REQUEST FOR ADDITIONAL INFORMATION 244-2094 REVISION 1

3/2/2009

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: Section 07.01 - Instrumentation and Controls - Introduction

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

07-14 Branch Technical Position-1

It should be specifically noted that approval of the SPM (MUAP-07017, R0) does not entail automatic approval of plant-specific project plan(s). If there are sections of the SPM that are the specific plans for the US-APWR then that should be noted and all guidance of BTP 7-14 should be followed for that section or plan. The plant-specific project plans will still be reviewed to ensure compliance with the SPM and with 10 CFR. When is MHI's intending to update the existing US-APWR Project Plan with the individual plan aspects identified in the SPM?

07-14 Branch Technical Position-2

In the SPM, MUAP-07017, R0, Section 3.3.5, Procedures, in Phase 1, Plant Requirement and System Requirement Phase, it is stated that "The V&V Team shall confirm the system specification adequately reflects all plant requirements and licensing commitments." No mention is made how this is done, particularly if a Requirements Traceability Matrix is used. MHI is requested to explain

Per BTP 7-14; "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 address is valuable. An initial Requirements Traceability Matrix is identified as a V&V Team Output from the SV&V Plan. However, it should be identified how the system specification will adequately reflect all plant requirements.

07-14 Branch Technical Position-3

In the SPM, MUAP-07017, Section 3.3.5, Procedures, in the very last sentence, the statement is provided "all software classes in this SPM." MHI is requested to provide the definition of "software classes" and reference to where and how they are used.

07-14 Branch Technical Position-4

In the SPM, MUAP-07017, R0, SQAP, Section 3.3.6, Record Keeping, does not identify the list of documents subject to software quality assurance oversight as recommended by BTP-14 nor the storage, handling, retention and shipping procedures for these documents and for project quality records. The document control method should also be specified.

BTP 7-14, B.3.1.3.2 Implementation Characteristics of the SQAP, in the paragraph beginning with "Record keeping", states "A list of the documents subject to software quality assurance oversight should be included. The SQAP should describe storage, handling, retention and shipping procedures for these documents and for project quality records. Document structures (such as an annotated table of contents) should be provided. The document control mechanism should be specified."

07-14 Branch Technical Position-5

In MUAP-07017, R0, SQAP Section 3.3.7, Methods and Tools, identifies that there will be 2 categories of application software, existing and original, that will be used in the US-APWR. To this point in time, the staff understood only the basic software could potentially use existing or original software modules. This should be explained in the Safety I&C System Description and Design Process, MUAP-07004, in a similar fashion as the existing basic software was presented in the Safety System Digital Platform-MELTAC, MUAP-07005 Topical Report. Also, the justification methods for using the existing application software appear different than the justification for using the existing basic software. MHI is requested to revise both the SPM and Safety I&C System Description and Design Process, MUAP-07004 topical reports accordingly.

07-14 Branch Technical Position-6

In the SPM, MUAP-07017, R0, Section 3.1.1, SMP, describes general functions of the software. Each of these general functions should be traceable to the system requirements which are one of the fundamental purposes of the Software Management Plan as described in BTP-14.

In BTP-14, B.3.1.1.1 Management Characteristics of the SMP, one of the purposes of the SMP should list "general functions the software will be expected to provide, and each of these functions should be traceable to the system requirements."

07-14 Branch Technical Position-7

In the SPM, MUAP-07017(R0), Section 3.1.4, Security, states "The software development tool shall be checked regularly to ensure it is free from “Trojan horses” computer viruses and any other malicious code." This is a guideline of BTP-14 but the description of the methods used should be identified.

BTP-14 section B.3.1.1.1 Management Characteristics of the SMP 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."

07-14 Branch Technical Position-8

What specific metrics, the methods and frequency of collection will be used to monitor the project? In the SPM, MUAP-07017(R0), Section 3.1.5 identifies the "management index" shall be used to monitor the status of the project.

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.”

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-9

In the SPM, MUAP-07017, R(0), SDP, Section 3.2.4, Risks, MHI is requested to address risks associated with the use of pre-developed software and program interfaces, particularly associate contractors and subcontractors. These will be significant factors in the final development and application of the MELTAC platform in the attempted use of existing software from the MELCO provider.

BTP-14, Section B.3.1.2.1 Management Characteristics of the SDP states risk factors that should be included include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of predeveloped software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.).

07-14 Branch Technical Position-10

In the SMP, MUAP-07017 (R0), SDP, Section 3.2.5, Measurement, states logic diagrams are developed using POL. The staff requests MHI to further describe POL. MHI is requested to further identify the software language origination, if it was completely developed by MHI or predeveloped as a commercially available product.

As defined by IEEE Std 100-2000, POL is a type or class of language for a given class of problems.

07-14 Branch Technical Position-11

In the SPM, MUAP-07017, SIP, Section 3.4.3, Measurement, MHI should identify that an error rate is maintained during integration activities and should be recorded, analyzed and reported.

BTP-14 Section B.3.1.4.2 Implementation Characteristics of the SIntP states "The error rate found during integration activities should be measured, recorded, analyzed and reported."

07-14 Branch Technical Position-12

Per the SPM, MUAP-07017, (R0), SIntP, Section 3.4.4, Procedures, should stipulate documentation of the various tests to be performed. If it is assumed that each usage of the word “procedure” means a document describing that activity, please identify that a documented procedure is the proper interpretation.

Per BTP-14, "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."

07-14 Branch Technical Position-13

In the SPM, MUAP-07017, (R0), Section 3.4.5, Methods/ Tools, should specifically state that the engineering tool, assumed to be the same as the MELTAC Platform Engineering Tool called “MELENS” in the Safety System Digital Platform – MELTAC Topical report, 1) can or cannot add defects to the software and 2) is used in such a manner that defects added by the tool or other defects already in the system will be detected by the V&V activities. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Clause 5.3.2, “Software tools” requires “that either a test tool validation program be used to provide confidence that the software tool functions properly, or that the software tool be used in a manner such that defects not detected by the software tool will be detected by V&V activities.”

In summary, the qualification of the engineering tool will have to be presented to the staff. The qualification requirements for software tools depend on what the tool is credited for as follows:

Software tools which are used as design or debugging tools do not require formal qualifications, however the tool should be suitable for use in the manner they are used. The output of these tools will require full verification and validation.

Software tools that are credited with assuring that the software is correct, where the output of the tool does not undergo a V&V process are required to be of the same quality as safety-related software. The software tool will be reviewed by the staff in the same manner as safety-related software.

07-14 Branch Technical Position-14

In the SPM, MUAP-07017, (R0), SInstP, 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." Section 3.12, Software Test Plan states "the Design Team is responsible for all testing." MHI should confirm that 1) this is the same test which both the Software Test Plan and the IEEE Std is discussing; 2) make changes to the SPM accordingly; and 3) provide adequate justification for why the design team is responsible for all testing since this is different from staff guidance that an independent verification and validation team be responsible for testing.

Per BTP-14, the critical part of the software installation is the system test (Note: per IEEE Std 1012-1998, Final System testing is considered a V&V test, and is the responsibility of the V&V group).

07-14 Branch Technical Position-15

In the SPM, MUAP-07017, (R0), SInstP, Section 3.5.1, Purpose, states to install the "correct software if the latest software is not previously installed at the factory." How was this software written and revised? Identify the process for revising the software in the field using the necessary V&V and tools?

07-14 Branch Technical Position-16

In the SPM, MUAP-07017, (R0), SInstP, Section 3.5.5, Methods/tools, states "In this phase, the PSMS controllers are configured to only allow the Engineering Tool to display the installed software condition and status of all inputs and outputs." This implies the capability to revise the application software is somehow disabled. Please further explain this statement.

Section 3.5.5 also does not explicitly state that "installation tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be installed using the tools" per BTP-14. Please include the statement and the qualification of the tools used.

BTP-14, Section B.3.1.4.3, Resource Characteristics of the SIntP, states "The SIntP should require that 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."

07-14 Branch Technical Position-17

In the SMP, MUAP-07017, SMaintP, Section 3.6.1, Purpose, states "if software is modified to accommodate design changes or new functions, the software lifecycle shall be re-executed including all necessary document revisions." The reference to modifying software to accommodate design changes or new functions should be removed. Part of the review process in the SMaintP is to determine that the proposed software maintenance is actually maintenance and does not introduce new functions or other design changes.

Per BTP 7-14, Section B.3.1.6.4, Review Guidance for the SMaintP, states "Make sure that the review process is required to determine that the proposed software maintenance is actually maintenance, and does not introduce new functions or other design changes."

07-14 Branch Technical Position-18

Section 3.6.6, Procedures, states "a regression analysis shall be performed to determine the extent of retesting required." Describe how the regression analysis verifies that the software maintenance has not inadvertently introduced new errors.

Per BTP 7-14, Section B.3.1.6.4, Review Guidance for the SMaintP, states "The regression testing requirements should specify that all the acceptance tests originally performed, or a carefully selected and justified subset of the acceptance tests be used to ensure that no new problem has been created."

07-14 Branch Technical Position-19

In the SPM, MUAP-07017, R(0), SMaintP, Section 3.6.6, Procedures, should require that reported problems be evaluated to allow the identification of nonconforming items and the performance of corrective actions as described in Sections XV and XVI of 10 CFR Part 50, Appendix B. MHI is requested to update the SPM accordingly.

This is the guidance on these issues in BTP-14 Section B.3.1.6.2, Implementation Characteristics of the SMaintP; "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."

07-14 Branch Technical Position-20

Per the SPM, MUAP-07017, R(0), SMaintP, Section 3.6.7, Resources, states the "tools used should be the same as used in the original development process." The SMaintP should include the discussion if any tool has changed and therefore should be qualified accordingly.

Per BTP-14 Section B.3.1.6.4, Review Guidance for the SMaintP, a provision in the SMaintP should be made for qualifying new revisions of the tools if the original version is no longer available.

07-14 Branch Technical Position-21

In the SPM, MUAP-07017, R(0), Section 3.9.2, SSP, Organization/ Responsibilities, of the Software Safety Plan does not 1) identify the single safety officer that has clear responsibility for the safety qualities of the software being constructed or 2) identify a separate software safety organization (currently the V&V Team). MHI is requested to justify the deviation or revise the document.

Both of these items are identified by BTP-14 Section B.3.1.9.1, Management Characteristics of the SSP.

07-14 Branch Technical Position-22

In the SPM, MUAP-07017, R(0), Section 3.9.2, Organization/ Responsibilities, of the Software Safety Plan 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.

Per BTP 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.

07-14 Branch Technical Position-23

In the SPM, MUAP-07017, R(0), SSP, Section 3.9.3, Risks, states that a safety analysis be performed on "each of the principal design documents: requirements, design descriptions, software logic diagram and test specifications."

However, BTP-14 Section B.3.1.9.1, Management Characteristics of the SSP, identifies each of the principal design documents as: "requirements, design descriptions, and source code." MHI is requested to explain the difference proposed in the SPM.

07-14 Branch Technical Position-24

In the SPM, MUAP-07017, R(0), SCMP, Section 3.11.2 identifies examples of items that are subject to configuration management and correctly states "All software items, associated documentation, databases and software development tools shall be controlled in such a manner as to maintain the items in a known and consistent state at all times." However, the staff will need to know specifically what configuration items or controlled documents will be included and part of a master list. MHI is requested to address a composite list of all items under the program and when in the life cycle process this would be available for audit by the NRC staff.

Also, the SCPM should address all items in Regulatory Position C.6 of Reg Guide 1.169 including items that may not change but are necessary to ensure correct software production, such as compliers.

07-14 Branch Technical Position-25

In the SPM, MUAP-07017, R(0), SCMP, Section 3.11.2, Scope, does not describe control points. MHI is requested to update this Section with the criteria related to control points.

NRC Regulatory Guide 1.169 in which Regulatory Position C.3 states "The software configuration management (SCM) plan should describe the criteria for selecting control

points and establish the correspondence between control points identified in the plan and baselines, project milestones, and life cycle milestones."

07-14 Branch Technical Position-26

In the SMP, MUAP-07017, R(0), SCMP, Section 3.11.3, Organization/ Responsibilities, does not discuss the use of configuration control board (CCB) as having the authority to all changes to baselines.

MHI is requested to address the functions of a CCB, per IEEE Std1042 as referenced by Regulatory Guide 1.169, in the SCMP.

07-14 Branch Technical Position-27

In the SPM, MUAP-07017, R(0), SCMP, Section 3.11.6.6, Software Change Request, should encompass the re-examination of any appropriate safety analysis related to the change per Regulatory Position C.10 of Regulatory Guide 1.169. MHI is requested to revise this section accordingly.

07-14 Branch Technical Position-28

In the SPM, MUAP-07017, R(0), Section 3.11.9, Standards, should include IEEE Std 1.169 which is referenced in Section 3.11.1, Purpose. MHI is requested to assure all standards are properly referenced in the SPM.

07-14 Branch Technical Position-29

MHI is requested to identify, in Section 3.12 (STP), of the SPM, the Software Test Plan includes component V&V test execution. This relates to the component testing as defined by IEEE Std. 1012.