


MITSUBISHI HEAVY INDUSTRIES, LTD.
16-5, KONAN 2-CHOME, MINATO-KU
TOKYO, JAPAN

March 3, 2010

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-10063

Subject: MHI's Responses to US-APWR DCD RAI No. 525-4009 Revision 5

Reference: 1) "REQUEST FOR ADDITIONAL INFORMATION 525-4009 REVISION 5, 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" dated February 1, 2010

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document entitled "Responses to Request for Additional Information No.525-4009 Revision 5."

Enclosed is the responses to Questions 07-14 Branch Technical Position-30 through 07-14 Branch Technical Position-41 that are contained within Reference 1.

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of the submittals. His contact information is below.

Sincerely,



Yoshiaki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosure:

1. Responses to Request for Additional Information No.525-4009 Revision 5

CC: J. A. Ciocco
C. K. Paulson

D081
NRD

Contact Information

C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146
E-mail: ck_paulson@mnes-us.com
Telephone: (412) 373-6466

Docket No. 52-021
MHI Ref: UAP-HF-10063

Enclosure 1

UAP-HF-10063
Docket No. 52-021

Responses to Request for Additional Information No.525-4009
Revision 5

March 2010

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

The US-APWR Software Program Manual (SPM), MUAP-07017, conforms to BTP7-14. The word "based on" in Section 1.1 of MUAP-07017 will be changed to "conforms" in the next revision.

All plans contained in SPM are considered complete, with the exception of the project specific information. As stated in Section 1.2 "Some plans require additional planning detail, which is also developed during the execution of a specific project. This additional planning detail shall be provided within an overall Project Plan..."

Each plan within the SPM addresses the specific Management, Implementation and Resource characteristics pertinent to that plan, as defined in the corresponding plan acceptance criteria of Section 3.1 of BTP 7-14. In most cases, there is a one-to-one correspondence between the subsections in the SPM and the corresponding characteristics in BTP 7-14. However, it is noted that as stated on page 11 of BTP 7-14, "Not all specific characteristics occur for every plan." In all sections, the SPM describes the method of compliance to the BTP 7-14 acceptance criteria. The only specific exceptions are discussed in subsequent RAI responses.

Impact on DCD

The last sentence of Section 1.1 Purpose of SPM (MUAP-07017) will be revised as follows:

This SPM provides the software program plans based in which conform to the guidance of Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based I&C Systems" (Reference 1).

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

Based on NRC agreement at the meeting of February 3, 2010 (ML100210769), MHI will revise the SPM (MUAP-07017) to incorporate that final validation testing can be conducted by the Design Team (for Factory tests) or by the Site Team (for site acceptance tests), while the V&V Manager is responsible for final validation tests.

Impact on DCD

The first and second paragraphs in Section 3.12.2 Organization/Responsibilities of SPM (MUAP-07017) will be revised as follows:

The Design Team is responsible for all most testing. However, the V&V Team is responsible for final validation testing. The test personnel may be different or the same as the software designers. Therefore, personnel from the Design Team or V&V Team may prepare procedures and conduct factory tests, and personnel from the site may prepare procedures

and conduct site tests. Regardless of who actually writes the test procedures and conducts the tests, the V&V Team is responsible for approving all test procedures and results that are credited for final system validation. The V&V Team will also verify all tests conducted prior to final validation.

The Design Team, V&V Team or site team establishes test methods and procedures. The Design Team, V&V Team or site team selects test input conditions and defines test output acceptance criteria in the form of documentation, and test practices. The Design Team, V&V Team or site team ~~is responsible for defining and implementing~~ shall define and implement practical tests. The testing personnel shall be fixed before the test is started.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

Section 3.11.6.6 of SPM (MUAP-07017) discusses the use of Software Change Requests. Each Software Change Requests must go through a defined approval process, including approval by 3 separate individuals (i.e., Project Manager, Lead software engineer in Design Team, V&V Team leader), before a change is permitted. This is equivalent to a Configuration Control Board (CCB).

Impact on DCD

The following will be added to the end of MUAP-07017 Section 3.11.1 Purpose:

The SCMP manages the configuration of the approved system design. The SCMP does

not cover design changes. Design changes are managed by the Software Change Request process described in Section 3.11.6.6. The approval process for Software Change Requests described in Section 3.11.6.6 is an equivalent function to the configuration control board (CCB) stated in IEEE Std 828-2005 and IEEE Std 1042-1987 (Reference 13 and 14) which are endorsed from RG 1.169.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

Section 3.3.5 states "The V&V Team shall confirm the system specification adequately reflects all plant requirements and licensing commitments." Also Section 3.10.6.1 states that a V&V output of the Requirements Phase is "Initial Requirements Traceability Matrix (RTM)". MHI will add that a Requirements Traceability Matrix (RTM) shall be used, in Section 3.3.5 of MUAP-07017.

Impact on DCD

The third paragraph in Section 3.3.5 Procedures of SPM (MUAP-07017) will be revised as follows:

The V&V Team shall confirm the system specification adequately reflects all plant requirements and licensing commitments using a Requirements Traceability Matrix (RTM). It is confirmed by the SVVP described in Section 3.10 that the requirements of the higher level design are accurately reflected in the lower level design.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

As stated in the responses to RAI No. 244-2094 (MHI Letter Number UAP-HF-09141, April 2009), "MHI's QA program for safety related documentation applies to all documentation for the PSMS", will be added to Section 3.3.6 of MUAP-07017. Therefore, all PSMS documents are stored and handled according to MHI's general QA procedures. The PSMS documents are identified with a unique system number. Since all PSMS documents are stored and handled in accordance with MHI's general QA procedures, there is no need to identify unique methods in this SPM.

Impact on DCD

There is no impact on DCD.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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 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?

ANSWER:

Software Development Tool

As defined in Section 4.1.4 of Topical Report, MUAP-07005, "Safety System Digital Platform -MELTAC-", the software development tool (The MELTAC Platform Engineering Tool (called "MELENS")) is installed on a non-safety Personal Computer running the Microsoft Windows Operating System. The second bullet of Section 3.1.4 will be modified as shown in "Impact on DCD".

Software Test Tool

Section 3.12.3 will be revised as shown in "Impact on DCD".

Impact on DCD

Section 3.1.4 Security of SPM (MUAP-07017) will be revised as follows:

Security management shall be performed throughout each phase of the software lifecycle, as follows:

- There shall be no connection between the PSMS application software development tool and the business Local Area Network (LAN) or the Internet.
- The software development tool shall be checked regularly to ensure it is free from “Trojan horses” computer viruses, worms and any other malicious code. Commercially available software tools shall be used. Since sources of malicious code vary over time and the methods of malicious code mature accordingly, the most up to date detection methods available shall be used.

In addition to the general security requirements described above, additional security measures for specific lifecycle phases are described in the other lifecycle plans described below.

Section 3.12.3 Security of SPM (MUAP-07017) will be revised as follows:

In order to prevent a possible virus such as a “Trojan horse”, the test shall be implemented while using tools that have not been connected and remain disconnected from external networks. Only those tools and software proven not to have an adverse effect may be used for testing.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

The SPM specifies that metrics are maintained for deficiencies generated by the Design Team and discovered by the V&V Team during document reviews, and during testing, as follows: Section 3.2.5 states "The number of review comments by V&V Team is also recorded and tracked as a quality metric." Sections 3.9.2 and 3.9.4 state "The V&V Team confirms that system documents define critical software functions, software hazards that can prevent the functions, and precautions to prevent these hazards. Metrics shall be maintained throughout the entire lifecycle process for safety analysis deficiencies that should have been included by the Design Team. Section 3.12.4 states "Metrics are maintained and evaluated for test exceptions throughout all test phases. As test phases progress, a decreasing number of test exceptions is a clear indication of software quality."

Impact on DCD

Following description will be added in Section 3.2.5, 3.9.2, 3.9.4 and 3.12.4 of SPM (MUAP-07017).

Metrics shall be periodically reported in the V&V reports.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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 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.

ANSWER:

As stated in Section 3.4.4, the process of installing software into the hardware is described in detail in Section 6.1.8 of MUAP-07005. This includes tests performed to ensure error-free software installation. Section 3.4.4 also states that this will be done using a formal documented procedure. It is not appropriate to put the detailed software installation description in two documents. It is also not appropriate to include detailed procedures in this SPM. It is noted that as stated in Section 3.4.1 "The SIntP and SInstP are limited to ensuring the hardware and software are functioning together. Complete testing to ensure the system performs all functions correctly is covered under the Software Test Plan (STP)."

Impact on DCD

The following will be added to Section 3.4.4 of SPM (MUAP-07017):

After installing the Application Software, and prior to initiating any application level testing, such as factory acceptance tests, for example, self-diagnostics shall be checked and input/output confirmation tests shall be performed to ensure Application Software, Basic Software and hardware are functioning together. This shall include confirmation that "Run/Active" lights are illuminated on all modules and that no module level self-diagnostic errors are being reported.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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).

ANSWER:

Per 10CFR52.47 (a)(9), each industry standard and regulatory guide identified in the Acceptance Criteria, Section B.3, of BTP 7-14 will be referenced in the appropriate section of the SPM. As explained in RG 1.169, IEEE1042 is a tutorial guide that explains how to comply with IEEE Std 828-1990. It is noted that references in BTP7-14 to industry standards and regulatory guidance for commercial grade dedication are not applicable to the SPM, since the SPM applies only to Application Software, which will be developed under a 10CFR50 Appendix B quality program. Commercial grade dedication applicable to the MELTAC platform itself, is addressed in MUAP-07005 and its references, including the MELTAC Re-evaluation Program Report.

In addition, each section of the SPM will be reviewed and amended as necessary to ensure the conformance method is described for each of the significant criteria in the standards identified from Item 1, above.

Impact on DCD

Section 3.1.10 Standards will be added in SPM (MUAP-07017) as follows:

3.1.10 Standards

Software management is performed in accordance with RG 1.173 (Reference 21), which endorses IEEE Std 1074-1995 (Reference 6).

Section 3.2.9 Standards of SPM (MUAP-07017) will be revised as follows:

~~The SDP Software development is performed in accordance with IEEE Std 603-1991, IEEE Std 7-4.3.2-2003 endorsed by RG1.152 (Reference 17), IEEE Std 1074-1995 (Reference 6) endorsed by RG 1.173 (Reference 22), and IEEE Std 830-1997 (Reference 7).~~

Section 3.3.8 Standards of SPM (MUAP-07017) will be revised as follows:

~~The SQAP Software quality assurance is performed in accordance with IEEE Std 603-1991, IEEE Std 7-4.3.2-2003 endorsed by RG1.152 (Reference 17), IEEE Std 1074-1995 endorsed by RG 1.173, IEEE Std 730-1989 (Reference 8), and IEEE Std 1028-1997 (Reference 9) endorsed by RG 1.168 (Reference 18). All aspects of the software life cycle program are conducted under MHI's 10CFR50 Appendix B QAP (refer to DCD Chapter 17).~~

Section 3.4.6 Standards will be added in SPM (MUAP-07017) as follows:

3.4.6 Standards

Software integration is performed in accordance with RG 1.173 (Reference 23), which endorses IEEE Std 1074-1995 (Reference 6).

Section 3.5.6 Standards will be added in SPM (MUAP-07017) as follows:

3.5.6 Standards

Software installation is performed in accordance with RG 1.173 (Reference 23), which endorses IEEE Std 1074-1995 (Reference 6).

Section 3.6.8 Standards will be added in SPM (MUAP-07017) as follows:

3.6.8 Standards

Software maintenance is performed in accordance with IEEE Std 7-4.3.2-2003 endorsed by RG1.152 (Reference 17).

Section 3.7.6 Standards will be added in SPM (MUAP-07017) as follows:

3.7.6 Standards

Software training is performed in accordance with RG 1.173 (Reference 23), which endorses IEEE Std 1074-1995 (Reference 6).

Section 3.10.8 Standards of SPM (MUAP-07017) will be revised as follows:

~~The SVVP Software V&V and associated reviews and audits are performed in accordance with IEEE Std 1012-1998 (Reference 11) and IEEE Std 1028-1997~~

(Reference 9), which are endorsed by RG 1.168.

Section 3.11.9 Standards of SPM (MUAP-07017) will be revised as follows:

The SCMP Software configuration management is performed in accordance with IEEE Std 1074-1995 (Reference 6) endorsed by RG 1.173 (Reference 23), RG 1.169 (Reference 19), IEEE Std 828-2005 (Reference 13) and IEEE Std 1042-1987 (Reference 14).

Section 3.12.8 Standards of SPM (MUAP-07017) will be revised as follows:

This STP is based on the guidance of IEEE Std 829-1983 (Reference 15), which is endorsed by RG 1.170 (Reference 20), and IEEE Std 1008-1987 (Reference 16), which is endorsed by RG 1.171 (Reference 21).

Description in Section 5.0 References will be revised as follows.

In this section, specific references referred in this SPM are provided. Other general applicable codes and regulatory guidance are described in US-APWR DCD Chapter 7, MUAP-07004 and MUAP-07005.

Section 5.0 References will be added as follows.

17. Regulatory Guide 1.152 Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
18. Regulatory Guide 1.168 Revision 1 "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", February 2004.
19. Regulatory Guide 1.170 Revision 0 "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
20. Regulatory Guide 1.171 Revision 0 "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
21. Regulatory Guide 1.172 Revision 0 "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
22. Regulatory Guide 1.173 Revision 0 "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER:

The change evaluation process requirements will be added.

Impact on DCD

The following sentence will be added to the end of Section 3.6.1 Purpose in SPM (MUAP-07017):

Design changes shall be evaluated in accordance with 10CFR50.59.

The following sentence will be added to the end of the first paragraph of Section 3.6.2 Organization/Responsibilities in SPM (MUAP-07017):

Errors shall be evaluated and reported in accordance with 10CFR21.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 07-14 Branch Technical Position-40

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

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.

ANSWER:

The Engineering Tool is a basic component of the MELTAC platform. Therefore it is not appropriate to address methods that ensure Engineering Tool software quality in this SPM, which is only for Application Software. Methods to ensure quality of Engineering Tool software revisions will be addressed in the next revision of MUAP-07005. The Engineering Tool is a configuration controlled component as defined in Section 3.11.2 (1).

Impact on DCD

There is no impact on DCD.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

3/3/2010

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 525-4009 REVISION 5

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

DATE OF RAI ISSUE: 2/1/2010

QUESTION NO.: 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.

ANSWER

Each NRC item requested in the RAI is addresses separately.

Preparation and update of the SSP

Section 3.9 of MUAP-07017 is the SSP. MHI does not anticipate changing this document after NRC approval.

Specification of the methods for acquisition and allocation of resources to ensure effective

implementation of the SSP

As stated in Section 3.9.2, the responsibilities of the SSP are divided between the Design Team and the V&V Team. The Design Team is responsible to ensure all critical software functions are contained within the appropriate design documents. The V&V Team is responsible to independently confirm the adequacy of this documentation. As for all other disciplines within MHI's organization, the Design Team Manager and V&V Team Manager are responsible to ensure adequate qualified staffing to implement their respective responsibilities.

Participation in audits of the SSP implementation

As explained throughout the SPM, audits are conducted by MHI's QA organization, customers and regulators. Audits are conducted on both Design Team and V&V Team responsibilities. QA audits will be coordinated by the QA manager in conjunction with the DTM and/or VTM, as appropriate. As stated in Section 3.3.5 AUDITS AND REVIEWS, Item 3 "External audits by customers or regulators shall be coordinated by the PM who will schedule personnel to be available if additional support is required."

Training of safety and other personnel in methods, tools, and techniques used in the software safety tasks

See response regarding qualified personnel above.

The key tasks defined in NUREG/CR6101 are addressed by the following software safety analysis requirements, as identified in Section 3.9.3:

- Critical safety functions
- Potential software hazards that may adversely affect the critical safety functions, including abnormal events, conditions and malicious modifications
- Mitigating design features or defensive measures to reduce the hazard potential
- Special tests to ensure the hazard potential has been minimized

As described in this section, these analysis tasks are conducted for each of the major design documents, therefore the software safety analysis is an ongoing process conducted throughout the software life cycle.

Impact on DCD

The following will be added to the DTM and VTM responsibilities defined in Section 2.2.2 of SPM (MUAP-07017):

The manager is responsible to ensure adequate qualified staffing to execute all responsibilities of the team, including the responsibilities for the Software Safety Plan, described in Section 3.9. Training shall be provided as necessary in methods, tools, and techniques used in the software safety tasks.

In addition, per the response to RAI DCD_07-14-21, the following will be added to Section 3.9.2 Organization/Responsibilities in SPM (MUAP-07017):

The V&V team manager shall be designated the single safety officer that has clear responsibility for the safety qualities of the software. The safety officer has clear authority for enforcing safety requirements in the software requirements specification, the design, and the implementation of the software. The safety officer has the authority to reject the use of pre-developed software if the software cannot be shown to be adequately safe or if, in using a tool, it cannot be shown that the tool will not impact the safety of the final software system.

Impact on COLA

There is no impact on COLA.

Impact on PRA

There is no impact on PRA.