REQUEST FOR ADDITIONAL INFORMATION 364-2655 REVISION 1

5/13/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

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

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

19-322

Please provide the following information related to your response to RAI Question 19-28:

(a) It is stated that the reactor trip system (RTS) consists of two separate digital controllers to achieve defense-in-depth through functional diversity. However, for the engineered safeguard features (ESF) system, it is stated that "there is no consideration of functional diversity," even though the ESF also includes two different controllers. Please discuss how functional diversity is modeled in the PRA and explain why no functional diversity is considered for the ESF.

(b) Explain how the failure of the power interface (I/F) module, which does not appear in Tables 19.28-1&2, was modeled in the PRA.

(c) It is stated in the response that several components/modules (e.g., CPU power supplies, E/O converters) will be considered during the PRA update. Please discuss how the failure of such components/modules will be modeled and state when the next PRA update is expected.

(d) Discuss how manual actuation signals were modeled in the PRA.

19-323

Please provide the following information related to your response to RAI Question 19-29:

(a) Discuss how the alternate ac (AAC) power signal is diverse from all other application signals and how the implementation of this diversity will be verified in the as-to-be-built, as-to-be-operated plant (e.g., through an ITAAC). Is this diversity with respect to both hardware and software?

(b) It is stated that a sensitivity study was performed to investigate the impact of complete dependency among all application software, except for AAC, on the PRA results. Please discuss the assumptions made in this sensitivity study. For example, was the same basic event designator assumed for all applications software but the one for AAC actuation? Explain the result of the sensitivity study (i.e., no impact on CDF) in terms of failed equipment and accident sequences involved. Discuss whether this result could be significantly different if the software failure probability was not assumed to be so low.

(c) How was the failure of sensors for the "other" signals (e.g., signal to start the standby component cooling water pumps) considered in the PRA?

(d) Are all "other" signals also generated by the diverse actuation system (DAS)?

19-324

Please provide the following information related to your response to RAI Question 19-30:

(a) It is stated that hardware CCF is not modeled for I&C systems because it is not significant. Table 19-30-1 of the response, reports an estimate of the ESF system hardware CCF as 4E-6. It is argued that hardware CCF is not significant since the ESF system hardware CCF probability (4E-6) is smaller than the application software failure probability (1E-5). However, these two probabilities are roughly of the same order of magnitude, especially when the associated uncertainties are considered. Furthermore, the modeling of the CCF of I&C hardware in the PRA is important for importance and sensitivity analyses as well as for risk-informed applications. Please discuss.

(b) Provide the basis for the very low component unavailability and discuss how the CCF of sensors and power interface modules was considered.

19-325

In the response to RAI Question 19-33 it is stated that the failure probability for each module type was estimated from the failure rates of the devices that compose the module, through a failure and effects analysis (FEA). It is also stated that the potential for detecting (self diagnosis) and repairing failed modules was considered. Please provide a list of failure and failure detection rates for each module modeled in the PRA as well as more detailed information regarding their basis.

19-326

Please provide the following information related to your response to RAI Question 19-34:

(a) It is stated that digital I&C room cooling is not modeled because the HVAC system is normally operating and therefore the probability to fail within the 24-hour mission time is small. However, the staff notes that according to Section 6A.14.4.1.3 of the PRA report on "Instrumentation and Control," the HVAC fans are in standby during normal operation, which implies that failure to start must also be modeled in the PRA. In addition, the staff notes that the failure to run rate of fans is in the range of 1E-3 to 1E-4 per hour, which does not appear to be negligible. Please discuss.

(b) Discuss how the failure of HVAC is detected during normal plant operation and what requirements are in place to ensure that the plant is not operating w/o room cooling for extended time intervals. Provide the basis (e.g., a combination of

analysis and supporting arguments) indicating that the lack of modeling of loss of I&C room cooling in the PRA does not impact the PRA results and insights.

19-327

In the response to RAI Question 19-35 it is stated that sensitivity studies were performed to address the uncertainty associated with the assumed probabilities for support and application software failure (1E-7/demand and 1E-5/demand, respectively). The staff believes that the assumed probability values in the sensitivity analysis need to be further increased to bound the associated uncertainties and gain a better understanding of the impact of software failure on the PRA results. Also, the digital I&C software failure probabilities should be tracked as an area of uncertainty to be taken into account when the PRA is used for decision making in risk-informed applications.

19-328

In the response to RAI Question 19-36 it is stated that different application software are installed in the two separate digital controllers of each train of the reactor protection system (RPS) and, therefore, the software failure will fail only one controller per train. Please explain how these application software are different for the two controllers. Are they diverse?
Also, it is stated that "application software failure for each digital controller will be modeled and the sensitivity will be studied" during the PRA update for RMTS Initiative 4b. Is this a COL action item? Please clarify.

19-329

In the response to RAI Question 19-38 it is stated that although two different designators were used for the CCF of the pressurizer pressure sensors basic event, it was judged to have a small impact on the PRA results. The staff review finds that even though the two different designators do not appear to have an impact on the results (since the current ATWS event tree model does not credit any mitigating systems, such as high head injection and emergency feedwater), this may not be the case when a more detailed model is developed in the future. Also, this issue may become significant in sensitivity studies where higher application software failure probabilities are used. Please discuss.

19-330

In the response to RAI Question 19-39 it is stated that the FV importance of the "failure of the SG isolation signal" event is very low and, therefore, this event does not need to be modeled in the PRA. The staff believes that the FV importance should be considered together with the RAW importance measure to determine risk significance. Please discuss.

Also, input is provided to DCD Ch. 17.4 in terms of "failure of signal" (e.g., failure of the SG isolation signal)." How will this information be interpreted and used in the reliability

assurance program (RAP) of a future plant? The RAP requires a list of SSCs. Is the provided PRA input to Chapter 17.4 related to both the software and hardware portions of a signal? Please clarify in both the PRA and the DCD.

19-331

In the response to RAI Question 19-40, the second part of the question was not addressed (i.e., explain the basis of the assumed CCF probabilities for the "SG isolation signal"). Please explain.

Also, even though in the response to Question 19-39 it is stated that the event "SG isolation signal CCF" was not supposed to be modeled in the PRA, the response to RAI Question 19-40 implies otherwise. Please clarify.

19-332

In the response to RAI Question 19-42 it is stated that there are shared sensors and distribution modules between the diverse actuation system (DAS) and the protection and safety monitoring system (PSMS). Please explain how these dependencies are modeled in the PRA.
Also, explain how the assumed reliability/availability goal of 1E-2 per demand will be verified.

19-333

In the response to RAI Question 19-43, a list of important "assumptions" made in the PRA regarding design features and operational requirements of the I&C systems (e.g., redundancy, separation, features to prevent spurious actuations, and testing and cooling requirements) is provided. However, this list does not appear to be adequately detailed and comprehensive. Please perform a systematic search to identify all important design and operational features of the I&C systems.