


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

April 1, 2009

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-09141

Subject: MHI's Responses to US-APWR DCD RAI No.244-2094 Revision 1

Reference: 1) "Request for Additional Information 244-2094 Revision 1 SRP Section: 07-14 Branch Technical Position – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, Application Section: 07.01 – Instrumentation and Controls – Introduction, dated 3/2/2009

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document as listed in Enclosures.

Enclosed are the responses to RAIs contained within References 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.244-2094 Revision 1

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

Contact Information

C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.

DO81
MFO

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-09141

Enclosure 1

UAP-HF-09141
Docket No. 52-021

Responses to Request for Additional Information No.244-2094
Revision 1

April 2009

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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?

ANSWER:

MHI does not intend to generate project specific plans for each section of the SPM, since the entire SPM is applicable to all projects. Where the SPM requires additional project specific information, that additional information will be included in the Project Plan. The Project Plan for the generic US-APWR PSMS will be provided within the DCD Chapter 7 RAI response to RAI 07.02-02, around the end of April 2009. This plan will encompass all activities that are generically applicable to all US-APWR plants.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

MHI considers that the design basis inputs for the requirements phase are the licensing commitments for the design and design process described in the US-APWR DCD, including its references to the design and design process described in Topical Reports, MUAP-07004, "Safety I&C System Description and Design Process" (Safety I&C TR) and MUAP-07005, "Safety System Digital Platform -MELTAC-" (Platform TR).

Impact on DCD

The third paragraph in Section 3.3.5 Procedures of SPM on page 18 will be revised as follows:

The PSMS system requirements specification shall be developed during this phase, in accordance with the ~~Software Development Plan and Software Safety Plan~~ licensing commitments from the US-APWR DCD, including the referenced Topical Reports.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

The discussion of software classes was originally included to allow distinguishing some software as "safety critical" and other software as "important to safety". However, MHI will treat all PSMS software the same. So the discussion of software classes can be deleted.

Impact on DCD

The last paragraph in Section 3.3.5 Procedures of SPM on page 21 will be revised as follows:

Problem reporting and corrective action procedures span the entire software lifecycle and all ~~software classes~~ identified in this SPM.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

MHI's QA program for safety related documentation applies to all documentation for the PSMS.

Impact on DCD

The first paragraph in Section 3.3.6 Record Keeping of SPM on page 21 will be revised as follows:

All activities shall be documented and recorded. The documents shall be controlled under configuration management and shall be stored properly in the library. Therefore, MHI's QA program for safety related documentation applies to all documentation for the PSMS.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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 USAPWR. 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.

ANSWER:

MHI will not reuse any Japanese software. All application software for the US-APWR will be new.

Impact on DCD

The fifth paragraph in Section 3.3.7 Methods/Tools of SPM on page 22 will be revised as follows:

For the US-APWR, the application software is basically the same as the application software used in digital safety systems for NPPs in Japan. ~~Many application units will be reused with minor changes to accommodate the US-APWR plant differences, such as the number of reactor coolant loops.~~ However, all application software for the US-APWR will be newly developed, in accordance with this SPM. Only application software developed in accordance with this SPM can be reused.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

The list of functions described in the SPM is simply to assist the reader in obtaining a high level understanding of the PSMS. The Software Specification defines these same functions and they will be traced by the V&V team using the RTM. Therefore, there is no need to trace these functions for the SPM.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

The software development tool was developed and is used under the following conditions, which thoroughly prevent contamination by viruses, Trojan hoses etc.

- Tool development phase: The Tool was developed by qualified persons, under a strictly control environment, such as an area with no connection to the internet etc. The tool after development, it is maintained under a strictly controlled environment by the qualified persons. The security for the Engineering Tool development is described in MUAP-07005, Section 6.1.6 Cyber Security Management.
- Application development phase using the tool: The application software is developed by qualified persons, under a strictly control environment, such as area, independent from internet etc. same as above. Under the controlled condition stated above, after initialized and formatted memory devises for temporarily use or hand carrying are used, this condition is free from viruses etc., and are used for this purpose only.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

Section 3.1.5 Measurement only defines management metrics. Metrics for each section of the SPM are separately defined within each section.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.).

ANSWER:

This section of the SPM already addresses "existing software" and "interfaces". MHI will change the SPM to clarify that the expression "existing" means "predeveloped", and the expression "interfaces" means "program interfaces (maintenance, user, associate contractors, subcontractors, etc.)".

Impact on DCD

The first paragraph in Section 3.2.4 Risks of SPM on page 16 will be revised as follows:

The potential risks of application software development shall be documented. These risks include system risk, mechanical risk, hardware risk, size risk, complexity risk, predeveloped existing software risk, schedule risk, technical risks, program interfaces (maintenance, user, associate contractors, subcontractors, etc.) interface risks.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

POL is the graphical interface programming language used in both MELENS and RAPID. POL allows application software to be developed by graphically interconnecting conventional function blocks that are familiar to process control engineers. In Japan application software based on POL has demonstrated good performance for many years. It is noted that the outputs from both RAPID and MELENS are confirmed through manual V&V activities. A description of POL will be added to the next revision of the Platform Topical Report, MUAP-07005, in Section 4.1.4.1(a) Creation of Application Software.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

During integration activities, the error rate shall be maintained, recorded, analyzed and reported.

Impact on DCD

The third paragraph in Section 3.4.3 Measurement of SPM on page 23 will be revised as follows:

When an error occurs during the process of software integration, the Design Team must identify the cause by determining, recording and analyzing the error. To perform these activities, the error rate during integration activities shall be maintained, recorded, analyzed and reported. Errors that may impact the schedule of the Design Team or the work being done by other teams shall be reported to other teams by the Design Team Leader.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

MHI uses a documented procedure for Software Integration.

Impact on DCD

The fourth paragraph in Section 3.4.4 Procedures of SPM on page 24 will be revised as follows:

The software integration sequence is implemented in compliance with the integration procedure. The relevant practice should refer to methods, procedures and management. The outcome of integration should be reported to all other teams. For these integration activities, including copying the software, comparing the software and deference checking, documented procedures are prepared and used.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

The outputs of the software tools are confirmed by (2) manually checking the function block interconnection drawing which is generated by the software development tool (verification) and (2) by manually testing the system with installed software which is generated by the software development tool (validation). By this method, any defects that may be generated by the software tool will be detected by V&V activities in accordance with IEEE 7-4.3.2 requirements.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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).

ANSWER:

The process defined as Software Installation in the SPM is the same process as defined as Installation and Checkout in IEEE-1012.

MHI believes the Design Team's responsibility does not end until a system is completely tested and thereby demonstrated to meet the original design requirements. If the Design Team were to transfer their responsibility to produce a high quality system that meets all system requirements to another organization, prior to complete testing, it would prematurely terminate the Design Team's responsibility. Since the V&V team performs all independent verification throughout the software life cycle, MHI consistently applies their independent review role to testing also.

MHI's approach is consistent with IEEE 7-4.3.2, since IEEE 7-4.3.2 defines testing distinctly from verification and validation, and there are many examples in IEEE 7-4.3.2 where testing is defined as part of the normal design/development process:

Section 5.3 defines testing as part of the development process:

A typical computer system development process consists of the following life cycle processes:

Testing the functions to assure the requirements have been correctly implemented

Section D.3 defines testing as an activity distinct from V&V:

The purpose of a hazard analysis is to explore and identify conditions that are not

identified by the normal design review and testing process. The normal design verification and validation process ensures that the design requirements are met by the safety system.

Section D.4.2.1 defines testing as part of the normal design process:

The hazard identification process should use the same system development and maintenance elements that are used during the normal design process, such as the following:

Testing (factory acceptance, simulation, and post-modification testing)

Section D.4.2.3 defines testing as part of the system development process:

A multi-discipline team approach should be used for the identification of the critical functions in all areas of the system development process (e.g., hardware and software development, operations, design, maintenance, and testing).

Section D.4.3.6 defines integration testing as part of computer development

Computer integration testing ... should occur as an inherent part of testing activities performed during computer development.

There is no requirement in IEEE 7-4.3.2 that testing be assigned to the V&V team.

MHI considered that "V&V team has responsibility of testing" described in the SRP section 3.1.5.4 means V&V team has a responsibility of the test result which reflected the all requirements for PSMS and all functions are correctly done. The Design Team is responsible for performing the test and to present the test result to V&V team.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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?

ANSWER:

Section 3.6 Software Maintenance Plan defines the software revision process. This process is executed in an identical manner regardless of implementation in the factory or the field; the same software development process and development tools are used. For the case where the software that is shipped with the system is not the final software, the final software is tested in a target system at the factory that adequately represents the field configuration. The adequacy of the test environment is verified by the V&V team.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

The capability to revise software within the MELTAC controller is disabled using a hardware interlock, as described in the Platform Topical Report (MUAP-07005) Sections 4.1.4.1 b) Download, 4.1.4.1 e) Adjustment of field changeable constants and setpoints, 4.3.4.2 Isolation, and 4.5.2 Control of Access for Software.

MHI does not rely on the Engineering Tool to ensure the software is downloaded correctly from the Engineering tool to the controller. The Platform Topical Report Section 6.1.8 Software Installation states:

After all Basic Software is installed, Integration Tests are conducted. The scope of the Integration Tests is determined based on the scope of the new/revised software, as discussed in Section 6.1.4, above. Integration Tests are designed to confirm all functions, including any errors that may have been introduced by the non-safety related Engineering Tool.

Therefore, qualification of the Engineering Tool is not necessary.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

The Software Maintenance Plan refers to modification of the current application software to correct design errors and does not pertain to the introduction of design changes or new functions.

Impact on DCD

The first paragraph in Section 3.6.1 Purpose of SPM on page 27 will be revised as follows:

~~Maintenance refers to modification of the current application software to correct design errors. The Software Maintenance Plan described in this section refers to modification of the current application software to correct design errors. This Software Maintenance Plan does not pertain to the introduction of design changes or new functions. Therefore, if~~ software is modified to accommodate design changes or new functions, the software lifecycle shall be re-executed including all necessary document revisions.

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

4/1/2009

US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

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.

Impact on DCD

The fifth paragraph in Section 3.6.6 Procedures of SPM on page 28 will be revised as follows:

Test the rectifications and non-rectifications of the system, define the assessment criteria and document them. A regression analysis shall be performed to determine the extent of retesting required. To verify that the software maintenance has not inadvertently introduced new errors, 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.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

Problems shall 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.

Impact on DCD

The third paragraph in Section 3.6.6 Procedures of SPM on page 28 will be revised as follows:

Defects and incompatibilities must furthermore be evaluated and reported according to 10 CFR Part 21. Problems shall 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.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

New revisions of the tools or new tools should be confirmed to be of the same quality as the original tools.

Impact on DCD

The first paragraph in Section 3.6.7 Resources of SPM on page 28 will be revised as follows:

~~Software maintenance shall be implemented in accordance with written procedures. The same tools shall be used as during the original software development process. If the original tools are not available, new revisions of the tools or new tools should be confirmed to be of the same quality as the original tools.~~

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

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.

Impact on DCD

The following sentence after the first paragraph in Section 3.9.2 Organization/ Responsibilities of SPM on page 33 will be added as follows:

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, if 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 the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

Section 3.9.2 Organization/ Responsibilities states:

The Design Team is responsible to ensure the requirements of the SSP are followed throughout the software life cycle. 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.

Therefore, the requirement is sufficiently satisfied.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

For the Application Software the "software logic diagrams" are equivalent to conventional "source code". The Application Software source code is described in a graphically symbolized manner using the program oriented language (POL), so that functions can be easily understood.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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 compilers.

ANSWER:

As stated in Section 3.11.2 Scope:

The SCM tracking system shall be used to managing configuration items, so that the revision history of each configuration item may be retrieved, and so that the latest revision of each configuration item may be easily identified.

The SCM tracking system is a living database that is updated throughout the project, as items requiring configuration control are created or revised. The SCM tracking system may be audited by the Staff at any time.

As stated in subsection 1 of Section 3.11.2 :

Configuration management of procured software, such as engineering tools, starts when the software is initially applied to the PSMS.

For the PSMS Application Software the only Engineering Tools used are MELENS and RAPID, which are placed under configuration control. Compilers or other tools are used only for Basic Software. Configuration controls for Basic Software, including related tools, is described in the Platform Topical Report, MUAP-07005.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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."

ANSWER:

The intent of Section 3.11.6 Procedures is to define the control points for configuration management. This section establishes the configuration management control points for all items managed under the configuration control plan for each life cycle phase.

Impact on DCD

The first paragraph in Section 3.11.6 of SPM on page 44 will be revised as follows:

Specific SCM activities are defined below in accordance with the software lifecycle phases. This section establishes the configuration management control points for all items managed under the configuration control plan for each life cycle phase. This plan creates a correlation between baselines, project milestones, and life cycle milestones.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

The responsibilities for configuration management are defined in Section 3.11.3 Organization/ Responsibilities. The proper execution of all software configuration management functions, conducted by the Design Team, is independently verified by the V&V Team. The proper execution of all configuration management functions is independently audited by the QA organization. Therefore, an additional configuration control board is not warranted and is not included in MHI's configuration management plan.

Impact on DCD

There is no impact on the DCD.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

The Item of software safety analysis will be added in Section 3.11.6.6 Software Change Request.

Impact on DCD

The Step 1 Software Change Request Initiation in Section 3.11.6.6 of SPM on 46 will be revised as follows:

The person or organization requesting the change, shall complete the predetermined form, and provide the following information.

- Logic diagram affected
- Software affected
- Documents affected
- Reason for the change
- Description of the change
- Name of person requesting the change
- Software safety analysis
- Date, etc.

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

RG 1.169 will be added in Section 3.11.9 Standards.

Impact on DCD

The first paragraph in Section 3.11.9 Standards of SPM on page 46 will be revised as follows:

The SCMP is performed in accordance with RG 1.169, IEEE Std 828-2005 (Reference 13) and IEEE Std 1042-1987 (Reference 14).

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

4/1/2009

**US-APWR Design Certification
Mitsubishi Heavy Industries
Docket No. 52-021**

RAI NO.: NO. 244-2094 REVISION 1
SRP SECTION: 07-14 BRANCH TECHNICAL POSITION
APPLICATION SECTION: 07.01 INSTRUMENTATION AND CONTROLS - INTRODUCTION
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 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.

ANSWER:

IEEE 1012 defines component testing as testing "for one software element (e.g., unit or module)..."

Impact on DCD

The first paragraph in Section 3.12.1 Purpose of SPM on page 48 will be revised as follows:

This Software Test Plan (STP) covers all testing done to the application software – component testing (e.g., module testing, unit testing) ~~module testing, unit testing~~, integration testing, validation testing, factory acceptance testing, installation testing.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.