

REQUEST FOR ADDITIONAL INFORMATION 398-1961 REVISION 1

6/18/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 17.04 - Reliability Assurance Program (RAP)

Application Section: 17.4 Reliability Assurance Program

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

17.04-46

The staff requested in RAI 17.04-9 that MHI describe in Section 17.4 of the US-APWR DCD the process to determine dominant failure modes for risk-significant SSCs in scope of D-RAP. In response to RAI 17.04-9, MHI described a process to determine dominant failure modes for risk-significant SSCs that are modeled in the PRA for which an importance analysis was performed. MHI's process does not, however, address: a) determination of dominant failure modes for risk-significant SSCs that are not modeled in the PRA, and b) use of PRA models for which importance measures were not determined (e.g., MHI's process to determine dominant failure modes would disregard the following PRA models because risk achievement worth's and Fussell-Vesely's were not computed, yet these models could identify other important failure modes: various plant operational states in the internal events at lowpower/shutdown (LPSD), internal fire at LPSD, internal flood at LPSD). The staff requests that MHI also describe in Section 17.4 of the US-APWR DCD: a) the process to determine dominant failure modes for risk-significant SSCs that are not modeled in the PRA, and b) how PRA models that do not compute importance measures would be used to identify dominant failure modes.

The staff requested in RAI 17.04-9 that MHI describe who is responsible for determining the dominant failure modes for risk-significant SSCs and include this as a COL information item, if necessary. Typically, a DCD will specify, through a COL information item, that the COL license holder is ultimately responsible for determining the dominant failure modes in accordance with the process described in that DCD. In response to RAI 17.04-9, MHI stated that they will be responsible for determining the dominant failure modes for risk significant SSCs. If these dominant failure modes are not included/referenced as part of the DCD, then the COL license holder that references the DCD would ultimately be responsible for determining these dominant failure modes. In this case a COL information item would need to be included in the DCD for the COL license holder to determine the dominant failure modes. The staff requests that MHI provide the dominant failure modes for the risk-significant SSCs in Section 17.4 of the US-APWR DCD or in a report and reference this report in Section 17.4 of the US-APWR DCD. Otherwise, include a COL information item in Section 17.4.9 ("Combined License Information") of the US-APWR DCD for the COL license holder being responsible for determining the dominant failure modes for risk-significant SSCs prior to initial fuel load and in accordance with the process provided in the DCD.

REQUEST FOR ADDITIONAL INFORMATION 398-1961 REVISION 1

17.04-47

The staff requested in RAI 17.04-10 that COL Information Item 17.4(2) in Section 17.4.9 of the US-APWR DCD, Revision 1 should also address (in accordance with SECY-95-132, Item E) establishment of: 1) reliability performance goals for risk-significant SSCs within the scope of RAP, and 2) performance and condition monitoring requirements to provide reasonable assurance that risk significant SSCs do not degrade to an unacceptable level during plant operations. In response to RAI 17.04-10, MHI stated "All SSCs identified as risk-significant within the scope of the D-RAP should be categorized as high-safety-significant (HSS) within the scope of initial Maintenance Rule." MHI's approach is acceptable provided that maintenance rule will be implemented by the COL license holder in accordance with guidance contained in Regulatory Guide (RG) 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." However, from COL Information Item 17.6(1), there are no requirements for the COL applicant to use RG 1.160 for development/implementation of maintenance rule. The COL applicant could choose to use other guidance for maintenance rule (in which case then the use of HSS may not ensure establishment of reliability performance goals and performance/condition monitoring requirements). Therefore, in general, categorizing all SSCs in scope of D-RAP as HSS may not necessarily lead to establishment of reliability performance goals and performance/condition monitoring requirements for those SSCs.

The staff requests that MHI revise COL Information Item 17.4(2) such that the integration of reliability assurance activities into existing operational programs will also address establishment of:

- 1) Reliability performance goals for risk-significant SSCs consistent with the existing maintenance and quality assurance processes on the basis of information from the D-RAP (for example, implementation of the maintenance rule following the guidance contained in RG 1.160 is one acceptable method for establishing performance goals provided that SSCs are categorized as HSS within the scope of the Maintenance Rule program), and
- 2) Performance and condition monitoring requirements to provide reasonable assurance that risk-significant SSCs do not degrade to an unacceptable level during plant operations.

17.04-48

The staff requested in RAI 17.04-16 that MHI include the remote shutdown panel/console (RSP) in Table 17.4-1 of the US-APWR DCD. Otherwise, provide the basis for not including RSP in Table 17.4-1. MHI stated in their response to RAI 17.04-16 that:

- "Remote shutdown panel is not considered risk-significant for the following reason.
- it is a backup system of the main control board in the event the MCR is uninhabitable and is not considered in PRA
 - it is kept isolated from HSIS while the MCR is inhabitable, and provides no impact on the plant safety and plant operation in the case of its failure"

For the following reasons, the staff found that MHI's response to RAI 17.04-16 does not provide a sufficient basis for excluding RSP from Table 17.4-1:

REQUEST FOR ADDITIONAL INFORMATION 398-1961 REVISION 1

- a) MHI stated that the RSP is not considered in the PRA. However, RSP is modeled (through operator actions at RSP) in the fire PRA at full power (US-APWR PRA, MUAP-07030, Revision 0).
- b) MHI stated that the RSP provides no impact on plant safety and plant operation in the case of its failure. However, RSP is implicitly modeled in the fire PRA at full power for main control room evacuation due to fire and, from a sensitivity analysis, the core damage frequency (CDF) due to RSP failure during main control room fire increases from $1.0E-08/ry$ to $5.8E-07/ry$ (i.e., Case 3, "Probability of Operator Manual Operation" provided in Section 2.3, "Sensitivity Analysis", of Chapter 23, Attachment R of the US-APWR PRA, MUAP-07030, Revision 0).
- c) From Table 23R-13 in MUAP-07030, Revision 0, basic event HPIOO02FWBD-R ("Operator Fails Bleed and Feed Operation at RSP") has a Fussell-Vesely (FV) of $5.9E-03$, which would make this event risk-significant based on the criteria used in Section 17.4.7.1 of the US-APWR DCD, Revision 1. From Table 23R-13 in MUAP-07030, basic event EFWOO01PW2AB-R ("Operator Fails to Open EFW Pit Discharge Cross Tie-Line for Continuous SG Feed Water at RSP") has a FV= $3.4E-03$. Failure of RSP would lead to failure of both human error events that were described above (i.e., these human actions are dependent on success of the RSP). This suggests that the RSP may be risk-significant. Note, the PRA assumption that RSP has a low failure probability and is bounded by the human error events does not provide a sufficient basis for excluding RSP from D-RAP. This assumption is only true if the RSP is subjected to appropriate reliability assurance activities. Therefore, the assumption in the PRA that the RSP has high reliability further emphasizes the need to include RSP in D-RAP (the intent of D-RAP is to ensure the reliability assurance activities that were accomplished prior to initial fuel load for the risk-significant SSCs provide reasonable assurance that the plant is designed and constructed in a manner that is consistent with the key assumptions and risk insights for the risk-significant SSCs).

The staff requests that MHI include RSP in Table 17.4-1 of the US-APWR DCD. Otherwise, provide a more acceptable basis for not including RSP in Table 17.4-1 of the US-APWR DCD.

17.04-49

The staff requested in RAI 17.04-17 that MHI include "hardware" of instrumentation and control (I&C) systems in Table 17.4-1 of the US-APWR DCD. Otherwise, provide the basis for not including hardware in Table 17.4-1. For the following reasons, the staff found that MHI's response to RAI 17.04-17 does not provide a sufficient basis for excluding hardware of I&C from Table 17.4-1:

- a) MHI's basis for not including hardware of I&C in Table 17.4-1 specifically relies on probabilistic arguments, which is not sufficient. As supported by DI&C-ISG-03 ("Task Working Group #3: Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments Interim Staff Guidance," Revision 0, August 11, 2008), uncertainties inherent with the probabilistic risk assessment (PRA) modeling of digital I&C are large (e.g., large uncertainties are associated with PRA modeling of digital I&C: common cause failures, dependencies, interactions between

REQUEST FOR ADDITIONAL INFORMATION 398-1961 REVISION 1

hardware and software, level of modeling detail, failure modes, unknown or unforeseen failure modes, failure data, software reliability, adequacy of modeling methods, interfacing digital system with the rest of the PRA). Therefore, it is not sufficient to specifically rely on PRA models and risk importance measures (e.g., risk achievement worth, Fussell-Vesely) alone to show that software/hardware of digital systems are not risk-significant. Other methods would need to be assessed (e.g., deterministic methods, defense-in-depth, expert panel).

- b) MHI stated in their response to RAI 17.04-17 that "CCF of software were modeled as basic events and showed high RAW values. In the PRA, CCFs of hardware of I&C systems were represented by CCF of software. This is because CCF probabilities of software used in the PRA model were assumed to bound the CCF probability of hardware that have similar impact on the system reliability." This statement suggests that hardware would have similar risk significance as software (i.e., similar high RAW values or impact on risk given a failure). This remains true even if the failure probability of hardware were much lower than that of software.
- c) MHI stated that software CCF probabilities were assumed to bound hardware CCF probabilities. This assumption does not provide a sufficient basis for excluding hardware from D-RAP. It is assumed in the PRA that hardware has high reliability. This assumption is only true if the hardware is subjected to appropriate reliability assurance activities. Therefore, the assumption in the PRA that the hardware has high reliability further emphasizes the need to include hardware in D-RAP (the intent of D-RAP is to ensure the reliability assurance activities that were accomplished prior to initial fuel load for the risk-significant SSCs provide reasonable assurance that the plant is designed and constructed in a manner that is consistent with the key assumptions and risk insights for the risk-significant SSCs).

The staff requests that MHI include hardware of I&C in Table 17.4-1 of the US-APWR DCD. Otherwise, provide a more acceptable basis for not including hardware in Table 17.4-1 of the US-APWR DCD.