REQUEST FOR ADDITIONAL INFORMATION 734-5659 REVISION 5

4/18/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems

QUESTIONS for Instrumentation, Controls and Electrical Engineering 2 (ESBWR/ABWR Projects) (ICE2)

07.01-37

General Design Criterion 1, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part, that appropriate records of the design and testing of systems and components important to safety be maintained. Regulatory Guide (RG) 1.172, Software Requirements Specifications, which endorses IEEE Std 830-1993, describes a method acceptable to the NRC staff for complying with the NRC's regulations for achieving high functional reliability and design quality in software used in safety systems. In particular, the method is considered consistent with GDC 1 and the criteria for quality assurance programs in Appendix B as they apply to the development of software requirements specifications.

In Section 3.9.8.1, "Plant Requirements Phase SSA," of the Application Software Program Manual (SPM), MUAP-07017, Rev. 3, on page 3.9-9, states “This phase of development is referred to as the Software Requirements Specification (SRS).” From the staff's perspective, the SRS is not a phase but a complete document associated with RG 1.172 as noted above. This document is not related to one phase but remains and evolves even if all details are not available at the time the project is initiated as IEEE Std 830-1993 explains. The staff requests MHI to address this and to revise Section 3.9.8.1 as necessary and ensure that the purpose and use of the SRS are consistent with the referenced RG.

07.01-38

Appendix B to 10 CFR Part 50 contain requirements that extend to software life cycle activities. Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis for those structures, systems, and components to which Appendix B applies are correctly translated into specifications, drawings, procedures, and instructions.

Regulatory Guide (RG) 1.173, which endorses IEEE Std 1074-1995, Developing Software Life Cycle Processes, states:

> 1) [See section C. 1.1] In addressing Appendix B, Criterion III, the descriptions of input information, life cycle activity, and output information that are required by

IEEE Std 1074-1995 must identify applicable regulatory requirements, design bases, and related guidance;

2) [See section C. 3.] To ensure that safety system software development is consistent with the defined system safety analyses, additional activities beyond those specified in IEEE Std 1074-1995 are necessary. Planned and documented software safety analysis activities should be conducted for each phase of the software development life cycle. RG 1.173 also identifies the inputs, activity descriptions and outputs for the software safety analysis.

Section 3.9.8.1, "Plant Requirements Phase SSA," of the Application Software Program Manual, MUAP-07017, Rev. 3, on page 3.9-9, states “All SSA (Software Safety Analysis) activities which shall be performed during the plant requirements phase have all been completed and finished for the generic US-APWR plant and the results of these SSA are described in the US-APWR DCD, including Chapter 7, Chapter 15, Chapter 19 and the related technical reports.” The staff finds this unacceptable as it does not follow the guidance as explained above. An SSA cannot be provided through the “body” of information submitted for the US-APWR design certification.

In addition, BTP 7-14 references NUREG/CR-6101 (as does MHI). In this guidance, Section 4.2.2, Requirements Safety Analysis, states that “The purpose of the safety analysis is to identify any errors or deficiencies that could contribute to a hazard and to identify system safety considerations not addressed in the SRS.”

Therefore, MHI is requested to address this issue and to revise the SPM to indicate a planned and documented SSA will be completed for the Requirements Phase when the requirements phase is completed. Consistent with the guidance stated above, MHI should indicate the SSA will be complete when the SRS has been completed and evolved to a complete document.

07.01-39

Appendix B to 10 CFR Part 50 contains requirements that extend to software life cycle activities. Criterion III, "Design Control," requires measures to ensure that applicable regulatory requirements and the design basis for those structures, systems, and components to which Appendix B applies are correctly translated into specifications, drawings, procedures, and instructions.

Regulatory Guide 1.173, which endorses IEEE Std 1074-1995, Developing Software Life Cycle Processes, states:

(1) In addressing Appendix B, Criterion III, the descriptions of input information, life cycle activity, and output information that are required by IEEE Std 1074-1995 must identify applicable regulatory requirements, design bases, and related guidance;

(2) To ensure that safety system software development is consistent with the defined system safety analyses, additional activities beyond those specified in IEEE Std 1074-1995 are necessary. Planned and documented software safety analysis activities should be conducted for each phase of the software development life cycle. RG 1.173 also identifies the inputs, activity descriptions and outputs for the software safety analysis.

Section 3.9.8.2.1, Preliminary Hazard Analysis, on Page 3.9-12 of the Application Software Program Manual (MUAP-07017, Rev. 3) states that, "The results of the preliminary hazard analysis are described in the technical report, JEXU-1015-1009, "MELTAC Platform Basic Software Safety Report.""

Section 3.9.5.1.1, Hazard Analysis, on Page 88 of the Basic Software Program Manual (JEXU-1012-1132, Rev. 2), makes a similar statement regarding hazards analysis being described in the technical report, JEXU-1015-1009.

However, the staff does not consider the MELTAC Software Safety Report (JEXU-1015-1009) to be a Software Safety Analysis (as discussed in RAI 665-5220). Therefore, the staff requests MHI to address this issue and remove this document as a reference for a software safety analysis in the Basic SPM and the Application SPM.