Enclosure 3

UAP-HF-09261
Docket No. 52-021

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

on

Topical Report MUAP-07004-P(R2)
Safety I&C System Description and Design Process

June 2009
(Non-Proprietary)

MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07004-P(R2) Safety I&C System Description and Design Process

Non-Proprietary Version

June 2009

**©2009 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 (R2), "Safety I&C System Description and Design Process".

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

The RAI, "Request for Additional Information MUAP-07004 Rev. 2", was issued on May 19, 2009.

RESPONSE TO THE RAI

Following provides the responses for the RAI.

RAI-03 Supplement
When can the staff expect complete features, analytical techniques and procedural methods of the application software life cycle process and the setpoint methodology meeting the guidance of the applicable SRP sections to be included in the topical report? This would then allow these two issues to no longer be identified as DAC as the response suggests.

1) Per 10 CFR 52.47 (a)(9), an evaluation of the plant design to that of the SRP, in effect 6 months prior to the submittal, is required including an evaluation where differences exist and how the proposed alternative provides and acceptable method of complying with the Commission's regulations. In the response, MHI noted the DAC originally intended for Chapter 7, that being application software and system setpoints, are no longer DAC items but as-built ITAACs. When the design is complete, use of as-built ITAACs can be used to confirm the plant has been built to the design description. For these two topics, specific statements to conform, or evaluation of the differences from the guidance, have not been provided. This staff guidance on these topics is provided by BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints, and BTP HICB-14, Guidance on SW Reviews for Digital Computer Based I&C Systems. Until the acceptable plans and procedures are developed as part of the design described by this topical report, and the staff has confirmed them to be of adequate content and scope, these two issues should be considered as DAC items.

2) The requirement of 10 CFR 52.47 (a)(9), an evaluation of the plant design to that of the SRP, should be applied to all sections of the SRP with conformance or differences with an evaluation discussed in this topical report. Section 3.4 of the topical report lists a number of branch technical positions were conformity, or an analysis of the differences, has not been presented.

Response
1. Application Software
The application software for the PSMS is a plant specific item. This application software will be developed under the software quality program described in Section 6.0 of MUAP-07004. Section 6.0 describes the basic requirement of Process Overview, Process Control, Requirements, Implementation and Design Output, and Life Cycle Process for application software lifecycle. Detailed descriptions of the software development program and QA program for the US-APWR specific application software are provided in Technical Report MUAP-07017,"Software Program Manual" (SPM), which is referenced in the US-APWR DCD. The SPM is based on the BTP7-14. Each section of Section 3 of the SPM corresponds to each section of Section B3.1 of BTP7-14. The application software of the US-APWR, which is planned, developed, designed and implemented based on the SPM, is confirmed as an as-built ITACC. Thus the application software is not required to be define as a DAC item in the DCD.

2. Setpoint Methodology
Setpoints for I&C systems are determined based on the Setpoint Methodology which is generally described in Section 6.5.4, Accuracy Analysis, of MUAP-07004. The Setpoint Methodology of MHI I&C system conforms to BTP 7-12 and RG 1.105. The actual setpoints for

the US-APWR will be determined using this Setpoint Methodology after the instruments are procured and the uncertainty of the specific selected instruments is known. Thus the setpoints are confirmed as an as-built ITACC. It is noted that the detailed setpoint methodology for the US-APWR project, which includes the description of conformance to BTP7-12 will be submitted by end of October 2009. Thus, the setpoint methodology is not required to be defined as a DAC item in the DCD.

The application software and setpoint methodology for existing plant will be prepared by project by project.

RAI-04 Supplement

In the original question the staff requested, "Are any methods other than a watchdog timer and a test used to prevent or detect failures?" The response was "Details of the self-diagnosis are described in Section 4.1.5 of Topical Report MUAP-07005, "Safety System Digital Platform - MELTAC-." Therefore, if the referenced section to the other report provides a listing of all the methods then that topical and section should be referenced in this topical.

Per the guideline of SRP 7.1-C, Evaluation of Conformance to IEEE Std 603, particularly Criterion 5.5, System Integrity, explains "Hardware or software failures detected by self-diagnostics should also place a protective function into a safe state or leave the protective function in an existing safe state." The staff needs to know, either in the topical report or as specific reference to docketed material how all possible failures are identified.

The staff also requested "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? The response was "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."

The response is not consistent with the methodology described by MUAP-07006, Defense-in-Depth and Diversity nor is the failure of basic software described in the MELTAC topical report as such. Also, as part of the April 14, 15 meetings between the staff and MHI, it was stated that the application software is diverse between controllers within the same division. MHI is requested to address these issues in both topical reports. This needs to be adequately discussed in order to address the independence criteria of Criterion 5.6 of IEEE Std 603.

Response

Self-diagnostics

As a reference for the methods of self diagnosis other than a watchdog timer and a test used to prevent or detect failure, reference to Section 4.1.5 in the Platform TR, MUAP-07005 will be added to Section 4.3 in the Safety I&C TR, MUAP-07004. Section A.4.11 Equipment Protective Provisions, will be clarified as follows:

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of component control. The as-is state is selected for failures that impair control but do not result in complete loss of component control. These states has been demonstrated ...

These fail-safe states also apply to failures detected by self-diagnostics.

in Section of MUAP-07004 3.3 NRC Regulatory Guides (1) RG 1.22 Periodic Testing of Protection System Actuation Functions states;

> Protection actuation functions are completely testable through a combination overlapping automatic and manual tests.

Automatic self-diagnostic test are described in MUAP-07005. Manual tests are described in Section 4.4 PSMS Manual Testing and Calibration Features.

CCF

Topical Report MUAP-07006 Section 5.1 Basic Principle 1- Defenses to Minimize the Potential for CCF credits the application level diversity within the PSMS and PCMS as a defensive measure, which minimizes the potential for a CCF that could concurrently affect all echelons of defense. Regardless of this low potential for CCF, a CCF is assumed to occur which disables all functions of the PSMS. The source of the CCF could be in any portion of the Basic Software, including the self-diagnostic functions. The source of the CCF is not relevant to the D3 coping analysis, since all PSMS functions are assumed to be disabled. There are some differences between the basic software of the PSMS and PCMS, therefore the D3 coping analysis considers the CCF in the PSMS with and without a concurrent CCF in the PCMS.

RAI-07 Supplement

In the response to the staff's question, MHI stated that "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." At the January 22, 23 meetings at ORNL with the staff, MHI agreed to clarify, in the DCD, that all "high reliability" statements are based on redundancy and self-diagnostics, not reliability data.

Criterion 4.9 of IEEE Std 603, requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design. Therefore MHI is requested to clarify, to the staff, the basis for statements regarding reliability.

Response

The following description will be added to Section 5.1.3 of the Safety I&C TR, MUAP-07004;

> The high reliability of the Operational VDUs is based on redundancy of components, independence of redundant components and self-diagnostic functions within the computers that support the Operational VDUs. Specific reliability data for individual VDU components is not credited.

RAI-45

Will the design of the MELTAC platform generically comply with RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," and if so, how?

Section 3.3, NRC Regulatory Guides, does not reference compliance to RG 1.204 for grounding and surge protection methods to assure that electrical transients resulting from lightning phenomena do not render I&C 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 I&C systems important to safety with respect to lightning protection.

Response

As explained in the previous RAI response to RAI-02 of the Safety I&C Topical Report (UAP-HF-08114), RG 1.204 should be conformed directly by power supply components not by I&C. Conformance to RG1.204 is described in Section 8.3.1.1.11 of DCD Chapter 8 for the US-APWR. The MELTAC platform, which is a safety I&C component, fully conforms to RG 1.180. It is noted that lightning impulse resistance of power line of the MELTAC platform is qualified to 4kV from JEC-210-1981, which is Japanese standards, referred in Section 4.1.1.4 of the Platform TR, MUAP-07005. Therefore, conformance to RG1.204 will be added to Section 3.3 (23) of MUAP-07004 as follows:

> Plant licensing documentation describes conformance to RG 1.204 for the plant's electrical and grounding systems (e.g., Section 8 of the FSAR). In addition, the MELTAC digital platform complies with the electrical surge requirements defined by RG 1.180. In aggregate, this conformance provides suitable lightening protection.

RAI-46
In section 4.0, System Description, incorrectly states "various plant parameters and transmits appropriate signals to the control systems during normal operation, and to the reactor trip and engineered-safety feature systems during abnormal and accident conditions."

MHI is requested to revise the statement to indicate the appropriate signals are transmitted to the reactor trip and engineered-safety feature systems during normal operation as well.

Response
MUAP-07004 Section 4.0 will be revised as follows:

> Nuclear power plant instrumentation senses various plant parameters, and continuously transmits appropriate signals to the control systems for normal plant operation, and to the reactor trip and engineered-safety feature systems to detect abnormal and accident conditions.

RAI-47
MHI is requested to provide a diagram, or revise an existing one , in the topical report with explanation of how much of the computer based processing is used in manual switch system actuation of the ESF system. MHI should consider how the guidelines of RG 1.62 are met in the diagram and explanation.

In discussion of the Operator Console in Section 4.1, p.19, it is stated that the switches "have hardwired signal paths that bypass as much computer based processing as is practical." However, Section 4.2.4,b, states "Hard controls are provided to initiate each system level ESF actuation signal. The switches are hardwired to the ESFAS." which does not address any computer based processing. 10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 6.2.1 of the standard states, in part, that the manual control means shall depend on the operation of a minimum of equipment. Reg. Guide 1.62 states the staff's position on the requirement by stating that the amount of equipment common to both manual and automatic initiation should be kept to a minimum.

Response

RAI-48
MHI is requested to identify in the topical report, how single failure criterion is met when each ESF Actuation System train performs two-out-of-two voting for manual actuation switches on the Operator Console which is discussed in Section 4.1, p.23, the overall I&C architecture Part b. the Protection and Safety Monitoring System (PSMS).

MHI is request to explain conformance with the requirements of IEEE-603, criterion 5.1 for this application.

Response
The two-out-of-two voting logic monitors inputs from two(2) contacts on one(1) switch within the same train to prevent spurious actuation of that train. For this function there is no cross train signal voting that could compromise single failure compliance. A separate system level manual actuation switch (each with two contacts) is provided for each train on the Operator Console. For two train systems a failure of one(1) system level manual actuation switch will prevent manual actuation of only one(1) train. Manual actuation of the second train is unaffected. For four(4) train systems, a failure of one system level actuation switch will prevent direct manual actuation of only one(1) train. Therefore, the single failure of one switch only results in one(1) train ESF actuation failure and this design complies with the single failure criterion. This configuration is shown in Figure A.6.2-1 of MUAP-07004. In addition it is noted that for four train systems the train can also be indirectly manually actuated via signals from the other trains, as shown in the figure above. For two train and four train systems, each train can also be manual actuated at the system level from the safety VDU for each respective train.

RAI-49
Item (3), Safety Logic System (SLS), p.24, explains that there are only two trains for some US-APWR systems. Which systems are they and why is there only two trains.

At the January 22, 23 meeting with the staff at ORNL, the MHI agreed to provide a statement how PRA goals are met with only two trains due to the limited time duration in the startup mode; this is confirmed on a plant specific basis.

Again, explanation of the two train systems should identify how each application then meets the requirements of IEEE-603 criterion 5.1.

Response
A two train design is used for some ESF functions and some reactor trip functions. Each is explained below.

ESF Functions
The number of trains of plant components for ESF functions controlled by the SLS is plant specific. In the US-APWR, for example, the isolation functions are two (2) trains systems. The following ESF functions have two (2) trains in the US-APWR. The detail is described in DCD section 7.3 of the US-APWR.

- Containment Isolation Phase A
- Containment Isolation Phase B
- Main Steam Isolation
- Main Feedwater Isolation
- Emergency Feedwater Isolation

- CVCS Isolation
- Containment Purge Isolation
- Main Control Room Isolation
- Block Turbine Bypass and Cooldown Valves

For all functions, either train can provide the isolation function, therefore the single failure criterion is met.

Reactor Trip Functions
Source range (SR) neutron flux and intermediate range (IR) neutron flux have only two (2) trains. The voting logic for reactor trip (RT) by high SR and IR neutron flux is one-out-of two, therefore the single failure criteria is met. The RT functions of SR and IR neutron flux are bypassed above 10% reactor power manually or automatically. The RT functions of SR and IR neutron flux are not required above 10% reactor power. The bypassed/inoperable condition is controlled by the Technical Specification. The two train design does not prevent spurious actuation, but this is acceptable due to the limited that this trip must be operable.

RAI-50
Types of sensors should be identified in Chapter 7 to agree with the assumptions in Chapter 19. That is the failure rates assumed in Chapter 19 were that of analog sensors reported by IEEE std 500-1984

In Section 4.2.5a, p.38, discusses instrumentation shared between safety and non safety systems. These types of sensors should be further described in the Topical Report. There should also be discussion as to susceptibility to a common cause failure. This would then result in the loss of information to both non-safety and safety systems. The CCF (hardware failure) of the sensors is discussed in responses to RAI 25 in UAP-HF-08131 but not Topical Report MUAP-07006. MHI is requested to address this inconsistency and its resolution. Depending on the result this would affect the D3 strategy per the guidelines of BTP-19.

Response
MHI uses only analog sensors for the shared sensors applied to PSMS and DAS as described in the response to RAI-01 (UAP-HF-08070R0) to D3 TR, MUAP-07006. The following will be added to MUAP-07004 Section 4.1 d. Diverse Actuation System:

> The DAS shares sensor inputs with the PSMS through analog interfaces that are not subject to the postulated CCF in the PSMS. The shared sensors are analog devices, therefore CCF of the sensors does not need to be considered. Interfaces to safety process inputs ...

RAI-51
MHI is requested to further explain in Section 4.2.5, p. 39, Plant Control and Monitoring System, Item (4), Safety Parameter Display System (SPDS), what is meant by "such as the capability to handle operator interaction and diagnostic analysis." Provide a limit of what types of future modifications could be.

Response
The SPDS description is provided only to allow a complete understanding of PCMS functions. The expandability of PCMS functions is not pertinent to this understanding. Therefore, the following sentence will be deleted:

The SPDS has the flexibility to allow future modifications to be incorporated, such as the capability to handle operator interaction and diagnostic analysis.

RAI-52

MHI is requested to identify links in 4.2.5.c. Safety Systems and Components Controlled from Operational VDUs, p. 41, Data processing independence, to where information is further described on this subject.

Provide the necessary drawings, diagrams, and description of the I&C architecture that clearly identifies the network and signal connections between various I&C systems/components. Specifically, identify the following:

1. All signal and network connections between I&C system/components and connections to outside systems.
2. Communication medium used (i.e., fiber optic, copper cable, etc.)
3. Communication protocol (if applicable). The description should be sufficient to determine if the protocol is deterministic/non-deterministic and bi-directional/oneway.
4. The data communicated from one system/component to another and the purpose for the data communications.
5. Physical separation of the I&C systems/components.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 5.3 of IEEE Std. 603-1991 requires, in part, independence between redundant portions of a safety system and between safety systems and other systems. Digital I&C Interim Staff Guidance No. 4, "Highly-Integrated Control Rooms – Communication Issues," provides staff guidance for determining adequate independence of safety systems. The staff recognizes the I&C systems/components as described in the material provided by the applicant. However, the level of detail was not sufficient to determine communications independence between redundant portions of a safety system and between safety systems and other systems. In particular, it is not clear that the material provided already adequately describes all the communication activity.

Response

New Section 4.2.7 Digital Data Communication will be added in MUAP-07004, as follows:

4.2.7 Digital Data Communication

The following digital data communication interfaces are provided in the I&C system;

- The Unit bus provides bi-directional communication between safety and non-safety systems for only non-safety functions. The safety system and non-safety system are functionally isolated by dedicated communication processors in each safety system controller, and priority logic within the safety train that ensure safety functions have priority over all non-safety functions. Unit bus uses optical fiber to achieve electrical independence of each train. Physical separation between safety and non-safety system is accomplished by locating the safety and non-safety trains in different areas. The Unit bus uses the Control Network digital communication technology described in MUAP-07005 Section 4.3.2.
- Communications between different safety divisions are one way data link communication between RPS trains and from RPS to ESFAS. Functional separation is achieved by communication controllers that are separate from functional processors and voting logic that processes the data from the different trains. Each data link uses optical fiber to

achieve electrical independence of each train. Physical separation between safety trains is achieved by locating in different areas. These interfaces are the data link digital data communication technology described in MUAP-07005 Section 4.3.3.

- Bi-directional communications between controllers in one(1) safety train are performed by the Safety Bus. The Safety Bus provides deterministic cyclical data communication. Functional independence is provided by separate communication processors within each controller. Fiber optic cable is provided to enhance EMI susceptibility. The Safety Bus uses the Control Network digital communication technology described in MUAP-07005 Section 4.3.2.
- Bidirectional communication between controllers and their respective I/O modules is provided by the I/O Bus described in MUAP-07005 Section 4.1.
- The PCMS sends information to other systems connected to the Station Bus, which is the plant Information Technology network, via the Unit Management Computer. The Unit Management Computer (UMC) provides only one way communication with a firewall to protect the critical PCMS and PSMS resources. The defensive approach for cyber security is described in Section 6.4.3. A plant specific cyber security plan will be provided in plant licensing documentation.

RAI-53

On p. 41, it is stated "The PCMS and PSMS will be controlled under the most stringent administrative controls for cyber security." The controls should be stated here or specific reference, by section and paragraph, to documents that do list these controls. Also, it states, "There is only one-way communication to other systems that are not under these same controls." What systems are these? Is this an application specific item?

IEEE Std 603 Criterion 5.9, Control of Access, states, "The design shall permit the administrative control of access to safety system equipment." The controls referred to here need to be further delineated.

Response

The cyber security aspects are described in Section 6.4.3 of MUAP-07004. Section 6.4.3 describes that the unidirectional communication is provided for PSMS/PCMS to outer IT network. Plant cyber security is plant specific item. The plant cyber security for the US-APWR is described in the US-APWR DCD Section 13.6 and US-APWR Cyber Security Program technical report, MUAP-08003. MUAP-08003 includes more information for cyber security of PSMS and PCMS and administrative cyber security control of the plant. A similar report to MUAP-08003 will be prepared for each specific project.

RAI-54

Response

RAI-55

Section 4.2.5.c), refers to Appendix C for the basis of multiple erroneous control commands is not considered credible. However, Appendix C and the staff, still considers this as credible failure, regardless of how small the probability. MHI is requested to address this failure, as a credible one, in the topical report.

IEEE Std 603, Criterion 5.6.3 (Independence), Between Safety Systems and Other Systems, states, "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."

Also, this section refers to the non-class IE devices being tested to the same seismic levels as the PSMS. How is this done if there is no Equipment Qualification program for non-safety

devices? Is there configuration control for operational VDUs? How is a configuration management program established for non-safety devices?

Response

[ ]

Software Quality Program
The following will be added to Section Appendix C:

> The software life cycle is managed according to a Quality Assurance Plan for high integrity components. That Quality Assurance Plan is referenced in plant licensing documentation. For example, for the US-APWR this QA plan is referenced in the US-APWR DCD Chapter 17.

Qualification Program
The following will be added to Section 4.2.5c:

> Reference to the qualification documentation and the configuration control program for Operational VDUs and MELCO MR Series processors is provided in plant licensing documentation. For example, for the US-APWR this QA plan is referenced in the US-APWR DCD Chapter 17.

RAI-56
Section 4.4.1, Manual Testing, P. 47, identifies a special test display screen that does not initiate any manual control actions and the details of this are described in the Platform Topical Report. Provide the Section, subsection and paragraph of the Platform Topical Report that discusses this.

Criterion 5.7, Capability for Test and Calibration, of IEEE Std 603, requires "Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. It is also not clear to the staff in which topical report safety evaluation MHI wishes to have the Safety VDUs address. If it is in the other topical report, then that report should be referenced, by chapter and section where the details are at.

Response
Section 4.4.2 will be revised as follows:

> The details of this test are described in the Platform Topical Report MUAP-07005, Section 4.2.4.

Details of the Safety VDU manual test methodology will be added in the Platform TR, MUAP-

07005 Section 4.2.4.

RAI-57
Section 4.4.3, Response Time, p. 49, states "The PSMS includes no components that have known aging or wear-out mechanisms that can impact response time." This statement needs to be further defined. Does this include all only cabinet electronics, signal I/O, impulse lines and sensors?

A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by Clause 4.10 of IEEE Std. 603-1991.

Response
Section 4.4.3 will be revised as follows:

> The MELTAC components of the PSMS and most PSMS instrumentation include no components that have known aging or wear-out mechanisms that can impact response time. Therefore response time can only be affected by random failures or calibration discrepancies. All random failures and calibration discrepancies are detected by the testing and calibration methods described above. Specific components of the PSMS that require periodic response time tests are identified in Plant Licensing Documentation, such as plant specific Technical Specifications. Periodic testing is typically applied to reactor trip circuit breakers and RTDs.

For other PSMS components, for which there is no periodic response time testing. The response time is confirmed analytically and through testing. As stated in Section 4.4.3 "Response time is calculated and independently verified and validated during the system design process, as described in Section 6.5. Section 6.5.3 of MUAP-07004 describes the response time evaluation method. This methodology confirms that the response time conforms to the real time performance requirement of IEEE 603 and BTP 7-21. Since the MELTAC platform performs all signal processing with fixed cyclical operation, there is no response time variation.

RAI-58
Section 4.5, PSMS On-line Maintenance, states that "Processor modules and I/O modules can be replaced while the PSMS controllers are powered. Other modules require power to be removed from the chassis, prior to module replacement." This must be further explained and delineated.

1. What is meant by processor modules? Is this a CPU module?
2. What if the single controller configuration is used? Can this be replaced while powered?
3. What are "other modules"? Please provide a listing

Will standby or redundant component failures alarm?

This information will provide the staff support for determining if Criterion 5.7, of IEEE Std 603, Capability for Test and Calibration will be met. This requirement states "Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions."

Response
Section 4.5 will be revised as follows:

> Failures detected by platform self-diagnostics are automatically diagnosed to the replaceable module level. Alarms are provided on Operational VDUs and failed module identification is provided on the Engineering Tool. Alarms are provided for failures detected by self-diagnostics in all processor configurations, single or redundant. Failed processor modules ...
>
> I/O modules can be replaced while the PSMS controllers are powered. Processor modules (e.g., CPU and digital communication modules), require power to be removed from the chassis, prior to module replacement. For failed processor modules in controllers configured for parallel or standby redundancy, the controllers will recover to their normal redundant configuration with no plant impact beyond the initial failure, as discussed above. For failed processor modules in single controller configurations, the plant level effects of the failure must be considered, including recognition that the controller must be powered down for module replacement. Replacement of I/O modules...

RAI-59
Section 5.1, Key Technical Issue, p. 53, lists credit for leak detection in Defense-in-Depth and Diversity analysis. This should be consistent with the NRC staff review and safety evaluation of Topical Report MUAP-07006-P (R2), Defense-in-Depth and Diversity. Section 5.1.6 should address this consistently as well. MHI is requested to provide information on how these inconsistencies will be resolved.

Response
MUAP-07004 and 07006 consistently credit leak detection in the Defense-in-Depth and Diversity strategy. MHI would expect the Staff to identify this as an Application Specific Action Item as was done in the Safety Evaluation for MUAP-07006.

RAI-60
Section 5.1.3, p.54, Operation under Degraded Conditions, discusses the potential failure of all Operational VDUs. How can the operability of Operational and Safety VDUs be verified? At the January 22, 23 meeting with the staff, MHI agreed to add justification for no periodic manual surveillance testing or offer some type of periodic surveillance to confirm Operational VDU is operating correctly.

Per IEEE Std 603, Criterion 5.7, Capability for Test and Calibration, "The capability for testing and calibration of safety system equipment shall be provided during power operation." This requirement does allow exceptions under certain conditions. MHI is requested to identify conformance of the Safety VDUs to this requirement.

Response
Processors of the Safety and Operational VDUs and their communication capabilities are checked continuously by self-diagnosis. In addition, the integrity of the Safety VDU panel is manually verified periodically by the test shown in Section 4.4.1 of Safety I&C TR MUAP-07004. The following will be added to Section 5.1.3:

In the event of complete failure ... very infrequent events. Failure of an individual Operational VDU is easily detected by operators, because the Operational VDU is continuously used for plant operation. The ability to detect individual Operational VDU failures and complete failure of all PCMS VDUs is confirmed during HSI validation testing.

RAI-61

Section 5.1.4, Integrated RPS & ESFAS with Functional Diversity, states "On the other hand, PRAs done for the MHI digital I&C show minimal benefit for additional RPS/ESFAS separation (with functional diversity)." Unless the specific results of the PRAs referenced are described here or reference to specific document (which is on the docket), section, subsection or paragraph, only reference to a PRA done does not provide the staff with sufficient information and reference to a PRA should be removed from the topical report.

At the January 22, 23 meeting, MHI agreed to revise the words regarding PRA goals vs. a definitive statement. For example, in section 4.2.1, it is stated "The PRA safety goals, the Single Failure Criterion, and GDC24 are met with only three trains in service." This should be changed to "The Single Failure Criterion and GDC24 are met with only three trains in service. The PRA goals are also expected to be met with only three trains in service; this is confirmed on a plant specific basis."

Response

The description in Section 4.2.1 of MUAP-07004, "The PRA safety goals, the Single Failure Criterion, and GDC24 are met with only three trains in service" will be changed to "The Single Failure Criterion and GDC24 are met with only three trains in service. The PRA goals are also expected to be met with only three trains in service; this is confirmed on a plant specific basis."

Section 5.1.4 will be revised as follows:

Instead of separating RPS and ESFAS... initiate protective actions. PRAs done for the MHI digital I&C design are expected to show significant benefit for this functional diversity; this is confirmed on a plant specific basis.

RAI-62

Section 5.1.8, Control System Failure Mode, discusses the high reliability features. The staff is requesting if the redundant standby controller configuration is used, is there indication that a controller has failed and switch over has been successfully accomplished?

[ ]

This must be adequately demonstrated, if this is part of the plant specific design where functions are assigned to different controllers this should be identified as a plant licensing submittal.

IEEE Std 603 Criterion 5.6.1, (Separation), "Between Redundant Portions of a Safety System" states "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the

capability to accomplish the safety function during and following any design basis event requiring that safety function."

Response
When a failure is detected by self-diagnostics, there is a group PSMS or PCMS trouble alarm in the MCR, which prompts operators to summon operations/maintenance personnel to diagnose the source of the alarm. Operations/maintenance personnel diagnose these group alarms using the drill down features of the Engineering Tool. In addition, when the redundant standby controller configuration is used, there is local indication on the controller front panel that the controller has failed and a switchover has been successfully accomplished.

The distribution of specific control functions to different controllers is a plant specific item. For the US-APWR the control function distribution is described in the DCD section 7.7. In this Topical Report, MHI is establishing the generic design basis for failures that must be considered in the plant specific safety analysis. The specific assignment of functions to controllers is not relevant to the Staff's acceptance that the controllers are sufficiently independent to limit the failures considered in the safety analysis to functions controlled by one controller.

It is noted that the distribution of non-safety control system functions has no relationship to the redundancy or independence between safety divisions, which is required by IEEE 603-1991. This issue pertains to the design basis events that must be considered in the safety analysis.

RAI-63
Section 5.1.9, Credit for Self-Diagnostics for Technical Specification Surveillance, this section should stipulate what surveillances are not longer necessary.
Additionally data should be provided that demonstrates the effectiveness of the self diagnostics.

Also, in the January 22, 23 meeting with the staff at ORNL, the MHI agreed to provide a description of how self-diagnostics are checked during manual surveillance tests. A history of self diagnostics success or failure (either specific factory or field data) is to be added to the topical report. The data should demonstrate that tests and operating experience 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. MHI is requested to make the above changes or provide justification for not including the information.

Response
The following will be added to Section 5.1.9:

> Plant specific technical specifications identify manual surveillance tests that confirm input signal calibration and propagation through the digital system. Manual surveillance tests are also provided to confirm command propagation through the digital system and correct control of plant components. The self-diagnostics discussed above are credited to eliminate manual surveillance tests of functional logic and algorithms, setpoints and constants.

A history of self diagnostics success or failure (either specific factory or field data) will be added to MUAP-07005. The data will demonstrate that tests and operating experience 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.

RAI-64

Section 5.1.10, Unrestricted Bypass of One Safety Instrument Channel, states that "The PSMS remains fully functional with the remaining two trains.." The plant may have one channel out of service but not two or they would not be able to have single failure protection and meet GDC 21. This should be explained in the topical report. MHI is requested to provide this explanation in the topical report.

GDC 21, Protection system reliability and testability, states "redundancy and independence designed in to the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. "

Response

The words "The PSMS remains fully functional with the remaining two trains", means that:

(1) When one of four channels is bypassed, the normal 2/4 voting logic will be automatically changed to 2/3 voting logic.
(2) If a single failure occurs during the above 2/3 condition, the remaining 2 (two) operable channels are sufficient to achieve the safety function.

The following will be added to Section 5.1.10:

> The PSMS remains fully functional with the remaining two trains, since two channels are sufficient to satisfy the 2-out-of-N voting logic.

RAI-65

Section 5.2.2, Environmental Qualification, states that

1) "A small margin for the alarm setpoint is provided to avoid nuisance alarms." What is meant by a small margin?
2) "Appropriate prevention for high dust influence must be provided." What types of features, if any, are provided for dust control?

Response

1) Section 5.2.2a will be changes as follows:

> A small margin for the alarm setpoint is provided to avoid nuisance alarms. The margin accommodates temperature instrument uncertainty.

2) As stated, dust control "preventions are discussed in Plant Licensing Documentation". These typically include dust filters provided on the cabinet door.

RAI-66

Section 5.2.4, EMI/RFI Compatibility, states that power line filters for input power sources are used. What are the criteria used for power line filters?

Response

The criteria used of power line are based on RG1.180. The EMI/RFI emission and susceptibility tests are performed for the MELTAC Platform based on the methods and acceptance criteria of RG1.180. The EMC qualification to RG1.180 is confirmed for the

MELTAC Platform. The tests are performed with a MELTAC cabinet fully equipped with a typical configuration of MELTAC components required for a safety protection system. These are described in Platform TR MUAP-07005, Section 5.3. The specification for EMC of the MELTAC Platform is described in MUAP-07005, Table 4.1-2 Environmental Specifications. This will be added in MUAP-07004.

RAI-67

Section 6.3, Requirements, Implementation and Design Outputs for Software Life Cycle Process, states "In accordance with BTP HICB-14, a summary of the requirements, the implementation and the design outputs for the Software Life Cycle Process in Figure 6.1-1 are described in this section." The staff guidelines for all the management, implementation and resource characteristics of each plan should be delineated here, as described in BTP HICB 7-14, or the software program manual for the application software be referenced, such as for the USAPWR Topical Report MUAP-07017. The descriptions presented here in their current form are not sufficient for approval on their own.

Per 10 CFR 52.47 (a)(9), an evaluation of the plant design to that of the SRP, in effect 6 months prior to the submittal, is required including an evaluation where differences exist and how the proposed alternative provides and acceptable method of complying with the Commission's regulations. Included in this should be statement of conformance to or the evaluation of the differences from BTP HICB 7-14.

Response

Section 6.3.1 will be revised as follows:

> This section describes the key contents of the software life cycle plans that govern the Application Software life cycle process. These key contents are generically applicable to Application Software for all systems and all projects. Each project references a software program manual that provides the detailed guidelines for the management, implementation and resource characteristics of each software life cycle plan. The software program manual may be a generic document or a project specific document. For example, for the US-APWR the software life cycle plans are documented in MUAP-07017, US-APWR Technical Report Software Program Manual. The software program manual is supplemented by additional information that is documented in the Project Plan, which is written uniquely for each project. If the referenced software program manual is a generic document, any deviations from the requirements in these generic plans are also documented in the Project Plan. The Project Plan also includes an assessment of the software project risk and the risk management plan.

RAI-68

Has the guidance of Reg Guide 1.152, Regulatory Positions 2.1 – 2.9 been followed concerning safety system security? Sections 6.4.1, Access Control, and 6.4.3 Cyber Security Management should follow the guidance beginning with the physical and logical security access control being based on the results of a cybersecurity qualitative risk analysis done during the design phase. MHI is requested to address all 9 positions of Reg Guide 1.152.

This regulatory guide, 1.152 Criteria for use of Computers in Safety Systems of Nuclear Power Plants, describes a method that the staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and cyber-

security for the use of digital computers in safety systems of nuclear power plants. General Design Criterion (GDC) 21, "Protection System Reliability and Testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," to Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," of the Code of Federal Regulations (10 CFR Part 50), requires, among other things, that protection systems (or safety systems) must be designed for high functional reliability commensurate with the safety functions to be performed.

Response
The following will be added to Sections 6.4.1 and 6.4.3:

> This section defines key cyber security requirements that are applicable to all projects. Cyber security controls applicable to the Basic Software of the MELTAC platform are described in Section 6.1.6 of MUAP-07005. In addition, each project references a cyber security program document(s) that provides the detailed guidelines for the management, implementation and resource characteristics of the plant specific cyber security program. For example, for the US-APWR Technical Report MUAP-07017 Software Program Manual describes the cyber security controls for each phase of the application software life cycle. In addition, Technical Report MUAP-08003, US-APWR Cyber Security Program describes the cyber security program management, critical asset assessment and resulting defensive model.

RAI-71
In topical report section 3.4, NRC Branch Technical Positions, the only discussion provided to conformance to BTP HICB-12, Guidance for Establishing and Maintaining Instrumentation Setpoints, is "See compliance to RG 1.105."
Conformance to BTP HICB-12 should be identified or differences and the analysis including an evaluation where differences exist and how the proposed alternative provides an acceptable method of complying with the Commission's regulations as required by 10 CFR 52.47 (a)(9) should also be provided.

In addition the staff has the following questions:

For Section 6.5.4, Accuracy Analysis Method, the staff has the following questions:
1. There are terms identified but no definitions of what each term includes. A thorough and complete description of each should be provided.
2. These terms or uncertainty components appear to not be addressed:
   i) Environmental Allowance
   ii) Process Measurement Accuracy
   iii) Electronics or Cabinet uncertainties such as M&TE, temperature and drift
3. There is no discussion of non-random and dependent allowances. This may depend on the definition of the individual allowances but this should be discussed in the definitions.
4. These mandatory data terms are required per ISA-67.04-2000. These should be identified and defined as well:
   i) Analytical Limit, Channel Instrument Accuracy, Channel Calibration Accuracy, Channel Instrument Drift, Primary Element Accuracy, Safety Limit, Limiting Safety System Setting
5. The definition of the allowable value and its relationship to the setpoint methodology and testing requirements in the technical specifications must be documented per RG 1.105.
6. If the relationships between these terms are identical to that of ISA S67-4-2000 Figure 1, is the allowable value the LSSS? If not a graphical representation of the setpoint

relationships should be provided, similar to Figure 1 of ISA S67-04-2000.
7. Calibration tolerance uncertainties depicted by region "E" of Figure 1 of ISA S67-04-2000 should be accounted for in the methodology.
8. No discussion is provided of what the Total Allowance is or how the Margin is calculated for each Protection System channel or example is provided.

Is this methodology used for non-safety instrumentation maintaining design limits described in the Technical Specifications? Is it used for monitoring instrumentation? And is it used for the DAS?

Response

MUAP-07004 describes the accuracy analysis as the basic uncertainty evaluation. MUAP-07004 will also be revised to add the basic concept required from this RAI. For the US-APWR, the Setpoint Methodology report including the conformance to BTP7-12 will be submitted as stated in the response to RAI-03 Supplement. The detailed requested information from this RAI will be included in the report.

The scope of setpoint methodology which conforms to RG1.105 is the safety system. Thus the conformance to RG1.105 for non-safety function and DAS setpoint is not required. However, the methodology and basic concept for setpoint determination and uncertainty calculation can I be applied to that of non-safety system.

Section 3.4 (11) will be revised as follows:

> Section 6.5.4 defines the methodology used to combine all uncertainties to establish limiting safety system settings (LSSS) and Allowable Values defined in the plant technical specifications.

The following will be added to Sections 6.5.4:

> This section defines key components of the setpoint methodology applicable to all projects. In addition, each project references a setpoint document that provides the detailed methodology applicable to LSSS and Allowable Values defined in the plant specific technical specifications. For example, for the US-APWR Technical Report. Setpoint Methodology describes the uncertainty calculation methods for safety system setpoints. Many uncertainties considered in the setpoint methodology for safety systems are also applicable to non-safety setpoints, including the Diverse Actuation System. Non-applicable uncertainties are specifically noted in the non-safety setpoint calculations. Non-safety setpoints also exclude limits specifically related to Technical Specifications, such as Allowable Values. The details of the setpoint methodology demonstrate compliance to BTP 7-12.

RAI-72

[

]

Response

[

]

[

]

RAI-74

[

]

Per IEEE Std 603, "This standard establishes functional and design criteria that are general in nature. It requires supportive standards containing both general and detailed criteria to comprise a minimal set of requirements for the safety system." Therefore for where specification of safety components, in this case fiber optic cables, are not cited there should be identification of the specifications used for fiber optic selection.

Response

[

]

RAI-75

Appendix A, A 5.6.3.2, Equipment in Proximity, describes an analysis adequacy of separation distances. Has an analysis been done on the MELTAC intercabinet, processor or module level that would meet the guidelines of RG 1.75/ IEEE Std 384 or will this all be done as part of the application specific project? If so this should be added to Table 7-1, Future Licensing Submittals.

Response

Section A5.6.3.2 will be revised as follows:

> In general, non-safety wiring is separated from safety wiring or separated with barriers, in accordance with RG 1.75 and IEEE 384. Where separation distances are less than those suggested by RG 1.75 and IEEE 384, plant licensing documentation references analysis or tests that justify the adequacy of the wiring routing.

RAI-76

MHI is requested to provide an explanation, in the topical report, concerning the diversity of application software in parallel controllers within a division.

At the April 14 Chapter 19, PRA, meeting MHI explained that the software is diverse between

parallel controllers within a division. Consistency between Chapters 19 and 7 is necessary for the staff to come to the same independent conclusion. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation. IEEE Std. 379-2000, Clause 5.5, identifies D3 as a technique for addressing common-cause failure, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

Response
The diversity of application software within parallel controllers is described in Section A.5.16 Common Cause Failure (IEEE 603-1998). Table A.5.16-1 Diverse Parameters in Two Separate Controller Groups describes the diversity for each reactor protection function. The last paragraph on Page 101 will be clarified as follows:

> The two diverse parameters are monitored by two separate sensors which interface to two separate digital controllers within the RPS. The two controllers each process these inputs through diverse application programs to generate reactor trip and/or ESF actuation signals.

RAI-77
Section 6.3.1, Software Life Cycle Process Requirements, item (4), Software Integration Plan should be expanded to clarify the V&V process for tool output, this was agreed to in the January 22, 23 meetings at ORNL with the staff,

The guidelines of BTP 7-14 address the issue of V&V of tool outputs. The evaluation required by 10 CFR 52.47 (a)(9) to the SRP should include the guidelines of BTP 7-14.

Response
Section 6.3.1 Item (4), Software Integration Plan, second bullet will be revised as follows :

> Requirements for verifying the output products of the Engineering Tools Verification shall manually compare the output of the Engineering Tool source documents, to confirm that the Engineering Tools have not introduced any errors.

RAI-78
At the January 22, 23 meeting with the staff, MHI agreed to provide MTBF for components referenced by the statement in 6.5.2 "The MTBF for other components is obtained from industry handbooks or manufacturers publications."

IEEE Std 603 Criterion 5.15 states that the applicant should justify the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed.

Response
Reliability data of I&C system components other than MELTAC platform will be shown in plant licensing documentation. For example, for the US-APWR, sensor and RTB reliability data are stated in the PRA report, and their reliability value is based on IEEE 500 and NUREG 6928. Section 6.5.2 will be revised as follows:

The MTBF for other components is obtained from industry handbooks or manufacturers publications. The actual reliability data and the source of the data for these components is identified in plant licensing documentation. The system reliability is calculated based on this system model and the MTBF of each component.