REQUEST FOR ADDITIONAL INFORMATION 680-5277 REVISION 0

1/18/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 07.01 - Instrumentation and Controls - Introduction

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

07.01-24

The NRC staff has completed an acceptance-like review of the SPMs, JEXU-1012-1132, Rev. 1 and MUAP-07017, Rev. 2 and has determined they do not provide the necessary level of detail, are incomplete, and do not adequately address the staff guidance directly associated with the software life cycle process. The safety system software should be developed to Title 10 of the Code of Federal Regulations (10 CFR) Section 50.55a(a)1, “Codes and Standards,” Section 50.55a(h), “Protection and Safety Systems” and 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” General Design Criterion (GDC) 1, “Quality Standards and Records,” which require safety related structures be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Also, in 10 CFR Part 50, Appendix B, Quality Assurance Criteria, criteria apply as they extend to the software elements.

As the significant lack of detail and specificity are the primary unacceptable elements of the SPMs preventing a detailed technical review, the staff provides some examples of the incompleteness of the processes and documentation described:

1. The SPMs do not identify several processes, and in other cases are not consistent with, software engineering processes used in the IEEE standards endorsed by the staff. *A few examples are:*
    a. All types of Quality Assurance (QA) audits
    b. The multiple sections of the Verification and Validation (V&V) plan
    c. The many topics to be addressed for each V&V activity
    d. The types of software safety analyses to be completed for each phase of the software life cycle
    e. A methodology for the identification of software metrics per the IEEE standard
    f. The use of Configuration Control Boards
2. The SPMs do not recognize the proper development of, or are in many instances not consistent with, documentation in the IEEE standards endorsed by the staff. *A few examples are:*
    a. The types of required V&V reports
    b. The types of test documents to implement the three categories of test documentation

c. The various classes of information in the Software Configuration Management Plan

3. The SPMs do not sufficiently identify the regulations, requirements and standards that form the basis for the plant safety analysis in the development plan or in the software requirements specifications. These should be as complete as known at the time and, if they are to be determined, a process per staff guidance, for changing, updating, tracking and identifying them as “To be Determined” should be developed.
4. Software Tools are not completely listed (examples: the engineering tool, RAPID and MELENs) nor the specific qualification, configuration controls or the organizational responsibilities for implementation.
5. Many terms and their definitions that are essential to describing the process or entities in the SPMs are missing or are not consistent with the standard for software engineering terminology identified by the staff in the endorsed regulatory guides.
6. As upper tier documents, SPMs should identify the relationship to and the actual software plans and procedures used to implement the software planning process. Outputs of the following lifecycle phases cannot be identified as “typical or “sample.”
7. All relavent, consistent information on the lifecycle process should be in the SPMs and only the SPMs, not in other licensing documents.
8. Also procedures not usually specific to software but are necessary to support the software plans should be specifically identified such as: Quality & Technical manuals, Training Databases, Project Risk management, work authorizations, sub-supplier procurement controls, document handling and storage, etc. If these do not exist, the SPM should be detailed enough to identify the procedure, responsibilities and documents generated including format and content.

MHI is requested to revise accordingly and resubmit both SPMs.