including these basic events and how the probabilities were estimated. Discuss why outages for other SSCs were not included.

19-218

Discuss how the shutdown PRA addresses the dependence between human errors that cause or contribute to initiating events and subsequent operator actions needed for mitigating system function. Address in the response both the detailed models for POS 8-1 and their extension to other POS, in which the number of human errors is counted to determine the correction factor.

19-219

For several of the human error probabilities (HEP) evaluated in the US-APWR PRA, the human reliability analysis (HRA) in Chapter 9 of the PRA states that “frequent training has made operators very familiar with the accident sequence, and the lower bound of total HEP is assessed.” Provide additional justification for this statement. How are these accident sequences and operator actions communicated to training developers to ensure that the sequences are as familiar to the operators as assumed? Revise DCD Table 19.1-113 to indicate which operator actions were given lower HEPs because of this training assumption.

19-220

Page 19.1-29 of the DCD states that a basic HEP of 0.03 was selected as a conservative HEP for type A (pre-initiator) human errors. A screening value of 0.05, not 0.03, is recommended for use in the Accident Sequence Evaluation Program HRA Procedure (ASEP) for cases where no plant visit or interaction is possible, as is the case at the design certification stage. (See page 3-32 of NUREG-1842 and page 4-2 of NUREG/CR-4772 for further details.) Justify the use of 0.03 as the basic HEP, and discuss, with support from sensitivity studies as necessary, the impact on the PRA results and insights of this choice.

19-221

Does the PRA assume that locked valves are locked via a “pull-to-lock” mechanism (or software equivalent) in the control room or by a physical lock (or de-energized breaker) that must be removed locally? Discuss the impact of this assumption on the HRA (e.g., RSSOO02RHR2, in which valves must be unlocked and opened).

19-222

Page 9-70 of the PRA indicates that “if the crew uses different control panel (window) to perform next action, then [the location of] these actions are defined as ‘different.’” For the dependent operator actions modeled in the shutdown PRA, provide additional justification for the assumption that different control panels are used and that this difference is equivalent to a different location. The discussion of the control room design in MUAP-07007 appears to describe a single operational visual display unit (VDU) for each operator.

19-223

(Follow-up to Question 19-56) The response to Question 19-56 did not justify the exclusion of failures (e.g., spurious operation or inadvertent opening of particular valves) that could result in a loss of reactor coolant system (RCS) inventory outside containment. Such losses of inventory would not return to the refueling water storage pit (RWSP), so the impact on mitigating systems would be different from that assessed for loss-of-coolant accidents (LOCA). Identify all flow diversion pathways that would lead to loss of RCS inventory outside containment and justify exclusion of associated failures and accident sequences from the shutdown PRA for both internal and external events.

19-224

(Follow-up to Question 19-56) The staff needs additional information on the HEP for inadvertent opening of valves 9815A/B/C/D (RHR valves MOV-025A/B/C/D). The errors from NUREG/CR-1278 referred to in Table 9.3.2-2 of the PRA are designated as “turn rotary control in wrong direction when there is no violation of populational stereotypes” and an error of omission when a long checkoff list is used. It is not clear that either of these error types applies to inadvertent opening of the valve during the two situations identified in the response to Question 19-56 (draining the refueling cavity and full-flow test of the RHR pump). Specifically:

a. Discuss why these error types were selected.

b. Discuss why the two identified situations are the only cases in which the valves could be inadvertently operated.

c. State which valve controls are expected to be near the controls for valves 9815A/B/C/D, such that inadvertent operation could occur.

d. Discuss how the design change to lock the valves closed (also addressed in RAI 88, Question 19-141) affects the HEP. If the HEP is reduced, discuss whether pipe ruptures, other failure modes of the valves, or other flow diversion pathways that are currently screened out become significant enough that they should be modeled as LOCA initiators.

19-225

The staff needs additional information to understand the modeling of the LOA top event (isolation following a LOCA during shutdown). Specifically:

a. The description of the LOAOO02LC human error in Chapter 9 of the PRA does not discuss how the operators decide whether the cause of the low RCS level is a LOCA or a failure to maintain water level (FLML) event. (The staff observes that the LOAOO02OD human error for over-drain (OVDR) and FLML events includes identification of the drain valve status.) Because different actions are taken in the two scenarios, this decision is important. Discuss how the operators make this decision and the mechanism for communicating this scenario to the developers of procedures and training.

b. The fault tree presented on page 20A.8.B-1 of the PRA represents isolation of a single train of RHR. If the only indication of a LOCA is low RCS water level, it may not be clear which train of RHR has the LOCA. Discuss how the operators determine which train to isolate, or whether all running trains of RHR are expected to be isolated. If more than one train of RHR will be isolated, revise the PRA as appropriate.

c. The fault tree presented on page 20A.8.B-1 of the PRA does not include common-cause failure (CCF) of the valves to close. Justify this omission.

d. The fault tree presented on page 20A.8.B-1 of the PRA does not include any support systems (e.g., electrical power) for the valves. This omission removes a potential dependency with other top events in the sequence. Justify the omission of support systems for the valves.

19-226

Discuss how each of the error types presented in Table 9.3.2-1 of the PRA (quantification of RCS drain operation failure) were selected. Several of these error types (e.g., set a rotary control to an incorrect setting) appear to be inappropriate for either the action taken or the type of control room interface assumed for the US-APWR. Additionally, justify the assumption that each of the valves operated in the fourth task is—as stated in item 1 in Table 20-13 of NUREG/CR-1278—clearly and unambiguously labeled and set apart from valves that are similar in size and shape, state, and presence of tags.

19-227

(Follow-up to Question 19-73) The RCS draining procedure outlined on page 9-7 of the PRA states that RCS water level is monitored by a temporary indicator (steps 7 and 10a). However, the response to Question 19-73 states that the three water level instruments are permanent equipment. Clarify whether water level during shutdown is monitored using temporary or permanently installed indication. Revise the DCD and/or PRA to correct the discrepancy.

19-228

(Follow-up to Question 19-73) The response to Question 19-73 states that “[i]f errors occur in the measurement [of RCS level] due to differential pressure caused by RCS inventory swept into the pressurizer, it can be considered that all RHR pumps are inoperable. In such a situation, water level in the core can be obtained by measuring the reactor vessel water level.” How will the operators be informed of this possibility and be directed to observe vessel level instead of RCS level? Discuss how this insight is communicated to the developers of procedures and training.

19-229

The HEPs for the RCS draining procedure are developed assuming that the operators are skilled and the stress level is optimum. Given that draining to mid-loop is a high-risk evolution that is likely to be performed only during infrequent refueling outages, provide additional justification for the skill and stress assumptions. What assumptions about shutdown procedures and training underlie the assumption about the operators' skill and stress levels?

19-230

Justify why a lower failure rate of 2.8E-6 per hour (/hr) was assumed for running component cooling water (CCW) pumps (e.g., CWSPCYRCCWPA-CG3) compared to running motor-driven pumps, for which a failure rate of 5.0E-6/hr is presented in DCD Table 19.1-14. The text above Table A.2.27-8 of NUREG/CR-6928, which is cited in DCD Table 19.1-14, states that "[b]ecause some system and failure mode data sets are limited (few or only one failure and/or limited demands or hours), the results should be viewed with caution." Discuss the impact of using two different pump failure rates on the shutdown PRA results and insights.

19-231

Page 20B.3-3 of the PRA states that a one-hour mission time was applied when developing the loss of CCW (LOCS) initiating event frequency. However, Table 20.B.3-5 shows mission times of 24 hours for piping leaks and 0.1 hours for heat exchanger plugging. Discuss why these failures were treated differently, and describe the impact on the shutdown PRA results and insights.

19-232

The CCF probability of the CCW heat exchangers presented in Table 20B.3-13 of the PRA is lower than the value expected based on the information in Tables 7.1-1 and 8.5-3 of the PRA. Discuss how the CCW heat exchanger CCF probability used in the shutdown LOCS model was developed.

19-233

The approach to developing the LOCS and loss of RHR (LORH) initiating event frequencies in the shutdown PRA depends on evaluating a system failure probability over a one-hour mission time and multiplying that probability by the appropriate POS duration and number of shutdown events per year. Discuss how failures on demand in both the main and support systems are handled differently from time-based failure rates in this assessment.

19-234

The CCF probabilities of the RHR pumps (both the group of two running pumps and the group of all three available pumps) and RHR heat exchangers listed in Section 20B.2.1 of the PRA are lower than the values expected based on the information in Tables 7.1-1 and 8.5-3 of the PRA. Discuss how the RHR CCF probabilities used in the shutdown LORH model were developed.

19-235

Table 20B.1-1 of the PRA indicates that the FLML initiating event is caused by either failure of the letdown line or failure of the chemical and volume control system (CVCS), combined with failure of letdown line isolation. These three failures are treated as independent and combined to determine an overall initiating event frequency for each applicable POS. Justify the assumption that these three failures are independent—that is, that no single failure or CCF (e.g., software, valves) could result in a FLML initiating event.

19-236

(Follow-up to Question 19-45) Chapter 20 of the PRA indicates that the SGs are credited for heat removal in POS 3, 4-1, 8-3, 9, and 11. According to DCD Tables 19.1-76 to 19.1-78, RCS level is at the nozzle center in POS 4 and 8 and the RCS is full in POS 3, 9, and 11. However, the analysis of reflux cooling performed in response to Question 19-45 addresses RCS levels only at the top, center, and bottom of the main coolant piping. NUREG-1410, cited in the response to Question 19-6, showed different results when the RCS was initially full (see Section 8.3.8 and Figures 8.6 to 8.8). Therefore, provide a description and results of a design-specific analysis demonstrating the effectiveness of reflux cooling in the US-APWR when the RCS is initially full, as in POS 3, 9, and 11. Identify, as in the response to Question 19-45, whether any operator actions (e.g., closing a vent) are critical to avoid core damage. Discuss the mechanism for communicating these critical actions to the developers of procedures and training.

19-237

The footnote to Table 20.7-1 in the PRA indicates that the RCS is opened in POS 4-2, 4-3, 8-1, and 8-2. The body of the table indicates that the reactor vessel upper plenum is open in POS 8-1 and the pressurizer safety valve is removed in POS 4-2, 4-3, 8-1, and 8-2. However, DCD Tables 19.1-76 and 19.1-77 state that the RCS is closed in POS 4-3 and 8-1 and open in POS 4-2 and 8-2. Additional clarification is needed:

a. Clarify what the footnote means by “RCS is opened” (i.e., which penetrations are assumed open, and their sizes). The treatment of POS 4-1 and 8-3 in Table 20.7-1 indicates that “vented” and “opened” have two different meanings.

b. State whether the RCS is open or closed in POS 4-3 and 8-1.

c. Discuss any impact of this discrepancy on the shutdown PRA.

d. Revise the DCD and/or PRA so that the designation is consistent.

19-238

(Follow-up to Questions 19-7 and 19-45) The response to Question 19-45 indicates that the operator must open the main steam depressurization valve (MSDV) to initiate steam generator cooling following a loss of RHR. Page 19.1-103 of the DCD states that the secondary cooling function fails if the main steam relief valves (MSRV) fail to open manually. Clarify whether the operator is expected to open the air-operated MSRV, the motor-operated MSDV, or both to enable secondary cooling during shutdown.

In addition, DCD Tables 19.1-107 to 19.1-114 appear not to include any valves from the main steam system as important SSCs for POS other than 8-1. Justify the exclusion of these valves and any required support systems from the tables of important SSCs and from any other programs that use the tables as input (e.g., RAP).

19-239

Section 20A.1.A of the PRA lists cutsets for the HPI2-LOSP and HPI2-LON fault trees, but these fault trees are not presented in Section 20A.1.B where the HPI2 tree is provided or described in the text of Section 20A.1. Provide the HPI2-LOSP and HPI2-LON fault trees, and revise the PRA accordingly.

19-240

Section 20A.1 of the PRA indicates that failure of limit switches associated with motor-operated valves (MOV) 8820A/B, 8805A/B, and 8807A/B (piping and instrumentation diagram (P&ID) designators MOV-001A/B, MOV-009A/B, and MOV-011A/B, respectively) are risk-significant, because spurious closure of these valves would disable the safety injection line. The staff needs additional information to understand these important failures. Specifically:

a. Discuss why the limit switches are modeled separately from other valve failures. The data source for MOV failures, NUREG/CR-6928, indicates that the MOV component boundary includes the valve, the valve operator, local circuit breaker, and local instrumentation and control circuitry.

b. Discuss why limit switches are only modeled for these three sets of valves in the safety injection system and not for any other valves or systems.

c. Justify the exclusion of CCF of the MOV limit switches from the shutdown PRA.

d. Discuss why the limit switches for the valves are not explicitly included in the RAP, although the valves themselves are.

19-241

For the HPIOO02S operator action, page 9-52 of the PRA states that the operators must start the SI pump, while page 20A.1-8 of the PRA states that the operators manually initiate the emergency core cooling system (ECCS) actuation signal. Clarify whether the operators are expected to start the pump directly or via the ECCS actuation signal, and revise the PRA accordingly.

19-242

In the shutdown PRA, the HPI2 fault tree transfers to the RWS fault tree to model RWSP failures. However, the RWS fault tree is not presented in Attachment 20A of the PRA, only in Section 6A.14.3.B. Discuss whether the at-power model of the RWSP is directly applicable to the shutdown PRA. If modifications to the RWS fault tree were made for the shutdown assessment, revise Attachment 20A of the PRA to include the fault tree.

19-243

The HPI-401A fault tree in the shutdown appears to model the parallel test line paths in the SI system: a 2-inch line with locked-open valve 8825A (P&ID designator VLV-023A) and 4-inch line with locked-closed valve 8813A (P&ID designator MOV-024A). The top event indicates that the failure represents “insufficient flow [in the SI system] due to test line A failure.” However, the fault tree models leaks and plugging of the components in the locked-open line and leaks in the locked-closed line. It is unclear how these failure mechanisms would result in insufficient flow in the SI system. Discuss the failures HPI-401A and HPI-401B, which is similar, are intended to represent and how these failures affect SI system operation.

19-244

The shutdown PRA appears not to model CCFs of equivalent valves in trains A and B of the SI system (e.g., CCF of valves 8820A and B to close). Justify the exclusion of these failures from the model.

19-245

The cutsets for the HPI2 fault tree in the shutdown PRA do not include CCFs of two trains of any support systems (e.g., electrical, CCW) that could disable the two SI trains. Because only the top 17 cutsets are presented, it is unclear whether support systems are modeled appropriately. Discuss, with support from additional cutsets as needed, how CCFs of SI support system components are modeled in the shutdown PRA. If cross-connects are available that allow more than two trains of support systems to support the two SI trains (and thereby requiring failures of larger groups of components to disable SI), describe these cross-connects and the operator actions needed to enable them.

19-246

Page 20A.3-1 of the PRA indicates that only a small amount of water is available in the refueling water storage auxiliary tank (RWSAT) in a certain POS because the RWSAT water is used for refueling. Clarify to which POS this statement refers, given that the PRA does not model the POS in which the refueling cavity is flooded. If the RWSAT is full during the POS modeled in the PRA, discuss why the PRA assumes that RWSAT makeup is needed. Discuss the impact of the use of RWSP water for refueling on the assumption that it is available for RWSAT makeup.

19-247

Page 20A.3-2 of the PRA indicates that the operator action to provide makeup to the RWSAT depends on the operator detecting a “small leakage” by volume control tank (VCT) level decrease, charging flow rate increase, or makeup water increase. However, RWSAT makeup is expected when charging injection to the RCS following a LOCA or OVDR depletes the inventory of the RWSAT. Clarify how these “small leakage” cues relate to this scenario. Discuss whether the cue for starting the refueling water recirculation (RWR) pumps is low VCT level or low RWSAT level. If the cue were low VCT level, then operator might be directed to start the RWR pumps any time the charging system is used for injection (i.e., both MC and CV top events).

19-248

According to the DCD, the charging pump and high head SI pump flow rates (275 gallons per minute (gpm) and 1540 gpm, respectively) are lower than that of the RHR pumps. The success criteria for the CV and SI top events require only one of either type of pump. Given that a single RHR train does not remove enough decay heat to prevent boiling in certain POS (see Questions 19-46 and 19-139), justify the success criteria for charging and SI for all modeled POS. As needed, provide a description and results of supporting thermal-hydraulic calculations.

19-249

Page 20A.3-8 of the PRA indicates that the VCT stop valves close and the RWSAT suction valves open when charging injection initiates. Are these valve manipulations automatic or manual? If they are automatic, discuss why related I&C failures are not modeled. If they are manual, discuss why failures to manipulate these valves are not included in the CHIOO02CV21 operator action.

19-250

Clarify how the CCF probabilities for the CHIMVCD121BC-ALL and CHIMVOD121DE-ALL (failures of VCT valves to close and RWSAT valves to open, respectively) were derived. The assumed probability of MOVs failing to open or close on demand is 1.0E-3 (PRA Table 7.1-1), and the assumed beta factor for two charging MOVs is 0.14 (PRA Table 8.5-3). In contrast, the CCF probability cited on Page 20A.5.A-21 of the PRA is 4.7E-5.

19-251

Clarify why the probability of a charging pump failing to start (CHIPMBDCHPA/B) is presented as 2E-3 in PRA Table 20A.3-5, as 1.796E-3 in the cutsets for the CHI and CHI21 fault trees, and as 1.8E-3 in PRA Table 18.2-1. Discuss the impact of this difference on the shutdown PRA results and insights.

19-252

The CHI11 fault tree in the shutdown PRA includes the RWSSTRWSP basic event for RWSP failure, rather than transferring to the RWS event tree, as in the HPI2 fault tree. The failure probability of RWSSTRWSP in the CHI11 fault tree is approximately ten orders of magnitude lower than the RWS failure probability indicated in the HPI2 fault tree. Discuss why RWSP failures are modeled differently for the charging system (where the RWSP provides makeup to the RWSAT) than for the SI system.

19-253

The CHI-13A fault tree, which models the A train of RWR for the shutdown PRA, models external leaks from valves 005 and 007 in the B train and from valve 006 in the A train. The CHI-13B fault tree models the B train similarly. Valves 005, 006, and 007 are in series in each train. Clarify why each fault tree includes equipment from the other train.

19-254

The shutdown PRA appears not to model CCFs of RWR pumps A and B. Justify the exclusion of these failures from the model.

19-255

The CHI fault tree, which models the CV top event in the shutdown PRA, includes the CHIOO02CV21 and CHIOO02CV2 operator actions. CHIOO02CV21 models operator failure to start the charging pump remotely to recover RCS level when SI fails following a LOCA or OVDR event. CHIOO02CV2 appears to model initiation of makeup to the RWSAT from the RWSP so that charging injection can continue long-term. However, CHIOO02CV2, as described on page 9-48 of the PRA, also includes operator failure to start the charging pump. Clarify why starting the charging pump is required for both operator actions. Does the charging pump trip on low RWSAT level and need to be re-started?

19-256

The CHIOO02CV212 basic event appears in many cutsets in Chapter 20 of the PRA, but could not be found in any of the fault trees in Attachment 20A. Chapter 9 indicates that the HEP for this basic event is the sum of the HEPs for CHIOO02CV21 and CHIOO02CV2. As discussed in the previous question, these operator actions appear to be dependent (i.e., both require starting the charging pump). Provide the fault trees in which the CHIOO02CV212 basic event is modeled, and justify the addition of the two HEPs.

19-257

Page 20A.3-3 of the PRA states that the CHI fault tree is used for “ALL initiating events except LOOP.” However, no fault tree for charging following a LOOP initiator could be located. Provide the fault tree that was used in this scenario, and revise the PRA accordingly.

19-258

For scenarios in which charging was successfully used to recover level immediately after a LOCA or OVDR (MC top event), does the PRA assume that the charging pumps would be stopped once level returns to normal? If the charging pumps continue to run, the operators would not need to start the pumps again if SI fails (CV top event). Discuss this scenario.

19-259

Discuss why the success criterion for the MC top event requires charging injection for 24 hours, given that the MC top event represents short-term charging injection to recover level and allow the standby RHR pump to start.

19-260

For the RSSOO02RHR2 operator action, page 9-55 of the PRA states that the operators must open five valves and start the standby RHR pump. The fault trees include failures of the five valves (9000C, 9001C, 9014C, 9015C, and 114C) to open and failure of the pump to start. However, page 20A.2-7 of the PRA states that the operators must manually initiate the ECCS actuation signal and containment spray (CS) actuation signal. In addition, page 20A.2-9 also states that the ECCS and CS signals must be manually actuated and does not include the discharge isolation valves (9014C and 9015C) and heat exchanger CCW inlet valve (114C) in the list of components that change status. Clarify whether the pump and valves are manipulated directly or must be actuated by manual ECCS and CS signals. If the actuation signals are used, clarify which components change state as a result of each signal. Revise the PRA as appropriate so that the various sections are consistent.

19-261

The CFACVELFSV6 basic event included in the RSS-02A fault tree is not defined anywhere in Chapter 20 of the PRA. Table 6-3 of the PRA indicates that the basic event corresponds to CSS-VLV-012, but this component could not be located in any P&ID. It appears likely that this basic event corresponds to an external leak in check valve 9012A (P&ID designator CSS-VLV-005A), of which there are no failures in the RHR fault trees. However, it is unclear why similar basic events are not included for the B and C trains of RHR. Clarify which component’s failure is represented by CFACVELFSV6, discuss why similar failures are not included for all RHR trains, and revise the PRA as appropriate.

19-262

In the shutdown PRA, the RHR model only credits the standby train of RHR following a LOCA or OVDR event. However, if the two running RHR pumps are tripped before they cavitate and are vented after level is restored by charging injection (MC top event), it is possible that the two additional trains of RHR could be used. Discuss whether the operators would be expected (e.g., in the shutdown procedures) to recover the initially running trains of RHR and how much time would be available for this action. Describe what the impact on the shutdown PRA results and insights would be if this recovery were modeled.

19-263

(Follow-up to Question 19-52) Table 1-1 provided in the response to Question 19-52 indicates that fire-induced LOCAs are only applicable in POS 3, 9, and 11. The staff needs additional information on this analysis. Specifically:

a. Describe the fire scenarios that result in a LOCA during shutdown.

b. State which flow diversion paths were considered to result in a LOCA. The staff observes that the design change to lock closed valves 9815A/B/C/D (RHR MOVs 025A/B/C/D) may make fire-induced operation unlikely. However, other flow diversion paths, which were screened as discussed in response to Question 19-56, may open spuriously in a fire scenario. If any flow diversion paths were considered to cause OVDR or FLML initiating events rather than LOCAs, discuss this treatment.

c. Justify the exclusion of fire-induced LOCA from all POS other than 3, 9, and 11.

19-264

Table 23U-2 of the PRA appears to list conditional core damage probabilities (CCDP) for the first five entries in the column titled “CCDP” and CDFs (several orders of magnitude smaller) for the remainder of the table. Correct the entries in this table and in any other parts of the PRA where data from this table was used.

19-265

The shutdown flooding cutsets presented in Chapter 22 of the PRA include basic event RAM-LOCS-FM, which has a value of 1E-3 and is designated as the failure probability of one train of CCW by random failure. Describe how this failure probability was derived and why a single basic event, rather than the CCW fault trees, was used.

19-266

It appears that the shutdown flooding analysis estimates the frequency of a flood at a CCW line, combined with random failure of the other CCW train, to obtain a flooding-induced LOCS frequency. However, because no LORH cutsets are presented in PRA Table 22.8-6, it is unclear whether the same treatment (i.e., flood disabling one train, combined with random failures of other trains) was used for LORH. Describe the approach used to develop initiating event frequencies in the shutdown flooding analysis.

19-267

The response to Question 19-18 indicates that LORH and LOCS were excluded from the fire-induced initiating event analysis during shutdown because of train separation. However, it appears (see previous question) that LORH and LOCS were evaluated in the shutdown flooding analysis by combining flood-induced and random failures. Discuss why the approaches taken for fire and flood initiating events assessment were different.

19-268

(Follow-up to Question 19-17) The response to Question 19-17 provided additional information on the FLML initiating event as a proprietary excerpt from the PRA. However, this information should be in the DCD so that all shutdown initiating events can be understood without reference to the PRA. Revise the DCD (e.g., page 19.1-104 where the text states that FLML does not apply to POS 8-1) to describe the failures that cause a FLML initiating event and how the initiating event frequency was derived.

19-269

Table 20A.4-5 of the PRA indicates that the PRS fault tree is used to evaluate CCW and ESW pump restart following a LOOP, but this fault tree could not be located in the PRA. Provide the fault tree used in this scenario, and revise the PRA accordingly.

19-270

(Follow-up to Question 19-137) The response to Question 19-137 indicates that a higher value of the “correction factor” was used for sequences that include combinations of mitigating functions that require the same operator actions. This approach appears to be applied inconsistently. In the PRA, it is only clear that the higher value was used for the SDLORH-0005 and SDLOOP-0027 sequences in POS 4-2 and 8-2. For these sequences, three operator tasks are required (two from POS 8-1 plus GI) and the correction factor is increased from 0.2 to 0.5. However, the following sequences also include combinations of CV and GI or GI and SC (both of which require the RWR pumps) but do not appear to have increased correction factors: SDLOCA-0006, SDLOCA-0011, SDLOCA-0015, SDLOCS-0003, SDLOOP-0006, SDLOOP-0009, SDLOOP-0015, SDLOOP-0018, and SDLOOP-0024. Discuss this discrepancy, and revise the PRA as needed.