

REQUEST FOR ADDITIONAL INFORMATION NO. 175-1676 REVISION 1

2/3/2009

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)

17.04-36

In Section 17.4.9 ("Combined License Information") of the US-APWR DCD, Revision 1, the applicant provides combined license (COL) information items 17.4(1) and 17.4(2). COL information item 17.4(1) states "The COL Applicant shall be responsible for the development and implementation of the Phases II and III of the D-RAP. ...The QA requirements should be implemented during the procurement, fabrication, construction, and pre-operation testing of the SSCs within the scope of the RAP." COL information item 17.4(2) states "The COL Applicant shall be responsible for the development and implementation of the O-RAP..."

- a) COL information items 17.4(1) and 17.4(2) do not specify when the associated activities are to be performed. The use of the term "COL Applicant" in the COL information items could suggest that all of these activities are to be performed during the COL application phase. In accordance with SECY 95-132, Phase II in information item 17.4(1) is performed during the COL application phase and updated/maintained during the COL license holder phase. Phase III in COL information item 17.4(1) is performed during the COL license holder phase and prior to initial fuel loading. A description of the proposed method for developing/integrating the operational RAP into operating plant programs (e.g., maintenance rule, quality assurance) under COL information item 17.4(2) is performed during the COL application phase. The development/integration of the operational RAP under COL information item 17.4(2) is performed during the COL license holder phase and prior to initial fuel loading.
- b) It is not clear in COL information item 17.4(1) as to who will develop the quality assurance (QA) requirements. Also, it is not clear that these QA requirements will address nonsafety-related SSCs within the scope of D-RAP, as required under SECY 95-132 (i.e., SECY 95-132 states that "The COL applicant will propose a method by which it will incorporate the objectives of the reliability assurance program into other programs for design or operational errors that degrade nonsafety-related, risk-significant SSCs.").

The staff requests that the applicant clarify COL information items 17.4(1) and 17.4(2) in Section 17.4.9 of the US-APWR DCD, Revision 1, taking into consideration the comments provided herein (i.e., specify when the activities under the COL information

REQUEST FOR ADDITIONAL INFORMATION NO. 175-1676 REVISION 1

items are to be performed, and clarify the QA requirements in COL information item 17.4(1)).

17.04-37

In accordance with SECY 95-132, the design reliability assurance program (D-RAP) should:

- Provide reasonable assurance that the plant is designed and constructed in a manner that is consistent with the assumptions and risk insights for the risk-significant systems, structures, and components (SSC) in D-RAP.
- Incorporate all aspects of reliability assurance that will be accomplished prior to fuel load (i.e., procurement, fabrication, construction, and preoperational testing phase).
- Be verified using Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC).

Table 2.13-1 in Section 2.13 ("Design Reliability Assurance Program") of the US-APWR DCD, Tier 1, Revision 1, provides the applicant's D-RAP ITAAC. The applicant's D-RAP ITAAC acceptance criteria is restated below:

"A report exists and concludes that the estimated reliability of the each as-built SSCs equals or exceeds the assumed reliability and that industry experience with similar SSCs (including operations, maintenance, and monitoring activities) was taken into account in estimating the reliability of the SSCs."

D-RAP ITAAC should not solely be based on numerical values because some numerical estimates (e.g., estimated reliability, assumed reliability) may not be available, and additional aspects of D-RAP are needed in the D-RAP ITAAC in order to address other key assumptions/risk insights (e.g., room temperature will not exceed the limits of the safety injection pumps during mission time given room cooling is unavailable). Therefore, the applicant's D-RAP ITAAC may not be practical/effective in providing reasonable assurance that the plant is designed and constructed in a manner that is consistent with the assumptions and risk insights for the risk-significant SSCs in D-RAP. It is important to have a process that would control reliability/availability of risk-significant SSCs.

The staff requests that the applicant revise the D-RAP ITAAC in Table 2.13-1 of Section 2.13 of the US-APWR DCD, Tier 1, Revision 1, taking into consideration the comments provided herein. Also, parts of Section 17.4 of the US-APWR DCD, Revision 1, (e.g., Sections 17.4.4, 17.4.8, and COL Information Item 17.4(1) in Section 17.4.9) would need to be revised appropriately to reflect the revised D-RAP ITAAC.

17.04-38

The staff finds that the list of risk-significant systems, structures, and components (SSC) provided under Instrumentation and Control System (I&C) in Table 17.4-1 of the US-APWR DCD, Revision 1 (page 17.4-26) is not adequate for the following reasons:

REQUEST FOR ADDITIONAL INFORMATION NO. 175-1676 REVISION 1

- 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, hardware/software interactions, 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 inappropriate 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).
- "SG(EFW) isolation signals", "CCW start signals", and "A~D-Emergency feed water pump start signals" are considered risk-significant SSCs in Table 17.4-1 of the US-APWR DCD, Revision 1. However, a signal is not a system, structure, or component. The SSCs associated with these signals and determined to be risk-significant should be specified in Table 17.4-1.
- Safety-related Protection and Safety Monitoring System (PSMS) and safety-related portion of the Human System Interface System (HSIS) include: reactor protection system, engineered safety features actuation system, communication system, safety visual display unit processors, safety logic system, main control room safety visual display units, system level conventional switches, and interlock systems important to safety for the plant (see Chapter 7 of US-APWR DCD, Revision 1). PSMS and HSIS are digital systems that have safety functions important to risk and should be included in Table 17.4-1 of the US-APWR DCD.
- Nonsafety-related Plant Control and Monitoring System (PCMS) and nonsafety-related HSIS (see Chapter 7 of US-APWR DCD, Revision 1) may have functions important to risk and should be evaluated (including use of deterministic methods, defense-in-depth, expert panel) for inclusion in Table 17.4-1 of the US-APWR DCD.

The staff requests that the applicant revise the list of risk-significant SSCs under I&C system in Table 17.4-1 of the US-APWR DCD, Revision 1 (page 17.4-26), taking into consideration the comments provided herein.

17.04-39

Section 17.4.4 (Quality Controls) of the US-APWR DCD, Revision 1 references the quality assurance program description (QAPD), which describes quality controls for both the safety-related and nonsafety-related systems, structures, and components (SSCs) within the scope of D-RAP. The QAPD should be listed as a reference in Section 17.4.10 of the US-APWR DCD.

The staff requests that the applicant list the QAPD as a reference in Section 17.4.10 of the US-APWR DCD.