

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

Details of Key Technical Issues
Resulting from the U.S. Nuclear Regulatory Commission Staff
Review of Software Program Manuals
United States - Advanced Pressurized Water Reactor Software Program Manual
MUAP-07017, Revision 2
MELTAC Platform Basic Software Program Manual
JEXU-1012-1132, Revision 1

The following provides the U.S. Nuclear Regulatory Commission (NRC) staff's findings and descriptions of the key technical issues from the review of the United States - Advanced Pressurized Water Reactor (US-APWR) Software Program Manuals (SPMs), "US-APWR Software Program Manual," (MUAP-07017, Revision 2) and "MELTAC Platform Basic Software Program Manual," (JEXU-1012-1132, Revision 1), both dated September 2010.

Functions of the SPMs

The SPMs serve the following primary functions:

1. Provides a framework for development of the software plans where the plans have not yet been fully developed or executed. Each software plan, for each application, is a specific implementation of the related portions of the manual (i.e., an instance of a process).
2. The SPMs describe a process of a complex set of software life cycle activities, implemented by various organizations, within which the safety system software will be developed as part of the overall development of the safety-related systems.
3. A carefully planned and formal process, as described by the NRC staff's guidance which endorses safety critical software standards, is essential for high-quality, high-integrity safety system software that cannot be 100 percent tested, due to its inherent complexities.

Regulatory Basis

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," require safety related structures be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. In 10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," apply as they extend to the software elements. Standard Review Plan (SRP) (NUREG-0800) Branch Technical Position 7-14 (BTP 7-14) of the NRC staff's guidance provides the application of these requirements and the US-APWR Design Control Document states that the design fully conforms to the guidance.

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

The NRC Staff Findings

The NRC staff has determined that the revised SPMs remain unacceptable to commence a detailed NRC staff review as much of the same key issues aforementioned remain unresolved. In other words, much of what was done to the SPMs, in the revisions, does not address the NRC staff's underlying issues. The added appendices (i.e., B-2 BTP 7-14 Compliance Matrix (MUAP-07017-P) and B-1-1 Compliance Matrix BTP 7-14 (JEXU-1012-1132)), provide information of how the existing SPMs are interpreted to meet the NRC staff guidance of SRP BTP 7-14. Therefore, the following reiterates much of the same issues that the NRC staff discussed with Mitsubishi Heavy Industries, Ltd. (MHI) during previous interactions and requests for additional information (RAIs).

The SPMs do not provide sufficient information on the safety system software planning process with respect to all 12 plans indentified in the NRC staff guidance, BTP 7-14, such that the safety system will perform its intended safety functions. Therefore, the safety system software is not in compliance with 10 CFR 50.55a(a)1, 10 CFR 50.55a(h), and 10 CFR 50 Appendices A and B as it applies to the software elements. The items discussed below summarize and provide examples of some significant issues which must be resolved.

Key Issues

Detail, Completeness and Specificity

1. MHI has not demonstrated that it has developed the SPMs that will be used to produce the software plans to the quality required for safety system software to be used in the instrumentation and control (I&C) safety systems. A significant lack of detail and specificity are the primary unacceptable elements of the NRC staff's findings. Examples of these are:
 - a. For each activity, the SPMs do not clearly identify a responsible individual or organization as specified by staff guidance.
 - b. Equivalent activities are sometimes identified with NRC staff guidance (e.g., configuration control board and quality assurance (QA) audit walkthrough) but explicit exceptions are not noted and the complete rational for doing so is not identified.
2. The SPMs do not identify several processes, and in other cases are not consistent with software engineering processes and terminology used in the Institute of Electrical and Electronics Engineers (IEEE) standards endorsed by the NRC staff. A few examples are:
 - a. The five types of QA audits per IEEE 1028-1997 as endorsed by Regulatory Guide (RG) 1.168.

- b. The eight sections of the Verification and Validation (V&V) plan per IEEE 1012-1998 as endorsed by RG 1.168.
 - c. The eight topics to be addressed for each V&V activity.
 - d. The types of software safety analyses, identified by BTP 7-14, to be completed for each phase of the software life cycle.
 - e. A methodology for the identification of software metrics per IEEE 1061-1998.
 - f. The function and use of Configuration Control Boards per IEEE 1042-1987 as endorsed by RG 1.169.
 - g. Commercial Grade Dedication per 10 CFR Part 21, "Reporting of Defects and Noncompliance."
 - h. The MHI "augmented" quality control program for non-safety (important to safety) software components.
 - i. Hardware development in the planning process.
3. The SPMs do not recognize the proper development of documentation, or are in many instances not consistent with the NRC-endorsed IEEE standards that identify the necessary documentation. A few examples are:
- a. All five types of required V&V reports per IEEE 1012-1998 as endorsed by RG 1.168.
 - b. The eight types of test documents to implement the three categories of test documentation in IEEE 829-1983 as endorsed by RG 1.170.
 - c. The six classes of information in the Software Configuration Management Plan per IEEE 828-1990 as endorsed by RG 1.169.
4. The SPMs do not identify the actual lower level software plans, procedures, manuals, checklists, etc., or a detailed description of the process including responsibilities, documents generated plus their format and content if these specific documents cannot be identified, that will be used to implement the planning and later life cycle phase activities.

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

- 4 -

- a. Checklists should be included as attachments to the SPM. Merely stating the checklist meets the requirements of a given standard or the NRC staff guidance is insufficient.
 - b. Also, outputs of later phases of the life cycle process cannot be identified as “typical” or “sample” or these outputs will be produced “as required.”
5. The SPMs are not self-sufficient as other reports for US-APWR contain information that provides some evidence of conformance to the NRC staff guidance that is applicable. Other information in these reports sometimes conflicts and initiates confusion of the intent to meet the NRC staff guidance.
- a. MUAP-07004-P, “Safety I&C System Description and Design Process,” identifies the program description for US-APWR, PQD-HD-19005, includes the storage of completed items affecting quality and the Error and Corrective Action Reporting Process for conditions adverse to quality. Neither SPM provides the information included in this program description or reference this document.
 - b. MUAP-07005-P, “Safety System Digital Platform – MELTAC,” lists the procedures used for implementing the Appendix B program. The SPMs neither lists the procedures nor addresses the relationship to the implementing procedures of the software planning phase.
6. By letters dated April 1, 2009 (ML090970864) and March 3, 2010 (ML100670089), MHI provided responses to 41 RAIs initiated by the NRC staff for the US-APWR SPM, MUAP-07017. RAIs 3, 5, 6, 9, 10, 11, 17, 18, 21, 23, 27 and 29 are considered closed. All remaining responses to the RAIs are considered open. Also, since these were originally written for the application SPM, all these RAIs are considered applicable to the MELTAC Platform Basic Software Program Manual, JEXU-1012-1132, Revision 1.

Identification of Regulations, Requirements and Standards

1. The SPMs do not 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. Identification of requirements, and the process for doing so, is a critical feature to be included in the planning phase.
2. Requirements should be specified as completely and thoroughly as is known at the time, even if evolutionary revisions can be foreseen as inevitable. The fact that they are incomplete should be noted per the NRC staff guidance.
3. The SPMs do not identify a formal change process that would be initiated to identify, control, track, and report projected changes. Also any entry that is incomplete, or “to be determined,” should provide the process for doing so per the NRC staff guidance.

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

4. The SPMs do not identify that the Requirements Traceability Matrix is used to show how every requirement is broken down into sub-requirements as the activity is defined by the NRC staff guidance.

Software Tools

1. The SPMs do not list all software tools and activities associated with them. Examples include:
 - a. The SPMs do not address the tools used for Field Programmable Gate Arrays.
 - b. The SPMs do not address the Engineering Tool, the MELENS software which is used to create the Application Software Execution Data and the “RAPID” CAD software package used to create the Functional Block Diagrams.
 - c. For these and the other tools identified, the SPMs do not adequately address:
 - i. The tool qualification processes and when they are done.
 - ii. The configuration controls used and when they are done.
 - iii. The responsible entity or person.
 - iv. The implementing procedures.