REQUEST FOR ADDITIONAL INFORMATION 266-2201 REVISION 1

3/9/2009

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

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

19-306

(Follow-up to Question 19-138) The response to Question 19-138 does not adequately justify exclusion of passive structures, systems, and components (SSC) from the steam generator (SG) and gravity injection (GI) systems from the lists of important SSCs in the design control document (DCD). Failure of these components (e.g., piping in the gravity drain line) could have the same risk impact as failure of active components already included in the reliability assurance program (RAP). Discuss the rationale for including only active components from these systems, and revise the DCD as appropriate.

19-307

(Follow-up to Question 19-139) The response to Question 19-139 does not address the implications of the residual heat removal (RHR) system success criterion completely. Provide additional information on the following subjects, and revise the DCD and probabilistic risk assessment (PRA) as appropriate.

a. Case 1 states that the reactor coolant system (RCS) condition during pressurization is within the design specification of the RHR system. Case 2 indicates that RHR fails only when level drops to the center of the main coolant piping. However, while the temperature cited is lower than the design temperature stated in DCD Section 5.4.7, it is unclear that the RHR system is designed to pump saturated or boiling water. Generic Letter (GL) 2008-01 indicates that gas accumulation of less than five percent by volume can degrade or fail pumps. Provide a description and results of a calculation of the percent gas by volume over time following a loss of RHR. Justify the assumption that the RHR pumps can operate without degradation when there is boiling in the RCS, with reference to GL 2008-01. Discuss how the function of decay heat removal is met with one RHR pump if boiling occurs in the RCS.

b. The response discusses the effect of a stricter success criterion only on the loss-of-RHR (LORH) initiating event during plant operating state (POS) 4-1. Discuss how the success criteria for support systems such as component cooling water (CCW), essential service water (ESW), and electrical power were modified when the RHR success criterion was changed. State the effects of these changes on the calculated initiating event frequencies and the overall PRA results and insights.

c. Following a loss-of-coolant accident (LOCA), over-drain event (OVDR), or failure to maintain water level (FLML), the success criterion for RHR is one of one train, given that one train is unavailable and two trains were disabled by the initiating event. If two trains of RHR are needed to remove decay heat, the RHR function would fail. Discuss the impact of this scenario on the PRA results and insights. (Note that Question 19-262 addresses recovery of additional RHR trains in this scenario.)

19-308

(Follow-up to Question 19-140) The response to Question 19-140 states that the "maintenance rule process and … configuration risk management program are implemented to evaluate the risk of configurations being entered during shutdown." The maintenance rule risk assessment process described in NUMARC 93-11, Section 11, presents incremental core damage probability (ICDP) and incremental large release probability (ILERP) thresholds that are compared to specific configurations and durations. Because the US-APWR PRA includes maintenance unavailability assumptions, the resulting values of core damage frequency (CDF) and large release frequency (LRF) may not be the same as the baseline values used for the maintenance rule. The staff estimated a core damage probability (CDP) of 5E-7 for POS 4-1 based on information in Tables 19.1-79 and 19.1-85. Since the US-APWR shutdown PRA assumes that CDF equals LRF, the large release probability (LRP) in this POS is also 5E-7. If this LRP represented the baseline LRP, configurations raising CDF and LRF by about a factor of three would result in an ILRP above the threshold for configurations that should not be entered voluntarily. The staff needs additional information to understand the use of the US-APWR shutdown PRA for the maintenance rule. Specifically:

a. State whether the assessment of "when the conditional risk impacts are high" will be made using the shutdown PRA or qualitative considerations.

b. If the shutdown PRA is expected to be used, discuss how the baseline CDF and LRF will be calculated during shutdown. Section 11 of NUMARC 93-11 indicates that the configuration-specific CDF may consider the zero-maintenance model, but allows use of the baseline average-maintenance model. During shutdown, certain equipment must be out of service (e.g., charging pumps disabled for low-temperature overpressure (LTOP) considerations), so "zero" maintenance may not be appropriate.

c. Provide estimates of baseline CDF and LRF in each POS, where the baseline is defined as above in part (b).

d. Discuss the impact of equating CDF and LRF on the maintenance rule configuration assessment.

19-309

(Follow-up to Question 19-210) The staff needs clarification on several aspects of the response to Question 19-210.

a. The response states that “[t]he analysis results showed that the ambient air temperature at 24 hours after ESFs [engineered safety features] operation is approximately below 120 F for each area.” Describe the analyses performed, including the initial temperature and any assumed operator actions (e.g., opening doors or installing fans). Define “approximately below 120 F.”

b. Operator actions such as opening doors and installing temporary fans are described to justify not modeling loss of heating, ventilation, and air conditioning (HVAC) for the class 1E electrical area. Discuss how long it will take the operators to detect a loss of HVAC and carry out these actions, and compare this duration to the time before the equipment overheats. Compare the combined failure probability of HVAC and the operator recovery action with the dominant failure probabilities of the related electrical equipment. If the failures are of similar likelihood, the HVAC failure and operator actions should be modeled.

c. Describe the assumed “bounding conditions” for external air temperature. Discuss the effect that higher ambient temperatures would have on the operator actions addressed above.

19-310

(Follow-up to Question 19-211) The staff needs additional information to understand several aspects of the shutdown accident management framework provided in response to Question 19-211.

a. Should the framework clarify when the GI and SG mitigating functions can be used?

b. If the framework will be used to develop detailed guidance and procedures, discuss whether the mitigating functions should be listed in the order they will be used (e.g., GI is not the first means of recovering RCS inventory).

c. Clarify the statement that the safety injection (SI) “system is forced off during [shutdown] operations for maintenance purposes; therefore it is highly likely that function of SI system is intact and available for core cooling.” DCD Table 19.1-81 indicates that at least two SI trains are in standby (not in maintenance) in all POS. Pumps that are out of service for maintenance are likely not to be intact and available for core cooling.

d. The statement that “operators are required to manually open the safety depressurization valves” (SDV) to avoid LTOP conditions conflicts with the response to Question 19-150, which states that the RHR relief valves are used to avoid LTOP and the SDVs provide backup if the relief valves fail. Clarify the actions taken when charging and SI are used during shutdown.

e. How do the operators determine that “an accidental incident is observed,” requiring immediate containment closure? How long will it take to close containment, with and without electrical power? Discuss how procedures and training, including the accident management framework, will ensure that containment is closed before steaming from the RCS makes operator action unachievable.

f. The response to Question 19-26 indicated that the shutdown response guideline will be developed ensuring that NUMARC 91-06 is satisfied. Discuss how the accident management framework addresses NUMARC 91-06 and the more detailed guidance in GL 88-17.

g. The response to Question 19-73 stated that the accident management program will ensure that indication of temperature, pressure, and level is available during shutdown, but the framework does not address this subject. Discuss how availability of these sensors and indicators will be ensured.

19-311

(Follow-up to Question 19-212) Justify the different offsite power recovery failure probabilities used for each POS. Discuss how the probabilities were adjusted given the simplified modeling of POS other than 8-1.

19-312

(Follow-up to Question 19-216) The response to Question 19-216 states that instrumentation and control (I&C) components (e.g., sensors, indicators) are not modeled for manual actions. Discuss the consequences of failure of the sensors listed in the response to Question 19-73. If these failures would significantly increase the likelihood of an initiating event (e.g., OVDR) or impede use of a mitigating system, justify their exclusion from the shutdown PRA and the RAP.

19-313

(Follow-up to Question 19-217) The response to Question 19-217 states that maintenance outages of fire suppression pumps and alternate gas turbine generators are considered in the PRA. These components are not listed in DCD Table 19.1-80. Amend this table to include all systems credited in the shutdown PRA for which maintenance outages are expected.

19-314

(Follow-up to Question 19-221) The response to Question 19-221 states that locked motor-operated valves (MOV) are controlled by breakers in the class 1E electrical room. This room is outside the control room on a different floor. However, the human reliability analysis (HRA) considers unlocking and manipulating such valves as a single subtask performed by a reactor operator (RO) with two senior reactor operators (SRO) checking the action. Discuss who will perform the breaker manipulation and who will check the action. Justify the current treatment or revise the HRA as needed.

19-315

(Follow-up to Question 19-224) The original description of the LOCA initiating event stated that a LOCA occurs if valves 9815A/B/C/D (RHR valves MOV-025A/B/C/D) are

opened. The design change to lock these valves closed has made inadvertent opening of the valves unlikely. The response to Question 19-224 suggests that the LOCA event represents failure to close the valves after the two situations identified in response to Question 19-56 (draining the refueling cavity and full-flow test of the RHR pump), spurious operation of the valves followed by operator failure to close them, or both. Revise the DCD to clarify the situation represented by the LOCA initiating event. State the POS in which the two operations are expected to occur. Given that the design change makes spurious operation unlikely, discuss whether the conservative inclusion of LOCA in every POS masks the importance of other initiating events (and their mitigating systems) to overall shutdown risk.

19-316

(Follow-up to Question 19-225) The response to 19-225(b) states that "[a]t the plant state on page 20A.8.B-1 [of the PRA], the number of operating trains of RHR is one." DCD Table 19.1-80 indicates that at least two trains of RHR are running in all POS. Technical specifications (TS) also require at least two trains of RHR to be in operation. Will procedures direct the operators to isolate all running RHR trains if level continues to drop after letdown isolation? Discuss how the HRA addresses isolation of multiple trains.

19-317

(Follow-up to Question 19-237) Information on the status of the pressurizer manhole, SG manhole, spray line vent, pressurizer safety valve, vessel head, SG nozzles, and other RCS penetrations is provided in the responses to Questions 19-4, 19-69, 19-144, 19-148, and 19-237, as well as DCD Tables 19.1-98 to 19.1-105. Add a table to the DCD that clarifies the status of all relevant RCS penetrations in all modeled POS, as well as the ability to use GI and SG as mitigating functions in each POS.

19-318

(Follow-up to Question 19-237) The response to Question 19-237 indicates that GI will now be credited as a mitigating function in POS 4-3 and 8-1. This function was previously not modeled in detail, since it was credited only in other POS. Describe the approach to developing a detailed model for the GI function, similar to other functions credited in POS 8-1. In addition, the open pressurizer manway in POS 4-3 and 8-1 means that surge line flooding, as described in Question 19-148, may impede the injection function (see the related notification from Westinghouse, Agencywide Documents Access and Management System (ADAMS) Accession No. ML013380174). Discuss how this issue has been addressed.

19-319

(Follow-up to Question 19-228) The response to Question 19-228 indicates that erroneous RCS level measurement is negligible because the "RCS is designed to prevent water seal in the surge line." Does this statement refer to surge line flooding? If the pressurizer manway is opened during POS 4-3 and 8-1 to provide an adequate vent

path, as stated in the response to Question 19-144, discuss how correct indication of RCS level is ensured.

19-320

(Follow-up to Question 19-262) The response to Question 19-262 states that, following a loss of inventory (i.e., LOCA, OVDR, or FLML), recognizing the event occurrence and tripping the RHR pumps will be difficult because detection measures are not specified. The staff agrees that not crediting the pump trip and subsequent recovery of RHR is conservative. However, it is unclear why "detection measures are not specified" when operators are generally trained to monitor water level during shutdown and have procedures for recovering a loss of inventory. This response contrasts with the responses to Question 19-223, which states that flow diversion pathways can be isolated by the operator upon detection of low RCS water level, and 19-225, which states that operators manually isolate letdown if automatic isolation fails and isolate RHR if level continues to drop. The automatic isolation of letdown on low level should provide a clear cue to the operators that level has reduced abnormally, even if they did not detect the level drop previously. The staff needs additional information to understand this scenario.

a. Compare these water levels: (1) the level at which operators, by procedure or training, would likely detect a loss of inventory, (2) the level at which letdown is automatically isolated, and (3) the level at which RHR pumps begin to cavitate. For the expected flow rates during the LOCA, OVDR, and FLML events, discuss how much time is available before each level is reached.

b. Discuss the expected training and procedures related to losses of inventory during shutdown. What would the operators be expected to do at each of the three levels described above?

c. Discuss the estimated risk benefit if an RHR recovery strategy (e.g., tripping the pumps before cavitation and restarting after level is restored) were included in training and procedures. Would this risk benefit increase if the pump trip were automated?

19-321

(Follow-up to Question 19-263) The fire-induced flow diversions listed in the response to Question 19-263 are in different locations than those modeled for internal events. Describe the procedures that will direct operators to isolate these flow diversions, and discuss how the HRA accounts for the different response to these events.