

# REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

2/1/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

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

Application Section: Branch Technical Position 7-14, Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1 (AP1000/EPR Projects) (ICE1)

07-14 Branch Technical Position-30

Address the differences in Management, Implementation, and Resource characteristics for each plan in Section B.3, Acceptance Criteria, as well as all other acceptance criteria found in SRP BTP 7-14. The Software Program Manual (SPM) should be revised accordingly to identify the exceptions, specifically, or the methods which are indicative of compliance.

10 CFR 52.47(a)(9) requires, in part, the identification and description of all differences in design features, analytical techniques, and procedural measures proposed for the design and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where a difference exists, the evaluation shall discuss how the proposed alternative provides an acceptable method of complying with the Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The staff is currently reviewing the US-APWR SPM using Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14. In SRP BTP 7-14, Section B.3, Acceptance Criteria, it states that "the reviewer must determine the type of conformance (partial or qualified) if the conformance is achieved and finally if the system is safe." During the review, the staff noted that the distinction between "based" and "conformance" to this particular BTP, and its associated standards, must be stipulated, and if there are any exceptions to this guidance and the associated standards, this should be identified also. Section 1.1 of the SPM states "This SPM provides the software program plans based on the guidance of Branch Technical Position (BTP) 7-14." The staff requests that if the SPM and software development plans conform to staff guidance that it is explicitly stated as conforms in the SPM. Otherwise, identify deviations from the staff guidance and the basis for why the deviations are acceptable.

In addition, if there are particular plans that are complete in the SPM, those should be identified. The staff will then consider all acceptance criteria in SRP BTP 7-14, prefaced by "should" in the guidance for that particular plan, is addressed in the plan and review the plan accordingly. Example; the manual will state in the Software Quality Assurance Plan Section that "a list of the documents subject to software quality assurance oversight is (or should) be included." The actual plan will specifically list and identify what those documents are.

## REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

### 07-14 Branch Technical Position-31

Describe how the US-APWR Software Program Manual (SPM) addresses the staff guidance with regards to the role of the verification and validation (V&V) group performing tests.

10 CFR Part 50, Appendix B, Criterion III, requires, in part, that design verification or checking be performed by individuals or groups other than those who performed the original design. Standard Review Plan Branch Technical Position 7-14, states in Section B.3.1.12.4, Software Test Plan, (STP), that final system testing is considered a V&V test, the STP assigns the responsibility of the definition, test design, and performance to the V&V group. Similar guidance is found in Regulatory Guide 1.168, "Verification & Validation Reviews and Audits," which references C.4.1 of IEEE Std 1012-1998 and states that the V&V responsibility "is vested in an organization that is separate from the development organization." However, the Section 3.12 of the US-APWR SPM, states "the Design Team is responsible for all testing." Also, Section 3.5.1, Purpose, states "PSMS functions that are not adequately tested in the factory are tested at the site in accordance with the Software Test plan." MHI is requested to identify in the SPM how the staff guidance and requirements are met in these two sections and revise these accordingly.

### 07-14 Branch Technical Position-32

Address the assignment of functions normally performed by a Configuration Control Board (CCB) for the Software Configuration Management Plan (SCMP).

10 CFR Part 50, Appendix B, Criterion VI, "Document Control," requires, in part, measures to assure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel and are distributed to and used at the location where the prescribed activity is performed. Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.1.11.1, states the SCMP should define the duties of the CCB. In addition, Regulatory Guide 1.169, which endorses IEEE 828 and IEEE 1042 without exception, provides guidance with regards to a CCB. IEEE 828 states the plan [software configuration management plan] shall identify each CCB and its level of authority for approving changes. Section 2.3.3 of IEEE 1042 states that "in most projects, the CCB is composed of senior level managers. They include representatives from the major software, hardware, test, engineering, and support organizations. The purpose of the CCB is to control major issues such as schedule, function, and configuration of the system as a whole. Also, the more technical issues that do not relate to performance, cost, schedule, etc, are often assigned to a software configuration control board (SCCB)." The staff finds that the US-APWR Software Program Manual does not discuss the use of CCBs, particularly in Section 3.11.3, "Organization/ Responsibilities." MHI is requested to address, in the SMP, the functions of a CCB as referenced by guidance documents for a SCMP.

## REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

### 07-14 Branch Technical Position-33

Provide additional information on the initiation, use, level of detail, and control of the requirements traceability matrix (RTM).

10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part, measures to for the selection and review of the suitability of the application of parts, material, equipment, and processes essential to safety-related functions. Per Standard Review Plan Branch Technical Position 7-14, a process characteristic is completeness. A requirements compliance matrix, showing all system requirements and where in hardware and software, software code, test, and the verification and validation process each of these individual requirements was addressed is valuable. In Section 3.3.5 of the US-APWR Software Program Manual, it is stated that the system requirements specification is turned over to the Verification and Validation team from the Design Team. Doesn't the level of detail necessitate the RTM to be generated at this point? No discussion is provided here if an RTM is used, although it listed as a V&V team output at the requirement phase, or what the level of detail the requirements are. The design basis inputs should not be limited to the topical report references but should also include specific plant licensing documentation.

### 07-14 Branch Technical Position-34

Identify the documents subject to software quality assurance and describe storage and handling of those documents.

10 CFR Part 50, Appendix B, Criterion XVII, "Quality Assurance Records," requires, in part, that sufficient records be maintained affecting quality. In the US-APWR Software Program Manual, the Software Quality Assurance Plan in Section 3.3.6, "Record Keeping," does not identify the list of documents subject to software quality assurance oversight as recommended by the Standard Review Plan Branch Technical Position 7-14. It would be acceptable for the manual to not specifically identify what those documents are. However, the actual plan should identify what those documents by name or other type of unique identifier. Also, the storage, handling, retention and shipping procedures for these documents and for project quality records are not specifically identified as would be included in a plan. The manual should address proper storage of these documents. The plant-specific plans will later be verified by the staff to ensure the actual storage, handling, retention and shipping procedures are completely described.

### 07-14 Branch Technical Position-35

Provide additional description in the US-APWR Software Program Manual (SPM) on the means for identifying malicious code, the tools and methods for checking the software development tool, and the connection of the tools to external networks.

Standard Review Plan Branch Technical Position 7-14, Section B.3.1.1.1, states "Security refers to a description of the methods to be used to prevent contamination of the developed software by viruses, Trojan horses or other nefarious intrusions." Section 3.1.4 of the US-APWR states "The software development tool shall be checked regularly to ensure it is free from "Trojan horses" computer viruses and any other malicious

## REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

code." The staff requests that a description of the methods used to ensure absence of malicious code be identified.

Also, in Section 3.12.3 of the US-APWR SPM states "In order to prevent a possible virus such as a "Trojan horse", the test shall be implemented while disconnected from external networks. Only those tools and software proven not to have an adverse effect may be used for testing." MHI is requested to identify in the SPM (1) What are the specific "methods" and "tool" used for checking the software development tool and (2) "while disconnected from external networks" implies at some time the tools are connected to the external network. When and why is this connection done?

### 07-14 Branch Technical Position-36

Provide clarification on the software metrics used and/or the metrics collection plan.

10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part, design control measures to provide for verifying and checking the adequacy of the design. Clause 4.5.3.6 of IEEE Std 1058-1998 states "The metrics collection plan shall specify the metrics to be collected, the frequency of collection, and the methods to be used in validating, analyzing, and reporting the metrics." Section 3.9.4 of the US-APWR Software Program Manual, states "However, metrics related to critical software functions shall be specifically identified." MHI is requested to state what the critical metrics, related to software functions are and other metrics used per IEEE Std 1058. If necessary, MHI is requested to state in the SPM that the guidelines of IEEE Std 1058-1998 will be used to specify the metrics collection plan if this information is not available for the SPM at this time.

### 07-14 Branch Technical Position-37

Identify the software integration tests, including a description of the tests. Also, identify the tools used for integration and the integration process.

10 CFR Part 50, Appendix B, Criterion V, "Instructions, Procedures, and Drawings," requires, in part, that activities affecting quality shall be prescribed by documented instructions, procedures, or drawings, of a type appropriate to the circumstances. Per Standard Review Plan Branch Technical Position 7-14, the Software Integration Plan (SIntP) should include methods, procedures and controls for software integration, and for combined hardware/software integration, and, when multiple vendors are involved, systems integration. Integration of design outputs and reports should be described. The SIntP should require documentation describing the software integration tests to be performed, the hardware/software integration tests to be performed, the systems integration, and the expected results of those tests. Also, the integration tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be created using the tools. Section 3.4.4, Procedures, of the US-APWR Software Program Manual, does not identify the documentation used describing any of the software integration tests being performed or what those tests are. MHI is requested to update the Section 3.4.4 identifying what those procedures are which make up the software integration plan. Section 3.4.5, Methods/tools, merely

## REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

states, "The tools to be used for integration activities shall not affect the safety application software." The tools that are used and how integration is performed should be specifically identified to complete the Software Integration Plan.

### 07-14 Branch Technical Position-38

Identify compliance with regulatory guidance associated with development of safety-related software.

10 CFR Part 50, Appendix A, General Design Criteria 1, "Quality Standards and Records," requires, in part, that structures, systems, and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions performed. The NRC staff has developed regulatory guidance on software used in safety systems. This guidance primarily is presented in Regulatory Guides (RG) 1.168 through 1.173. All provide NRC staff endorsements, and exceptions as necessary, of associated industry standards as well as regulatory positions on each subject. The US-APWR Software Program Manual (SPM) references only RG 1.169. The staff does not find the requirements of the standards endorsed by this regulatory guide, IEEE Stds 828 and 1042, or the regulatory positions in Section C of the document, have been adequately addressed. Also, the SPM does not provide references to the remaining regulatory guides. More importantly, the SPM does not identify the extent of conformance to these Regulatory Guides or the associated standards. MHI is requested to: 1) reference each of these remaining regulatory guides in the SPM; 2) Identify the level of conformity of each subject matter, for the regulatory guide and associated standard, within the text of the SPM 3) Confirm this level of conformity by addressing each of the significant criteria in the standards (eg. "shall" and "should" statements).

### 07-14 Branch Technical Position-39

Address the change evaluation process requirements associated with 10 CFR 50.59.

10 CFR 50.59 describes the requirements associated with design changes made to a facility. The guidance in Standard Review Plan Branch Technical Position 7-14, Section B.3.1.6.2, "Implementation Characteristics of the SMaintP," states that evaluation of nonconforming items and corrective actions should include, as appropriate, an evaluation with respect to the requirements of 10 CFR 50.59 as well as reporting per the requirements of 10 CFR Part 21. However, the US-APWR Software Program Manual (SPM) does not address the change evaluation process requirements of 10 CFR 50.59. MHI is request to address this requirement and the guidance in the SPM.

### 07-14 Branch Technical Position-40

Describe the procedure for software maintenance using tools that have been revised.

## REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5

10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part, that design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design. Per Standard Review Plan Branch Technical Position 7-14, Section B.3.1.6.4, "Review Guidance for the SMaintP," a provision in the Software Maintenance Plan should be made for qualifying new revisions of the tools if the original version is no longer available. The US-APWR Software Program Manual, Section 3.6.7, states the "tools used should be the same as used in the original development process." The SMaintP should include the procedure if any tool has changed and therefore should be requalified according to procedure and how this is documented.

### 07-14 Branch Technical Position-41

Identify and describe the software safety tasks, including responsibility.

10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part, that design control measures be provided for verifying or checking the adequacy of design. Per Standard Review Plan Branch Technical Position 7-14, Section B.3.1.9.1, Management Characteristics of the SSP, the SSP should specify the person or group responsible for each software safety task. Section 3.9.2 of the US-APWR Software Program Manual, does not specify the person or group responsible for each software safety task. In light of the request to not have a separate software safety organization, the staff considers assignment of each software safety task an even more important feature. The following is, but not necessarily limited to, the tasks which should be addressed:

- Preparation and update of the SSP.
- Specification of the methods for acquisition and allocation of resources to ensure effective implementation of the SSP
- Participation in audits of the SSP implementation
- Training of safety and other personnel in methods, tools, and techniques used in the software safety tasks

A more complete list of organizational responsibilities and tasks can be found in NUREG CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems.