

Request For Additional Information

07/01/2009

**US-APWR TOPICAL REPORT:  
Safety System Digital Platform – MELTAC MUAP-07005-P(R3)**

**Mitsubishi Heavy Industries, Inc.  
Docket No. 52-021  
ICE1 Branch**

**2<sup>nd</sup> round MHI US-APWR Topical Report MUAP-07005-P R3, “Safety System  
Digital Platform -MELTAC”**

The following are the NRC Follow-up Requests for Additional Information (RAI), based on original RAI's and Applicant responses:

Number	Description
Supplement RAI-01	Original question: (In part) Identify the specific differences in the MELTAC equipment applied for non-safety applications vs. the equipment applied to safety applications.

Response: (In part) [ (Proprietary information withheld under 10 CFR 2.390)

]

NRC Supplement: [

(Proprietary information withheld under 10 CFR 2.390)

]

Supplement Original question: Item 53 indicates compliance with IEEE 7-4.3.2, "2003 Criteria

Request For Additional Information

RAI-04 for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," yet exceptions on Verification and Validation (V&V) have been taken due to the development of the system under Japanese standards. Please clarify. Has the code remained in Japanese or has it been translated into English? If the code has been translated, please discuss the traceability, V&V, testing, and management of the translation.

Response: (In part) [

(Proprietary information withheld under 10 CFR 2.390)

]

NRC Supplement: [

(Proprietary information withheld under 10 CFR 2.390)

]

Supplement Original question: Identify how the MELCO internal design documents are marked RAI-05 for the safety and non-safety MELTAC systems. Section 3.0, Applicable Code, Standards and Regulatory Guidance, (item 62), referencing IEEE 494 1974 (this is also required by IEEE Std 603-1991, Criterion 5.11) states that documents used for internal use do not contain the "Nuclear Safety Related" designation. Also discuss how documents for the non-safety MELTAC system are differentiated from the safety related system.

Response: [The software document titles for the Safety MELTAC contain "MELTAC Nplus-S", where S means Safety, while the titles for the non-safety (conventional) MELTAC is "MELTAC Nplus." These titles are applicable to all MELTAC software documents used internally by MELCO. The hardware components are common for the safety and non-safety MELTAC. Therefore, there is no distinct identification for the hardware documents inside MELCO.

]

NRC Supplement: The staff considers, for documents, there are two issues per the requirements of IEEE Std 603-1991 and IEEE Std 494 1974; 1) The term to be used is "nuclear safety related" and is to be used on all documents described by IEEE 494. 2) This shall apply to all documents pertaining to software and hardware to the extent described in IEEE Std 494.

For identification of equipment, there are two issues per IEEE Std 603-1991 and IEEE 420, 1) which states in part, "All equipment and wiring should be permanently marked and identified on the interior of Class IE control boards, panels, or racks 2) Also states in part, "Class IE equipment and its wiring shall be identified as such, so that personnel may easily confirm its independence from non-Class IE and redundant Class IE equipment and wiring." MHI is requested to describe in the Topical Report how IEEE Std 603-1991, Criterion 5.11, will be specifically met.

Supplement Original question: In Section 4.3.1, General Description, the design basis is RAI-11 discussed. The communications link is not protected against common mode failures in hardware or software; however, self-testing and diagnostics are in place to detect a failure if it occurs. Please discuss.

## Request For Additional Information

Response: The D3 Topical Report, MUAP-07006, describes many features of the MELTAC platform that provide protection against common mode failure. [

(Proprietary information withheld under 10 CFR 2.390)

]

NRC Supplement:

[

(Proprietary information withheld under 10 CFR 2.390)

]

Supplement RAI-12 Original Question: In section 4.3.2, Control Network, item (b), the discussion indicates that the communication network has the capability of communicating with other divisions or non-safety system. DI&CISG-04, "Task Working Group #4: Highly Integrated Control Room - Communications Issues (HICR)" describes approximately 20 NRC staff positions on interdivisional and safety to non-safety communication. Please discuss any of these positions for which the MELTAC platform may not be in full compliance.

Response: (In Part) As a result of researching the requirements No.1 through 20 of "1 .INTERDIVISIONAL COMMUNICATION", the MELTAC platform is in full compliance, except the following.

NRC Supplement:

1) Staff Postion 10

a) [

(Proprietary information withheld under 10 CFR 2.390)

## Request For Additional Information

]

b) [

(Proprietary information withheld under 10 CFR 2.390)

]

c) [

(Proprietary information withheld under 10 CFR 2.390)

]

Also, MHI is requested to describe in sufficient detail how the MELTAC system complies with DI&C-ISG-04 including all 20 Staff positions. The following are examples where the staff has concerns:

2) Staff Position 1; "A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function." [

(Proprietary information withheld under 10 CFR 2.390)

]

3) Staff Position 3; "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system." In accordance with this guidance in DI&C-ISG-04, provide a description of all data flows from the PCMS to the PSMS, and provide justification for each communication channel as to how it enhances the performance of the safety function.

4) Staff Position 8: "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that

Request For Additional Information

does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.” [ (Proprietary information withheld under 10 CFR 2.390) ]

5) Staff Position 14; “Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.” [

(Proprietary information withheld under 10 CFR 2.390)

]

6) Staff Position 18: “Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.” [ (Proprietary information withheld under 10 CFR 2.390) ]

Supplement RAI-13

Original Question (partial): Data Link communication is discussed in Section 4.3.3.1, Configuration. The various interconnections for the communication systems are listed and named in the topical report. The information describes the network connections but does not give a graphical representation. No information is provided that would substantiate the claim that the communications network design provides physical, electrical or functional isolation of the interconnections at any level of the communications stack.

Response (partial): Figure 4.3-5 provides a graphical representation of the data link connections between redundant safety divisions. This figure is expanded in Figure 13-1 in this response. This figure shows all the data link components described in Section 4.3.3.1 of Topical Report MUAP-07005.

NRC Supplement: Figure 13-1 and text should be included in the topical report.

Supplement RAI-14

Original Question: [

(Proprietary information withheld under 10 CFR 2.390)

] An audit of the test

procedures and reports identifying the results and any corrective action is needed to complete acceptance of the MELTAC equipment qualification.

Response: EMC, Environmental and Seismic Qualification Test Reports will be available at the MELTAC audit.

NRC Supplement:

- 1) During the recent audit, the staff was provided a summary report of the EMI/RFI test reports that were in Japanese. The staff noted that the summary report did not have sufficient information available that appeared to be in the full EMI/RFI test report. For example, the position of the antennas

### Request For Additional Information

and whether the doors are open or not would impact the test results. Therefore the staff is requesting a report to be submitted to the NRC. The report should have sufficient information (and quality of information) for the staff to come to an independent conclusion that all test procedures, configurations, and results were adequate and the MELTAC system meets RG 1.180.

- 2) During the same audit, the staff questioned whether the optical switch was tested in the bypassed condition to see if it affects the operation of the control network. MELCO stated that the optical switch was not tested in the bypassed configuration, but will consider testing such configuration to address any operation limitations such as Technical Specification limitations that may apply for a bypassed optical switch. The staff is requesting, to be put on the docket, complete testing procedures and results and any operational considerations that may be imposed on the MELTAC platform when an optical switch is in the bypass mode. Note the listing of modules in Section 5.1.2.1 identifies the modules included for the environmental test which does not list the optical switch module. This must be addressed also. The staff is requesting a list of modules that were included in each qualification test. The staff refers MHI to IEEE Std 7-4.3.2, endorsed by RG 1.152, Section 5.4.1 Computer System testing, which states, in part, "All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing." As this appears to be a finding in the development process, the staff is requesting the Corrective Action Report, in English, that identifies the omitted optical switch bypass mode test with English translated copies of the updated test procedures, reports and V&V reports.
- 3) During the Jan 21, 22 meeting, MHI agreed to provide Seismic Test Response Spectrum curves to the topical report. Included should be a description of test configuration and any special mounting restrictions or interface requirements to ensure specific applications are bounded by seismic test.

Supplement  
RAI-20 Original Question: Will (did) the Failure Mode and Effect Analysis follow the guidance of any standard?

Response: None

NRC Supplement: Identify the guidance of any standards followed for the FMEA.

RAI- 23  
(New) The staff is requesting additional information to be docketed for the MELTAC Platform Certification. See the Attachment titled: "Attachment to RAI 23, Additional Information to be Docketed"

RAI-24  
(New) MHI is requested to further provide design information, in Section 4.1.2.4, Power Interface Module. At a minimum, the following should be provided:

1. At the Jan. 22, 23 meeting, MHI agreed to clarify, in the topical report, that there are two priority logic functions – one is software based within MELTAC CPU (priority between PSMS and PCMS functions), one is hardware based within PIF module (state based priority to ensure either DAS or PSMS can place component in the credited safety state). Also, a

### Request For Additional Information

typical functional logic for PIF for at least one component type (i.e. one IPL subboard) will be added.

2. Description of the specific interfaces between the different sections of the PIF; Communication Interface, Interposing Logic and Switching Device part.
3. During the March Audit in Kobe, the staff observed that daughter boards implement part of the priority logic path. Currently, MELCO only has daughter boards for system-based priority logic. Daughter boards are being created using state-based priority logic for the US-APWR. The staff is requesting schematics and necessary logic diagrams associated with the discrete (non-software) portions of the device
4. At the March Audit in Kobe, the staff observed that the communications interface portion of the PIF module was implemented using an ALTERA field-programmable gate array (FPGA). Additionally, as with the MELTAC basic software, the FPGA development process did not originally incorporate adequate independent verification and validation. The entire lifecycle process of the software portion in the Communication Interface Part, and other uses of FPGAs in the MELTAC platform, needs to be addressed in the topical report including the FPGA development process and how the communication interface part of the PIF module was approached in the UCP. Similarities/differences with other software in the MELTAC platform would be advantageous to the staff understanding of this particular issue.
5. Section 4.1.2.4 also states "Therefore, periodic replacement is unnecessary in contrast to electro-mechanical relays." MHI is requested to add the expected service life of the PIF modules to substantiate this comparison.

RAI-25  
(New)

At the Jan. 22, 23 meeting MHI agreed to provide design information of the Isolation Modules identified in Section 4.1.2.3. Either by including in this Section or by separated docketed material, at a minimum the information should include:

1. Specific information, should be provided to explain the voltage isolation method (e.g. Transformer, opto-coupler) and current interrupting / limiting method (e.g. Thermistor, voltage regulator) by schematic or detailed description, of the circuits involved, how isolation circuit is maintained under all conditions and inputs.
2. How they are tested during manufacturing and production
3. How they are included in the equipment qualification program

RAI-26  
(New)

MHI is requested to provide the Japanese QA standards, with the equivalent U.S. standards, that were used, if any, for the original software quality assurance program.

Section 3.0, "Applicable Code, Standards and Regulatory Requirements," states that "An assessment of the QA program in place during the original development of this Equipment is provided in this TR." Section 6.1.1 states "The original quality assurance program (referred to as Original QAP) used for the MELTAC Platform development was based on the Japanese Standard JEAG4101 and ISO9001." However, in a letter from Masahiko Kaneda to R. David B. Matthews, dated March 7, 2007, a table comparing U.S. and Japanese Quality Assurance

### Request For Additional Information

requirements was provided in reference for the US-APWR design certification. In that table it states that "JEAG4101-1993 did not specifically address computer program testing" therefore no equivalent requirements to ASME NQA-1-1994, Part II, subpart 2.7, "QA Requirements of Computer Software," can be provided.

RAI-27  
(New) MHI is requested to identify the U.S. NRC recognized standards that would be equivalent to the Japanese Domestic Standards 84 through 87 of Section 3.0 and provide the translated English versions. Also, Section 4.1.1.4, "Environmental Specifications," identifies JIS-C0704-1995 as a Japanese standard.

MHI is requested to identify the U.S. NRC recognized standards that would be equivalent to, and identify the differences to, the Japanese Domestic Standards 84 through 87 of Section 3.0

RAI-28  
(New) MHI is requested to identify, in the topical report, if in the single controller and redundant parallel configuration, the subsystem will stay in the Failure Mode after initial power activation then the power is momentarily lost.

Section 5.6.3.3, Effects of a Single Random Failure, of IEEE Std 603, states that "the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure."

RAI-29  
(New) In Section 4.1.1.3, "Scale and Capacity," the software cycle time is identified between 20msec to 1 sec. This should be explained in the topical report relative to Section 4.1.3.1, Basic Software, also states that "If processing time exceeds 80% the application is divided into two or more controllers, as necessary." MHI is requested to identify in the topical report if the range for software cycle time is programmable or user definable once it is in the field. Also, is the 80% limit relative to the 20msec to 1 sec range?

Per BTP 7-21, Guidance on Digital Computer Real-Time Performance, timing measurements should meet projections or the anomalies should be satisfactorily explained. It is not clear how this technical position is met.

RAI-30  
(New) Section 4.2.1.1, "CPU Module (PCPJ-11)," states the Futurebus+ will be used for data transmission using the Bus Master and Control Network Modules. Briefly describe the features of this bus architecture. Include if the data transfer is asynchronous and if all components will have separate clocks therefore not requiring time stamps to be provided by identified sources.

The staff believes IEEE Std 603 Criterion 5.6, Independence, will be adequately met if asynchronous operation can be proven and the safety division is not dependent upon any information or resource originating outside its own safety division to accomplish its safety function. This is discussed in staff position 1.1 of DI&C-ISG-04.

RAI-31  
(New) The topical report, in Section 4.1.2.1.6, should identify how the Status Display Module connects with the controller(s) and other devices giving it the capability to display the mode and alarms of the other subsystems. The topical report should indicate what and how it is displayed.

## Request For Additional Information

Criterion 5.8.2, System Status Indication, of IEEE std. 603 states; "Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status."

- RAI-32 (New) In Section 4.1.2.7.3, identifies a "fan stop detection circuit." Does this detect fan rotation or loss of power? MHI is requested to identify this in the topical report.
- RAI-33 (New) For Section 4.1.2.8, Power Supply Module, the staff has the following concerns that should be addressed directly in this section of the topical report:
- 1) Each of the different power supplies, identified within the different types, should be identified, explained and appropriately noted on Figure 4.1-8.
  - 2) The question of the independent sources being different divisions of DC power is answered in 4.1.2.10. But what is meant by "as independent as practical" as explained in 4.1.2.10?
  - 3) PS-1 & PS-2 are noted as mounted outside the chassis. A figure should be provided as to how and where they are mounted and why that is the case.
  - 4) It is stated that overcurrent protection lowers the output voltage level but does not trip the unit. Is this always the case?
  - 5) When AC power is lost, an alarm signal is sent to the Subsystem. Explain;
    - (i) How this is done with no input power
    - (ii) What the subsystem is?
    - (iii) Where the subsystem is physically located in Fig. 4.1-8?
- RAI-34 (New) For Section 4.1.2.9, Controller Cabinet, the staff has the following concerns that should be addressed directly in this section of the topical report:
- 1) [ (Proprietary information withheld under 10 CFR 2.390) ]
  - 2) Does each chassis consist of multiple modules and do these pullout to provide access to each module for replacement?
  - 3) What modules can be replaced at power (i.e. hot swappable?). Describe the basis and system functional impact of the lack of hot swap capability, including any limiting conditions of operation, for any MELTAC system modules designed as such.
  - 4) [ (Proprietary information withheld under 10 CFR 2.390) ]
- RAI-35 (New) In Section 4.1.5, Self-Diagnostics, the staff has the following questions:
- 1) This section states "When the error is severe, the Controller makes a transition from the Control or Standby mode to the Failure mode." Completely discuss what errors are "severe", what errors do not require a transition to another controller? , and how they are identified to the operator?
  - 2) Each description of the three types of self-diagnostic features ends with an "etc." This apparently means there are other checks done but not identified here. MHI is requested to complete the list consistent with the current MELTAC platform basic software. If there are additional features to be added, will the reliability analysis be affected per IEEE 7-4.3.2? Will the cycle time calculation be affected?

Request For Additional Information

- 3) In part 2) Alarm, states “The minor abnormality with which the system can continue” The topical should state specifically what these “minor abnormalities” are that the system can continue with.
- 4) In part 3) I/O Alarm states “the input values are kept as they are in the normal state” This section does not states what cause an I/O alarm. What is kept at normal state? And what is normal state?
- 5) At the January 22,23 meeting with the staff, MHI agreed to provide a description of how self-diagnostics are checked during manual surveillance tests – memory and I/O. Also, a history of self-diagnostics success or failure (either factory or field data – field data is preferable) should be added. The topical report should demonstrate that manual tests did not detect something that self-diagnostics were expected to detect, and that self-diagnostics did not incorrectly report errors that were later determined to be acceptable

IEEE Std 7-4.3.2 provides the reasoning for types of diagnostics to be used and in when they should be used. It is not clear to the staff the full extent of the diagnostics that MHI is proposing and if the guidelines of this standard are met.

RAI-36 (New) Also with regards to the guidelines provided in IEEE Std 7-4.3.2 on Fault detection and self-diagnostics, in Section 4.1.5.2.1, CPU Module, the staff has the following questions:  
[

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-37 (New) [

(Proprietary information withheld under 10 CFR 2.390)

]

This, again, leads to the staff’s understanding of the MELTAC platform meeting the guidelines of IEEE Std 7-4.3.2 section 5.5.3, Fault detection and self-diagnostics.

RAI-38 (New) Section 4.2.1.2.1, Configuration of the Safety VDU Processor, part c) Control Network Interface should specifically state, and it should be shown on Figure 4.2-1, if the Control Network is inter or intra divisional.

## Request For Additional Information

This is essential to meeting the requirements of IEEE Std 603 criteria 5.6, Independence.

RAI-39  
(New) In Section 4.2.2.1, Basic Software, it is stated “With fixed cycle control and no-interrupts, the Basic Software provides high reliability, and deterministic processing.” Per Section 4.1.3.1, Basic Software, “Interrupts are not employed for any processing other than error processing.” MHI is requested to revise the topical report to clarify the apparent contradiction. It should be further explained, in the topical report, what types of errors do cause an interrupt.

One of the purposes of BTP-21, Guidance on Digital Computer Real-Time Performance, is to assist the reviewer, and the applicant, in the extensive efforts required to verify techniques, such as interrupts. Use of interrupts can be a risky design practice, as this guidance suggests, MHI is requested to thoroughly explain the interrupt technique mentioned here.

RAI-40  
(New) Section 4.3.2, Control Network states the network “can also be used to communicate data between different divisions including non-safety systems.” Is the verb “can” the same as “is”? The following sentence supports the non committal claim by stating “This **may** be between multiple Controllers in different divisions.” How is communication accomplished to all non safety systems in lieu of only “predetermined data size and structure” is used? Is there a dual port memory buffer to each interface between safety and non safety?

The IEEE Std 603 requirement, 5.6.3, is that “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” It is not apparent to the staff that the MELTAC platform meets this requirement as explained in the topical report.

RAI-41  
(New) Table 4.3-1, Configuration of Control Network, needs to be further described beginning with resolution of the following staff comments:

[

(Proprietary information withheld under 10 CFR 2.390)

]

In IEEE Std 1012-1998, which is endorsed by Reg Guide 1.168, performance criteria that includes attributes such as speed and critical configuration data should be included in the design life cycle. How the control network is configured and described needs to support how the guidelines of Reg Guide 1.168 is met.

RAI-42  
(New) Section 4.3.2.2, Specifications, states: [

(Proprietary information withheld under 10 CFR 2.390)

## Request For Additional Information

]

Staff position 1.14 of DI&C-ISG-04, states that “ Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable).” This is what the staff is attempting to verify.

RAI-43  
(New) In Section 4.3.2.4, Self Diagnosis, MHI is requested to identify in Table 4.3-3;  
[

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-44  
(New) [

(Proprietary information withheld under 10 CFR 2.390)

]

This information is needed to confirm conformance to IEEE Std 603 criterion 5.4, Equipment Qualification and the associated standards.

RAI-45  
(New) In Section 6.1.4, Development, states that [

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-46  
(New) In Section 6.1.5.7, Reviews, the Existing Platform Assessment states that [

(Proprietary information withheld under 10 CFR 2.390)

]

Per BTP 7-14, “Of particular interest is the method by which the output of software tools, such as compilers or assemblers, will be verified to be correct.” The criterion from IEEE Std 7-4.3.2-2003 is that “software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If this is not possible, the tool itself should be safety-related.” [

Request For Additional Information  
(Proprietary information withheld under 10 CFR 2.390)

]

RAI-47  
(New) [

(Proprietary information withheld under 10 CFR 2.390)

]

These are only some of the attributes of what constitutes software test documentation. At a minimum the information that should be included to meet regulatory requirements as applied to software test documentation can be found in regulatory position C.1, Software Testing Documentation, of Reg Guide 1.171, Software Unit Testing. MHI is requested to address all the attributes of documentation required by the 8 bullets in position C.1. As per stated in this position "Any of the above information items that are not present in the documentation selected to support software unit testing must be incorporated as additional items." Therefore, MHI is requested to address the information that was not present in this manner, accordingly.

RAI-48  
(New) [

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-49 Table 6.1-9, Software Upgrades Relation, [  
(New)

(Proprietary information withheld under 10 CFR 2.390)

] ISG-04

position 10 which states " Safety division software should be protected from alteration while the safety division is in operation." This section of the Table needs to be corrected, revised and/or restated, accordingly, to address the guidance.

RAI-50 Section 6.1.12, Software Safety Plan, briefly discusses [  
(New)

(Proprietary information withheld under 10 CFR 2.390)

]

### Request For Additional Information

BTP 7-14, Section B.3.1.9 describes the management, implementation, resource characteristics and the review guidance the staff uses with regards to Software Safety Plans. MHI is requested to address BTP-14 with regards to the Software Safety Plan in the topical report.

RAI-51 (New) Section 6.2.2.2, Troubleshooting Summary, discusses the information received on issues from the field on the MELTAC platform [

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-52 (New) Table 7.5-1, List of Periodic Replacement Parts, lists the frequency to replace the parts. How or what was the basis for the replacement cycle?

IEEE Std 603, Criterion 5.3, requires "Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates."

RAI-53 (New) Section 4.3.4.2 Isolation indicates electrical isolation of the Maintenance Network from the System Management Module as required by IEEE 603-1991, Clause 5.6 for independence of the Class 1E system. IEEE Std 384 provides methods that are acceptable for electrical isolation of Class 1E and non-Class 1E circuits. Section 4.3.4.2 indicates that MELTAC platform was qualified in the configuration shown in Figure 4.3-8. This isolation method as shown would be in compliance with the requirement for independence and the regulatory guidance for electrical isolation. However, no device for electrical to optical isolation of an Ethernet connection is indicated in Table A.7. [

(Proprietary information withheld under 10 CFR 2.390)

]

Please provide English translations of these engineering records for audit purposes.

RAI-54 (New) [

(Proprietary information withheld under 10 CFR 2.390)

## Request For Additional Information

]

RAI-55  
(New) [

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-56 (New) As per 10 CFR 50.47(a)(9), Content of Applications; technical information, in part, states an evaluation shall be provided to include all differences in the design and those corresponding SRP acceptance criteria.  
In Section 3.0, "Applicable Code, Standards and Regulatory Guidance, many Branch Technical Positions are listed which do not have statements of conformance or, more importantly, to direct where statements of conformance can be found. Also, statements are made that there is conformance to a Reg. Guide. This can not imply conformance to the Standard Review Plan. Example; item 43 is BTP HICB-14, "Guidance on SW Reviews for Digital Computer-Based I&C Systems" states "see conformance to RG 1.168 thru 1.173." MHI is expected to provide and substantiate conformance to the standard review plan, or if the MELTAC process does not conform, then the differences should be identified, evaluated and presented to the staff.

RAI-57 (New) At the Jan 22, 23 meeting, MHI committed to provide more detail on the I/O bus. Explanation, in the topical report, [

(Proprietary information withheld under 10 CFR 2.390)

Request For Additional Information

]

RAI-58 (New) 10 CFR 52.47(a)(22) requires applicants to incorporate into their plant designs relevant operating experience. Information Notice 2005-25 describes an event at the Millstone plant where a tin whisker resulted in a reactor trip. Although the risks of tin whiskers increases with the use of lead-free solder material, the electronics industry is moving away from lead-based solder material due to the environmental concerns with such material. At the recent audit in Kobe, Japan, inspection of the manufacturing process yielded these concerns which the staff is requesting a response to:

- 1) The staff questioned how much of the MELTAC production process is lead-free,
- 2) If any part is still lead based will the availability require change to all lead free in the near term.
- 3) The staff requested what the mitigation strategy that MELCO is currently using and will use in the future as the lead free process becomes predominate.
- 4) At the Jan 22, 23 meeting with the staff, MHI agreed to provide a summary for history of changes of the MELTAC platform in the topical report including reason for change (eg. Software error, functional performance improvement, etc.)

RAI-59 (New) For the staff to further assess compliance of the MELTAC platform to Criteria 5.6, Independence, of IEEE Std. 603, the following must be addressed in the topical report with regards to the synchronization activities between CPUs. [

(Proprietary information withheld under 10 CFR 2.390)

]

RAI-60 The topical report should describe what happens [

(Proprietary information withheld under 10 CFR 2.390)

]

Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std. 603-1991. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant/licensee's software safety analysis activities.

Attachment to RAI 23  
Additional Information to be Docketed

- (1) Letter dated December 18, 2007, Stephanie M. Coffin to Keith Paulson,
- (2) Letter dated January 29, 2008, Keith Paulson to Jeffrey A. Ciocco,

The following is the identification of information and documents to be submitted on the docket for the review of the MELTAC digital platform. In Reference 1, the staff requested MHI to provide information, pertaining to the software life-cycle processes of the MELTAC digital platform, to begin the review of the topical reports. Reference 2 identified where some of the information can be found; a subset of the information is already submitted and on the docket, this is considered in the information below. These documents are part of the official licensing basis and must be translated to English.

Reference (2) stated "Section 6 of MUAP-07004 describes the entire Safety System Design Process." However, MUAP-07004, Section 6.0, specifically states "This section describes key elements of the Design Process conducted by MHI to implement the PSMS, at the application level." Therefore that section of the document, as written, applies to the application software. Also that section does not go into detail with regards to the individual plans as MUAP-07017, "US-APWR Technical Report; Software Program Manual," does for the application software.

NUREG-0800, Standard Review Plan, Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems." (BTP-14) identifies guidelines for evaluating software life-cycle processes for digital computer-based instrumentation and control (I&C) systems. Primarily, the staff used BTP-14 as the bases for the content of the following. Consistent with BTP-14, note that a separate document is not required for each topic or section of information. If the information must be included as part of the application specific information or to be included as part of the application software lifecycle software process, MHI is requested to identify that in response to the RAI. It should be identified if this information should be an existing submittal or future submittal, possibly as a Design Acceptance Criteria (DAC) item in the application such as for the US-APWR. MHI is requested to identify in the response, at the document level, if the information is applicable to the basic software, application software or both.

- 1. The Life Cycle Process for the MELTAC platform basic software is discussed in Section 6.1 of Topical Report MUAP-07005. This portion of the Topical Report does not address BTP-14 process planning or the 11 process plans as required by 10 CFR 52.47(a)(9). MHI is requested to specifically address and docket, as part of the MELTAC platform application, the information normally contained in the documents listed in Section B.2.1 of BTP-14.

2. Equipment Qualification Program Documents

- Environmental Test Plan, Procedure & report

- Seismic Test Plan, Procedure & report

- Including testing of the optical switch in the bypassed mode and resulting operating restrictions, if any, when a switch is in the bypassed mode.

- Surge/Isolation Test Plan, Procedure & report

- EMI/RFI Test Plan & Procedure

- EMI/RFI test report for the MELTAC Platform

- Complete version providing pictures and descriptions, as necessary, for the staff to arrive at independent conclusion that all procedures, configurations and results were adequate

- ESD Test Plan, Procedure & report

Attachment to RAI 23  
Additional Information to be Docketed

3. Hardware & Software Architecture Descriptions<sup>1, 2</sup>
4. Requirements Safety Analysis<sup>1,3</sup>
5. Design Safety Analysis<sup>1,3</sup>
6. V&V Requirements Analysis Report<sup>1,3</sup>
7. V&V Design Analysis Report<sup>1,3</sup>
8. Configuration Management Requirements Report<sup>1,3</sup>
9. Configuration Management Design Report<sup>1,3</sup>
10. System Requirements<sup>4</sup> Document or Specification
11. Master or System Test Plan (composite of all hardware & software testing)<sup>1</sup>
12. Software Tool Development and Verification Program<sup>1, 5</sup>
13. Software Requirements Specification<sup>2</sup>
14. Requirements Traceability Matrix
15. Factory Acceptance Test procedure / reports (Including FAT)
16. Maintenance manuals
17. Operations procedures

These documents, or contents thereof, include the information through the planning, requirements and design activity groups of the Software Lifecycle as identified by BTP-14. This information is the level of completion the staff would expect via “a rigorous safety related design process that ensures suitable hardware and software quality and reliability for critical applications such as RPS or ESFAS” as Topical Report MUAP-07005 states.

These documents are also requested. These are referenced by documents, already on the docket:

18. Q-7302.1 (V&V Detailed Proc. & Checklists)
19. Q-7302.2 (Configuration Management Detailed Procedures)

---

<sup>1</sup> For guidance on what the staff is requesting, see NUREG-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems”

<sup>2</sup> Design output identified by BTP-14

<sup>3</sup> Part of the process implementation during Requirements and Design Activities per BTP-14, Fig. 7-A-1.

<sup>4</sup> Discussed in BTP-14 as an overall safety system requirement document

<sup>5</sup> Applies to the Engineering Tool and verification of other software tools, such as compilers or assemblers, per BTP-14, Section B.3.1.2, Software Development Plan

Attachment to RAI 23  
Additional Information to be Docketed

In addition, the staff is requesting the following documents identified, or related to those identified, in the audit performed in the MNES offices in Arlington, VA on Sept 2-5, 2008:

20. Q-7104, "Guideline for Creating Safety System Digital Platform Project Plan"
21. Current MELTAC US-APWR project plan, JEXU-1015-0002
22. MELTAC Software Development Plan; including a MELTAC U.S. Conformance Program (UCP) assessment (Section 6.1.4 of MUAP-07005-P, Revision 2)
23. MELTAC Platform Specification and Requirements Traceability Matrix (in accordance with Q-4102 per Section 6.1.7.1 of MUAP-07005-P, Revision 2)
24. MELTAC Software Specification; including the regression analysis for the UCP (Section 6.1.7.2 of MUAP-07005-P, Revision 2)
25. MELTAC Hardware Specifications, original conformance to U.S. standards (Section 6.1.7 of MUAP-07005-P, Revision 2). This would include the single processor specification presented in the audit but also the remaining hardware should be addressed as well. (cabinets, modules, cards etc.)
26. Category -1 software; Assessments for Software Units (Section 6.1.7.3 of MUAP-07005-P, Revision 2)
27. Category – 2 software; Assessments for Software Units (Section 6.1.7.3 of MUAP-07005-P, Revision 2) Final V&V report following new Integration Tests for UCP (Section 6.1.7.4 of MUAP-07005-P, Revision 2) and any further information

Finally, for docketing:

28. Category – 2 Any further materials regarding V&V which may assist the staff in determining regulatory compliance without relying on operating experience of these modules.
29. Commercial Grade Dedication Plans
31. Reliability Analysis
32. System description at the block diagram level\
33. Addressing the issue of a Diversity and Defense-in-Depth approach for operating plants

Preliminary Versions of documents; to be submitted but not docketed at this time:

34. Preliminary FMEA

Attachment to RAI 23  
Additional Information to be Docketed

Documents Available to be inspected at the next audit: These may be docketed in the Future :

1. Documents to support a thread audit of a Category 2 module
2. Documents identifying the design review process that constituted the V&V reporting of the Existing Platform.
3. Cyber security procedures for the Mitsubishi Corporate Electronic Archive System (CEAS) and the software development facility. These procedures would be those used for adding, deleting or changing files via identified forms of storage devices and the limitations on those devices. Also, included should be procedures for security practices describing what is authorized and unauthorized access to the CEAS security system and how this is maintained, how audits are done and the results of such audits, if available.
4. Design and V&V documents to support a thread audit of the PIF module communication interface.

Documents Available For Possible Future Audits – Non Docketed

1. Configuration Management Reports
2. Detailed system and hardware drawings
3. Final circuit schematics
4. Final Software Integration Report
5. Individual completed test procedures / reports
7. Individual V&V Problem reports up to FAT
8. Set point calculations
9. Software code listings.
10. Training manuals & course material
11. Vendor Build Documentation