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

August 22, 2008

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-08144

**Subject: MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process**

With this letter, Mitsubishi Heavy Industries, LTD. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") the document entitled "MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process", a package based on Requests for Additional Information dated July 3, 2008.

As indicated in the enclosed materials, this document contains information that MHI considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential. A non-proprietary version of the document is also being submitted in this package (Enclosure 3). In the non-proprietary version, the proprietary information, bracketed in the proprietary version, is replaced by the designation "[ ]".

This letter includes a copy of the proprietary version (Enclosure 2), a copy of the non-proprietary version (Enclosure 3), and the Affidavit of Yoshiki Ogata (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials designated as "Proprietary" in Enclosure 2 be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

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

Sincerely,

Y. Ogata

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

D081
NRO

Enclosures:
1 - Affidavit of Yoshiki Ogata
2 - MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process (proprietary)
3 - MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process (non-proprietary)

CC: J A. Ciocco
C. K. Paulson

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

**ENCLOSURE 1**

Docket No. 52-021
MHI Ref: UAP-HF-08144

**MITSUBISHI HEAVY INDUSTRIES, LTD.**

**AFFIDAVIT**

I, Yoshiki Ogata, state as follows:

1. I am General Manager, APWR Promoting Department, of Mitsubishi Heavy Industries, LTD ("MHI"), and have been delegated the function of reviewing MHI's US-APWR documentation to determine whether it contains information that should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

2. In accordance with my responsibilities, I have reviewed the enclosed document entitled "MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process" dated August 2008, and have determined that portions of the document contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[ ]". The first page of the document indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

3. The information identified as proprietary in the enclosed document has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.

4. The basis for holding the referenced information confidential is that it describes the unique design of the safety I&C system design, developed by MHI and not used in the exact form by any of MHI's competitors. This information was developed at significant cost to MHI, since it required the performance of Research and Development and detailed design for its software and hardware extending over several years.

5. The referenced information is being furnished to the Nuclear Regulatory Commission ("NRC") in confidence and solely for the purpose of information to the NRC staff.

6. The referenced information is not available in public sources and could not be gathered readily from other publicly available information. Other than through the provisions in paragraph 3 above, MHI knows of no way the information could be lawfully acquired by organizations or individuals outside of MHI.

7. Public disclosure of the referenced information would assist competitors of MHI in their design of new nuclear power plants without incurring the costs or risks associated with the design and testing of the subject systems. Therefore, disclosure of the information contained in the referenced document would have the following negative impacts on the competitive position of MHI in the U.S. nuclear plant market:

A. Loss of competitive advantage due to the costs associated with development of the safety I&C system. Providing public access to such information permits competitors to duplicate or mimic the safety I&C system design without incurring the associated costs.

B. Loss of competitive advantage of the US-APWR created by benefits of enhanced plant safety, and reduced operation and maintenance costs associated with the safety I&C system.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information and belief.

Executed on this 22th day of August, 2008.

Y. Ogata

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

Enclosure 3

UAP-HF-08144
Docket No. 52-021

# MHI's Response to NRC's Requests for Additional Information

**on**

# Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process

August 2008
(Non-Proprietary)

# MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R1) Safety I&C System Description and Design Process

**Non Proprietary Version**

**August 2008**

**©2008 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved**

## INTRODUCTION

This report documents Mitsubishi Heavy Industries' (MHI's) responses to U.S. Nuclear Regulatory Commission's (NRC's) request for additional information (RAI) on the MHI Topical Report, MUAP-07004-P (R1), "Safety I&C System Description and Design Process".

This report describes the responses for the requests for information from the NRC.

The RAI, "Draft Request for Additional Information based on the Review of Topical Report MUAP-07004-P, Rev.1, "Safety I&C System Description and Design Process"", was issued on July 3, 2008 (ML080790297).

## RESPONSE TO THE RAI

Following provides the responses for the RAI.

**RAI-01**

With regards to Section 3.1, Code of Federal Regulations, evaluation of instrumentation and controls system contributions to design margin for reactor coolant systems are a part of the review of the adequacy of instrumentation and controls protective and control functions. The instrumentation and controls systems may contribute to reactor coolant system design margin in many ways, for example, by providing better than the minimum required performance, as conservatism in setpoint calculations, or by system features that make the protection or control systems more fault tolerant. Thus, General Design Criterion (GDC) 15 is applicable. To understand the margins provided in the design of the APWR and to confirm there is reasonable assurance that adequate margin is provided; MHI should address how the design meets the requirements of GDC 15.

**Response**

MHI will add the description of conformance to GDC 15 into Section 3.1.

**RAI-02**

GDC 2, "Design Bases for Protection Against Natural Phenomena," set forth in Appendix A to 10 CFR Part 50, requires, in part, that structures, systems, and components (SSCs) that are important to safety in nuclear power plants must be designed to withstand natural phenomena. Section 3.3, NRC Regulatory Guides, does not reference compliance to Regulatory Guide (RG) 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," for grounding and surge protection methods to assure that electrical transients resulting from lightning phenomena do not render instrumentation and controls systems important to safety inoperable or cause spurious operation of such systems. Table 7.1 in NUREG-0800 identifies RG 1.204 as acceptable for meeting the requirements for instrumentation and control systems important to safety with respect to lighting protection. Will the design of the US-APWR comply with RG 1.204, and if so, how?

**Response**

RG 1.204 states "Specifically, this guidance applies to the design and installation of lightning protection systems (LPSs) to ensure that electrical transients resulting from lightning phenomena do not render safety-related systems inoperable or cause spurious operation of such systems." The US-APWR LPS conforms to RG 1.204. The LPS design is described in Section 8.3.1.1.11 of the DCD.

As stated in RG 1.204 "The scope does not cover testing and design practices that are specifically intended to protect safety-related I&C systems against the secondary effects of lightning discharges [i.e., low-level power surges and electromagnetic and radio-frequency interference (EMI/RFI)]. These practices are covered in Regulatory Guide 1.180 ..." RG 1.180 is referenced in this Topical Report and the PSMS fully conforms to the requirements of RG 1.180.

Therefore, MHI will add RG 1.204 into Section 3.1, with the following clarification:

Conformance to RG 1.204, regarding the design of the plant's lightening protection system (LPS), is described in plant licensing documentation.

The LPS description will also be added to Table 7-1 Future Licensing Submittals.

**RAI-03**

Item 16—Branch Technical Position HICB-16—has been withdrawn by the NRC. A reference for the level of detail required for design certification applications under 10 CFR Part 52 would be RG 1.206. Will MHI comply with this RG? Also, this item states that design acceptance criteria (DAC) applies to system application software and system setpoints. The US-APWR design certification document does not list any DAC in the Tier 1 Section. Briefly identify where DAC will be identified and discussed.

**Response**

At the time of this Topical Report submittal, RG 1.206 was not published. MHI will add the description of conformance to RG 1.206 and delete BTP-16. The content of the US-APWR DCD is based on the information and level of detail required by RG 1.206. All DAC items are listed in the Attachment 2 of the DCD submittal letter (UAP-HF-07170). The following two items are assigned as DAC in the I&C area.

- HSI Design
- US Operator V & V

MHI will submit the technical reports to close the above two DAC items.

As-built I&C system features, including application software and system setpoints, are treated as ITAACs in Section 2.5 of US-APWR DCD tier 1. MHI is planning to close these ITAACs prior to fuel load for the first US-APWR.

**RAI-04**

In Section 4.1, Overall Instrumentation and Controls System Architecture, self-diagnostics is credited for various features and advantages. The software architecture should support the claim that a failure of the diagnostic software would not interfere with the operation of the safety function. Are any methods other than a watchdog timer and a test used to prevent or detect failures? Can a failure in the online diagnostic system cause some type of failure of the system? Can the online diagnostics give false information that could lead to incorrect responses by the operator and unsafe conditions? Were common cause failures (CCFs) of the diagnostic software considered such that the failure of the software could lead to a failure of the trip function to be performed?

**Response**

There is no claim in the Topical Report that "a failure of the diagnostic software would not interfere with the operation of the safety function". This may indeed happen. But these failures are much less likely than the failures that the self-diagnostic features are designed to detect.

There are many self-diagnosis methods other than watchdog timers. Self-diagnostics includes hardware based detection process, software based detection process, and software/hardware combination. Details of the self-diagnosis are described in Section 4.1.5 of Topical Report MUAP-07005, "Safety System Digital Platform -MELTAC-"..

While highly unlikely, a failure of the self-diagnostics could lead to erroneous shutdown of a single PSMS controller. This failure is limited to only one PSMS train because of following features.

- Self-diagnosis is part of the MELTAC basic software. All parts of the MELTAC basic software are developed using a Class 1E design process, including independent verification and validation.
- Failure of any part of the basic software , including the self-diagnostics, does not affect other trains because redundant trains are appropriately isolated from each other.

Failure of the self-diagnostics is unlikely to lead to failure of the trip function, since a self-diagnostic failure is likely to lead to controller shutdown. This will result in that controller generating trip outputs, due to the fail-safe design of the RPS. If there is a common defect in the self-diagnostics which leads to a CCF, all controllers will generate trip outputs which will generate a plant trip. Regardless of this most likely failure scenario for the self-diagnostics, MHI's defense-in-depth and diversity strategy assumes all software defects lead to non-conservative CCFs (i.e., no protective action). CCF of self-diagnosis is included in the overall system CCF that disables all PSMS safety functions, CCF is considered in Topical Report MUAP-07006, "Defense-in-Depth and Diversity" and Technical Report MUAP-07014, "Defense-in-Depth and Diversity".

**RAI-05**

Section 4.1.d states that "The DAS consists of hardwired or digital components." This sentence is confusing because of the "or." The *Defense-in-Depth and Diversity* Topical Report (MUAP-07006-P, Rev. 1) states that the diverse actuation system (DAS) will be a conventional analog system, yet the "or" indicates that the DAS may contain digital components, or that a digital option may be available for the US-APWR or for upgrades of instrumentation and controls systems. Clarification among these statements needs to be provided. Clarify the statement "The DAS consists of hardwired or digital components." If a portion or portions of the DAS may be digital, identify why this may be necessary and the possible technologies to be used.

**Response**

This Topical Report is for the PSMS, not the DAS. Therefore, the description states the basic requirement for the DAS, which is just to be diverse from safety digital I&C system, regardless of digital or analog implementation technology. The actual DAS technology, for any specific plant, is defined in plant specific licensing documentation.

Please note that in the context of all MHI topical reports for digital I&C and HSI, and within the context of these RAI responses, the US-APWR is a plant specific application. A unique US-APWR for a specific COL applicant is referred to as site-specific.

For the US-APWR, the DCD describes a completely conventional analog DAS, based on Japanese practice. Topical Report MUAP-07006 also describes this conventional analog DAS.

**RAI-06**

Section 4.2.1, Reactor Protection System, states that "Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS." What is the methodology embedded in the analog-to-digital converters? Has their accuracy and method of performance been evaluated for possible rounding or cumulative error fault?

**Response**
It is not appropriate to include this level of detail in this Topical Report, since this report describes the PSMS at a system level. This level of detail is more appropriated for Topical Report MUAP-07005, which describes the MELTAC digital platform, including the analog input modules. MHI will add the following to Topical Report MUAP-07005:

A 16 bit successive approximation type A/D converter is applied for the analog input module of the MELTAC platform. The rounding error for the applied range is approximately 1E-3%FS, which is negligible compared with the accuracy of the analog input module itself. The accuracy of the analog input module is 0.25%FS as described in Appendix A of MUAP-07005. Cumulative error, which is a problem of integrating type A/D converters, is not a problem for the successive approximation type A/D converter due to its operating principle.

**RAI-07**
Section 5.1.3, Operation under Degraded Conditions, discusses the potential failure of all Operational visual display units (VDUs). Has a failure modes and effects analyses (FMEA) and/or probabilistic risk assessment (PRA) been performed on the failure of all Operational VDUs? Even though these Operational VDUs are non-safety, the bases for the reliability of the components and system should be provided to support the statement "high reliability." In other words, the bases for any reliability statements should be provided. The operating experience of the components and systems should be discussed.

**Response**
Statements regarding the high reliability of the Operational VDU are based on the redundancy and independence within the HSI system configuration, and the unique nuclear design attributes of the Operational VDU. The Operational VDU, including the MELCO MR series processor, is specially developed for nuclear applications. This special development of the Operational VDU for nuclear applications is described in Appendix C.1.

Regardless of the high reliability expected for the Operational VDUs, the worst case failure could be due to a software defect which cannot be predicted by a FMEA or the PRA. Therefore, MHI provides a defensive strategy for this failure. The coping strategy for all degraded HSI conditions is described in Section 4.11 of Topical Report MUAP-07007, "HSI System Description and HFE Process".

**RAI-08**
Section 5.1.8, Control System Failure Mode, discusses the non-safety plant control and monitoring system (PCMS) having high reliability. CCFs need not be considered for hardware failures, yet are of concern for software. Were single failures and CCFs of the software included in the analysis?

**Response**
The AOOs considered in the plant safety analysis bound all single failures in the PCMS, whether those failures originate in hardware or software. Due to the continuous operation of the PCMS and therefore the self-announcing nature of software defects, it is reasonable to assume that software defects in single controllers of the PCMS are detected and corrected, before they become CCFs that adversely affect multiple PCMS controllers. Therefore, CCFs within the PCMS are not considered in the plant safety analysis. This design basis is

consistent with the resent DI&C-ISG-02, Problem Statement 4 Effects of Common Cause Failures. A software defect that remains hidden (undetected) and results in a CCF in the PCMS is considered a beyond design basis event. This failure is considered in the D3 coping analysis described in Topical Report MUAP-07006 and Technical Report MUAP-07014.

**RAI-09**

Section 5.1.9 discusses Self-Diagnostics for Technical Specification Surveillance. Online, periodic testing is a feature of most digital systems. Ostensibly this technique adds to the respective safety and reliability by continually monitoring and verifying normal operation of sensors and logic system. This feature is not a regulatory requirement but is a common feature on most digital protection systems. The feature is briefly described; the information is not detailed, and essentially only two failure modes are considered and the use of a watchdog timer and a test are used to prevent or detect these failures. The concern is that a failure in the online diagnostic system causes some type of failure of the system. The online diagnostics might give false information, e.g. indicating the system is operational when it is not or indicating it is failed when it is operational, which could lead to incorrect responses by the operator and unsafe conditions. Another type of failure of the diagnostic software could lead to a failure of the trip function to be performed due to common mode failure. Have the failure modes that have occurred in the operating experience been examined? Based on operating experience, what are the causes of software failures and the effects of those failures? Were any failures unannounced? Are any methods other than a watchdog timer and a test used to prevent or detect failures? Can a failure in the online diagnostic system cause some type of failure of the system? Can the online diagnostics give false information that could lead to incorrect responses by the operator and unsafe conditions? Were CCFs of the diagnostic software considered such that the failure of the software could lead to a failure of the trip function to be performed?

**Response**

Refer to the response for RAI-04.

**RAI-10**

Section 5.1.12 discusses "Computer Based Procedures." On what computer system are the procedures loaded? What communication is provided between the system containing the procedures and the Operational VDUs? Are the procedures available on the Safety VDUs given a failure of the Operational VDUs? Are hardcopies available? Are the electronic procedures pdf copies of the hardcopies or specifically developed for electronic viewing and hyper linking?

**Response**

Computer based procedures are loaded on several COTS PCs which drive the Operating procedure VDUs distributed throughout the MCR. The Operating procedure VDU communicates with the Operational VDU processors and the Alarm VDU processors. Figure 4.1-1 Overall Architecture of the I&C System, will be revised to correctly show this communication interface.

The Safety VDUs do not display operating procedures. Instead paper-based procedures are provided for use with the Safety VDUs. These backup paper based procedures are described in the degraded HSI strategy of MUAP-07007, Section 4.11.3.

The procedures are installed in the Operating Procedure VDUs as PDF format, which is converted from MS Word. The PDF format includes hyperlinks for navigation between procedure sections and between related procedures and hyperlinks to corresponding information on Operational VDUs. The computer based procedure system is described in MUAP-07007, Section 4.8.

**RAI-11**

The DAS is described briefly in this topical report and in more depth in the topical report for *Defense in Depth and Diversity.* Will the US-APWR comply with Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That is not Safety-Related?" Section 3.1 of the topical report also states that "This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10 CFR Part 50 Appendix B. Other licensing documents describe this equivalence. An approved 10 CFR 50 Appendix B quality program is now in effect for all Equipment." In addition, a safety software quality assurance (QA) process that meets the life cycle requirements of IEEE 7-4.3.2-2003 was used. Provide sufficient details to show that the software QA process met the life cycle requirements of IEEE 7-4.3.2-2003. The software was not developed in compliance with NRC regulations and an equivalency comparison has not been provided. The topical report needs to address that it complies with guidance and was not written to that guidance. Acceptance of software cannot be determined without a mapping of requirements the software was written to against the NRC requirements or guidance. Provide the reference that "an approved 10 CFR Part 50 Appendix B quality program is now in effect.

**Response**

The quality requirements for the DAS are described in Section 6.2.1.7 of MUAP-07006. This includes conformance with Generic Letter 85-06. As described in the response for RAI-05, the DAS of the US-APWR is conventional analog system, including no software. QA process of the PSMS software is mentioned below.

The quality program for the basic software of the MELTAC platform is described in MUAP-07005, Section 6.0. This section refers to current MELTAC quality assurance procedures, which have been submitted for Staff review. The section also evaluates the quality program for MELTAC software, which was developed prior to the current software quality program.

The application software for the PSMS is not previously developed software. This software will be developed under the software quality program described in Section 6.0. A detailed description of this SQA program is provided in Technical Report MUAP-07017,"Software Program Manual", which has also been submitted for Staff review.

**RAI-12**

Section 6.1, Design Process Overview, includes number (7) Operational phases. Portions of the constructed instrumentation and controls installation is likely to have been subject to normal maintenance if not improvement and resultant design changes to the process and configuration. The topical report is moot on the discussion of the stability, over time, of the first installation relative to the last, how the configuration has been managed over this time period and what the determinants of stability in design and functionality are relative to the history of performance of the original installation. Please discuss the design history including the changes which would have affected safety functions, how the configuration has been

managed over this time period and what the determinants of stability in design and functionality are relative to the history of performance of the original installation.

**Response**

For the application software of the PSMS, Section 6.3.1 (10) and 6.3.2 (3) describe the software configuration management plan, Section 6.4.2 describes the design change management process and Section 6.4.4 describes the corrective actions process. These processes are described in more detail in MUAP-07017, Sections 3.6 Software Maintenance Plan, 3.11 Software Configuration Management Plan.

For the basic software of the MELTAC platform, the software life cycle processes are described in Section 6.0 of MUAP-07005. These processes include configuration management and design change management. Section 6.1.7 of MUAP-07005 explains the assessment of previously developed software, including the additional quality activities applied to previously developed software modules, which is dependent on their operating history.

**RAI-13**

Also with regards to (7) Operations phase, this mentions obsolescence. Has MHI evaluated the obsolescence and replacement of MELTAC digital components?

**Response**

Obsolescence Management for the MELTAC platform is described in Section 6.2.3 of MUAP-07005.

**RAI-14**

The verification and validation (V&V) testing will be conducted according to a V&V plan.

- What details regarding V&V testing, tests, and testing runs are expected to be included in the V&V plan?
- For any test and test run, show the determination of the specific confidence limits of acceptance of the software module despite the failure of detecting an existing fault?
- For any two tests or test runs relating to any one software module, show the determination of independence of the confidence limits of each.

Requirements determination for the performance of the systems must be known and understood relative to the criteria presented by NRC regulation and plant design. In all instances the decomposition of requirements will be complete at the first level that metrics can be applied (equations are metrics too). But the degrees of possible error in the metric could render the determinism invalid and the accumulation could lead to an un-verifiable and undocumented risk. Each metric must have a known boundary condition and the metric and boundary must be traceable to regulatory requirement, as well.

- If requirements are properly decomposed, how will that decomposed and empirical measure be traced to the regulatory determination?
- Show the traceability from the determinant of performance to the regulatory requirement.
- Show the analysis which determines the contribution of digital systems to the overall plant PRA.
- Show the decomposition of a regulatory requirement to its constituent measures and metrics of performance.

Show how the constituent performance requirements of any part of any safety critical digital system encompasses, exclusively and comprehensively, the respective physics of the reactor.

**Response**

For the application software, the contents of the V&V plan are briefly described in Section 6.3.1 (9). This section states "Methods for using a Requirements Traceability Matrix to confirm all requirements are addressed in each phase of the design". The V&V plan is described in detail in MUAP-07017 Section 3.10. This section describes the use of the RTM for verification in each phase of the design process.

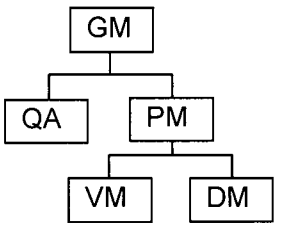
For the basic MELTAC platform software, the software development process, including the activities of the V&V Team and use of the RTM in each phase of development, are described in Section 6.1.4 of MUAP-07005. The internal procedures that govern these activities were also submitted for Staff review. Section 6.1.7 of MUAP-07005 describes the special V&V activities applied to previously developed software.

**RAI-15**

Section 6.2.1 of Software Life Cycle Process Control, presents the organizational structure to control the software life cycle process. It is unknown if the QA organization is an independent agent from Project Management. In addition, it seems that the purview of the QA organization is limited to the platform and systems implementation/ installation at the specific site/plant and all that can be done at this point in time is to confirm plant specific application programming interfaces (API's) and interfaces have been properly completed. Describe the organizational structure, including internal and external organizations, and their independence. Please explain how the V&V process described is not merely use case limited? Please also explain the methods appropriate to V&V of MELTAC versus all other safety system components?

**Response**

For both the MELTAC basic software and the system application software, the QA organization is independent from the Project Management organization.
Figure 6.2-1 is the organization structure for application software. For clarification, MHI will revise Figure 6.2-1 organization structure, as follows,:




GM – general manager
QA – quality assurance organization
PM – project manager
VM – V&V team manager
DM – design team manager

The organization of life process control for the MELTAC basic software is described in Topical Report MUAP-07005 Section 6.1.3.1.

For the system application software the V&V process is briefly described in Section 6.3.1 (9). The V&V process is described in detail in MUAP-07017, Section 3.10.

For the MELTAC basic software the V&V process is described in MUAP-07005, Section 6.1.4. The MELCO V&V procedure, [ ], has also been submitted for Staff review.

**RAI-16**

With respect to Section 6.3, Requirements, Implementation and Design Outputs for Software Life Cycle Process, how is the trace of each requirement (including, for example, data specific requirements, data exchange requirements, network operational requirements, network functional requirements, constraint determination and tracking, refined specification) to include empirical measures of performance and identification?

**Response**

The life cycle process design outputs for each design phase, as described in Section 6.3.3, are confirmed by the V&V Team, using the requirements traceability matrix (RTM), prior to being used as input into the next design phase. This verification includes traceability of design requirements into empirical test procedures.

For the US-APWR application software, the use of documentation outputs for requirements traceability is generally described in Technical Report MUAP-07017 Section 2.3.3. The use of the RTM is described in Section 3 for each life cycle plan.

For the MELTAC basic software, use of the RTM in each phase of the software development process, is described in Table 6.1-2 of MUAP-07005.

**RAI-17**

Section 6.3.1 discusses some of the software development plan. Without complete and specific traceability, digital system(s) failure modes and reliabilities contributing to overall plant PRA(s) cannot be fully and deterministically understood in the systems engineering sense of completeness. How will the software safety plan be developed to accommodate this requirement? Once completeness, validity and verification is accomplished for the digital system requirements, constraints and their respective empirical measures, what will be the method and empirical basis by which the plant PRA will be accomplished for the category of the US-APWR as well as for each specific plant design?

**Response**

MHI's process includes complete and specific requirements traceability (see response to RAI-16).

For the application software, the software safety plan is described in MUAP-07017, Section 3.9. For the MELTAC basic software, the software safety plan is described in Section 6.1.12 of MUAP-07005.

The PRA is included in plant licensing documentation, such as Chapter 19 of the US-APWR DCD. The PRA is not within the scope of this Topical Report.

**RAI-18**

Does Section 6.3.2, Software Life Cycle Process Implementation, apply to just the plant-specific tasks and corresponding components of deployment or the full set of component hardware and software comprising the entirety of the deployment?

**Response**

This Topical Report describes tasks for plant specific applications. These tasks pertain primarily to the plant specific hardware configuration and the plant specific application software. However, when the application software is integrated with the MELTAC basic software and the plant specific hardware configuration for testing, then the plant specific tasks encompass the full set of component hardware and software comprising the entirely of the deployment.

The software life cycle process for the MELTAC digital platform basic software is described in Topical Report MUAP-07005 Section 6.2.

**RAI-19**

For Section 6.4.1, Access Control, please show that the envelope of controlled access completely surrounds the protective functions within the system and that no loophole is available. Is access control and security of the MHI Safety System(s) protected by a single system–specific password, a single per user or how? If user-specific passwords are employed, does a user with access to multiple systems and levels use one password for all or one password for each access?

**Response**

**RAI-20**
Section 6.4.3, discusses "Cyber Security Management". With respect to cyber security, how are passive threats detected and understood?

**Response**

**RAI-21**
With respect to Cyber Security Management in Section 6.4.3, if virus, worm, or other active or passive breaches occur, how is the Engineering Tool protected from contamination? Won't this PC have rotating media drives and therefore a need for anti-virus software?

**Response**

**RAI-22**
Section 6.4.3 states when the final application software is transferred from the Engineering Tool to the protection and safety monitoring system (PSMS), software checks are used to detect no errors or changes have been introduced. Confirm that this is a repeatable maintenance function, although this is one control method, indentified in the introduction, done

during the design phase. If the system response is "no errors or changes have been introduced", how are the files maintained in the system? Is this a complete file comparison, a compiler partial or complete check?

**Response**

**RAI-23**
Section 6.4.4 item (2), Error and Corrective Action Reporting, discusses error and corrective action reporting for life cycle management. What will be MHI's QA involvement and how will the QA function be maintained between MHI and the licensee during the operations and maintenance portion of these system(s) life cycle?

**Response**
The PSMS will be managed by the plant's organization level QA program during the operation phase of its life cycle. The plant's organization level QA program for the operational phase is described in plant licensing documentation. For the US-APWR this is described in COLA FSAR Chapter 17 for each utility. Each program requires Error and Corrective Action reporting. MHI may have contracted responsibility for PSMS maintenance during plant operation; this will vary with each utility. Regardless, the plant specific organization level QA program will be used.

For application errors that are reported to MHI for correction, MHI will execute corrective actions under its own software quality program and its own organization level QA program. For the US-APWR, the software QA program for application software is described in Technical Report MUAP-07017; the software quality assurance plan, which includes problem reporting and corrective actions, is described in Section 3.3. The organization level QA for US-APWR is described in Chapter 17 of the DCD. If a specific utility executes application corrective actions on their own, they will still follow MHI's SQA program, MUAP-07017, but this program will be administered under their own organization level QA program.

All corrective actions related to the basic MELTAC software will be executed by MELCO. This corrective actions program is described in Section 6.2.2 of MUAP-07005.

**RAI-24**
With regards to Section, 6.5.2, Reliability Analysis Method, the defense in depth and diversity review has to consider all the systems that, in total, contribute to a highly reliable safety system. The overall strategy is discussed in MUAP-07006-P, *Defense in Depth and Diversity*. However, in the topical report under review—MUAP-07004-P—CCFs are not modeled in the

fault tree, nor are operator errors or recovery actions. It is not apparent that these human errors or those introduced during upgrades of hardware and software are in included in Sect. 6.5.2 or Fig. 6.5-1. Describe how the typical fault tree analysis discussed in Sect. 6.5.2 will be used in determining the overall reliability of the safety system.

**Response**
Section 6.5.2 of this Topical Report explains the design basis and process used in the reliability analysis. Since the fault tree analysis requires a plant specific system configuration, as stated in this section "The reliability analysis for specific plant applications are discussed in Plant Licensing Documentation." For the US-APWR the detailed fault tree analysis is described in Technical Report MUAP-07030 "US-APWR Probabilistic Risk Assessment" Section 6A.12 and 6A.13 for the US-APWR.

The fault tree analysis described in Section 6.5.2 is just one aspect of the PRA. Section 6.5.2 is limited to the discussion of system level reliability, since this is typically of specific interest to the I&C Branch. The PRA also considers CCFs and human performance errors. Digital I&C hardware CCF is described in the MHI response to US-APWR DCD RAI No.25 19-30, which is enclosed in the letter of UAP-HF-08131. Therefore, questions related to these areas should be directed to MUAP-07030 or DCD Chapter 19.

**RAI-25**
Section 6.5.2, Reliability Analysis Method, the reliability of the safety instrumentation and controls system to perform its safety functions is analyzed. Provide a reference for the PRA analyses, and discuss the method of performance and compliance for each step.

**Response**
Refer to response to RAI-24.

**RAI-26**
In Section 6.5.2, Reliability Analysis Method, the reliability analysis credits the immediate detection of module failures that are tested by self-diagnostics. Discuss the self diagnosis of components, including the sampling rate, error detection probability, and history and reliability of self diagnostics.

**Response**
Self-diagnostics are a basic feature of the MELTAC platform. Self-diagnostics, including sampling rate, coverage and operating history, are described throughout MUAP-07005.

Treatment of self-diagnosis in the PRA is described in the MHI response to US-APWR DCD RAI No.25 19-33, which is enclosed in the letter of UAP-HF-08131.

**RAI-27**
Are software failures explicitly accounted for in the PRA model? If so, does the model include "application software" and "support software"?

**Response**
This is a generic topical report applicable to new plants and operating plants. The PRA is a plant specific document. Refer to response to RAI-24.

**RAI-28**
Section 6.5.2 references "industry handbooks" and "manufacturers publications." Provide a reference for the failure data and a discussion on the operating history of the components and if this was factored in to the failure data. Indicate if the data will be different for plant specific analyses.

**Response**
The failure rate of MELTAC components is generically applicable to all MELTAC applications. MELTAC component reliability, including operating history, is described in Section 7.0 of MUAP-07005.

The calculation of safety function unavailability for specific plant applications is provided in plant licensing documentation. For the US-APWR this is described in the MHI response to US-APWR DCD RAI No. 25 19-33, which is enclosed in the letter of UAP-HF-08131.

**RAI-29**
Does the FMEA evaluate input, output, communication, resource allocation, and processing errors due to software failures? Any other software elements considered? If so, what and how.

**Response**
The FMEA ensures the system can achieve its safety function, as described in Section 6.5.1, in the presence of any random single failure. MHI consider only random failures for the FMEA. This includes credible random hardware failures, which also bounds credible random software failures. Systematic software failure is the result of design errors. Per IEEE-379, design errors are not considered single failures, therefore systematic software errors are not considered in the FMEA. Systematic software failure, which leads to CCF of multiple safety divisions, is evaluated in MUAP-07006 and MUAP-07014.

**RAI-30**
The response time analysis method is presented in Sect. 6.5.3, Response Time Analysis Method. The response time of the safety functions is used in the plant safety analysis. The response time of each safety function is calculated by adding the response time of each component that makes up the system, from the process measurement to the actuation of the final component.

- What is the basis for selecting the response times?
- What are the uncertainties of the response times?
- Any standard or guideline used as a basis for performing the response time analysis?
- What is the basis of the response time value used in the plant Safety Analysis Report?
- Which statistical value is used for validation of the time response?

**Response**
For sensors, the response time is based on vender specifications with uncertainties added based on operating experience. For MELTAC components, the response time is based on the processing times and the calculation method defined in Section 4.4 of MUAP-07005. This method accounts for all processing time uncertainties.

As stated in Section 3.4, the real time performance for the PSMS conforms to BTP 7-21.

The response time value used in the Safety Analysis is determined based on historical precedence and engineering judgment. As stated in Section 6.5.3, the actual response time calculation, described in Section 6.5.3, confirms that the Safety Analysis value bounds the actual response time of the PSMS.

The statistical methods used during response time validation testing, are described in V&V procedures. These procedures are plant specific documents. For the US-APWR V&V procedures are within the life cycle process, which is covered by an ITAAC.

**RAI-31**

The heat load of the components within each PSMS enclosure (i.e. cabinet or console in which PSMS equipment is mounted) is calculated to establish room Heating Ventilating and Air Conditioning (HVAC) sizing requirements. The short description does not specify any guidance. It is unknown if the analysis accounts for a loss of forced ventilation airflow or reduced airflow. Provide a reference or standard for the guidance used to perform the heat load analysis, along with the reference for the documented analysis. Does the analysis account for a loss of forced ventilation airflow or reduced airflow?

**Response**

The use of forced ventilation within the PSMS cabinets is irrelevant to the calculation of component heat load to determine room air conditioning size. The same heat must be dissipated from the I&C equipment room, whether there is forced ventilation or not.

As stated in Section 6.5.5, the calculation to determine component temperature within the PSMS cabinets, ensures components operate below their maximum normal temperature, and below their maximum qualified temperature. This is to ensure component longevity and reliability. Since the PSMS cabinet ventilation system is fully qualified, this calculation is performed considering normal forced ventilation conditions.

**RAI-32**

Section 6.5.8 discusses that plant fire protection analyses performed to demonstrate the ability to achieve safe shutdown with a fire in one fire zone of the plant and a failure of an instrumentation and controls component within that fire zone. It is unknown if a fire assessment has been performed and what, if any, guidance was followed. Has a fire assessment has been performed and what, if any, guidance was followed?

**Response**

This section defines the basis for I&C failures that must be considered in the plant's fire analysis. That fire analysis is a plant specific document. For the US-APWR, fire hazard

analysis has been performed in compliance with RG 1.189 and NEI 00-01. This analysis is described in the DCD Chapter 9.

**RAI-33**

The switches that experience a fire are assumed to not change state. A basis for this assumption should be provided. In addition, the reliability of the switches and their failure modes should be addressed. Further, any tests under such conditions should be cited. If no tests have been performed, this should be cited too.

**Response**

**RAI-34**

In the Appendix A on Conformance to IEEE 603, it is not clear in the topical report whether or not communication independence criteria, Section A.5.6, are determined and are met with regard to IEEE Std 603-1991 and IEEE Std 7-4.3.2. Such additional empirical evidence is required. Does the function processor gain access within the allotted time consistent with the loop cycle time and to meet the overall response time of the safety function? Does the function processor perform handshaking with other systems? Does it accept interrupts from outside its own division? Does the communications processor and the function processor operate asynchronously, and does the function processor have priority in the event that both processors desire access to a shared resource? Is this method in compliance with Section 1, Interdivisional Communications, of ISG D instrumentation and controls-ISG-04?

**Response**

The communication independence addressed in this section of the Topical Report pertains to system level aspects of the design. The communication independence criteria referred to in this RAI, pertains to generic features of the MELTAC platform. As shown in Figure 4.2-2, each MELTAC controller includes a function processor (CPU), which is independent and asynchronous from all communication processors. The function processor operates completely deterministically. It performs no handshaking with other systems and it accepts no external interrupts. For shared memory, the write and read cycles of both the function processor and the communication processor are totally independent and asynchronous. Neither module has to wait for the other module to complete its read or write operations. The generic MELTAC communications design meets all requirements of DI&C-ISG-04. The details of the MELTAC communication design are described in Section 4.3 of MUAP-07005

**RAI-35**

In A.5.6.3.1, Interconnected Equipment, it would be applicable to discuss the possibility for a malfunctioning PCMS channel to cause the protection system to take erroneous actions. Since

there is communication from the PCMS to the safety systems at the Operational VDU is it possible for a signal to be transmitted between the systems via the VDU. Discuss the operational experience with this interface.

**Response**
A malfunction in the PCMS can cause the PSMS to take an erroneous action. However, as stated in Section 4.2.5.c, "Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g. non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis." The malfunction analysis considers a single spurious data set from a PCMS Operational VDU or multiple spurious actuation signals from a single PCMS controller.

All communication from the Operational VDU to the PSMS is via the Unit Bus. There is no direct communication to the PSMS from the Operational VDU.

**RAI-36**
Section A.5.6.3.3 discusses "The Effects of a Single Random Failure." Does the safety system design preclude the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines. And are there any other features which could compromise the independence of redundant portions of the safety system?

**Response**
There are no electrical components that are common to redundant portions of the safety system. Each train is completely electrically independent from each other train. The only shared component that is common to redundant portions of the safety system is the instrument sensing line for reactor coolant flow measurement used for the low reactor coolant flow reactor trip signal. This common instrument sensing line is used for all four flow instruments (i.e., there is a separate flow instrument for each PSMS train). The instrument sensing line extends reactor coolant system pressure to the flow transmitters. A common instrument sensing line is used to obtain accurate pressure for the flow transmitters. In addition the common sensing line is used to minimize penetrations into the reactor coolant system pressure boundary and thereby reduce the potential for small breaks compared to using four separate instrument sensing lines.

**RAI-37**
In paragraph (f) of B.5.6, Independence it states "Manual controls from the Safety VDU can have priority over any non-safety controls from the PCMS." (emphasis added) This statement implies that there are instances where the Safety VDU does not have priority over the non-safety controls from the PCMS; these instances should be described.

**Response**

**RAI-38**

In Appendix C "Prevention of Multiple Spurious Commands and Probability Assessment", the definitions of terms like "credible," "incredible," "no credible failures," "infrequent", "unlikely" should be provided either numerically if the basis is quantitative, or by discussion if qualitative (e.g., x number of failures must occur). In addition, the probability assessment in Appendix C is a qualitative assessment. Has a quantitative assessment been performed? The fault tree in Sect. 6.5.2 implies that all detectable failures are detected with a probability of 1.0. Is this correct? Are undetected latent defects addressed?

**Response**

To demonstrate compliance to DI&C-ISG-04 Section 5 Malfunctions and Spurious Actuations, the following will be added to appendix C:

**RAI-39**
For the purposes of reviewing this topical report, the digital platform topical report and the US-APWR design certification, provide the following definitions: 1) MELTAC basic software and 2) MELTAC application software as MELCO identifies these products. Also please provide the differences.

**Response**
The basic software of the MELTAC platform consists of the following:

This software is the same for all applications. The basic software of the MELTAC Platform is described in various sections of MUAP-07005. As described in Section 4.1.2.1.1 of MUAP-07005, the basic software of the MELTAC platform resides in Ultra-Violet Erasable Programmable Read Only Memory (UV-ROM). It is changeable only by physically replacing the UV-ROM with a new UV-ROM device supplied by MELCO. Processors which contain these UV-ROM devices have strict physical access controls.

The application software configures the I/O, data communication interfaces, icon and function block libraries uniquely for each application. The application software also includes setpoints and constants. The application software is developed and changed using a graphical user interface. As described in Section 4.1.2.1.1 of MUAP-07005, the application software resides in Flash Electrically Erasable Programmable Read Only Memory (F-ROM). The application software is changeable, by the end-user, by enabling the hardware write permission switch on a specific processor and then downloading new application software from the Engineering Tool. The hardware write permission switches have strict physical access controls.

**RAI-40**
Typical methods to identify failure modes for analog systems are FMEA and HazOp analysis. Was a systematic method applied for identifying failure modes of the basic components of the digital system and their impact on the system?

**Response**
The FMEA method for the basic components of the MELTAC platform is described in Section 7.4 of MUAP-07005.

**RAI-41**
Was operating and maintenance feedback used for insights and input to the PRA models? Has the feedback process provided information on unforeseen scenarios or unanalyzed configurations? Have all digital system failures resulting from identified causes been within the acceptable level of a system's reliability?

**Response**
Questions related to the PRA should be directed to MUAP-07030 or DCD Chapter 19 for the US-APWR.

This reliability of the MELTAC platform, including history of operation, module MTBF and reliability modeling, is described in Section 7.0 of MUAP-07005.

**RAI-42**
Will there be any special hardware or software features in specific plant applications in the U.S. that differ from Japanese Nuclear Power Plants?

**Response**
Like any digital product line from US manufacturers, the MELTAC platform evolves over time for product improvement and new functionality.

**RAI-43**
What software initiating events have been considered in the PRA and safety analysis?

**Response**
Questions related to the PRA should be directed to MUAP-07030 or US-APWR Chapter 19.

The AOOs described in the safety analysis are based on worst case plant system failures, regardless of the failure (hardware or software) that may initiate them. For example, the cause of an excess feedwater event or an inadvertent rod withdrawal event is irrelevant. The event may be caused by hardware failure or software failure. Functions and components controlled from the PSMS and PCMS are distributed to separate controllers so that disturbances that can result from a single controller failure (due to either hardware or software failure) are bounded by the AOOs considered in the safety analysis. Control System failure modes are described in Section 5.1.8.

**RAI-44**
Does the digital instrumentation and controls introduce any new degradation conditions that are different from an analog system? What are the safety system responses when

encountering these new degradation conditions? What are the provisions proposed for coping with these new degradation conditions?

**Response**

A CPU failure results in loss of multiple non-safety control functions or multiple functions in one safety train. This situation is different from the signal processing in a conventional analog system, which has more functional partitions, and therefore more limited failure modes.

Failure of multiple control functions from one PCMS/PSMS controller is considered in the FMEA for the PCMS/PSMS to ensure the failures are bounded by the AOOs considered in the safety analysis.

Failure of multiple safety functions from one PSMS controller doesn't affect the overall plant level safety function, because redundant and independent safety trains, which meet single failure criterion, are provided.