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

April 28, 2011

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-11127

Subject: **MHI's Responses to US-APWR DCD RAI for Chapter 7 and mark up of Chapter 7 on Revision 3**

References:

1) "REQUEST FOR ADDITIONAL INFORMATION 692-5433 REVISION 2, SRP Section: 07.01 – Introduction, Application Section: Section 07.01" dated February 10, 2011.

2) "REQUEST FOR ADDITIONAL INFORMATION 698-5490 REVISION 2, SRP Section: 07.01 – Introduction, Application Section: Section 07.01.3" dated February 28, 2011.

3) "REQUEST FOR ADDITIONAL INFORMATION 720-5539 REVISION 2, SRP Section: 07.01 – Introduction, Application Section: Section 07.01" dated March 21, 2011

4) "REQUEST FOR ADDITIONAL INFORMATION 700-5406 REVISION 2, SRP Section: 07.08 – Diverse Instrumentation and Control Systems, Application Section: Section 07.08" dated February 28, 2011.

5) "REQUEST FOR ADDITIONAL INFORMATION 701-5229 REVISION 0, SRP Section: 07.09 – Data Communication Systems, Application Section: Section 07.09" dated February 28, 2011.

6) "REQUEST FOR ADDITIONAL INFORMATION 710-5493 REVISION 2, SRP Section: 07.09 – Data Communication Systems, Application Section: Section 07.09" dated March 7, 2011.

7) "REQUEST FOR ADDITIONAL INFORMATION 568-4588 REVISION 1, SRP Section: 07.05 – information systems important to safety, Application Section: Section 07.05" dated April 13, 2010.

8) "REQUEST FOR ADDITIONAL INFORMATION 656-5127 REVISION 2, SRP Section: 07.09 – Information system important to safety, Application Section: Section 07.09" dated November 15, 2010.

9) "REQUEST FOR ADDITIONAL INFORMATION 239-2033 REVISION 0, SRP Section: 07.06 – Interlock Systems Important to Safety, Application Section: 07.06, dated March 2, 2009

D081
NRO

10) "REQUEST FOR ADDITIONAL INFORMATION 638-5032 REVISION 0, SRP Section: 07.06 – Interlock Systems Important to Safety, Application Section: 07.06, dated September 23, 2010

11) "REQUEST FOR ADDITIONAL INFORMATION 688-5273 REVISION 2, SRP Section: 07.06 – Control Systems, Application Section: 07.06, dated January 31, 2011

12)"REQUEST FOR ADDITIONAL INFORMATION 677-5325 REVISION 2, SRP Section: 07.06 – Diverse Instrumentation and Control Systems, Application Section: Technical Report MUAP-07014, dated January 10, 2011

13) "REQUEST FOR ADDITIONAL INFORMATION No. 665-5220 REVISION 2, SRP Section: 07-14 Branch Technical Position – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems - Application Section: Section B.3.1.9" dated November 22, 2010.

14) "REQUEST FOR ADDITIONAL INFORMATION 593-4565 REVISION 1, SRP Section: 07-21 Branch Technical Position – Guidance on Digital Computer Real – Time Response, Application Section: Chapter 7, dated June 8, 2010

15) "REQUEST FOR ADDITIONAL INFORMATION on Topical Report MUAP-07004(R1) Safety I&C System Description and Design Process dated July 3, 2008"

16) "REQUEST FOR ADDITIONAL INFORMATION US-APWR Topical Report: Safety System Digital Platform – MELTAC MUAP-07005-P(R3)" dated July 1, 2009"

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

Enclosure 2 and 3 are the responses to RAIs contained within Reference 1 through 6, and enclosure 4 and 5 are the amended responcss to RAIs contained within Reference 7 through 16. Enclosure 4 and 5 are based on RAI evaluation meeting held from January to March of 2011 with the NRC.

Enclosure 6 and 7 reflect the response to RAIs contained within Reference 1 through 16, and RAI708-5455 and RAI671-5126 as request of the NRC.

As indicated in the enclosed materials, this submittal 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 with the information identified as proprietary redacted and replaced by the designation "[ ]".

This letter includes copies of the proprietary version of the RAI responses (Enclosures 2 and 4), copies of the non-proprietary version of the RAI responses (Enclosures 3 and 5), and the Affidavit of Yoshiki Ogata (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials designated as "Proprietary" in Enclosures 2 and 4 be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

This letter also includes two versions of mark up DCD Chapter 7 (Enclosures 6 and 7). One version includes certain information, designated pursuant to the Commission guidance as sensitive unclassified non-safeguards information, referred to as security-related information ("SRI"), that is to be withheld from public disclosure under 10 C.F.R. § 2.390. The information that is SRI is identified by brackets. The second version omits the SRI and is suitable for public disclosure. In the public version, the SRI is replaced by the designation "[Security-Related Information - Withheld under 10 CFR 2.390]."

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

Sincerely,

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

Enclosures:

1. Affidavit of Yoshiki Ogata

2. Response to Request for Additional Information for Chapter 7 (Proprietary Version)

3. Response to Request for Additional Information for Chapter 7 (Non-Proprietary Version)

4. Amended Response to Request for Additional Information for Chapter 7 (Proprietary Version)

5. Amended Response to Request for Additional Information for Chapter 7 (Non-Proprietary Version)

6. CD1: "Mark up of DCD Chapter 7 on Revision 3 (SRI Included)"

- Version containing Safety Related Information

7. CD2: "Mark up of DCD Chapter 7 on Revision 3 (SRI Excluded)"

- Version not containing Safety Related Information

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: ck_paulson@mnes-us.com
Telephone: (412) 373-6466

Enclosure 1

Docket No. 52-021
MHI Ref: UAP-HF-11127

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 documents entitled "Response to Request for Additional Information for Chapter 7" and "Amended Response to for Additional Information for Chapter 7" dated April 2011 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 28th day of April, 2011.

Y. Ogata

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

Enclosure 3

Docket No. 52-021
UAP-HF-11127

Response to Request for Additional Information for Chapter 7

April 2011

Non-Proprietary Version

This Enclosure includes following response of RAIs

RAI No. 692-5433 Revision 2, Question No.: 07.01-25

RAI No. 698-5490 Revision 2, Question No.: 07.01-26

RAI No. 720-5539 Revision 2, Question No.: 07.01-28

RAI No. 700-5406 Revision 2, Question No.: 07.08-16

RAI No. 701-5229 Revision 0, Question No.: 07.09-19

RAI No. 701-5229 Revision 0, Question No.: 07.09-20

RAI No. 701-5229 Revision 0, Question No.: 07.09-21

RAI No. 701-5229 Revision 0, Question No.: 07.09-22

RAI No. 710-5493 Revision 2, Question No.: 07.09-23

Responses to Request for Additional Information No.692-5433
Revision 2

SPR Section 7.1
Instrumentation and Controls - Introduction

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.692-5433 REVISION 2**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS – INTRODUCTION**
APPLICATION SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS – INTRODUCTION**
DATE OF RAI ISSUE:	**02/10/2011**

QUESTION NO. : 07.01-25

Request to address four basic design principles and one attribute in DCD

During the January 19, 2011 meeting between the NRC staff and MHI, the staff requested MHI to consolidate information in the US-APWR design control document (DCD) section 7.1 to address four digital instrumentation and control design principles. Those principles are: (1) redundancy, (2) independence, (3) the need for defined determinism in data processing and communication, and (4) implementation of a diversity and defense-in-depth (D3) philosophy, as well as one subjective attribute – simplicity.
Although these design principles have been discussed in various technical reports to satisfy the IEEE Standard 603-1991 requirements, consolidating the information in DCD Section 7.1 will improve its conciseness and clarity, as well ease its availability for staff and stakeholders to review and reference. Similar documentation has been documented in the other design centers such as ESBWR DCD Section 7.1, and South Texas Project Units 3 and 4, Appendix 7DS.

ANSWER:

MHI agrees with the staff's request.

Additional description to demonstrate safety digital I&C design conformance to essential safety criteria (redundancy, independence, determinism, diversity and simplicity) embodied in the underlying basis of IEEE 603-1991 will be added in Section 7.1 of the DCD and technical report.

Summary description will be added in Section 7.1 of the DCD Rev. 4. Detailed description, including propriety information, is included in Appendix F of "Safety I&C System Description and Design Process", MUAP-07004 Rev. 6 and a pointer to this report will be added in Section 7.1 of the DCD Rev. 4.

Impact on DCD
As described in Attachment 1 (Markup for the DCD Rev. 4), the summary description will be added in Subsection 7.1.4, and successive sections will be renumbered as Subsections 7.1.5 and 7.1.6.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Responses to Request for Additional Information No.698-5490
Revision 2

SPR Section 7.1
Instrumentation and Controls - Introduction

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 698-5490 REVISION 2**
SRP SECTION:	**07.01 - INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01.3**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.01-26

In response to RAI 229-2022, question 07.01-15, MHI stated that continuous self-diagnostic features can eliminate most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are specifically provided for functions with no self-diagnostics features. The applicant addressed that the coverage of self-diagnostics and manual testing is described in TRs, MUAP-07004, and MUAP-07005. But, these TRs did not describe the Technical Specification (TS) surveillance requirements for the self-diagnostic features.

The staff requests MHI to provide the TS surveillance requirements for the self-diagnostic features themselves in accordance with SRP BTP 7-17 as guidelines. In BTP 7-17, automatic test features which are credited with performing surveillance test functions should be verified during periodic surveillance testing consistent with the technical specifications and plant procedures. Also, 10 CFR Part 50 Appendix B, Criterion XII, "Control of Measuring and Test Equipment," requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy with necessary limits. As delineated in RG 1.118, periodic testing consists of functional tests and checks, calibration verification, and time response.

Reference: MHI's Responses to US-APWR DCD RAI No. 229-2022... ; MHI Ref: UAPHF- 09196; dated April 28, 2009; ML091250290.

ANSWER:
The verification of self-diagnostic features is performed by the combination of (1) manual periodic surveillance tests, that confirm the integrity of all program memory within each MELTAC controller in the PSMS, including the software memory that controls the self-diagnostic functions, and (2) manual periodic surveillance tests that confirm that each controller can correctly execute that program memory. The overlap of these periodic surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

The self-diagnostic features are also confirmed by manual periodic tests and continuous on-line tests that are diverse from the self-diagnostic features. These tests confirm the operability of each MELTAC controller in the PSMS, thereby ensuring that failures have not been missed by the self-diagnostic features.

As to the memory integrity check, the integrity of the self-diagnosis is confirmed by a periodic manually initiated software memory check, which includes the software memory that is used for self-diagnosis, as described in DCD Section 7.1.3.10.

Also, as to the surveillance test overlaps, the following is described in DCD Section 7.1.3.10.

> Also, when I/O is checked by manual sensor calibration and output actuation of plant components, the digital components which are self-tested are also re-checked. This provides manual confirmation for the integrity of all digital functions. The coverage of self-diagnosis and manual test is described in Technical Report MUAP-07004, Sections 4.3 and 4.4.

In addition, the Section 1.1 Definition of the US-APWR Technical Specification for CHANNEL OPERATIONAL TEST (and ACTUATION LOGIC TEST) is described as follows:

> A COT (An ACTUATION LOGIC TEST) is a check of the PSMS software memory integrity to ensure there is no change to the internal PSMS software that would impact its functional operation or the continuous self-test function.

And Bases 3.3.1 the US-APWR Technical Specification describes as follows:

> The CHANNEL CALIBRATION, COT, ACTUATION LOGIC TEST and TADOT, which are manual tests, overlap with the CHANNEL CHECK and self-testing and confirm the functioning of the self testing.

The TS periodic manual surveillance tests confirm the accuracy of the self-diagnostic features, thereby complying with 10 CFR Part 50 Appendix B, Criterion XII.

The calibration equipment which will be used to during CHANNEL CALIBRATION as described in Section 4.2 must also satisfy the requirements of 10 CFR Part 50 Appendix B, Criterion XII, "Control of Measuring and Test Equipment," which requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy with necessary limits.

However, the coverage of self-diagnosis is not described clearly in MUAP-07004. Therefore, the description and figures will be revised in MUAP-07004, Section 4.4.

Impact on Safety I&C Technical Report

The following is added to the end of Section 4.3 of MUAP-07004 Rev.6.

> <u>The integrity of safety-related function of the PSMS is continuously checked by their self-diagnostic features. The verification of the self-diagnostic features in the PSMS is confirmed through two diverse test methods:</u>
>
> 1. <u>The verification of the self-diagnostic features in all MELTAC controllers in the PSMS is performed during technical specification periodic surveillance testing through the</u>

combination of the manually initiated CHANNEL OPERATIONAL TEST (COT) – Digital or ACTUATION LOGIC TEST (ALT) – Digital, and the manually conducted CHANNEL CALIBRATION, TRIP ACTUATION DEVICE OPERATIONAL TEST (TADOT) or Safety VDU (S-VDU) test. For each MELTAC controller in the PSMS, the COT-Digital or ALT-Digital checks each bit of the MELTAC Basic Software, which controls the execution of all PSMS functions, including the self-diagnostic features. In addition, for each MELTAC controller in the PSMS, the CHANNEL CALIBRATION, TADOT and/or S-VDU test verifies that the controller can correctly execute program memory instructions.

Since the TS periodic surveillance test manually confirms that each controller can correctly execute program memory instructions, and the TS periodic surveillance test manually confirms that all memory instructions are correct, including the memory that controls self-diagnosis, the combination of these TS surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

2. The TS periodic manual surveillance tests described above (COT-Digital, ALT-Digital, CHANNEL CALIBRATION, TADOT and S-VDU test) confirm the operability of each MELTAC controller in the PSMS through manual testing methods that are diverse from the self-diagnostic features. If a failure is detected that should have been detected by the PSMS self-diagnostic features, a failure of the PSMS self-diagnostic features is also identified.

   The continuous automatic CHANNEL CHECK, which is also a technical specification surveillance, is conducted by the PCMS, based on signals that are processed by the RPS controllers. This test confirms the operability of the RPS controllers through automated testing that is diverse from the MELTAC self-diagnostic features. If a failure is detected that should have been detected by the MELTAC self-diagnostic features, a failure of the MELTAC self-diagnostic features is also identified. The operability of the automatic CHANNEL CHECK is confirmed through periodic manual CHANNEL CALIBRATION.

Section 4.4 of MUAP-07004 Rev.6 is revised as follows:

The integrity of safety-related function of the PSMS is continuously checked by their self-diagnostic features. The continuous PSMS ~~platform and system level~~ self-diagnostic features allow elimination of most manual surveillances required for Technical Specification compliance.

The verification of self-diagnostic features is performed by the combination of (1) manual periodic surveillance tests, that confirm the integrity of all program memory within each MELTAC controller in the PSMS, including the software memory that controls the self-diagnostic functions, and (2) manual periodic surveillance tests that confirm that each controller can correctly execute that program memory. The overlap of these periodic surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

The self-diagnostic features are also confirmed by manual periodic tests and continuous on-line tests that are diverse from the self-diagnostic features. These tests confirm the operability of each MELTAC controller in the PSMS, thereby ensuring that failures have not been missed by the self-diagnostic features.

~~Manual testing and manual calibration is only provided for functions with no self-diagnosis. Manual testing overlaps with self-diagnosis to ensure the integrity of the self-diagnosis.~~

The coverage of self-diagnosis and manual testing is shown in Figure 4.4-4, and the description of each testing in Figure 4.4-4 is described in Section 4.4.1 and 4.4.2.

Sections 4.4.1 and 4.4.2 of MUAP-07004 Rev.6 is revised as follows:

4.4.1 Manual Testing

Manual test features are provided for system level manual actuation of reactor trip and ESF actuation signals, the safety VDU touch screens, binary process inputs and final actuation of plant process components. An additional manual test is conducted to confirm the integrity of the PSMS software memory. Most manual tests may be conducted on-line without full system actuation and without plant disturbance. Each of these manual tests is described in the sections below.

- Manual Reactor Trip (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  The manual reactor trip actuation signals are tested by actuating the conventional switches on the Operator Console ~~and the Remote Shutdown Console~~, one train at a time. Also, TADOTs are conducted from the O-VDU or S-VDU for the separate undervoltage and shunt trip functions of the reactor trip breakers, as shown in Figure 4.4-1. Correct functionality is confirmed by status signals sent from the RTBs to the O-VDU or S-VDU via the RPS controllers. When the reactor trip function is tested one train of reactor trip breakers will open, but the plant will not trip, since breakers in two trains must open to de-energize the CRDMs.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the reactor trip breakers. The test frequency for the reactor trip breakers is described in the US-APWR DCD Chapter 16.

  This test is equivalent to tests of the reactor trip breakers and manual actuation switches in conventional plants. For the PSMS, this test is credited to confirm ~~system~~ input ~~processing~~ and output interfaces, and the program memory processing capability ~~generation~~ of the RPS. This test overlaps with self-diagnostic tests as shown in Figure 4.4-4.

- Manual ESF Actuation (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  The manual ESF actuation signals are tested on-line by actuating the conventional switches on the Operator Console. Correct functionality is confirmed by status signals sent from the PSMS to the O-VDU or S-VDU ~~PCMS HSI~~. These status signals are generated by the PSMS controllers, so there is overlap between the manual test and the platform self-diagnosis. To prevent train level actuation during this test, a Bypass for Manual Test is activated prior to the test. This blocks all manual actuation signals for one train within the ESFAS logic. In accordance with RG.1.47, the block is alarmed with SDCV display to indicate the ESFAS train is bypassed. Removal of the bypass is verified when the alarm has cleared.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

  This test is equivalent to test of the system level manual actuation switches in

conventional plants. For some conventional plants, this test is credited to confirm actuation of the complete system. For the PSMS, this test is credited to confirm input and output interfaces, program memory ~~actuation of the complete system. For the PSMS, this test is credited to confirm input operability including signal~~ processing, communication and display capability of the ESFAS. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Safety VDU Test
  Safety VDU touch screens are tested by manually touching screen targets and confirming correct safety VDU response.

The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

There is no test similar to the safety VDU test in conventional plants. For the PSMS, this test is credited to confirm the touch response and display operability of the S-VDUs, the interface between the S-VDU and the S-VDU controllers, program memory processing, communication and display capability of the S-VDU and the S-VDU controllers. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Analog and Binary Process Inputs (CHANNEL CALIBRATION)
  Analog and binary process inputs are tested in conjunction with manual calibration of the process measurement device, as described in Section 4.4.2, below. CHANNEL CALIBRATION is applicable only to binary process devices that have drift potential, such as undervoltage relays and turbine trip oil pressure switches. Correct functionality is confirmed by reading analog or binary values on any VDU driven by the signal processed by the PSMS.

  This test is equivalent to tests of process measurement devices in conventional plants. For the PSMS, this test is also credited to confirm the process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communication and display capability of the RPS or ESFAS. This test overlaps with platform self-diagnostic tests and automated ~~cross-channel checks~~CHANNEL CHECK as shown in Figure 4.4-4.

- Binary Process Inputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  Binary process inputs to the PSMS are tested periodically by manipulating the process to stimulate a state change in the process monitoring device. This test applies to binary devices with no drift potential, such as main feedwater pump trip status signals. This test is also applicable to binary devices with drift potential, as described above, to grossly check their operability on a more frequent basis than CHANNEL CALIBRATION. Correct functionality is confirmed by status signals sent from the PSMS to any VDU driven by the binary status signal generated from the PSMS. ~~the PCMS HSI. These status signals are generated by the PSMS controllers, so there is overlap between the manual test and the platform self-diagnosis.~~

To avoid spurious actuations during this test, the test is conducted with the train that receives the signal in a bypass mode or with the input channel in a bypass mode. This prevents spurious actuation of this train and it prevents propagation of the input signal state change to other trains.

The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, these tests may be conducted more frequently, if required by the reliability of the process monitoring device. The test frequency for binary process monitoring devices is described in DCD Chapter 16.

This test is equivalent to tests of binary inputs in conventional plants. For some conventional plants, this test is credited to confirm operability of internal system logic functions. For the PSMS, this test is credited to confirm process measurement devices, the interface from those devices to the PSMS, input ~~operability, including~~ signal processing, program memory processing, communication and display capability of the RPS or ESFAS (depending on which controller processes the input). This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Final Actuation Outputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)

Either test, individual or group, also confirms the functionality of the SLS output module and the interface to the plant component. Since the control signals are generated by the SLS controllers, there is overlap between the manual test and the platform self-diagnosis. The Reliability Analysis method, which demonstrates the need to conduct manual tests of the SLS outputs no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the plant process components. The test frequency for the plant process components is described in the US-APWR DCD Chapter 16.

This test is equivalent to tests of system outputs in conventional plants. For the PSMS, this test is also credited to confirm the program memory processing capability ~~complete system operability from manual control input to component actuation~~ of the SLS and the COM controllers, the PSMS output device (including the priority logic in the Power Interface Module), the interface from the PSMS to the plant components and the plant components themselves. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- ~~Software~~ Memory Integrity Check (CHANNEL OPERATIONAL TEST - Digital and ACTUATION LOGIC TEST-Digital)

This function is used during periodic surveillance tests to confirm that the software in the controller is the same as the off-line version, and therefore has not changed. This test confirms the functional integrity of PSMS software applications without the need to perform functional logic tests. The ~~Software Memory Integrity test~~ Menory Integrity Check is conducted with the train for the controller to be tested in a bypass condition.

The Reliability Analysis method, which demonstrates the need to conduct ~~Software Memory Integrity test~~ Menory Integrity Check s no more frequently than once per 24 months, is described in Section 6.5.

This test ensures the integrity of the software credited to execute system safety-related functions, including correct setpoints, constants and logic functions. This test also ensures the integrity of the software credited to execute the self-diagnostic and testing functions. The ~~software memory integrity test~~ Menory Integrity Check overlaps with platform self-diagnostic tests, automated cross-channel tests, and the manual tests described above and as shown in Figure 4.4-4.

Figure 4.4-1 shows the overlap testability for reactor trip. Figure 4.4-2 shows the overlap testability for ESF Actuation. Figure 4.4-3 shows the overlap testability for the safety VDU.

4.4.2 Manual Calibration (CHANNEL CALIBRATION)

PSMS analog input modules and power supplies are continuously checked for failure by the platform self diagnosis. In addition, redundant analog input channels are continuously compared between trains to detect failures and unexpected drift, as discussed in Section 4.3 above.

However, to correct for expected time dependent drift that can commonly affect all redundant analog instruments and analog processing components, these components are periodically checked for accuracy and calibrated as needed. The calibration check for PSMS components is most easily conducted in conjunction with the calibration check for plant process instrument.

Plant process instruments are calibrated using various techniques that stimulate the instrument's sensing mechanism. During the calibration of the instrument, the analog or binary signal generated by the instrument is monitored on any VDU (e.g., operational VDU or safety VDU). This monitoring ensures the functionality of the signal path from the sensor to the PSMS, and the accuracy of the signal processing within the PSMS, including the analog or binary input module and power supplies. Since the VDU signals are generated by the RPS or ESFAS controllers, there is overlap between the manual calibration and the platform self-diagnosis.

Process instruments are calibrated one train at a time. During the calibration the instrument channel is bypassed in the RPS. This prevents erroneous RPS or ESFAS actuation due to a single failure of another channel during the calibration.

The Accuracy Analysis method, described in Section 6.5, demonstrates the need to check the calibration of PSMS power supplies and analog input modules no more frequently than once per 24 months. However, this test may be conducted more frequently, if required by the reliability of the plant process instrumentation. The test frequency for the plant process instrumentation is described in the US-APWR DCD Chapter 16.

This manual calibration is equivalent to tests of process measurement devices in conventional plants. For the PSMS, this manual calibration is credited to confirm the process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communication and display capability of the RPS or ESFAS (depending on which controller processes the input). This test overlaps with platform self-diagnostic tests and automated CHANNEL CHECK as shown in Figure 4.4-4.

Attached Figure 4.4-4 will be added to Section 4.4 of MUAP-07004 Rev.6.

Impact on DCD

The following will be added to the end of Subsection 7.1.3.10 of the DCD Rev.4.

As explained above, periodic surveillance tests manually confirm that all program memory instructions are correct, including the memory that controls self-diagnosis. In addition, when the periodic I/O surveillance tests manually confirm the integrity of all digital functions, they also confirms that each controller can correctly execute program memory instructions, including memory instructions that control the self-diagnostic functions. Therefore, the combination of these surveillance tests confirms that the MELTAC self-diagnosis are fully operable.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Figure 4.4-4 Coverage of Self-diagnosis and Manual Testing

Responses to Request for Additional Information No.720-5539
Revision 2

SPR Section 7.1
Instrumentation and Controls - Introduction

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 720-5539 REVISION 2**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01**
DATE OF RAI ISSUE:	**03/21/2011**

QUESTION NO. : 07.01-28

MHI is requested to address the issue of embedded digital systems in actuated equipment (pumps/valves/etc.) beyond PSMS/PCMS.

US-APWR Software Program Manual, MUAP-07017 (R3), section 3.6.6.4, states, "There are no commercial grade items used in the PSMS including application software. All systems, structures, and components [SSCs] in the PSMS use the qualified MELTAC Platform and Basic Software as described in Technical Report "Safety System Digital Platform –MELTAC– " (MUAP-07005), which are produced and maintained as Basic Components by MELCO under a 10 CFR 50 Appendix B QAP [quality assurance program]."

MHI is requested to address the issue of embedded digital systems in SSCs such as embedded digital devices in pumps, valves, motor control centers, electrical switchgear, and etc. These embedded digital devices/components can be subject to the issues identical to those digital devices/components used in reactor protection and engineered safety features systems. Notably, they can be subject to potential software common cause failures, and sensitive to electromagnetic interference (EMI). These issues can impact the reliability of the SSCs. If the devices/components are part of the safety-related SSCs, their software should conform to the required software quality assurance suitable to safety applications. From the staff's perspective, the embedded digital devices/components are part of plant's I&C systems. It is important that the design control document (DCD) identifies these issues to the COL holders and provides safeguards to address the issues.

ANSWER:
Only MELTAC platform or analog equipment is planned to be used for safety-related equipment. If equipment with embedded software must be employed, the software will be qualified for suitability in Class 1E applications. Qualification methods will depend on the procured equipment. These methods include:

i. The supplier may have a 10 CFR 50 Appendix B quality program with previously qualified Class 1E software.

ii. Other software may be sufficiently simple to allow for 100% testing.
iii. Other software maybe commercially dedicated in accordance with EPRI TR-107330 or TR-106439, as applicable.

Non-safety equipments may contain embedded digital sub-components. For these equipments, MHI's QA program for non-safety equipments is applicable. This program includes configuration control of hardware and software.

For non-safety digital equipment which requires augmented qualification, the application software life cycle commitments described in Appendix D of MUAP-07017 encompass embedded software in the same manner that it encompasses the basic software of the PCMS as described in MHI's response to RAI 668-5273 Question 07.07-32.

Impact on DCD
Title of Subsection 7.1.3.8 will be changed as follows:

7.1.3.8 ~~Unified Architecture~~Scope of Digital System

The following description will be added to Subsection 7.1.3.8 of the DCD Rev. 4.

Embedded software in equipment outside the PSMS and PCMS is addressed as follows:

a. Non-safety equipment – MHI's QA program for non-safety equipments is applicable. This program includes configuration control of hardware and software.

b. Augmented quality equipment – The application software life cycle commitments described in Appendix D of the US-APWR Software Program Manual (Reference 7.1-18) encompass embedded software in the same manner that it encompasses the basic software of the PCMS.

c. Safety-related equipment – Only MELTAC platform or analog equipment is planned to be used. If equipment with embedded software must be employed, the software will be qualified for suitability in Class 1E applications. Qualification methods will depend on the procured equipment. These methods include:

   i. The supplier may have a 10 CFR 50 Appendix B quality program with previously qualified Class 1E software.

   ii. Other software may be sufficiently simple to allow for 100% testing.

   iii. Other software may be commercially dedicated in accordance with EPRI TR-107330 (Reference 7.1-33) or TR-106439 (Reference 7.1-34), as applicable.

d. Safety or non-safety equipment credited in the diversity and defense-in-depth analysis – Only analog equipment is planned to be used. If equipment with embedded software must be employed, conformance to the diversity and defense-in-depth analysis will be demonstrated.

e. All qualification and analysis documentation will be maintained in accordance with MHI's quality assurance program.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Responses to Request for Additional Information No.700-5406
Revision 2

SPR Section 7.8
Diverse Instrumentation and Control Systems

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 700-5406 REVISION 2**
SRP SECTION:	**07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS**
APPLICATION SECTION:	**07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.08-16

In the Technical Report, "Defense-in-Depth and Diversity Coping Analysis," (MUAP- 07014) Revision 2, MHI states that they will be adding additional information identified in the technical report as part of a future revision of the DCD. MHI has identified the following changes to be incorporated in a future DCD revision:

> Section 3.5.3 "Erroneous Signals," for "(1) Reactor Trip, Turbine Trip and Main Feedwater Isolation," states that the DCD will be revised to reflect a change made from earlier descriptions of the DAS blocking logic for reactor trip, turbine trip and main feedwater isolation that appear in the current DCD revision and MUAP-07006.
>
> Section 3.5.3 "Erroneous Signals," for "(3) Main Steam Line Radiation (N-16) Alarm," states that the blocking logic for the N-16 alarm is not described in the DCD or MUAP-07006 and that the DCD will be revised to add a description.
>
> Section 3.5.3 "Erroneous Signals," for "(5) Low-Low Pressurizer Pressure Alarm," states that this alarm and blocking logic are not described in the DCD or MUAP- 07006 and the DCD will be revised to add the alarm details.

The staff requests that the applicant address the above missing information and incorporate or identify where this additional information is located in the DCD.

ANSWER:

The DAS blocking logic for reactor trip, turbine trip and main feedwater isolation has been included in Subsection 7.8.1.2.1 of the DCD Rev. 3. This blocking logic is provided for consideration against partial CCF condition. For detailed consideration, see Section 3.5 of D3 Coping Analysis Technical Report MUAP-07014.

The second paragraph of Subsection 3.5.3 of MUAP-07014 will be revised as follows to keep consistency between the DCD and MUAP-07014:

> The DAS automatic reactor trip, automatic turbine trip and automatic main feedwater isolation functions are blocked only when the DAS receives signals hardwired directly from the reactor trip switchgear and low turbine emergency oil pressure signals ~~hardwired directly from the turbine isolation valves~~ (ie. down stream of the postulated digital CCF). These hardwired signals indicate that the required number of circuit breakers and ~~valves~~ turbine emergency trip oil pressure trip signal have correctly actuated.

The description of blocking logic for the N-16 alarm and Low-Low Pressurizer Pressure Alarm will be added to the DCD Rev. 4. In addition, a description of the DAS high-high steam generator alarm will be added.

Impact on DCD

Second paragraph of Subsection 7.8.1.1.2 of the DCD Rev. 4 will be revised as follows;

> Failure information about the DAS, such as power supply failure, or module deenergization or removal, is alarmed as a "DAS failure summary alarm" on the Alarm VDU in the MCR. The configuration of the DAS alarms is described in Topical Report MUAP-07006 Section 6.2.2.1. High main steam radiation (N-16), ~~and~~ high-high steam generator water level and low-low pressurizer pressure are alarmed and indicated on DHP. DAS alarms for high main steam radiation (N-16), high-high steam generator water level and low-low pressurizer pressure are blocked during non CCF conditions, as described in Subsection 3.5.3 of the D3 Coping Analysis Technical Report (Reference 7.8-2). These blocks prevent unwanted DAS alarms. The blocking logic considers both complete CCF and partial CCF conditions. Section 3.5 of D3 Coping Analysis Technical Report (Reference 7.8-2) provides the analysis for these conditions. Technical Report MUAP-07014 provides the specific information of the alarms credited for D3 coping analysis.

Following sentence will be added after the last paragraph of Subsections 7.8.1.2.1 and 7.8.1.2.2 of the DCD Rev. 4;

> The blocking logic considers both complete CCF and partial CCF conditions. Section 3.5 of D3 Coping Analysis Technical Report (Reference 7.8-2) provides the analysis for these conditions.

Impact on R-COLA
There is no impact on the R-COLA

Impact on S-COLA
There is no impact on the S-COLA

Impact on PRA
There is no impact on the PRA

Responses to Request for Additional Information No.701-5229
Revision 0

SPR Section 7.9
Data Communication Systems

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.701-5229 REVISION 0**
SRP SECTION:	**07.09 – DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.09-19

MHI is requested to additional information to demonstrate how staff guidance in DI&CISG-04, Staff Position 1.8, is met. Staff Position 1.8 of ISG-04 states that "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."

US-APWR DCD Tier 2, Section 7.9.2.7 only provides a general description of the DCS communication independence. MHI is requested to provide all types of data exchange (voting logic, bypass, etc.,) between safety divisions. For each data exchange, demonstrate how communication independence between safety divisions is maintained in sufficient detail (by expanding the currently submitted information).

ANSWER:

MHI agrees with the staff's request.

Additional description to demonstrate ISG-04 conformance will be described in Subsection 7.9.2.7 of the DCD Rev.4 (Refer to RAI 07.09-12).

The detailed conformance to the Staff Position 1.8 is described in Subsection F.1.2.3 and F.2.2.3 of Technical Report MUAP-07004.

Impact on DCD
A design summary of the interdivisional communication independence will be added to Subsection 7.9.2.7 of the DCD Rev.4 as shown in RAI 07.09-12.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 701-5229 REVISION 0**
SRP SECTION:	**07.09 – DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.09-20

MHI is requested to demonstrate in additional detail how guidance in ISG-04, Staff Position 1.8, is met. Staff Position 1.8 of ISG-04 states that "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."

Section 3.2.8 of TR JEXU-1015-1009-P (R3) and Appendix E, Section E1, "Staff Position 1.8," of TR MUAP-07004-P (R5) provide conflicting information with regard to whether the priority logic is being implemented at application level. The former document discusses logic implementation at the application level (the latter document), while the latter refers to the former document.

MHI is requested to provide all data exchanged between redundant safety divisions or between safety and nonsafety divisions, priority logic for each such exchange, and describe how data exchange for each applicable input would not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

ANSWER:

MHI interprets Staff Position 1.8 as requiring communication independence. Therefore, Appendix E of MUAP-07004 is correct as written. JEXU-1015-1009 will be revised to eliminate the discussion of functional independence through priority logic. The priority logic used to ensure functional independence is described in compliance to Staff Positions 2 and 3.

The detailed conformance to this Staff Potion 1.8 is described in Subsections F.1.2.3 and F.2.2.3 "Communication Independence" in Appendix F of the Safety I&C Technical Report MUAP-07004 Rev.6.

Impact on DCD
A design summary of the interdivisional communication independence will be added to Subsection 7.1.4 of the DCD Rev.4 as shown in as shown in RAI 07.01-25, and Subsection 7.9.2.7 of the DCD Rev.4 as shown in RAI 07.09-12.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 701-5229 REVISION 0**
SRP SECTION:	**07.09 – DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.09-21

Staff Position 1.3 of ISG-04 states, in part, that "Receipt of information from out-side the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division."

MHI is requested to demonstrate in additional detail how the guidance in ISG-04, Staff Position 1.3, is met. The demonstration should include whether potential software coding errors from non-safety operational VDUs could affect one or more than one safety division and how to mitigate these problems.

ANSWER:

MHI agrees with the staff's request.

Additional description to demonstrate ISG-04 conformance will be described in Subsection 7.9.2.7 of the DCD Rev.4 (Refer to RAI 07.09-12).

The detailed conformance to the Staff Position 1.8 is described in Subsections F.1.2.4 and F.2.2.4 in Appendix F of the Safety I&C Technical Report MUAP-07004 Rev.6. (Refer to RAI 07.01-25)

Impact on DCD
A design summary of the interdivisional communication independence will be added to Subsection 7.9.2.7 of the DCD Rev.4 as shown in RAI 07.09-12.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 701-5229 REVISION 0**
SRP SECTION:	**07.09 – DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.09**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07.09-22

MHI is requested to demonstrate in additional detail how guidance in ISG-04, Staff Position 1.12, is met. Staff Position 1.12 states, in part, that "Communication faults should not adversely affect the performance of required safety functions in any ways. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A."

DCD Tier 2, Section 7.9.2.7 refers to Appendix A of Technical Report MUAP-07004 for methods used to ensure independence between safety trains and between safety and non-safety systems. TR MUAP-07004, Appendix A, Section A.5.6.3.1 states, in part, that "Signals from the PSMS are transmitted to the PCMS and DAS through conventional analog/binary isolation devices or fiber optic cables. Conventional analog/binary isolators are part of the safety system and are tested to confirm that credible failures on the non-safety side of the isolation device do not prevent the PSMS from meeting its performance requirements."

MHI is requested to address the following:

- For communication independence, TR MUAP-07004 states only that the communication modules are separate from processing modules. It is not clear that this method alone can prevent all communication errors. MHI is requested to address how the effects of the communication errors listed below are mitigated. Provide a separate explanation for each of the errors listed.
    - Data corruption[1]
    - Unintended repetition[1]
    - Incorrect sequence[1]
    - Data loss[1]
    - Unacceptable delay[1]
    - Unexpected data insertion[1]
    - Invalid data "masquerade" as valid ones[1]
    - Incorrect address/wrong destination[1]
    - Broadcast storm[1]
    - Commission fault
    - Inconsistency[1]
    - Excessive jitter[1]
    - Data collision[1]
    - Buffer overflow[1]

- Out of range[1]
- Incorrect ordering[1]
- Out of sync[1]
- Incorrect encoding/decoding[1]
- Interruption

[1] Source: RG 1.152, DI&C-ISG-04, and NUREG/CR 6991, "Design Practices for Communications and Workstations in Highly Intergraded Control Rooms"

ANSWER:

A description of the effects of the following types of communication errors has been provided in MELTAC Platform Basic Software Safety Report (JEXU-1015-1009 Rev.3), Subsection 3.3, Delectability of Communication Faults.

- Data corruption
- Unintended repetition
- Incorrect sequence
- Data loss
- Unacceptable delay
- Unexpected data insertion
- Incorrect address/wrong destination
- Broadcast storm
- Buffer overflow
- Out of range
- Incorrect ordering

JEXU-1015-1009 will be revised to add descriptions of the effects of the following types of communication faults and their mitigations.

- Invalid data "masquerade" as valid ones
- Commission fault
- Inconsistency
- Excessive jitter
- Data collision
- Out of sync
- Incorrect encoding/decoding
- Interruption

JEXU-1015-1009 will be renamed and the content will be limited to evaluation of conformance to ISG-04 as discussed in the second response to RAI 655-5220.

For invalid data masquerade as valid messages (i.e., those that pass all communication error checks defined in this Staff Position) that contain undetected erroneous or spurious commands, the priority logics ensure the safety-related functions of the PSMS cannot be inhibited by the non-safety signals as shown in Appendix D of the Safety I&C Technical Report MUAP-07004 Rev.6. Therefore, regardless of any normal or spurious component positioning from the PCMS, the RPS, ESFAS and SLS can perform all necessary safety-related functions.

Additional description to demonstrate ISG-04 conformance will be described in Subsection 7.9.2.7 of the DCD Rev.4 (Refer to RAI 07.09-12).

The detailed conformance to the Staff Position 1.12 is described in Subsections F.1.2.3 and F.2.2.3 in Appendix F of the Safety I&C Technical Report MUAP-07004.

For the PSMS design, Appendix E, Section E1, Staff position 1.12 of Technical Report MUAP-07004 is revised as follows.

Staff Position 1.12

Requirement
Communication faults should not adversely affect the performance of required safety-related functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the followings: Messages may be corrupted due to errors in communications processors, errors introduce in buffer interface, errors introduced in the transmission media, or from interface or electrical noise. • Messages may be repeated at an incorrect point in time. • Messages may be sent in the incorrect sequence. • Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of message. • Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages. • Messages may be inserted into the communication medium from unexpected or unknown sources. • Messages may be sent to wrong destination, which could treat the message as a valid message. • Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption. • Messages may appear valid, but data may be placed in correct locations within the message. • Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm). • Message headers or addresses may be corrupted.
Analysis for Interdivisional Communications among Safety-related Systems ~~Divisions~~
[ ]

Evaluation
Conforms

Impact on DCD
A design summary of the interdivisional communication independence will be added to Subsection 7.9.2.7 of the DCD Rev.4 as shown in RAI 07.09-12.

Impact on R-COLA
There is no impact on the R-COLA

Impact on S-COLA
There is no impact on the S-COLA

Impact on PRA
There is no impact on the PRA

Responses to Request for Additional Information No.710-5493
Revision 2

SPR Section 7.9
Data Communication Systems

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.710-5493 REVISION 2**
SRP SECTION:	**07.09 – DATA COMMUNICATION SYSTEMS**
APPLICATION SECTION:	**07.01, 07.09**
DATE OF RAI ISSUE:	**03/07/2011**

QUESTION NO. : 07.09-23

The staff's 10 CFR 50 review of Chapter 7 is focused on addressing the Secure Development and Operational Environment (SDOE) per RG 1.152. RG 1.152 has been in a process of revision for the past year, with the latest draft (DG-1249 on the NRC's website, ML100490539) having been proposed in June 2010 and presented to the ACRS on February 23, 2011. This revision, along with RG 5.71, will make changes in how 'cyber security' is handled in nuclear power plant safety systems. Specifically, with the issuance of 10 CFR 73.54 and its companion staff guidance, RG 5.71, 'cyber security' is reviewed under Chapter 13 during COL reviews. RG 1.152, Revision 3, and RG 5.71 were discussed at the public meeting on February 23, 2011. MHI currently is committed to Revision 2 of RG 1.152. Staff requests MHI to consider following the updated guidance of the future Revision 3. If MHI agrees, the NRC staff requests MHI to remove all references to cyber security in Chapter 7 DCD and technical reports. Some examples from MHI's submittals for Chapter 7 that references cyber security include: US APWR DCD, Rev 2, Sections 7.1.3.17, 7.7.2.10, and 7.9.2.6; MUAP-07005-P(R6), Section 6.1.6.

ANSWER:
MHI agrees with staff's requests and will follow the updated guidance of RG 1.152, Revision 3.

MHI has removed references to cyber security from DCD Tier 2 Chapter 7 (Subsections 7.1.3.1.7, 7.7.2.10 and 7.9.2.6) and has included a new COL item 7.9 (1) in DCD Rev.3. These changes have been submitted as UTR Rev.7.

Also, references to cyber security from Tier 1 Subsection 2.5.1.1 (Design Description and Table 2.5.1-6 #24) has been removed in DCD Rev.3.

In addition, all references to cyber security in Technical Reports is removed or the term "cyber security" is replaced with other words as follow:

Section 3.3 (13) of MUAP-07004 Rev.6 is revised as follows:

The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment complies with these requirements. The life cycle process for the digital platform software is described in the Digital Platform Topical Report, MUAP-07005. The life cycle process for the system application software is described in MUAP-07017~~ and briefly summarized in this report. The methods used for controlling cyber threats throughout the life cycle are described in these documents~~.

The description of Subsection 4.2.5 of MUAP-07004 Rev.6 is deleted as follows:

~~• Additional protection against cyber threats~~

~~The PCMS and PSMS will be controlled under the most stringent administrative controls for cyber security. There is only one-way communication to other systems that are not under these same controls.~~

The description of Subsection 4.2.7 of MUAP-07004 Rev.6 is revised as follows:

~~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.~~

The description of Sybsection 5.1.1 of MUAP-07004 Rev.6 is deleted as follows:

~~• Additional protection against cyber threats~~

Subsection 6.4.3 of MUAP-07004 will be deleted.

The description of Section 8.0 of MUAP-07004 Re.6 is revised as follows:

6. ~~Cyber Security Program for Nuclear Power Reactors, NEI 04-04, February 2005~~ Deleted.

The description of Section B.5.6 of MUAP-07004 Rev.6 is deleted as follows:

e. ~~Additional protection against cyber threats~~ Deleted

~~The PCMS and PSMS will be controlled under the most stringent administrative controls for cyber security. There is only one-way communication to other systems that are not under these same controls.~~

The description of Subsection 6.1.6 of MUAP-07005 Rev.6 is revised as follows:

6.1.6 ~~Cyber Security~~ Secure Development Environment Management

The ~~Cyber Security~~ Secure Development Environment Management Program is in accordance with NPD Standard [Q-6403], which conforms to RG1.152. The overall ~~Cyber Security~~ Secure Development Environment Management Program ensures the followings:

The title of Subsection 6.1.6.3 of MUAP-07005 Rev.6 is revised as follows:

6.1.6.3 ~~Cyber Security~~ Secure Development Environment Measures During System Operation

The description of Subsection 6.1.6.4 of MUAP-07005 Rev.6 is revised as follows:

6.1.6.4 Existing Platform ~~Cyber Security~~ Secure Development Environment Assessments based on Original UCP

[

]

In the same manner, all references to cyber security in MUAP-07017 and JEXU-1012-1132 will be removed or the term "cyber security" will be replaced with other words in the next revision.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
Corresponding change to adding a new COL item 7.9 (1) will be incorporated to R-COLA.

Impact on S-COLA
Corresponding change to adding a new COL item 7.9 (1) will be incorporated to S-COLA.

Impact on PRA
There is no impact on the PRA.

Enclosure 5

Docket No. 52-021
UAP-HF-11127

Amended Response to Request for Additional Information for Chapter 7

April 2011

Non-Proprietary Version

This Enclosure includes following response of RAIs

RAI NO.: 568-4588 Revision 1, Question No.: 07.05-18

RAI NO.: 656-5127 Revision 2, Question No.: 07.05-20

RAI NO.: 239-2033 Revision 0, Question No.: 07.06-3

RAI NO.: 239-2033 Revision 0, Question No.: 07.06-16

RAI NO.: 638-5032 Revision 0, Question No.: 07.06-21

RAI NO.: 688-5273 Revision 2, Question No.: 07.07-30

RAI NO.: 688-5273 Revision 2, Question No.: 07.07-31

RAI NO.: 677-5325 Revision 2, Question No.: 07.08-11

RAI NO.: 665-5220 Revision 1, Question No.: 07.14 Branch Technical Position-42

RAI NO.: 593-4565 Revision 1, Question No.: 07.21 Branch Technical Position-1

RAI NO.: 593-4565 Revision 1, Question No.: 07.21 Branch Technical Position-2

RAI NO.: 593-4565 Revision 1, Question No.: 07.21 Branch Technical Position-4

Safety I&C 1st Set, RAI-30 (UAP-HF-08114 R1)

MELTAC 1-MELTAC (UAP-HF-09393 R1)

MELTAC 5-MELTAC (UAP-HF-09393 R1)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 568-4588 REVISION 1**
SRP SECTION:	**07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.05**
DATE OF RAI ISSUE:	**4/13/2010**

QUESTION NO.: 07.05-18
Provide a complete explanation of the differences between Table 7.5-3, Post Accident Monitoring System (PAMS) Variables, and all information in 1) Type A variables and those found in Table 3.3.3-1, of NUREG-1431 and 2) Types B through E variables and those found in Regulatory Guide 1.97 Rev. 3, Table 3. (This request was discussed in the public meeting with MHI and the NRC staff on March 16, 2010)

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13, requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for accident conditions as appropriate to ensure adequate safety. GDC 64 requires, in part, means for monitoring the reactor containment atmosphere, spaces containing components to recirculate loss-of-coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released as a result of postulated accidents. One bounding list of PAMS instruments are those identified in the standard technical specifications for operating reactors and the list of PAMS instruments in Regulatory Guide 1.97, Revision 3. As stated in RAI No. 463-3746, Question No. 16-299, Table 7.5-3 provides a list of PAMS variables that has been developed based on a combination of previous revisions of RG 1.97, Japanese domestic and US operation plant experience and EOPs, and known differences between the US-APWR and current operating PWRs. The staff noted that some instrumentation in the US-APWR bounding list were absent when compared to the PAMS instrument lists in the standard technical specifications and Regulatory Guide 1.97, Revision 3. Additionally, there was no basis mentioned for the absent instrumentation. Substantiate to the staff that the list of PAMS variables in Table 7.5-3 is indeed a bounding list and complete. Specifically, identify and explain the reason for the missing instrumentation as compared to Table 3.3.3-1 of NUREG-1431 and Table 3 of Regulatory Guide 1.97, Revision 3.

ANSWER:
As stated in the response to RAI No. 463-3746, Question 16-299, the US-APWR PAM list provided in DCD Table 7.5-3 was developed to be in compliance with the guidance of RG 1.97 Rev. 4 and IEEE 497-2002. MHI utilized a combination of previous versions of RG 1.97, Japanese domestic and US operational experience and emergency procedures, and known differences between current operating plants and the US-APWR design to develop a bounding and complete PAM list for the US-APWR. The following sections describe the selection basis for the Type A, B, C, D, and E variables for the US-APWR.

- **Type A**

NUREG-1431 Table 3.3.3-1 provides a generic list of PAM instrumentation for a Westinghouse NSSS plant based on the guidance in RG 1.97 Rev. 3; however, a reviewer's note in NUREG-1431 requires that

this table be amended by individual licensees to add all RG 1.97 Type A and Category 1 non-Type A variables to this generic list in accordance with the plant's RG 1.97 Safety Evaluation Report. Therefore the PAM list provided in NUREG-1431 is a minimal list of Category 1 variables (any Type) for a typical Westinghouse NSSS plant.

MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type A accident monitoring variables for the US-APWR. IEEE 497-2002 defines Type A variables as follows.

> Type A variables are those variables that provide the primary information required to permit the control room operating staff to:
>
> a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
> b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

As described in the response to RAI No. 07.05-9 in MHI letter UAP-HF-09196 dated April 28, 2009, the SGTR is the only event that assumes planned operator actions using the Type A variables listed in DCD Table 7.5-3. Planned operator actions required for other events are initiated by an alarm or they are based on a time limit.

In the event of an SGTR, the DBA analysis assumes the following specific operator actions:

- Identify and Isolate Ruptured SG
- Cool Down Primary Coolant System
- Depressurize Primary Coolant System to Equalize Pressure between Primary and Secondary
- Terminate Safety Injection Flow

Some Type A variables are monitored before the operator takes the above manual actions. These Type A variables are shown in Table A.

Regarding the LOCA event, RWSP level is an important indication in some currently operating plants because operator action is needed to realign the injection of ECCS from the RWSP to the containment sump before the RWSP becomes empty. In the US-APWR, the RWSP is located at the bottom of the containment and the suction of both the SIP and CS/RHRP is the RWSP from the beginning. Therefore, it is not necessary to confirm the RWSP level during the LOCA event and this variable is not included as a Type A variable for the US-APWR.

The analyses of the Steam Line Break (SLB) and Feedwater Line Break (FLB) assume EFW isolation from a faulted SG. However, this action is performed automatically by the low steam line pressure signal EFW isolation function. Therefore, there are no PAM instruments related to operator actions assumed in the SLB and FLB analyses.

In all DBA analysis, except for the SGTR previously discussed, explicit operator actions are not assumed based on primary information from PAM instruments. However, SI termination and long-term core cooling from secondary heat sink are necessary to bring the plant to cold shut down conditions. Operator actions for SI termination and core cooling are already included in the operator actions assumed in the SGTR analysis. Therefore, the instruments associated with these functions have already been included in the bounding PAM list provided in DCD Table 7.5-3.

Table A compares all of the Category 1 variables (any Type) functions in NUREG-1431 Table 3.3.3-1 to the US-APWR Type A variables listed in DCD Table 7.5-3 and summarizes the bases for differences between the Type A variables in the MHI PAM list and the Category 1 PAM for a typical Westinghouse 4-loop PWR plant.

- **Type B**

Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type B variables to monitor. However, MHI

utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type B accident monitoring variables for the US-APWR. Therefore, there are some differences between the RG 1.97 Rev. 3 and MHI Type B variable lists. IEEE 497-2002 defines Type B variables as follows.

> Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions. Any plant critical safety functions addressed in the EPGs or the plant specific EOPs that are in addition to those identified above shall also be in included.

The ultimate goal of the plant safety systems is to prevent an uncontrolled release of radioactive material. This is accomplished by ensuring that certain parameters related to plant critical safety functions are not exceeded. The US-APWR Functional Restoration Guidelines (FRGs) provide protection of these plant critical safety functions. The FRGs establish predefined function-related restoration strategies for responding to emergency transients where the initiating event is unknown and the transient is not predefined. The restoration strategies utilize available plant equipment to restore the parameters used for entry conditions to values sufficient to ensure protection of the plant critical safety function.

The most essential and important methods of protecting the plant critical safety functions are the concepts of (1) Shutdown, (2) Cooldown, and (3) Contain, where each of these concepts is defined as follows.

- "Shutdown" means that the plant should be subcritical in order to reduce the thermal energy in the core to as low as the decay heat level during the emergency conditions.
- "Cooldown" means that the heat should be removed from the core (fuel rods) to protect the integrity of the cladding. Decay heat should be removed from the Reactor Coolant System (RCS).
- "Contain" refers to the integrity of the RCS and containment vessel. Heat should be removed from the containment to the ultimate heat sink.

The US-APWR Type-B PAM variables are selected from the concept of the FRGs described above. The Type B functional category of "Reactivity Control" is related to the FRG concept of "Shutdown". The functional categories of "Core Cooling" and "Reactor Coolant System Integrity" are related to the FRG concept of "Cooldown". And the Type B functional category "Containment Integrity" is related to the FRG concept "Contain".

Table B describes the bases for the differences between the Type B variables included in the MHI PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

- **Type C**

Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type C variables to monitor. However, MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type C accident monitoring variables for the US-APWR. Therefore, there are some differences between the RG 1.97 Rev. 3 and MHI Type C variable lists. IEEE 497-2002 defines Type C variables as follows.

> Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

Table C shows the bases for the differences between Type C variables in the MHI PAM list and the variables included in RG 1.97 Rev. 3 Table 3.

- **Type D**

Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type D variables to monitor. However, MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type D accident monitoring variables for the US-APWR. Therefore, there are some differences between the RG 1.97 Rev. 3 and MHI Type D variable lists. IEEE 497-2002 defines Type D variables as follows.

> Type D variables are those variables that are required in procedures and LBD to:

a) Indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events.
b) Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
c) Verify safety system status.

The US-APWR Type D variable list is almost identical to the Type D variables included in Table 3 of RG 1.97 Rev.3. One notable departure is the variable to monitor flow in the low pressure injection system. The accumulators and high head safety injection system in US-APWR are designed to replace the entire low head safety injection function; therefore, this system is not part of the US-APWR design and this monitoring variable is not applicable to the US-APWR.

Another notable departure from the RG 1.97 Rev.3 Type D variable list involves the chemical volume and control system (CVCS). The high head injection system and emergency letdown system of the US-APWR has a required safety function to ensure a means for feed and bleed for boration and make up water for compensation of shrinkage if the normal CVCS is unavailable. Since the US-APWR SI system performs the necessary RCS inventory and boration functions, the CVCS-related monitoring variables are not necessary for the US-APWR design and thus not included in the MHI Type D variable list.

Table D shows the bases for differences between Type D variables in the MHI PAM list and Type D PAM included in RG 1.97 Rev. 3 Table 3.

• **Type E**
Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type E variables to monitor. However, MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type E accident monitoring variables for the US-APWR. Therefore, these are some differences between the RG 1.97 Rev. 3 and MHI Type E variable lists. IEEE 497-2002 defines Type E variables as follows.

> Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.
>
> The selection of these variables shall include, but not be limited to, the following:
> a) Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).
> b) Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).
> c) Monitor radiation levels and radioactivity in the plant environs.
> d) Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

Table E shows the bases for differences between Type E variables in the MHI PAM list and Type E PAM included in RG 1.97 Rev. 3 Table 3.

The Safety I&C Technical Report MUAP-07004 is revised as follows:

The following sentence is added to second paragraph of Subsection 4.2.4.c of MUAP-07004 Rev.6.

> The bases for the selection of the US-APWR PAM variables is described in Appendix H.

The Appendix H is added in MUAP-07004 Rev.6 as follows:

Appendix H Bases for the Selection of the US-APWR PAM Variables

The US-APWR PAM list provided in the DCD Table 7.5-3 was developed to be in

compliance with the guidance of RG 1.97 Rev. 4 and IEEE 497-2002, which is endorsed by RG 1.97 Rev. 4. The US-APWR PAM variables are utilized by a combination of previous versions of RG 1.97, Japanese domestic and US operational experience and emergency procedures, and known differences between current operating plants and the US-APWR design to develop a bounding and complete PAM list for the US-APWR. The following subsections describe the selection basis for the variables included in the DCD Table 7.5-3.

Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type B, C, D, and E variables to monitor. However, The US-APWR PAM variables are utilized by the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type B, C, D, and E accident monitoring variables for the US-APWR. Therefore, there are some differences between the RG 1.97 Rev. 3 and the US-APWR PAM lists for these variable types. Additionally, Type A variables were not included in RG 1.97 Rev. 3, so a slightly different methodology was utilized to select the bounding list of Type A variables for the US-APWR. A discussion of the variable selection basis for each type of PAM variable is described below. The specific basis for the inclusion or exclusion of a specific variable in the DCD Table 7.5-3 is provided in Tables H.1-1 through H.5-1 for each variable classification type.

The variables required by 10 CFR 50.34(f)(2)xvii are included in RG 1.97 Rev.3. Therefore, conformance to 10 CFR 50.34(f)(2)xvii are also shown in Tables H.1-1 through H.5-1

H.1 Type A Variables

NUREG-1431 Table 3.3.3-1 provides a minimal list of Category 1 variables (any Type) for a typical Westinghouse NSSS plant based on the guidance in RG 1.97 Rev. 3. The US-APWR PAM variables are utilized this list as an initial starting point for the US-APWR Type A PAM list. Then the US-APWR PAM variables are utilized by the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the specific Type A accident monitoring variables for the US-APWR. IEEE 497-2002 defines Type A variables as follows.

> Type A variables are those variables that provide the primary information required to permit the control room operating staff to:
>
> a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety-related systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
>
> b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

The SGTR is the only event that assumes planned operator actions using the Type A variables listed in Table 7.5-3. Planned operator actions required for other events are initiated by an alarm or they are based on a time limit.

In the event of an SGTR, the DBA analysis in Subsection 15.6.3 assumes the following specific operator actions:

- Identify and Isolate Ruptured SG
- Cool Down Primary Coolant System
- Depressurize Primary Coolant System to Equalize Pressure between Primary and Secondary

- Terminate Safety Injection Flow

Some Type A variables are monitored before the operator takes the above manual actions. These Type A variables are shown in the DCD Table 7.5-11.

Regarding the LOCA event, RWSP level is an important indication in some currently operating plants because operator action is needed to realign the injection of ECCS from the RWSP to the containment sump before the RWSP becomes empty. In the US-APWR, the RWSP is located at the bottom of the containment and the suction of both the SIP and CS/RHRP is the RWSP from the beginning. Therefore, it is not necessary to confirm the RWSP level during the LOCA event and this variable is not included as a Type A variable for the US-APWR.

The analyses of the Steam Line Break (SLB) in the DCD Subsection 15.1.5 and Feedwater Line Break (FLB) in the DCD Subsection 15.2.8 assume EFW isolation from a faulted SG. However, this action is performed automatically by the low main steam line pressure signal EFW isolation function. Therefore, there are no PAM instruments related to operator actions assumed in the SLB and FLB analyses.

In all DBA analysis, except for the SGTR previously discussed, explicit operator actions are not assumed based on primary information from PAM instruments. However, SI termination and long-term core cooling from secondary heat sink are necessary to bring the plant to cold shut down conditions. Operator actions for SI termination and core cooling are already included in the operator actions assumed in the SGTR analysis. Therefore, the instruments associated with these functions have already been included in the bounding PAM list provided in the DCD Table 7.5-3.

Table H.5-1 compares all of the Category 1 variables (any Type) functions in NUREG-1431 Table 3.3.3-1 to the US APWR Type A variables currently listed in the DCD Table 7.5-3 and summarizes the bases for differences between the Type A variables in the US-APWR PAM list and the Category 1 PAM for a typical Westinghouse 4 loop PWR plant. The above described methodology serves as the basis for the selection of the US-APWR Type A PAM variables included in the DCD Table 7.5-3.

H.2 Type B Variables

IEEE 497-2002 defines Type B variables as follows.

> Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions. Any plant critical safety functions addressed in the EPGs or the plant specific EOPs that are in addition to those identified below shall also be included.

The plant critical safety functions are those functions necessary to prevent a direct and immediate threat to public health and safety. The following basic critical safety functions are defined in RG 1.97 Rev. 3 and IEEE 497-2002:

- Reactivity Control,
- Core Cooling,
- Maintaining Reactor Coolant System Integrity,
- Maintaining Containment Integrity (including radioactive effluent control).

Plant safety is accomplished by ensuring that certain parameters related to the plant critical safety functions are not exceeded. The US-APWR Emergency Response Guidelines (ERGs) provide protection of these plant critical safety functions. The ERGs establish predefined function-related restoration strategies for responding to emergency transients where the initiating event is unknown and the transient is not predefined. The restoration strategies utilize available plant equipment to restore the parameters used for entry conditions to values sufficient to ensure protection of the plant critical safety function.

The bounding US-APWR Type B PAM variables are selected ensure availability of the variables needed to implement the functional restoration portion of the ERGs as described above. Table H.2-1 describes the bases for the differences between the Type B variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.3 Type C Variables

IEEE 497-2002 defines Type C variables as follows.

> Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

Table H.3-1 describes the bases for the differences between the Type C variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.4 Type D Variables

IEEE 497-2002 defines Type D variables as follows.

> Type D variables are those variables that are required in procedures and LBD to:
>
> a) Indicate the performance of those safety-related systems and auxiliary supporting features necessary for the mitigation of design basis events.
>
> b) Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
>
> c) Verify safety-related system status.

The US-APWR Type D variable list is almost identical to the Type D variables included in Table 3 of RG 1.97 Rev.3. One notable departure is the variable to monitor flow in the low pressure injection system. The accumulators and high head safety injection system in US-APWR are designed to replace the entire low head safety injection function; therefore, this system is not part of the US-APWR design and this monitoring variable is not applicable to the US-APWR.

Another notable departure from the RG 1.97 Rev.3 Type D variable list involves the chemical volume and control system (CVCS). The high head injection system and emergency letdown system of the US APWR has a required safety-related function to ensure a means for feed and bleed for boration and make up water for compensation of shrinkage if the normal CVCS is unavailable. Since the US-APWR SI system performs the necessary RCS inventory and boration functions, the CVCS-related monitoring variables are not necessary for the US-APWR design and thus not included in the US-APWR Type D

variable list.

Table H.4-1 describes the bases for the differences between the Type D variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.5 Type E Variables

IEEE 497-2002 defines Type E variables as follows.

> Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.
>
> The selection of these variables shall include, but not be limited to, the following:
>
> a) Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).
>
> b) Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).
>
> c) Monitor radiation levels and radioactivity in the plant environs.
>
> d) Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

Table H.5-1 describes the bases for the differences between the Type E variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

Also, Tables A to E is added as Tables H.1-1 to H.5-1 of MUAP-07004, respectively.

Impact on DCD

There are typographical mistakes in the Tier 2, DCD Chapter 7, Table 7.5-3. DCD Table 7.5-3 will be revised as shown below to add an additional category to Reactor Coolant Pressure, Containment Pressure, and Containment High Range Area Radiation.

Table 7.5-3 PAM Variables
(Sheet 1 of 3)

Variable	Range	Monitored Function or System	Quantity	Type
Reactor Coolant Pressure	0 to 3000 psig	Core Cooling Maintaining RCS Integrity	2	A,B, C,D
Containment Pressure*2	-7 to 80 psig	Maintaining RCS Integrity Maintaining Containment Integrity	4	B,C, D

Table 7.5-3 PAM Variables
(Sheet 2 of 3)

Variable	Range	Monitored Function or System	Quantity	Type
Containment High Range Area Radiation*2	1 to 1E-7 R/hr	Containment Radiation	4	C,E

The description of Section 7.5.1.1 in DCD Rev.4 will be revised as follows:

IEEE Std 497-2002 (Reference 7.5-2) provides ~~selecting and categorizing~~ principles for the selection and categorization of PAM variables. Table 7.5-1 provides a summary of these selection criteria and source documents for each PAM variable type.

Table 7.5-2 provides the US-APWR design attributes ~~for~~ applied to each variable type.

Table 7.5-3 provides a list of US-APWR PAM variables, their ranges, monitored functions or systems, quality and variable type. ~~To further clarify the US-APWR PAM variable selection basis,~~ Tables 7.5-6 though 7.5-10 ~~show~~ summarize the specific PAM variables by variable type and associated their required functions. Additional information regarding the bases for the selection of the PAM variables included in Table 7.5-3 is provided in Appendix H of the Safety I&C Technical Report (Reference 7.5-5).

The COL applicant is to provide a description of site-specific PAM variables, which are ~~t~~Type D variables for monitoring the performance of the UHS and ~~t~~Type E variables for monitoring the meteorological parameters.

Instrumentation for monitoring severe accidents is discussed in Subsection 19.2.3.3.7. which summarizes the necessary equipment survivability for achieving and maintaining shutdown of the plant and maintaining containment integrity for severe accidents. A detailed description of the analysis on equipment survivability, including instruments required for severe accident monitoring, is provided in Chapter 15 of PRA Technical Report, MUAP-07030 (Reference 7.5-15).

The Type A, B, and C variables/instrument functions are those determined by the application of the NRC-endorsed PAM instrumentation determination process, which is based on supporting the site-specific AOPs and EOPs, as stipulated in RG 1.97 Rev. 4 (Reference 7.5-1). The PAM variables in Table 7.5-3 are verified upon completion of the EOPs and AOPs.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

Table A: Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Reactivity Control	Indication of subcritical conditions	Power Range Neutron Flux	-	There are no credited manual actions prompted by indications of subcritical conditions and no credited manual actions that require monitoring subcritical conditions. Wide Range Neutron Flux is a Type B and D variable for the US-APWR.
Reactivity Control	Indication of subcritical conditions	Source Range Neutron Flux	-	There are no credited manual actions prompted by indications of subcritical conditions and no credited manual actions that require monitoring subcritical conditions.
Core Cooling	Indication of core cooling; Manual action; Long-term core cooling	RCS Hot Leg Temperature	Reactor Coolant Hot Leg Temperature (Wide Range)	Intact loop hot leg temperature is applied for determining the termination of RCS cooldown and initiation of RCS depressurization in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
Core Cooling	Indication of core cooling; Long-term core cooling	RCS Cold Leg Temperature	Reactor Coolant Cold Leg Temperature (Wide Range)	This parameter is not explicitly assumed in safety analysis; however, monitoring of this parameter is necessary for cooling down after mitigating a PA or AOO. Therefore, this is a Type A parameter for the US-APWR.
Core Cooling; Maintaining RCS Integrity; RCS Pressure Boundary; Primary Coolant System	-SGTR Safety Analysis Manual Action -RCS Depressurization based on EOPs for SGTR event	RCS Pressure (Wide Range)	Reactor Coolant Pressure	No difference.
Core Cooling	To ensure RCS inventory	Reactor Vessel Water Level	-	This parameter is not applied in the safety analysis. RV Water Level is a Type B and D variable for the US-APWR.
Core cooling; Maintaining RCS Integrity; RCS Pressure Boundary	Indication of core cooling function for RWSP switchover and status of ECCS recirculation delivery	Containment Sump Water Level (Wide Range)	-	This parameter is not applied in safety analysis since the US-APWR RWSP is located inside containment and does not require switchover to the recirculation sump. RWSP level is a Type B and D variable for the US-APWR.

Table A: Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Maintaining Containment and RCS Integrity; RCS Pressure Boundary	Indication of containment integrity function	Containment Pressure	-	This parameter is not applied in the safety analysis. Containment Pressure is a Type B and D variable for the US-APWR.
Containment Isolation/Integrity	Indication of containment integrity function	Penetration Flow Path Containment Isolation Valve Position	-	This parameter is not applied in the safety analysis. C/V Isolation Valve Position is a Type B and D variable for the US-APWR.
Containment Radiation; RCS Pressure Boundary	Identify challenge to fission product barrier	Containment Area Radiation (High Range)	-	This parameter is not applied in the safety analysis. Containment Area Radiation is a Type C and E variable for the US-APWR.
Primary Coolant System; RCS Pressure Boundary	To ensure proper operation of the pressurizer	Pressurizer Level	Pressurizer Water Level	No difference.
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	Steam Generator Water Level (Wide Range)	-	This parameter is not applied in the safety analysis. SG narrow range level is applied in safety analysis and US-APWR ERG instead of this parameter. SG Wide Range Level is a Type B and D variable for the US-APWR.
Auxiliary Feedwater System	Indication of ability to maintain SG heat sink and indication of long-term AFW operation	Condensate Storage Tank Level	-	The EFW pit has enough water to maintain long-term core cooling; therefore, this variable is not applied in the safety analysis. This is a Type B and D variable for the US-APWR.
Core Cooling; Fuel Cladding Integrity; Maintain RCS Integrity; RCS Pressure Boundary; Primary Coolant System	Indication of core cooling	Core Exit Temperature – Quadrant [1]-[4]	-	This parameter is not applied in the safety analysis. Core Exit Temperature is a Type B and C variable for the US-APWR.
Auxiliary Feedwater System	Verification of automatic actuation and ability to satisfy heat sink requirements	Auxiliary Feedwater Flow	EFW Flow	No difference. This parameter is used to determine if the ECCS termination criteria are met in the SGTR analysis.

Table A: Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Secondary System	Verification of manual action for SGTR termination (along w/ RCS Pressure)	-	Main Steam Line Pressure	This parameter is applied for determining the termination of RCS cooldown and initiation of RCS depressurization in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	-	SG Water Level (Narrow Range)	This parameter is monitored for the operator to determine if the ECCS termination criteria are met in the SGTR analysis. This parameter is also used in the ERGs to identify ruptured SG(s). Therefore, this is a Type A variable for the US-APWR.
Core Cooling	Indication of core cooling	-	Degrees of Subcooling	This parameter is monitored for the operator to determine if the terminating RCS depressurization criteria or ECCS termination criteria are met in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.

Table B: Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Reactivity Control			
Neutron Flux	Function detection; accomplishment of mitigation	Wide Range Neutron Flux	No difference
Control Rod Position	Verification	-	The primary indication of reactor shutdown is neutron flux (Type B). Therefore, for the US-APWR control rod position is provided, but it is not identified as a PAM variable.
RCS Soluble Boron Concentration	Verification	Reactor Coolant Soluble Boron Concentration	No difference
RCS Cold Leg Water Temperature	Verification	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference
Core Cooling			
RCS Hot Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Hot Leg Temperature (Wide Range)	No difference
RCS Cold Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference
RCS Pressure	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Pressure	No difference
Core Exit Temperature	Verification	Core Exit Temperature	No difference
Coolant Inventory	Verification; accomplishment of mitigation	RV Water Level	No difference
Degrees of Subcooling	Verification and analysis of plant conditions	Degrees of Subcooling	No difference

Table B: Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Maintaining Reactor Coolant System Integrity			
RCS Pressure	Function detection; accomplishment of mitigation	Reactor Coolant Pressure	No difference
Containment Sump Water Level	Function detection; accomplishment of mitigation; verification	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	No difference. The US-APWR RWSP is located inside containment, essentially combining the function of the sump and RWSP.
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference
Maintaining Containment Integrity			
Containment Isolation Valve Position (excluding check valves)	Accomplishment of isolation	Containment Isolation Valve Position (Excluding Check Valves)	No difference
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference
Other			
-	-	Pressurizer Water Level	This parameter is important to monitor because it is related to the SI termination criteria, which is related to maintaining adequate RCS inventory to assure core cooling.
-	-	Main Steam Line Pressure	This parameter is important to monitor the efficiency of removing the decay heat of core, which is related to core cooling.
-	-	SG Water Level (Wide Range)	This parameter provides indication of heat sink availability and is selected to monitor core cooling.
-	-	SG Water Level (Narrow Range)	This parameter provides indication of heat sink availability and is selected to monitor core cooling.
-	-	EFW Flow	This parameter provides verification of the automatic actuation of EFW and is selected to monitor core cooling.
-	-	EFW Pit Water Level	This parameter provides indication of heat sink availability and is selected to monitor core cooling.

Table C: Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Fuel Cladding			
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	Detection of breach	Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	No difference
Core Exit Temperature	Detection of breach	Core Exit Temperature	No difference
Analysis of Primary Coolant (Gamma Spectrum)	Detail analysis; accomplishment of mitigation; verification; long-term surveillance	-	In the US-APWR, concentration of each radioactive nuclide is derived from RCS sampling. RG 1.97 Rev.3 allows analysis of primary coolant by sampling.
Reactor Coolant Pressure Boundary			
RCS Pressure	Detection of potential for or actual breach; accomplishment of mitigation; long-term surveillance	Reactor Coolant Pressure	No difference
Containment Pressure	Detection of breach; accomplishment of mitigation; long-term surveillance	Containment Pressure	No difference
Containment Sump Water Level	Detection of breach; accomplishment of mitigation; long-term surveillance	-	Containment Pressure is a more direct indication of a potential containment breach. Therefore, RWSP level is not included as a Type C variable for the US-APWR.
Containment Area Radiation	Detection of breach; verification	Containment High Range Area Radiation	No difference.
Effluent Radioactivity - Noble Gas Effluent from Condenser Air Removal System Exhaust	Detection of breach; verification	-	Coolant leakage outside containment to secondary system due to an actual breach of the reactor coolant pressure boundary can be detected by RCS pressure, SG water level, and pressurizer water level. These variables are PAM variables. Therefore, it is not necessary to include effluent radioactivity as a Type C variable.

Table C: Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment			
RCS Pressure	Detection of potential for breach; accomplishment of mitigation	Reactor Coolant Pressure	No difference
Containment Hydrogen Concentration	Detection of potential for breach; accomplishment of mitigation; long-term surveillance	-	This instrumentation is used for monitoring severe accidents. Therefore, it does not need to be a Type C variable.
Containment Pressure	Detection of potential for or actual breach; accomplishment of mitigation	Containment Pressure	No difference
Containment Effluent Radioactivity - Noble Gas Effluent from Identified Release Points	Detection of breach; accomplishment of mitigation; verification	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type C variable for the US-APWR.
Effluent Radioactivity - Noble Gases (from buildings or areas where penetrations and hatches are located, e.g., secondary containment and auxiliary buildings and fuel handling buildings that are in direct contact with primary containment)	Indication of breach	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type C variable for the US-APWR.

Table D: Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Residual Heat Removal (RHR) or Decay Heat Removal System			
RHR System Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference
RHR Heat Exchanger Outlet Temperature	To monitor operation and for analysis	-	Proper operation of the RHR system is verified by CS/RHR flow rate. Additionally, T_{hot} and T_{cold} are available to monitor RHR system performance with respect to decay heat removal. Therefore, it is not necessary to include the RHR heat exchanger outlet temperature as a Type D variable in the US-APWR PAM list.
Safety Injection System			
Accumulator Tank Level and Pressure	To monitor operation	Accumulator Water Level, Accumulator Pressure	No difference
Accumulator Isolation Valve Position	Operation status	-	Accumulator water level and accumulator pressure are available to monitor operation status. Therefore, it is not necessary to include isolation valve position as a separate Type D variable in the US-APWR PAM list.
Boric Acid Charging Flow	To monitor operation	-	The safety injection system delivers boric acid water to the RCS in the US-APWR. Safety Injection Pump Discharge Flow and Safety Injection Pump Minimum Flow are available to monitor the flow. Therefore it is not necessary to include this as a Type D variable in the US-APWR PAM list.
Flow in HPI System	To monitor operation	Safety Injection Pump Discharge Flow Safety Injection Pump Minimum Flow	No difference
Flow in LPI System	To monitor operation	-	The US-APWR design allows the accumulators and high head safety injection system to fully replace the safety function associated with the low head safety injection system. Therefore, the US-APWR PAM list does not need any variables to indicate LPI system performance.

Table D: Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Refueling Water Storage Tank Level	To monitor operation	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	No difference
Primary Coolant System			
Reactor Coolant Pump Status	To monitor operation	-	The safety analysis does not rely on the RCP to mitigate design basis events. The RCPs are also not necessary to achieve and maintain a safe shutdown condition. CCW header pressure is available to monitor CCW performance related to its function to deliver seal flow to the RCP in order to maintain its RCS pressure boundary function. Therefore, RCP status is not included as a PAM variable for the US-APWR.
Primary System Safety Relief Valve Positions (including PORV and code valves) or Flow Through or Pressure in Relief Valve Lines	Operation status; to monitor for loss of coolant	-	RCS pressure, Reactor Coolant Hot Leg Temperature, and Reactor Coolant Cold Leg Temperature are available to monitor operation status of the primary coolant system. Consistent trends in changes to the values of these variables are indicative of a loss of coolant. Therefore, it is not necessary to include position indication or flow indication for the primary relief valves in the PAM list.
Pressurizer Level	To ensure proper operation of pressure	Pressurizer Water Level	No difference
Pressurizer Heater Status	To determine operating status	-	Pressurizer water level and RCS pressure are indicative of the performance of the pressurizer heater. Therefore it is not necessary to separately include heater status in the PAM list.
Quench Tank Level	To monitor operation	-	This component is not necessary to mitigate design basis events, and not necessary to achieve and maintain a safe shutdown condition. Therefore, it is not included in the US-APWR PAM list.
Quench Tank Temperature	To monitor operation	-	Same as above
Quench Tank Pressure	To monitor operation	-	Same as above

Table D: Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Secondary System (Steam Generator)			
Steam Generator Level	To monitor operation	SG Water Level (Wide Range), SG Water Level (Narrow Range)	No difference
Steam Generator Pressure	To monitor operation	Main Steam Line Pressure	No difference
Safety/Relief Valve Positions or Main Steam Flow	To monitor operation	-	Main steam line pressure is indicative of main steam flow and is available to monitor its SG operation. Therefore it is not necessary to separately include this variable in the PAM list.
Main Feedwater Flow	To monitor operation	-	SG water level and main steam line pressure are indicative of adequate feedwater flow. Since these variables are available to monitor SG operation, it is not necessary to separately include MFW flow in the PAM list.
Auxiliary Feedwater or Emergency Feedwater System			
Auxiliary or Emergency Feedwater Flow	To monitor operation	EFW Flow	No difference
Condensate Storage Tank Water Level	To ensure water supply for auxiliary feedwater	EFW Pit Water Level	No difference
Containment Cooling Systems			
Containment Spray Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference
Heat Removal by the Containment Fan Heat Removal System	To indicate accomplishment of cooling	-	The containment fan heat removal system is not credited in design basis events since containment spray is credited to maintain containment integrity. Therefore this variable is not included in the PAM list.
Containment Atmosphere Temperature	To monitor operation	Containment Temperature	No difference

Table D: Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Sump Water Temperature	To monitor operation	-	Containment pressure, containment temperature, and containment spray flow are utilized to monitor containment cooling system performance. Therefore it is not necessary to include this variable in the US-APWR PAM list.
Chemical and Volume Control System (CVCS)			
Makeup Flow - In	To monitor operation	-	Since RCS inventory and boration are achieved by the safety injection system in the US-APWR, the monitoring variables related to CVCS are not necessary PAM variables for the US-APWR design.
Letdown Flow - Out	To monitor operation	-	Same as above
Volume Control Tank Level	To monitor operation	-	Same as above
Cooling Water System (CCW)			
Component Cooling Water Temperature to ESF System	To monitor operation	-	CCW header pressure provides indication of the performance of the cooling water system. Therefore it is not necessary to separately include this variable in the PAM list.
Component Cooling Water Flow to ESF System	To monitor operation	-	Same as above
Radwaste Systems			
High-Level Radioactive Liquid Tank Level	To indicate storage volume	-	The US-APWR design precludes the need for this variable. This component is not necessary to mitigate design basis events and not necessary to achieve and maintain a safe shutdown condition. Addition of additional radioactive waste to the liquid or gaseous radwaste system following an accident is precluded by design and is not postulated. Therefore, this variable is not included in the US-APWR PAM list.
Radioactive Gas Holdup Tank Pressure	To indicate storage capacity	-	Same as above
Ventilation Systems			
Emergency Ventilation Damper Position	To indicate damper status	-	Containment Isolation Valve Position provides indication of containment integrity. The combination of isolation valve position status and a lack of radioactive release as indicated by the plant vent monitor provides verification of proper automatic ventilation path isolation. Therefore, damper position indication is not included in the US-APWR PAM list.

Table D: Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Power Supplies			
Status of Standby Power and Other Energy Sources Important to Safety (electric, hydraulic, pneumatic) (voltages, currents, pressures)	To indicate system status	Status of Standby Power and Other Energy Sources Important to Safety Class 1E ac Bus Voltage Class 1E dc Bus Voltage	No difference
Other			
-	-	Reactor Coolant Hot Leg Temperature (Wide Range)	This variable indicates the performance of the primary coolant system for maintaining core cooling.
-	-	Reactor Coolant Cold Leg Temperature (Wide Range)	Same as above
-	-	Reactor Coolant Pressure	This variable indicates the performance of the primary coolant system for maintaining core cooling and RCS integrity.
-	-	Degrees of Subcooling	This variable is used to indicate the performance of the primary coolant system for core cooling.
-	-	RV Water Level	This variable provides direct indication of inventory available for maintaining core cooling.
-	-	Wide Range Neutron Flux	This variable directly indicates reactivity control and allows for the monitoring of the performance of the control rod assemblies.
-	-	Containment Pressure	This variable is used to indicate the containment integrity status.
-	-	Containment Isolation Valve Position (Excluding Check Valves)	This variable is used to indicate the containment integrity status.
-	-	CCW Header Pressure	This variable is used to indicate the performance of the CCW system.
-	-	ESW Header Pressure	This variable is used to indicate the performance of the ESW system.

Table E: Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Radiation			
Containment Area Radiation - High Range	Detection of significant releases; release assessment; long-term surveillance; emergency plan actuation	Containment High Range Area Radiation	No difference
Area Radiation			
Radiation Exposure Rate (inside buildings or areas where access is required to service equipment important to safety)	Detection of significant releases; release assessment; long-term surveillance	-	This parameter can be measured by area monitors located where personnel enter areas after the accident. Additional personnel protection will be provided by the use of portable radiation monitors and air sampling. Therefore, it is not necessary to include this variable in the US-APWR PAM list.
Airborne Radioactive Materials Released from Plant			
Noble Gases and Vent Flow Rate			
Containment or Purge Effluent	Detection of significant releases; release assessment	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. These variables can be measured by plant vent radiation monitor (including high range) and therefore are not included as separate Type E variables for the US-APWR.
Reactor Shield Building (if in design)	Detection of significant releases; release assessment	-	
Auxiliary Building (including any building containing primary system gases, e.g., waste gas decay tank)	Detection of significant releases; release assessment; long-term surveillance	-	
Condenser Air Removal System Exhaust	Detection of significant releases; release assessment	-	

Table E: Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Common Plant Vent or Multipurpose Vent Discharging Any of Above Releases (if containment purge is included)	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Vent From Steam Generator Safety Relief Valves or Atmospheric Dump Valves	Detection of significant releases; release assessment	-	This variable is measured by main steam line monitor. Therefore it is not included as a separate Type E variable for the US-APWR.
All Other Identified Release Points	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Particulates and Halogens			
All Identified Plant Release Points (except steam generator safety relief valves or atmospheric steam dump valves and condenser air removal system exhaust). Sampling with Onsite Analysis Capability	Detection of significant releases; release assessment; long-term surveillance	-	This can be measured by plant vent sampler (accident sampler). Therefore it is not included as a separate Type E variable for the US-APWR.
Environs Radiation and Radioactivity			
Airborne Radiohalogens and Particulates (portable sampling with onsite analysis capability)	Release assessment; analysis	Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	No difference
Plant and Environs Radiation (portable instrumentation)	Release assessment; analysis	Plant and Environs Radiation (Portable Instrumentation)	No difference

Table E: Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Plant and Environs Radioactivity (portable instrumentation)	Release assessment; analysis	Plant and Environs Radioactivity (Portable Instrumentation)	No difference
Meteorology			
Wind Direction	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Wind Speed	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Estimation of Atmospheric Stability	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Accident Sampling Capability (Analysis Capability On Site)			
Primary Coolant and Sump · Gross Activity · Gamma Spectrum · Boron Content · Chloride Content · Dissolved Hydrogen or Total Gas · Dissolved Oxygen · pH	Release assessment; verification analysis	-	These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.

Table E: Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Air · Hydrogen Content · Oxygen Content · Gamma Spectrum	Release assessment; verification analysis	-	These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.
Other			
-	-	MCR Area Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	MCR Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	TSC Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the technical support center.
-	-	Plant Vent Radiation Gas Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Main Steam Line Radiation	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	GSS Exhaust Fan Discharge Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Plant Air Vent High Concentration Sampling System	To monitor the magnitude of releases of radioactive materials through identified pathways.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.656-5127 REVISION 2**
SRP SECTION:	**07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.05**
DATE OF RAI ISSUE:	**11/15/2010**

QUESTION NO. : 07.05-20

In Section 7.5.1.3, "Plant Annunciator (Alarm) System," of the US-APWR DCD Revision 2, states "As for all PCMS components, the alarm system is powered by redundant UPSs. The alarm system is designed and tested to a similar environmental, seismic, and EMI/RFI requirement as the PSMS." The staff requests MHI to provide a clarification and additional details on what the actual difference is between the PCMS and the PSMS systems in terms of their software V&V, seismic qualifications and environmental testing in accordance with GDC 1, "Quality standards and records".

ANSWER:

Actual differences between the PCMS and the PSMS for software V&V, seismic qualification and environmental testing are described in the amended response to RAI 688-5273 Question No. 07.07-32.

Impact on DCD
The impact on the DCD Rev. 3 is described in the amended MHI response to RAI 688-5273 Question No. 07.07-32. These changes will be reflected in DCD Rev.4.
In addition, Subsection 7.5.1.3, "Plant Annunciator (Alarm) System," of the US-APWR DCD Revision 3, will be revised as follows:

> As for all PCMS components, the alarm system is powered by redundant UPSs. The alarm system is designed and tested to environmental, seismic, and EMI/RFI requirements as described in Table 3.2-5.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 239-2033 REVISION 0**
SRP SECTION:	**07.06 – INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.06**
DATE OF RAI ISSUE:	**3/2/2009**

QUESTION NO.: 07.06-3
Discuss how GDCs 20, 21, 22, 23, and 29 are applied to the design of interlock systems important to safety. Update Table 7.1-2 if necessary.

Though not listed in SRP Table 7-1 as applicable to information systems required for safety, DCD Table 7.1-2 cites compliance with GDCs 20, 21, 22, 23 and 29 for the PSMS in Section 7.6. Section 7.6 indicates that detailed compliance to the GDC is described (in general, not specifically related to interlock systems) in TR MUAP-07004-P(R1) Section 3. It is unknown how GDCs 20, 21, 22, 23, and 29 are applied to the design of interlock systems important to safety.

ANSWER:
Interlock systems important to safety are implemented within the PSMS safety related software and hardware. Therefore, the PSMS is credited for compliance to these GDCs and these GDCs are listed for Section 7.6 in Table 7.1-2. Requirements met by the PSMS itself, such as equipment qualification, are described in DCD Subsection 7.1.3.

For conformance to the single failure criterion, these interlocks are redundantly controlled from at least two trains of the PSMS, except for CS/RHR pump hot leg isolation valves. Justification for the single train CS/RHR pump hot leg isolation valve open permissive interlock design is discussed in RAI 07.06-15.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 239-2033 REVISION 0**
SRP SECTION:	**07.06 – INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.06**
DATE OF RAI ISSUE:	**3/2/2009**

QUESTION NO.: 07.06-16
Describe in detail the "Pull Lock" feature of the motor operated isolation valve (MOIV), the conditions under which this feature could be used and, assuming this feature of the MOIV, how the accumulator discharge design meets position 4 of BTP 7-2, "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines."

In Section 7.6.1.4, which describes the ECCS accumulator interlock system, it is stated that if the (MOIV) was closed in the "Pull Lock" mode, the accumulator discharge valves will not automatically open, therefore the affected accumulator will be un-available for its designed ESF function. This appears to violate Position 4 of BTP 7-2, which requires "utilization of a safety injection signal to remove automatically (override) any bypass feature that may be provided to allow an isolation valve to be closed for short periods of time..." The DCD indicates that the "Pull Lock" function is described in Topical Report MUAP-07007 Section 4.5.3.a. However, the staff's review of this document for the referenced section showed that Section 4.5.3.a of the Topical Report MUAP-07007, "HSI System Description and HFE Process," only discusses operation-related information display features of ON/OFF switches. The only reference to the "Pull Lock" feature is a display button in Figure 4.5-4, "Soft Operation Switch Moving Feature."

ANSWER:
As described in Subsection 7.6.1.4, "the ECCS actuation signal will automatically open the valve and make the accumulator system available", except when the valve is manually closed and manually put in the Pull Lock condition. This requires two distinct and deliberate manual operator actions. The pull lock condition for the accumulator discharge valve is applied only when the associated accumulator is re-charged with gas or water. Recharging is a maintenance activity, which occurs only when the accumulator pressure or water level is lower than required. Under this condition, the accumulator itself is inoperable, therefore automatically opening the accumulator discharge valve would have no safety benefit. The accumulator bypass or inoperable condition is managed by Technical Specification in DCD Chapter 16 Section 3.5.1.

In addition, interlock systems important to safety, including the accumulator discharge valve interlock, are indicated by BISI, as described in DCD Subsection 7.5.1.2.2.

Impact on DCD
The following description will be added to Subsection 7.6.1.4 of the DCD Rev.4.

The ECCS actuation signal will automatically open the valve and make the accumulator system available, except when the valve is manually closed and manually put in the Lock condition. The Lock condition for the accumulator discharge valve is applied only when the associated accumulator is re-charged with gas or water. Recharging is a maintenance activity, which occurs only when the accumulator pressure or water level is lower than required. Under this condition, the accumulator itself is inoperable; therefore, automatically opening the accumulator discharge valve does not provide the accumulator design function. The accumulator discharge valve interlock is indicated on the BISI, and the accumulator bypass or inoperable condition is managed by the technical specifications in Subsection 3.5.1 of the DCD Chapter 16.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 638-5032 REVISION 0**
SRP SECTION:	**07.06 - INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.06 - INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
DATE OF RAI ISSUE:	**09/23/2010**

QUESTION NO. : 07.06-21

MHI is requested to effectively demonstrate how to conform to guidance RG 1.206, "Combined License Applications for Nuclear Power Plants," with regard to interlock to prevent over pressurization of the primary coolant system during low-temperature operations of the reactor vessel.

Subsection C.I.5.2.2.2 of RG 1.206 states that "Applicants should describe the design of overpressure protection during low-temperature operations, including the capability to relieve pressure during all overpressure events during startup and shutdown conditions at low temperatures, particularly during water-solid conditions. Applicants should provide the analysis that demonstrates how overpressure protection is achieved, assuming any single active component failure. This section should identify all overpressure events and, as a subset, identify the events that can be prevented by preventive interlocks or locking-out power. Applicants should describe how the overpressure protection system is enabled, the alarms and indications associated with the system, and the power source for the system."

Subsection 7.6.3 of the DCD states that "There are no interlocks necessary to prevent over pressurization of the RCS during low-temperature operations of the RV. Refer to Subsection 5.2.2."

Subsection 5.2.2 identifies overpressure events but instead of identifying the events that can be prevented by preventive interlocks or locking-out power as described in RG 1.206 above, this subsection further states that "An important aspect of RCS overpressure protection at low temperatures is the use of administrative controls which are discussed in paragraph 5.2.2.2.2.2, Administrative Controls. Although specific alarms do not exist to invoke specific administrative procedures, annunciation is provided to alert the operator to arm the cold overpressure mitigation system."

It is not clear how the guidance in RG 1.206 with regard to interlock to prevent overpressurization of the primary coolant system during low-temperature operations of the reactor vessel is met.

ANSWER:

The LTOP system for US-APWR consists of CS/RHR pump suction relief valves, which are spring-loaded relief valves. Therefore, preventive interlock to activate the LTOP system is not

needed.

These valves are equipped with direct position indication in accordance with a requirement of Section II.D.3 of the TMI Action Plan. When LTOP event occurs, these relief valves operate reactor coolant pressure and a valve position alarm alerts the operator.

In order to ensure the LTOP system is operable status at the correct plant condition during cooldown, the technical specifications require surveillances of the following status (Reference DCD Chapter 16, SR 3.4.12.1 through 3.4.12.7.).

- Number of available Safety Injection (SI) pump
- Number of available Charging pump
- Accumulators are isolated
- RHR suction motor-operated valves are open
- RHR suction motor-operated valves are locked open with operator power removed

Please refer to responses provided to RAI No.103, UAP-HF-08303, which pertain to the LTOP system.

Therefore, since the LTOP system does not need preventive interlock, there is no interlock provided to prevent overpressurization of the primary coolant system during low-temperature operation of the reactor vessel.

Impact on DCD

The second bulleted item of Subsection 7.6.3 of the DCD Rev. 4 will be changed as follows:

- Interlocks to prevent overpressurization of the primary coolant system during low-temperature operations of the RV:

  - There are no interlocks necessary to prevent overpressurization of the RCS during low-temperature operations of the reactor vessel since the spring-loaded CS/RHR pump suction relief valves provide low-temperature overpressure protection for the RCS. When an LTOP event occurs, these relief valves discharge the RCS inventory to the refueling water storage pit in the containment, and a valve position alarm alerts the operator. ~~RV.~~ Refer to Subsection 5.2.2.

Impact on R-COLA
There is no impact on the R-COLA

Impact on S-COLA
There is no impact on the S-COLA

Impact on PRA
There is no impact on the PRA

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.688-5273 REVISION 2**
SRP SECTION:	**07.07 – CONTROL SYSTEMS**
APPLICATION SECTION:	**07.07 – CONTROL SYSTEMS**
DATE OF RAI ISSUE:	**01/31/2011**

QUESTION NO. : 07.07-30

On Table 7.1-2, "Regulatory Requirements Applicability Matrix," of Tier 2 of the USAPWR DCD, 10 CFR 50.55a(a)(1) is not addressed under PCMS or DAS. 10 CFR 50.55a(a)(1) states that "*Structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed*". In the SRP Chapters for 7.7 (Control Systems) and 7.8 (Diverse Instrumentation and Control Systems), 10 CFR 50.55a(a)(1) is part of the acceptance criteria.

The staff requests MHI to include 10 CFR 50.55a(a)(1) in Table 7.1-2 of the DCD, to fully address how US-APWR complies with the requirement.

ANSWER:

MHI agrees with the staff's request.

DCD Table 7.1-2 will be revised to indicate that 10 CFR 50.55a(a)(1) applies to the PCMS and the DAS.

Impact on DCD
Item a. of Table 7.1-2 of the DCD Rev. 4 will be revised as shown in the following table markup.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Table 7.1-2 Regulatory Requirements Applicability Matrix (per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 1 of 8)

Applicable Criteria		Title	I&C System							Related Section in US-APWR DCD
			RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS	
		1. 10 CFR 50 and 52								
a.	50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	X	X	X	X	X	X	7.2 to ~~7.6~~7.9

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.688-5273 REVISION 2**
SRP SECTION:	**07.07 – CONTROL SYSTEMS**
APPLICATION SECTION:	**07.07 – CONTROL SYSTEMS**
DATE OF RAI ISSUE:	**01/31/2011**

QUESTION NO. : 07.07-31

In the response to RAI 240-2045, question 07.07-11, MHI stated that "*...conformance with RG 1.180, which is only for safety systems, is not required for the PCMS.*" But RG 1.180 (page 1.180-5, 2nd paragraph) also states that "*While non-safety-related systems are not part of the regulatory guidance being developed, control of EMI/RFI from these systems is necessary to ensure that safety-related I&C systems can continue to perform properly in the nuclear power plant environment. When feasible, the emissions from non-safety-related systems should be held to the same levels as safety-related systems.*"

The staff requests MHI to demonstrate how the US-APWR design is in conformance with RG 1.180 in relation to the PCMS and how the emissions from nonsafety-related systems do not affect the safety systems.

Reference: MHI's Responses to US-APWR DCD RAI No.230-2028, No.227-2020, No.238-2030, No.228-2021, and No.231-2037, Revision 0; MHI Ref: UAP-HF-09196; DATED APRIL 28, 2009; ML091250290.

ANSWER:

The augmented quality functions of the PCMS, and the DAS, are tested to demonstrate compliance to RG 1.180. Regulatory Position C.3, EMI/RFI Emissions Testing, of RG 1.180, which is applied to all of the PCMS and the DAS, ensures that the PCMS and the DAS emissions are limited to acceptable levels that will not affect the safety-related systems.

Impact on DCD
Item a. of Table 7.1-2 of the DCD Rev. 4 will be revised as shown in the following table markup.

Following description will be added in the 4th paragraph of Subsection 7.1.3.7 in the DCD Rev. 4.

> The augmented quality functions of the PCMS, and the DAS, are tested to demonstrate compliance to RG 1.180. Regulatory Position C.3, EMI/RFI Emissions Testing, of RG 1.180, which is applied to all of the PCMS and the DAS, ensures that the PCMS and the DAS emissions are limited to acceptable levels that will not affect the safety-related systems.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Table 7.1-2 Regulatory Requirements Applicability Matrix (per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 5 of 8)

Applicable Criteria		Title	I&C System							Related Section in US-APWR DCD
			RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS	
s.	RG 1.180	Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related I&C Systems	X	X	X	X	X	X	X	7.2 to 7.6, 7.9

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.677-5325 REVISION 2**
SRP SECTION:	**07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS**
APPLICATION SECTION:	**TECHNICAL REPORT MUAP-07014**
DATE OF RAI ISSUE:	**1/10/2011**

QUESTION NO. : 07.08-11

Regulatory Guidance: DI&C-ISG-05, Part 3, Section 1.B, last bullet states that, "The analysis of the action sequence identifies credible operator errors and the estimate of time required includes sufficient margin for recovery from any single credible operator error."

Question: MUAP-07014-P(R2), Section 5 outlines the analyses supporting credited manual operator actions. These sections generally state that the time margin for the manual action is sufficient to accommodate operator errors. Credible operator errors are not specifically identified. The time margin is also not addressed.

Identify credible operator errors for the credited manual actions evaluated in MUAP-07014. Identify appropriate time margins for the events or explain why the margin is unnecessary.

ANSWER:

The credible operator errors for the credited manual actions are identified in Table 9.5.1 of the PRA Technical Report, MUAP-07030.

MUAP-07014-P (R2) provides both the time available and the time required for the events concurrent with CCF which require the performance of manual actions. Table 7.11 below summarizes the times from the topical report and lists the corresponding time margin available for correcting potential operator errors. Adequacy of the time margin will be validated in the integrated HSI validation tests. Credited operator actions must meet the timing requirements specified in the validation implementation plan. The training program will be developed to ensure the operators are well trained. The validation and operator training are encompassed by the existing HFE Inspection, Test, Analysis and Acceptance Criteria (ITAACs).

Table 7.11: Time Margin for Each Event Concurrent with CCF

Event	Time Available (minutes)	Time Required (minutes)	Time Margin (minutes)
Boron Dilution	61.2 (PCMS disabled) 73.0 (PCMS unaffected)	31.5	29.7 41.5
CVCS Malfunction	> 60	31.5	> 28.5
Failure of Small Lines with Primary Coolant	180	31.5	148.5
SG Tube Rupture	15	15	(Note 1)
Small Break LOCA	10	2	8 (Note 2)
Large Break LOCA	6	2	4 (Note 2)

Notes:

1 The time available from initiation of the SGTR event to the manual reactor trip from the DHP is 15 minutes, which is the same as the DCD safety analysis assumption. This is because the operator can perform a manual reactor trip based on equivalent indication and alarm on the DHP using an equivalent SGTR DHP procedure.

2 Additional information about the determination of the response time and corresponding time margin for LOCA events is provided in the response to Question No. 07-08-14.

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 655-5220 REVISION 2**
SRP SECTION:	**07-14 BRANCH TECHNICAL POSITION - GUIDANCE ON SOFTWARE REVIEWS FOR DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROLS SYSTEMS**
APPLICATION SECTION:	**B.3.1.9**
DATE OF RAI ISSUE:	**11/22/2010**

QUESTION NO. : 07-14 Branch Technical Position-42

Criterion III, Design Control, of 10 CFR 50, Appendix B, requires measures to ensure that applicable regulatory requirements and the design basis are correctly translated into specifications, drawings, procedures and instructions. Also, RG 1.173 specifies additional activities beyond those identified by IEEE Std 1074-1995, which it endorses, to ensure safety system development is consistent with defined system safety analyses.

The MELTAC Basic Software Safety Report, JEXU-1015-1009-P(R3), is found to not be the type of document described by this regulatory guidance, or staff guidance, for a software safety analysis. This is because it does not describe, per RG 1.173, the types of software safety analyses, by inputs, outputs or activity description, or how this analysis was done in each phase of the software development life cycle.

Also, this document does not describe the types of analyses performed as cited in NUREG/CR-6101 by BTP 7-14, Section B.3.1.9.
The safety analyses that were done for the MELTAC Basic Software should be explained in the commercial grade dedication report in each phase, with the differences to all staff guidance noted and adequately explained. Also, for future MELTAC Basic Software development activities, the software safety plan should adequately present the software safety analyses which will be done and how each attribute in staff guidance is met.

Therefore, this document should be retitled "Analysis of the MELTAC Basic Platform to Guidance of ISG-04" as ISG-04 is the only identified guidance within the document, which is not consistent with a software safety analysis, and will only be used by the staff for compliance to ISG-04.

ANSWER:

MELCO submitted the response of this RAI to the NRC on 12/20/2011.
But MELCO was informed during the face to face meeting on 2/23/2011 that the response was not accepted.
Based on this feedback, MELCO has prepared the amended response as follows.

MELCO has identified three specific requests in the RAI as below.
Our response to each request is as follows.

1) Evaluation of the past safety analysis of the MELTAC platform should be in the CGD Report.

   CGD (MRP: MELTAC Re-evaluation Program) for the legacy MELTAC Platform has been performed in accordance with EPRI-TR107330 and EPRI-TR106439.
   These EPRI reports require the hazard analysis described in IEEE Std 1012-1998, which has already been assessed in the MRP. Additional software safety analysis per RG 1.73 or NUREG/CR-6101 are not required. Therefore no additional assessment of Software Safety Analysis for the legacy MELTAC Platform is planned.

2) The software safety plan (SSP) should be established to ensure that software safety analysis for future MELTAC development will be performed in accordance with staff guidance:
   - RG1.173;
   - BTP7-14 B3.1;
   - NUREG/CR6101.

   The description that states software safety analysis will be performed for all future MELTAC development in accordance with the requirements of RG 1.173, BTP7-14 B3.1, and NUREG/CR-6101 has been added in the MELTAC SSP, Section 3.9 of the "MELTAC Platform Basic Software Program Manual" (JEXU-1012-1132), submitted on January 31, 2011.
   Subsection 3.9.5 describes "the multiple software safety analysis activities, which were conducted to generate the documentation submitted to the NRC, to obtain approval of the MELTAC digital platform" and thereby establish the MELTAC licensing basis. For new MELTAC development Subsection 3.9.5 also describes "the software safety analyses for each phase of the MELTAC Basic Software life cycle. For each phase, the software safety analyses ensure the original MELTAC licensing basis is maintained, and that no new safety hazards are introduced."
   A specific internal implementation procedure for analysis has also been included in accordance with the above standards.

3) The analysis in the current SSR is not in accordance with staff guidance (see No. 2).
   The document should be retitled to "Analysis of the MELTAC Basic Platform to Guidance of ISG-04" as any other applicable guidelines are not covered.

   Per the staff's request, the document title will be changed to "MELTAC Platform ISG-04 Conformance Analysis" (JEXU-1015-1009) and this report will be revised to exclude all sections other than those pertinent to the ISG-04 conformance assessment (Sections 3.2 through 3.5 will be retained).
   In addition, the revised document will exclude the application level examples, which were previously included in the discussion of ISG-04 issues related to functional independence. Conformance to the Staff Positions of ISG-04 related to functional independence are

addressed at the application level (i.e., in Appendix E of the Safety I&C Technical Report MUAP-07004 for the US-APWR).

In addition, the remaining portions of the current "MELTAC Platform Software Safety Analysis Report " (JEXU-1015-1009), including Sections 3.1 (Detectability of Input, Operation, and Output hazards) and 3.6 (Analysis of Self-Diagnosis Function), will be described in a new Appendix (Appendix E) entitled "MELTAC Basic Software Critical Function Analysis", that will be attached to the "Safety System Digital Platform – MELTAC" Technical Report (MUAP-07005).

This analysis will be retained because it is an important component of the Hazard Analysis conducted for the legacy MELTAC platform. The complete Hazard Analysis, which includes the MELTAC Basic Software Critical Function Analysis and the MELTAC Platform ISG-04 Conformance Analysis, is described in the MRP, and in the US-APWR SPM (MUAP-07017) Software Safety Plan.

The MRP and US-APWR SPM will be revised to refer to JEXU-1015-1009 "MELTAC Platform ISG-04 Conformance Analysis" and the new Appendix "MELTAC Basic Software Critical Function Analysis".

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 593-4565 REVISION 1**
SRP SECTION:	**07-21 BRANCH TECHNICAL POSITION – GUIDANCE ON DIGITAL COMPUTER REAL-TIME PERFORMANCE**
APPLICATION SECTION:	**CHAPTER 7**
DATE OF RAI ISSUE:	**6/8/2010**

QUESTION NO.: 07-21 Branch Technical Position-1
Clearly identify the performance requirements for the US-APWR safety Instrumentation and Control (I&C) system.

10 CFR 52.47 states in part, that the information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. It appears within Technical Report MUAP-09021, "US-APWR Response Time of Safety I&C System," the values within Section 3.4 should be changed to state "basis" for the time response requirements, not "assumptions". This should include how each of the following factors was determined, what estimates were made, and what facts ensure that these are the bounding requirements.

1. The values identified in Tables 4.0-1 and 4.0-2 as T1 through T4, and T1, T2, respectively. Clearly explain estimates madeand how they are deterministic. Provide justification that shows that the allocations can be reasonably expected to be satisfied by the plant design. Section 3.4 states "The response time allocated to the individual components (i.e., response time of sensor, digital controller) are based on MHI experience of digital I&C system in Japanese PWR plant" is not acceptable.
2. Using the Figure 4.4-1 and Figure 4.4-2, of MUAP-09005, MELTAC Topical Report, show the calculation of the maximum, and minimum, response time which is equal to each of the digital controller times, T2, by safety function presented in MUAP-09021.

   a) Identify each of the values, t1 through t10, in Figure 4.4-1 for the MELTAC Fundamental Cycle and how this can vary for each of the safety functions.

   b) Identify the differences between the typical MELTAC hardware configuration in Figure 4.4-2 and that used to determine each of the response time calculations.

ANSWER:
MHI agrees to change the word "assumptions" to "basis". Section 3.4 of MUAP-09021 will be revised as the follows.

MUAP-09021 Section 4.2 will be revised as follow.

Allocated response times from T1 to T4 in Tables 4.1-1, 4.1-2 are determined as values which envelop the values based on the specifications of the individual equipments that applied to US-APWR. The values based on specifications are addressed in a column "Expected Response Times Based on Specification" in Tables 4.2-1 and 4.2-2. Tables 4.2-1 and 4.2-2 show there is margin between the expected response times and the allocated response times or the expected response time is equal to the allocated response time. Therefore, the allocated response times for RT and ESF actuation components are to be met by the installed equipment in the actual plant.

The model numbers shown in Table 4.2-1 are only to establish credibility for the response time allocations, based on the actual performance specifications of known components. The actual US-APWR model numbers may be different.

Subsection 4.2.1 "Basis for Response Time Allocations for Sensors, RTBs and CRDMs" and Subsection 4.2.2 "Basis for Response Time Allocations for Digital Controller" will be added in MUAP-09021.
The following description and Figures 4.2-1, 4.2-2, 4.2-3 and Tables 4.2-3, 4.2-4 will be added in MUAP-09021 Subsection 4.2.2.

4.2.1 Basis for Response Time Allocations for Sensors, RTBs and CRDMs.

Equipments assigned to sensor part in Tables 4.2-1 and 4.2-2 of this document are transmitters and RTDs of the general vendors in U.S. The response times of these sensors are addressed in the vender specifications and we can find the vender specifications in each vendor web site. The response times T1 of NIS and RCP Speed are negligible and the bases are described Sections 5.2 and 5.3 respectively. Response time T3 (0.1 sec) is in accordance with the specification of RTBs. The response time of RTBs applied to Japanese Pressurized Water Reactor (PWR) is less than 0.1 sec. RTBs of the same specification will be applied to US-APWR. Also, response time T4 (0.15 sec) is in accordance with the specification of CRDMs as addressed in DCD (Reference 1) Section 3.9.4.2.1.

4.2.2 Basis for Response Time Allocations for Digital Controller

Maximum response times are calculated by the method provided in Table 4.4-1 of the MELTAC Platform Technical Report (Reference 3). The system scale of digital controller is considered for estimating some of response times. To estimate the maximum response times, the system scale is determined by adding some margins to the system scale based on the DCD (Reference 1). The system scale applied to the estimation of maximum response times are shown in Table 4.2-3.

All estimated values above are less than 80% of response time requirement addressed in the column of allocated response times in Tables 4.2-1 and 4.2-2. Therefore, allocated response times T2 in Table 4.2-1, 4.2-2 are appropriate.

Figure 4.2-1 System Configuration of Case 1

Figure 4.2-2 System Configuration of Case 2

Figure 4.2-3 System Configuration of Case 3

Table 4.2-3 The System Scale Applied to the Estimation of Maximum Response Times

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 1 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 2 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 3 of 4)

Table 4.2-4 Response Time Calculation for Maximum, Minimum and Safety Evaluation in Each Component (Sheet 4 of 4)

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 593-4565 REVISION 1**
SRP SECTION:	**07-21 BRANCH TECHNICAL POSITION – GUIDANCE ON DIGITAL COMPUTER REAL-TIME PERFORMANCE**
APPLICATION SECTION:	**CHAPTER 7**
DATE OF RAI ISSUE:	**6/8/2010**

QUESTION NO.: 07-21 Branch Technical Position-2
With regards to response time guidance of BTP 7-21, a basis should be provided for systems, particularly, that have not been implemented and tested on a full scale basis. In Technical Report MUAP-09021, "Time Response of Safety I&C System," the basis should include, but not be limited to,

1. A description of the effects of adding sensors, divisions, communication links, controller, computer nodes, or actuation devices required to scale the system to full scale or that which was previously built.
2. A description of the cycle which demonstrates that the watch-dog timer is correctly implemented. The description of the WDT cycle time in MUAP-09021 is not that identified in MUAP-09005 nor that identified as typical in BTP 7-21.
3. The time required for the application modules does not exceed the allotted time given in the architecture timing budget, and diagnostics and other support modules will not cause the allotted time to be exceeded.

10 CFR 52.47 states in part, that the information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. MHI is requested to provide a basis for systems that have not been implemented and tested on a full scale basis.

ANSWER:
The following description is added to the next revision of MUAP-09021 Section 4.2.2 to address system scaling.

The description of the watch dog timer in MUAP-09021 Section A.6 is revised to be consistent with the description in the MELTAC Topical Report, MUAP-07005, as follows:

~~"the watch-dog timer is set at the beginning of each cycle and reset after the completion of application module"~~

The hardware timer is set based on the calculation of T3, which is described in the RAI response above. The following is added to MUAP-09021 Section 4.2.2.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO. 593-4565 REVISION 1**
SRP SECTION:	**07-21 BRANCH TECHNICAL POSITION – GUIDANCE ON DIGITAL COMPUTER REAL-TIME PERFORMANCE**
APPLICATION SECTION:	**CHAPTER 7**
DATE OF RAI ISSUE:	**6/8/2010**

QUESTION NO.: 07-21 Branch Technical Position-4
In Technical Report MUAP-09021, "US-APWR Response Time of Safety I&C System," MHI is to correct the list of variables in Table 4.0-1 or the list of variables in Table 7.2-3 of the DCD so that they are specifically consistent.

Table 7.2-3 of the DCD provides a list of reactor trip variables, ranges, accuracies, response times, and setpoints. Similarly, Table 4.0-1 in MUAP-09021 provides a list of reactor trip variables and their response times. However, the list of variables in Table 4.0-1 in the MUAP-09021 do not agree with the list of variables in Table 7.2-3 of the DCD. Also, Table 4.0-1 in Technical Report MUAP-09021 includes the ECCS signal, which is not listed in Table 7.2-3. On the other hand, Table 7.2-3 includes high source range and high intermediate range neutron signal, and high positive and high negative rate of change of the power range flux signal. None of these signals are listed in Table 4.0-1 of Technical Report MUAP-09021. In the response to the RAI, MHI is to explain why these were different and which table will be revised.

ANSWER:
Table 7.2-3 of the DCD provides the response times of all RT variables. So, the item ECCS actuation has been added to Table 7.2-3 of the DCD Rev.3. And it will be revised in the DCD Rev.4. On the other hand, Table 4.1-1 in MUAP-09021 provides response times of typical RT variables assumed for the transient analyses in Table 15.0-4 of the DCD as described in MUAP-09021 Section 1.2. ECCS is included because it is a reactor trip initiator included in Table 15.0-4. The response times of the variables which are addressed in Table 7.2-3 of the DCD and not addressed in Table 15.0-4 of the DCD, are determined based on the response times of the variables in Table 4.1-1 of MUAP-09021 and Table 15.0-4 of the DCD. The response times T2, T3 and T4 are common to the variables only addressed in Table 7.2-3 of the DCD and the variables addressed in Table 15.0-4 in the DCD. The response time T1 of the variables addressed only in Table 7.2-3 of the DCD also can be decided from response time T1 of the variables which are addressed in Table 15.0-4 in the DCD and have sensors of the same type. Therefore, it should not pose any problem even if list of variables in Table 4.1-1 in MUAP-09021 does not agree with list of variables in Table 7.2-3 of the DCD.

Impact on DCD
The item ECCS actuation will be added to Table 7.2-3 of the DCD Rev.4 as follows.

Table 7.2-3 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal)

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy*[1,2]	Response Time*[1,2]	Setpoint *[3]
		...			
Manual Reactor Trip Actuation	Switch Position	N/A	N/A	N/A	N/A
Reactor Trip on ECCS Actuation	N/A	N/A	N/A	3.3 sec	N/A
~~ECCS Actuation~~	~~Pressurizer Pressure~~	~~1700 to 2500 psig~~	~~2.5% of span~~	~~3.3 sec~~	~~1765 psig~~
	~~Main Steam Line Pressure~~	~~0 to 1400 psig~~	~~3% of span~~	~~3.3 sec~~	~~525 psig~~
	~~Containment Pressure~~	~~-7 to 80 psig~~	~~2.8% of span~~	~~3.3 sec~~	~~6.8 psig~~

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

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.

MUAP-09021 describes the allocation of "Time Delay" for RTS and ESF functions in Table DCD 15.0-4, not the response time calculation methodology. Therefore, MUAP-07005 is the appropriate reference document for the response time calculation for MELTAC components.

As stated in Section 3.4, the real time performance for the PSMS conforms to BTP 7-21. Conformance to BTP 7-21 is described in MUAP-09021.

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.

Impact on DCD

There is no impact on the DCD.

MHI's Responses to 3rd round RAI on MUAP-07005-NP (R6) "Safety System Digital Platform -MELTAC-"

Non-proprietary Version

April 2011

©2011 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved

INTRODUCTION

This report provides responses to the comments on "MHI Responses to 2nd round RAI on Topical Report MUAP-07005-P(R3),"Safety System Digital Platform –MELTAC-""(UAP-HF-09393) received from the NRC at the NRC meeting on January 21, 2011.

This report describes responses to two comments received from the NRC.

RESPONSE TO THE RAI (March 31, 2011)

Following provides the responses to RAI.

RAI-01

Question:

Identify the specific differences in the MELTAC equipment applied for non-safety applications vs. the equipment applied to safety applications. Section 1.0 briefly mentions this as differences "in Quality Assurance methods for design and other software life cycle processes." This difference is also described in compliance to Branch Technical Position 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

Response:

The MELTAC Basic Software for the non-safety applications was developed according to the Original Quality Assurance Program (QAP), which is based on the Japanese standards, described in Section 6.0. [

]

Additional Request from NRC:

Original question: (In part) Identify the specific differences in the MELTAC equipment applied for non-safety applications vs. the equipment applied to safety applications.
Response: (In part) The differences between the safety and non-safety platform are primarily in system configuration and application software. The Basic Software of the two platforms is essentially the same.
NRC Supplement:
The information should provide sufficient details to allow the NRC staff to understand all the differences and arrive at an independent conclusion that the regulations and guidance for the safety system are met in comparison to the non-safety system. The "specific" differences, at a minimum, would be included in the design and quality assurance (QA) programs that incorporate software QA and verification and validation (V&V) as discussed by RG 1.152, Criteria for use of Computers in Safety Systems of Nuclear Power Plants. Therefore the hardware and software that use the same safety or non-safety process would be identified, how they are marked and how the processes are different.
At the January 22, 23 meeting with the staff, MELTAC agreed to identify the MELTAC modules that are common to safety and non-safety are interchangeable. Clarify that there are unique MELTAC hardware and software modules that can only be used in non-safety applications.

The topical report should state that total safety module set is described in TR Appendix, but additions can be made following same process for hardware and software development, as described in TR. The topical report should describe differences in identification for safety vs. non-safety hardware and software modules.

Additional Information from MHI:

Since they are the same in function as the modules manufactured for the non-safety system, the modules manufactured for safety system can be applied to the non-safety system. However, the module manufactured for non-safety system cannot be applied to the safety system. The modules will be identified to clarify for which system they are manufactured. The Topical Report will be revised to clarify that there are modules for non-safety system, different in function from the modules for the safety system written in the TR Appendix.

Additional Information from the NRC Meeting on 1/21/2011:

MELCO received the comment on RAI-1 and RAI-5 for the MELTAC TR from the NRC, as described below. "MELTAC Technical Report RAI 1 and 5, which pertain to PCMS quality and identification remain open."
(The NRC said that "Staff will clarify what they expect from MHI for these items" but we have not yet received any additional information. So we plan to submit a draft response to the above NRC comment, based on our own interpretation.)

Additional Information from MHI:

Since the QAP and the identification method for the safety MELTAC system and the non-safety MELTAC system are different, the safety platform is not applied to the non-safety platform, and the non-safety platform is not applied to the safety platform.
The differences in quality between MELTAC PSMS and PCMS are as below:
[

]

Impact on DCD

There is no impact on the DCD

Impact on COLA

There is no impact on the COLA

Impact on PRA

There is no impact on the PRA

RAI-05

Question:

Identify how the MELCO internal design documents are marked for the safety and non-safety MELTAC systems.

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

Response:

[

]

Additional Request from NRC:

Original question:

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

Response:

[

]

NRC Supplement:

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

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

Additional Information from MHI:

The following will be added to the Topical Report:
The software document titles for the Safety MELTAC contain "MELTAC Nplus-S", where S means Safety, while the titles for the non-safety (conventional) MELTAC is "MELTAC Nplus." These titles are applicable to all MELTAC software documents used internally by MELCO. The hardware components are common for the safety and non-safety MELTAC. Therefore, there is no distinct identification for the hardware documents inside MELCO; all hardware is identified as "MELTAC Nplus".
Application specific documentation (eg. cabinet layout and wiring diagrams, technical manuals, etc) for MELTAC Nplus-S systems will be marked "nuclear safety related". Cabinets and enclosures containing MELTAC Nplus-S equipment will be clearly marked externally and internally by system name and safety division, so that its Class 1E designation is clearly indicated. Where a single cabinet or enclosure contains equipment or wiring from divisions other than the division of the cabinet marking, the other equipment or wiring will be clearly marked for its own division. Wiring and equipment belonging to separate divisions will have suitable barriers and/or separation.

Additional Information from the NRC Meeting on 1/21/2011:

MELCO received the comment on RAI-1 and RAI-5 for the MELTAC TR from the NRC, as described below.
"MELTAC Technical Report RAI 1 and 5, which pertain to PCMS quality and identification remain open."
(The NRC said that "Staff will clarify what they expect from MHI for these items" but we have not yet received any additional information. So we plan to submit a draft response to the above NRC comment, based on our own interpretation.)

Additional Information from MHI:

Related Document
(1) Safety System Digital Platform MELTAC (MUAP-07005)
Response
Since the response to RAI-5 previously submitted has a misleading description, we will revise the response to RAI-5 as described below.

Distinction in designation will be made for all components (hardware, software, documents) of the safety MELTAC system to provide clear identification.
[

]

Impact on DCD
There is no impact on the DCD

Impact on COLA
There is no impact on the COLA

Impact on PRA
There is no impact on the PRA

ATTACHMENT 1

FILES CONTAINED IN CD 1

CD 1: "Mark up of DCD Chapter 7 on Revision 3 (SRI Included)"
- Version Containing SRI

Contents of CD

File Name	Size	Sensitivity Level
DCD_Ch7(SRI Included).pdf	14MB	Proprietary

ATTACHMENT 2

FILES CONTAINED IN CD 2

CD 2: "Mark up of DCD Chapter 7 for Revision 3 (SRI Excluded)"
- Version Not Containing SRI

Contents of CD

File Name	Size	Sensitivity Level
DCD_Ch7(SRI Excluded).pdf	14MB	Proprietary